My Vulnerability Testing Toolbox

CERT.be

May 2022

TLP: White

CERT.be The Federal Cyber Emergency Team

CENTRE FOR CYBER SECURITY BELGIUM

Content

1 EXECUTIVE SUMMARY

If not patched and looked after regularly, a company network infrastructure and website will present flaws or weaknesses, called vulnerabilities, that can be exploited by an opponent to cause damage or perform unauthorized actions. This could result in compromising the confidentiality (e.g. private information leakage), the integrity (e.g. unauthorized modification of data), or the availability (e.g. website down) of resources.

That's why organizations should use vulnerability assessment tools to spot security holes in their networks, website or web applications. Then appropriate remediation measures can be taken regarding the security flaws discovered.

A good practice is to act early to minimize the chances of a successful attack.

This document presents a summary of some of the most relevant but free or inexpensive tools on the market.

While most of the tools described can be used by non-expert users, there might be cases where professional help is required, such as simulating advanced attacks.

Liability waiver

The Centre for Cyber Security Belgium (CCB) provides technical and organizational advice on how to deal with / prevent cyber incidents, but is not involved in carrying out these operations.

The software tools mentioned in the present document have been tested and are used on a regular basis, but the CCB cannot be held responsible for any unintentional damage resulting from the normal use of these tools.
The responsibility for managing cyber incidents and taking actions remains with the Network and Information Systems Manager.

Additionally, as the General Data Protection Regulation (GDPR) has come into effect recently to protect data and privacy of EU citizen, every organization has the responsibility to take the necessary actions to secure their applications and data in consequence.

2 CONSIDERATIONS

A comprehensive way to detect flaws on a website or in a network is to make use of vulnerability analysis tools. In fact, trying to spot security issues manually is at best tedious, but most of the time impracticable, especially for a non-expert person. Using an automated tool will save time and is effective in most cases. Additionally, no programming knowledge is required to perform security testing with tools. But special attention should be taken regarding accuracy concerns, as these tools do not provide full accuracy and may overlook some security flaws and at the same time generate false positive and false negative.

A false positive is a detection error in which the tool indicates the presence of a vulnerability when in reality it is not present. False negatives are more annoying, as the tool couldn't identify security issues and left the door open to potential opponents.

Note that some scanning tools are software that have to be installed on the company's infrastructure before operating them, others function as a service (called Software as a Service or SAAS) where the tools are hosted in the cloud and operate from a remote environment.

There are two types of analysis: static and dynamic

- Static analysis consists of inspecting the program to identify potential vulnerabilities, when dynamic analysis checks the behavior of the website/web application against a set of test cases at run time. Each approach has its advantages and drawbacks. Through a static analysis, the testing tool will have access to the code to search for security bugs.
- Dynamic analysis testing could discover security issues not disclosed by static analysis. And oftentimes organizations prefer black-box testing (dynamic analysis) that simulate an attack in the context of a penetration testing. Regarding dynamic analysis, the test cases may not cover all cases and also be insufficient to verify some situations.

In case of homemade developed tools, organizations should take actions at early stages of the development lifecycle to detect and correct security issues. As technologies evolve at a fast pace and security flaws are discovered on a daily basis, it is also recommended to perform security analysis at regular intervals.

Another consideration is the supporting system. Some tools work on Windows, Linux and Mac environment, while others only support a subset of these platforms.

Some analysis tools available on the market and reported by OWASP (Open Web Application Security Project) are:

Name	Owner	Licence	Platforms
AppTrana Website Security Scan	AppTrana	Free	SaaS
Arachni	Arachni	Free for most use cases	Most platforms supported
Grabber	Romain Gaucher	Open Source	Python 2.4, BeautifulSoup and PyXML
Grendel-Scan	David Byrne	Open Source	Windows, Linux and Macintosh
GoLismero	GoLismero Team	GPLv2.0	Windows, Linux and Macintosh
Nikto	CIRT	Open Source	Unix/Linux
Vega	Subgraph	Open Source	Windows, Linux and Macintosh
Wapiti	Informática Gesfor	Open Source	Windows, Unix/Linux and Macintosh
WebCookies	WebCookies	Free	SaaS
Wikto	Sensepost	Open Source	Windows
w3af	w3af.org	GPLv2.0	Linux and Mac
Xenotix XSS Exploit Framework	OWASP	Open Source	Windows
Zed Attack Proxy	OWASP	Open Source	Windows, Unix/Linux and Macintosh
Acunetix WVS	Acunetix	Commercial / Free (Limited Capability)	Windows
Application Security on Cloud	IBM	Commercial	SaaS
AppScan	IBM	Commercial	Windows
App Scanner	Trustwave	Commercial	Windows
AppSpider	Rapid7	Commercial	Windows
AVDS	Beyond Security	Commercial / Free (Limited Capability)	SaaS
BlueClosure BC Detect	BlueClosure	Commercial, 2 weeks trial	Most platforms supported
Burp Suite	PortSwiger	Commercial / Free (Limited Capability)	Most platforms supported
Contrast	Contrast Security	Commercial / Free (Full featured for 1 App)	SaaS or On-Premises
Detectify	Detectify	Commercial	SaaS
Digifort- Inspect	Digifort	Commercial	SaaS
edgescan	edgescan	Commercial	SaaS
GamaScan	GamaSec	Commercial	Windows
Gravityscan	Defiant, Inc.	Commercial / Free (Limited Capability)	SaaS
IKare	ITrust	Commercial	N/A
ImmuniWeb	High-Tech Bridge	Commercial / Free (Limited Capability)	SaaS
Indusface Web Application Scanning	Indusface	Commercial / Free Trial	SaaS
N-Stealth	N-Stalker	Commercial	Windows
Nessus	Tenable	Commercial	Windows
Netsparker	MavitunaSecurity	Commercial	Windows
Nexpose	Rapid7	Commercial / Free (Limited Capability)	Windows/Linux
ParosPro	MileSCAN	Commercial	Windows
Probe.ly	Probe.ly	Commercial / Free (Limited Capability)	SaaS
Proxy.app	Websecurify	Commercial	Macintosh
QualysGuard	Qualys	Commercial	N/A
Retina	BeyondTrust	Commercial	Windows
Securus	Orvant, Inc	Commercial	N/A
Sentinel	WhiteHat Security	Commercial	N/A
SOATest	Parasoft	Commercial	Windows / Linux / Solaris
Tinfoil Security	Tinfoil Security, Inc.	Commercial / Free (Limited Capability)	SaaS or On-Premises
Trustkeeper Scanner	Trustwave SpiderLabs	Commercial	SaaS
Web Security Scanner	DefenseCode	Commercial	On-Premises
WebApp360	TripWire	Commercial	Windows
WebInspect	HP	Commercial	Windows
WebReaver	Websecurify	Commercial	Macintosh
WebScanService	German Web Security	Commercial	N/A
Websecurify Suite	Websecurify	Commercial / Free (Limited Capability)	Windows, Linux, Macintosh

Source: https://owasp.org/www-community/Vulnerability_Scanning_Tools

3 TOOLS

CERT.be tested some of the most popular vulnerability analysis tools, they can be classified in different categories:

Scanning tools can help you analyze your network, see what services are running on which port, footprint your infrastructure:

- Nmap
- Netcraft
- Hacker Target

Web application vulnerability enumeration

- Nikto
- Burp Suite
- Owasp Zap

Network vulnerability enumeration

- Nessus Free or Pro version
- OpenVas

Encryption configuration validation

- Qualys SSL Lab (https://www.ssllabs.com/ssltest/)

Website's CMS (Content Management System) vulnerability assessment tools

- Droopescan for Drupal
- WPscan and Wpsec.com for Wordpress
- Joomla-security-scan for Joomla

DMARC (Domain-based Message Authentication, Reporting & Conformance) online checker

- Mxtoolbox free DMARC check

Active Directory Security Tool

- PingCastle

Of course, there are many more assessment tools on the market. The choice of a suitable cloud service should match the user's needs and requirements.

The information provided below regarding the tools is subject to change. In fact, providers may update their tools at any time.

Remember that vulnerability scans may trigger faults, crashes or locking of the targeted web application and server.

Disclaimer: use these tools at your own risks, CCB (CERT.be) cannot be held responsible for any damages made to your website, infrastructure or application resulting from their use. CCB (CERT.be) does not endorse any of the vendors or scanning tools by testing them in this report. This report has been done as an educational resource for companies, CCB (CERT.be) cannot guarantee the outcome resulting from the usage of the tools.

3.1 Scanning & Foot printing Tool

Nmap [Windows-Linux-macOS]

Skill level

Beginner to expert.

Description

Nmap (Network Mapper) is an open-source tool for network discovery and security auditing. Amongst many features, Nmap has the ability to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use. It can also be used to perform vulnerability scans via the Nmap Scripting Engine (NSE).

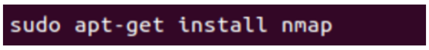
Nmap supports most operating systems (Windows, Linux, macOS). It comes with a command-line executable but also includes a graphical user interface and result viewer (Zenmap).

How to use Nmap?

1. Installation

Nmap installation is quite straightforward, if you want to install it on Windows operating systems, we recommend you download and use the graphical version of Nmap called Zenmap.

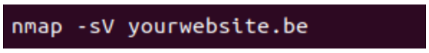
If you are on Debian or Ubuntu (Linux systems), just run the following command to install Nmap:



```
sudo apt-get install nmap
```

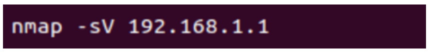
2. Scanning

Nmap requires root privileges in order to run properly. With the following command we can detect open services on a host or a server (i.e. yourwebsite.be). The command will also tell the version of the program in use which is useful when looking for vulnerabilities.



```
nmap -sV yourwebsite.be
```

Alternatively, we can specify the IP:

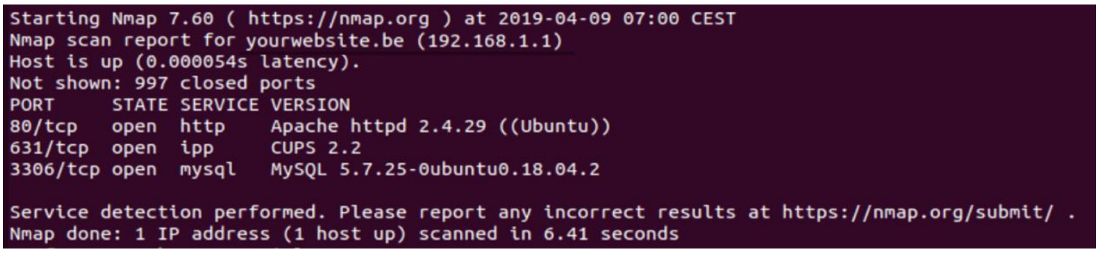


```
nmap -sV 192.168.1.1
```

An address range in CIDR notation can also be used:

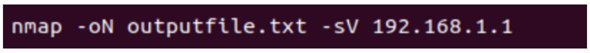
```
nmap -sV 192.168.1.0/24
```

Here is an example of a scan result for open services:



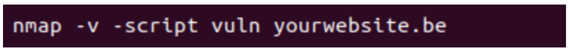
```
Starting Nmap 7.60 ( https://nmap.org ) at 2019-04-09 07:00 CEST
Nmap scan report for yourwebsite.be (192.168.1.1)
Host is up (0.000054s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
631/tcp  open  ipp     CUPS 2.2
3306/tcp open  mysql   MySQL 5.7.25-0ubuntu0.18.04.2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.41 seconds
```

If needed, the result can be saved to a file using the option -oN:



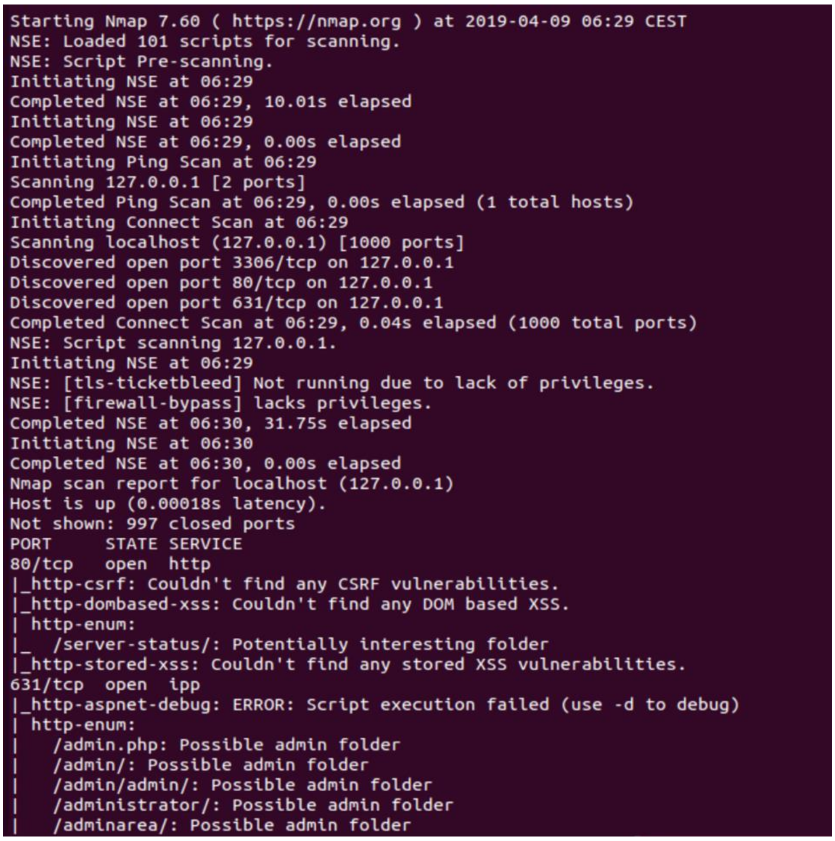
```
nmap -oN outputfile.txt -sV 192.168.1.1
```

Nmap includes scripts which will search for security issues on hosts:



```
nmap -v -script vuln yourwebsite.be
```

Here is an excerpt of the scan result for vulnerabilities:



```
Starting Nmap 7.60 ( https://nmap.org ) at 2019-04-09 06:29 CEST
NSE: Loaded 101 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:29
Completed NSE at 06:29, 10.01s elapsed
Initiating NSE at 06:29
Completed NSE at 06:29, 0.00s elapsed
Initiating Ping Scan at 06:29
Scanning 127.0.0.1 [2 ports]
Completed Ping Scan at 06:29, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 06:29
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 3306/tcp on 127.0.0.1
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 631/tcp on 127.0.0.1
Completed Connect Scan at 06:29, 0.04s elapsed (1000 total ports)
NSE: Script scanning 127.0.0.1.
Initiating NSE at 06:29
NSE: [tls-ticketbleed] Not running due to lack of privileges.
NSE: [firewall-bypass] lacks privileges.
Completed NSE at 06:30, 31.75s elapsed
Initiating NSE at 06:30
Completed NSE at 06:30, 0.00s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00018s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
80/tcp   open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|_  /server-status/: Potentially interesting folder
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
631/tcp  open  ipp
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
| http-enum:
|   /admin.php: Possible admin folder
|   /admin/: Possible admin folder
|   /admin/admin/: Possible admin folder
|   /administrator/: Possible admin folder
|   /adminarea/: Possible admin folder
```

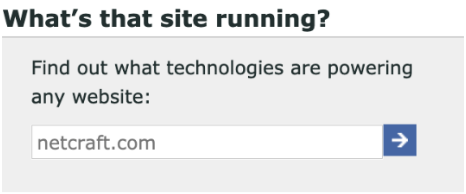
Nmap.org website has a lot of docs and extra tools you can use if you want to go deeper: https://nmap.org/

Netcraft [Cloud-based]

Skill level

Beginner.

Netcraft provides a free online search **tool** that allows users to query its databases for host information. This tool is very effective and can give you some valuable information about the technologies used on your website (https://www.netcraft.com/).

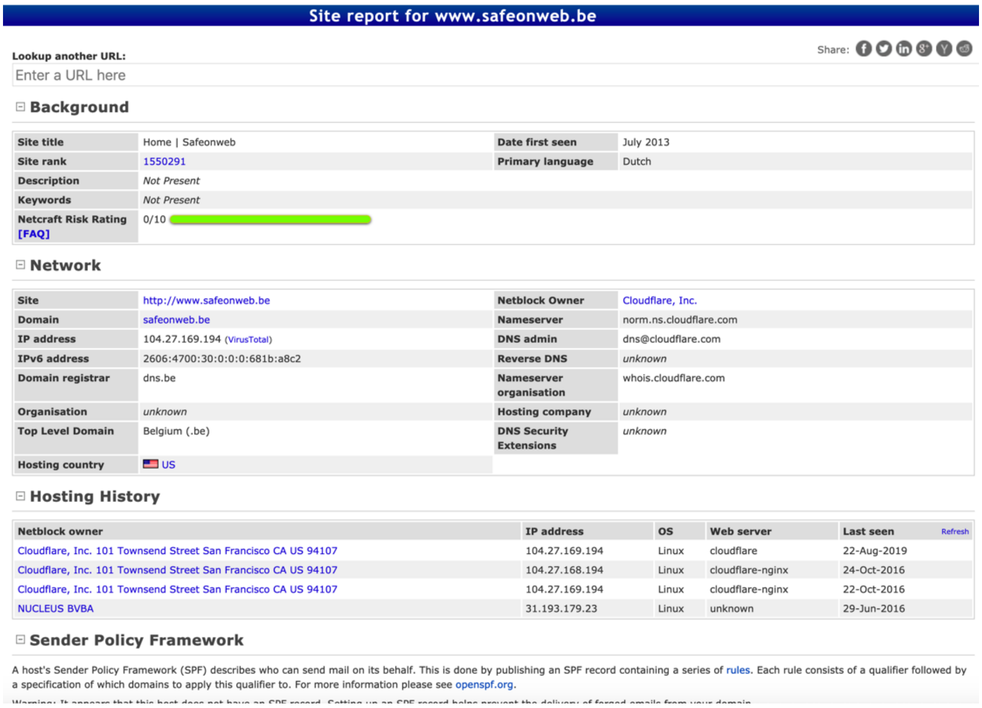


What's that site running?

Find out what technologies are powering any website:

netcraft.com

Figure 1 - Netcraft search box (https://sitereport.netcraft.com)



Site report for www.safeonweb.be

Lookup another URL:

Enter a URL here

⊟ Background

Site title	Home | Safeonweb	**Date first seen**	July 2013
Site rank	1550291	**Primary language**	Dutch
Description	*Not Present*		
Keywords	*Not Present*		
Netcraft Risk Rating **[FAQ]**	0/10 🟩		

⊟ Network

Site	http://www.safeonweb.be	**Netblock Owner**	Cloudflare, Inc.
Domain	safeonweb.be	**Nameserver**	norm.ns.cloudflare.com
IP address	104.27.169.194 (VirusTotal)	**DNS admin**	dns@cloudflare.com
IPv6 address	2606:4700:30:0:0:0:681b:a8c2	**Reverse DNS**	*unknown*
Domain registrar	dns.be	**Nameserver organisation**	whois.cloudflare.com
Organisation	*unknown*	**Hosting company**	*unknown*
Top Level Domain	Belgium (.be)	**DNS Security Extensions**	*unknown*
Hosting country	US		

⊟ Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.27.169.194	Linux	cloudflare	22-Aug-2019
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.27.168.194	Linux	cloudflare-nginx	24-Oct-2016
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.27.169.194	Linux	cloudflare-nginx	22-Oct-2016
NUCLEUS BVBA	31.193.179.23	Linux	unknown	29-Jun-2016

⊟ Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see openspf.org.

Warning: It appears that this host does not have an SPF record. Setting up an SPF record helps prevent the delivery of forged emails from your domain.

Figure 2 - Netcraft search query result

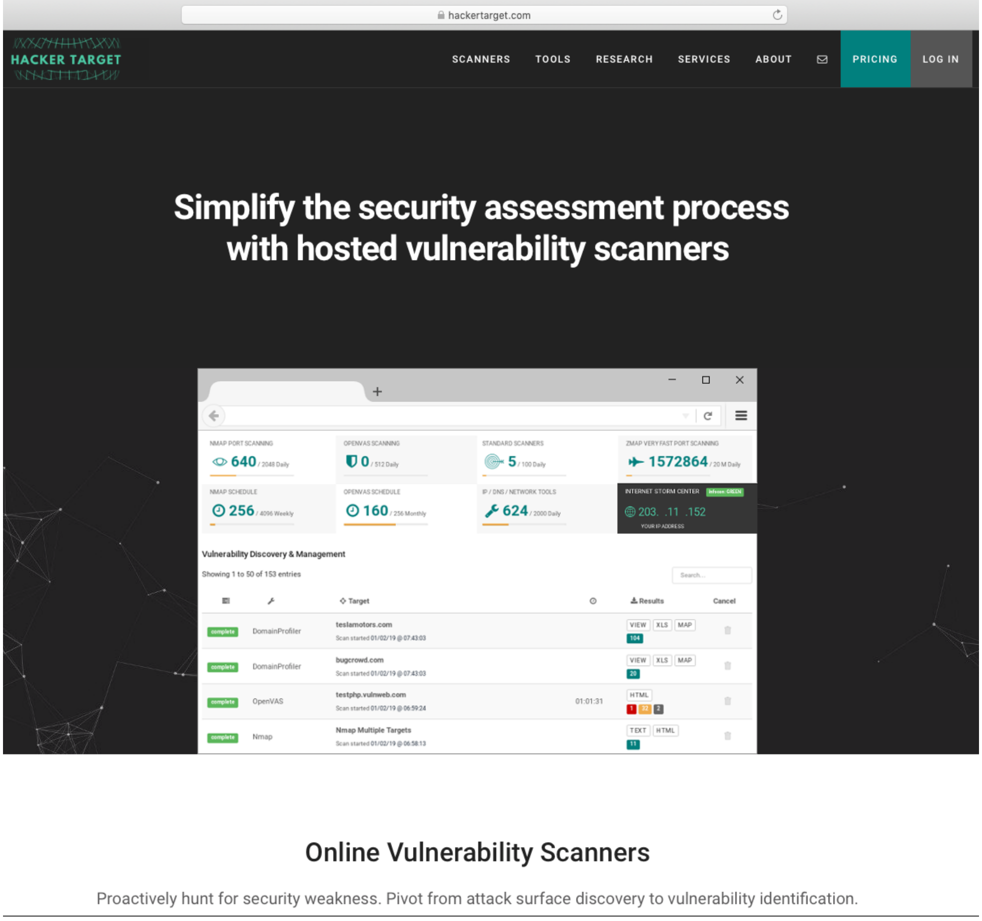
Hacker Target [Cloud-based]

Skill level needed

Beginner.

Description

Hacker Target (https://hackertarget.com) is an online cloud-based vulnerability scanner solution, this “software as a service” platform offers to run a selection of vulnerability scanners against your network infrastructure or your website for an affordable price.



Simplify the security assessment process with hosted vulnerability scanners

NMAP PORT SCANNING	OPENVAS SCANNING	STANDARD SCANNERS	ZMAP VERY FAST PORT SCANNING
640 / 2048 Daily	0 / 512 Daily	5 / 100 Daily	1572864 / 20 M Daily
NMAP SCHEDULE	OPENVAS SCHEDULE	IP / DNS / NETWORK TOOLS	INTERNET STORM CENTER Infocon: GREEN
256 / 4096 Weekly	160 / 256 Monthly	624 / 2000 Daily	203. .11 .152 YOUR IP ADDRESS

Vulnerability Discovery & Management

Showing 1 to 50 of 153 entries

Search...

		Target		Results	Cancel
complete	DomainProfiler	teslamotors.com Scan started 01/02/19 @ 07:43:03		VIEW XLS MAP 104	
complete	DomainProfiler	bugcrowd.com Scan started 01/02/19 @ 07:43:03		VIEW XLS MAP 20	
complete	OpenVAS	testphp.vulnweb.com Scan started 01/02/19 @ 06:59:24	01:01:31	HTML 1 32 2	
complete	Nmap	Nmap Multiple Targets Scan started 01/02/19 @ 06:58:13		TEXT HTML 11	

Online Vulnerability Scanners

Proactively hunt for security weakness. Pivot from attack surface discovery to vulnerability identification.

Figure 3- Hacker Target Website

It is an easy-to-use solution if you don’t want or don’t have the time to install and setup these tools by yourself.

3.2 Web application Vulnerability assessment tools

Nikto [Windows-Linux-macOS]

Skill level needed

Beginner.

Description

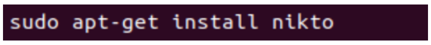
Nikto (https://github.com/sullo/nikto) is an open-source web server scanner. It examines a web server to find potential problems and security vulnerabilities such as server and software misconfigurations, default files and programs, insecure files and programs, and outdated servers and programs.

Nikto will run on most operating systems (Windows, Linux, MacOS) but requires Perl to be installed. It doesn't provide a graphical user interface. Instead, the user must use the command line interface to run the scans.

How to use Nikto?

1. Installation on Debian or Ubuntu

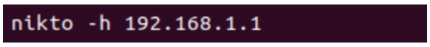
On Debian or Ubuntu (Linux systems), run the following command:



```
sudo apt-get install nikto
```

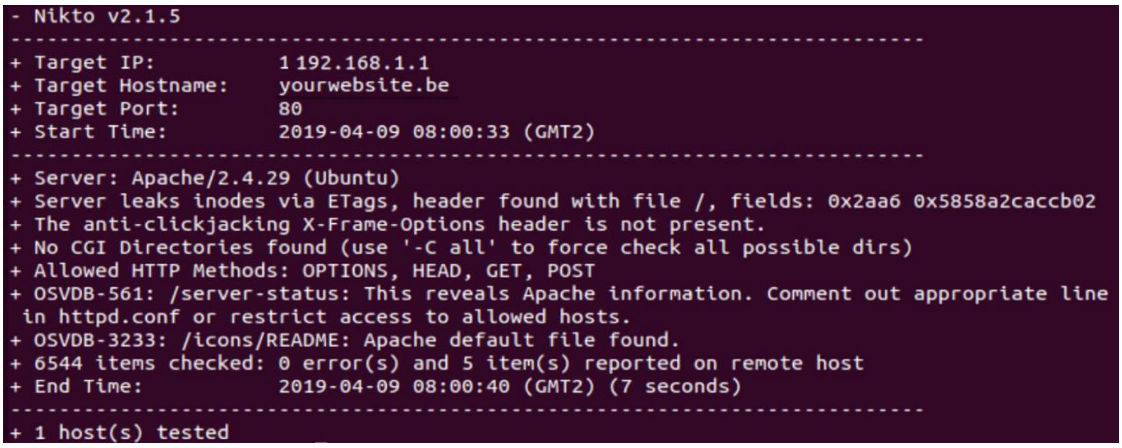
2. Scanning

To scan vulnerabilities on a host (i.e. 192.168.1.1), we can use the option -h. By default (without specifying a port number), nikto will scan on port 80.



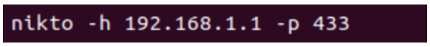
```
nikto -h 192.168.1.1
```

Here is an example of scan result:



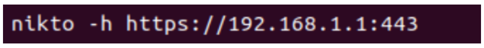
```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          1 192.168.1.1
+ Target Hostname:    yourwebsite.be
+ Target Port:        80
+ Start Time:         2019-04-09 08:00:33 (GMT2)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x2aa6 0x5858a2caccb02
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ OSVDB-561: /server-status: This reveals Apache information. Comment out appropriate line
 in httpd.conf or restrict access to allowed hosts.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6544 items checked: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2019-04-09 08:00:40 (GMT2) (7 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

The same scan specifying a (different) port number using option -p (i.e. port 443):



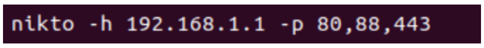
```
nikto -h 192.168.1.1 -p 433
```

Alternatively, for the same scan using a full URL syntax:



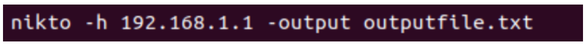
```
nikto -h https://192.168.1.1:443
```

Nikto can scan multiple ports (i.e. 80, 88, 443) in the following way:



```
nikto -h 192.168.1.1 -p 80,88,443
```

To output the result to a file, use the option -output:



```
nikto -h 192.168.1.1 -output outputfile.txt
```

Burp Suite [Windows-Linux-macOS]

Skill level

Might be complex to use: from intermediate to expert.

Description.

Burp (https://portswigger.net/burp) is a vulnerability scanner and is one of the leading software for web security testing.

Burp runs on most operating systems (Windows, Linux, MacOS) and is shipped with a graphical user interface.

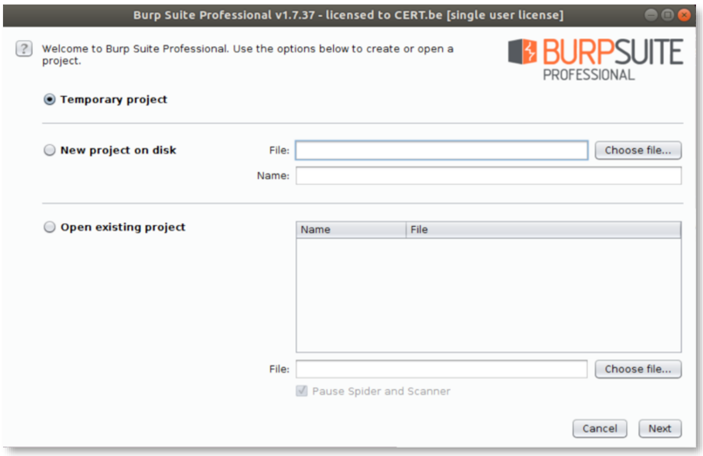
Burp has a free community release which already offers some great functionalities but if you want to use the web vulnerability scanner you have to purchase the professional edition sold at 349€.

How to use Burp?

In the present description, we used Burp Suite Professional v1.7.37 deployed on a Linux system.

1. Project configuration

Scans are organized by projects that will allow the user to persist the states of his scans to a file and share that file. Use the options to create or open a (temporary) **project** (fig. 3.1).



Burp Suite Professional v1.7.37 - licensed to CERT.be [single user license]

Welcome to Burp Suite Professional. Use the options below to create or open a project.

● Temporary project

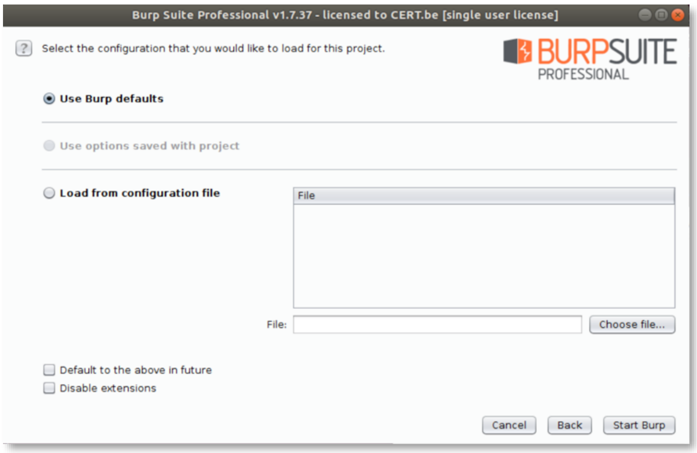
○ New project on disk

○ Open existing project

☑ Pause Spider and Scanner

Figure 3.1 – Create a project

The user can leave Burp default **configuration** or load an existing configuration from a file (fig. 3.2).



Burp Suite Professional v1.7.37 - licensed to CERT.be [single user license]

Select the configuration that you would like to load for this project.

● Use Burp defaults

○ Use options saved with project

○ Load from configuration file

File:

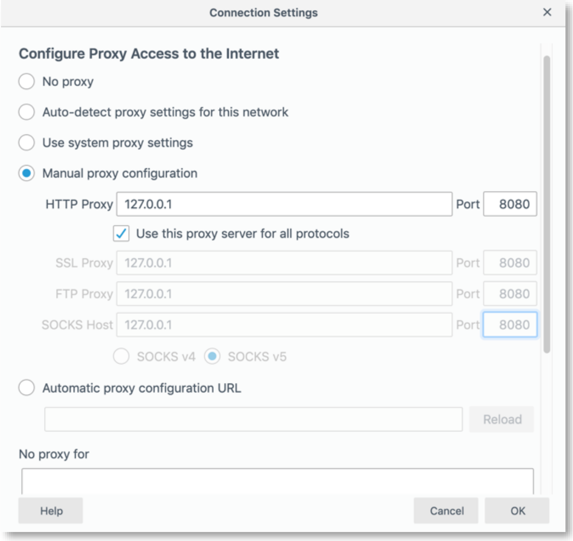
□ Default to the above in future

□ Disable extensions

Figure 3.2 – Select Burp configuration

2. Proxy configuration

Before performing a vulnerability scan, Burp must know the website. To this end the web browser (Firefox, Chrome, Edge) has to be configured to route the traffic to Burp proxy server. An example of configuration in Firefox is showed here under (fig. 3.3). By default, Burp Proxy server uses a proxy listener at 127.0.1:8080 (fig. 3.4). But it is possible to configure Burp server to listen on another interface using the Edit button.



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☑ Use this proxy server for all protocols

SSL Proxy 127.0.0.1 Port 8080

FTP Proxy 127.0.0.1 Port 8080

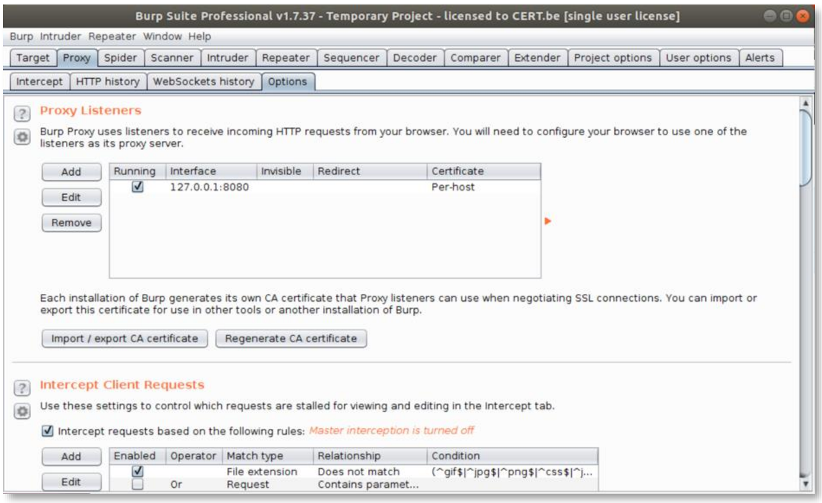
SOCKS Host 127.0.0.1 Port 8080

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

No proxy for

Figure 3.3 – Web browser (Firefox) proxy configuration


Burp Suite Professional v1.7.37 - Temporary Project - licensed to CERT.be [single user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Add | Edit | Remove

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8080			Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export this certificate for use in other tools or another installation of Burp.

Import / export CA certificate | Regenerate CA certificate

Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☑ Intercept requests based on the following rules: *Master interception is turned off*

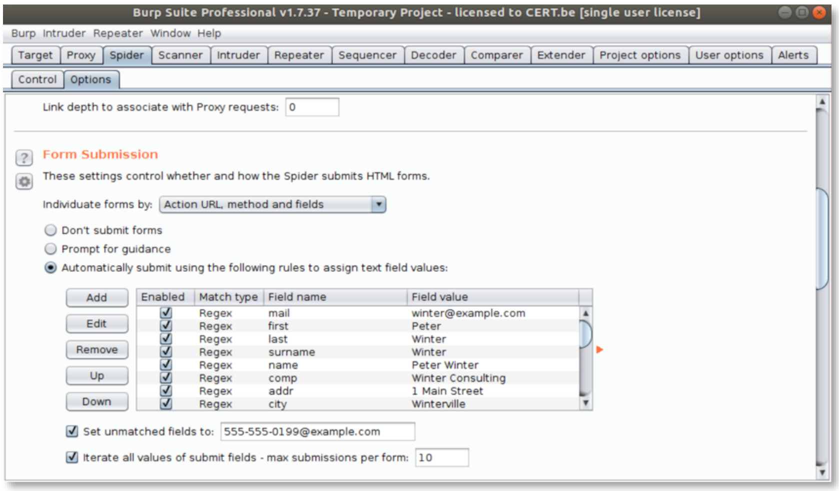
Add | Edit

Enabled	Operator	Match type	Relationship	Condition
☑		File extension	Does not match	(^gif$\|^jpg$|^png$\|^css$|^j...
□	Or	Request	Contains paramet...	

Figure 3.4 – Proxy listener

3. Spider configuration

To analyze (crawl) a website structure automatically, Burp has a feature called Spider. In the tab **Spider**-> **Options**, different settings are available. In particular, under the section “Form submission” (fig. 3.5) and “Application Login” (fig. 3.6), three options allow the user to specify what to do when Burp encounters a form on a web page. By default, Burp will automatically assign pre-defined values in forms and prompt the user when the page contains a login form.


Burp Suite Professional v1.7.37 - Temporary Project - licensed to CERT.be [single user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Control Options

Link depth to associate with Proxy requests: 0

Form Submission

These settings control whether and how the Spider submits HTML forms.

Individuate forms by: Action URL, method and fields

○ Don't submit forms
○ Prompt for guidance
● Automatically submit using the following rules to assign text field values:

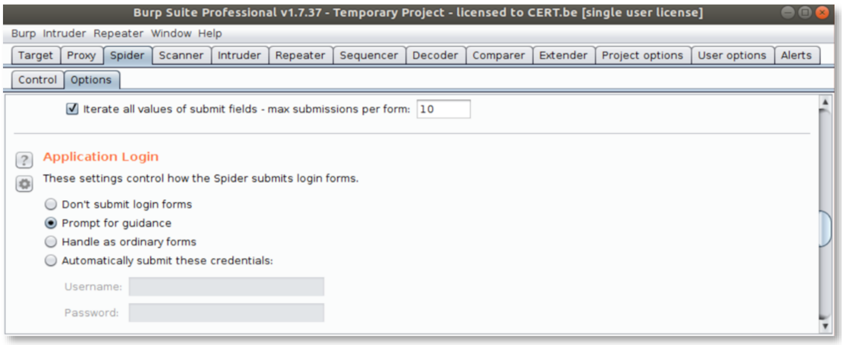
Add | Edit | Remove | Up | Down

Enabled	Match type	Field name	Field value
☑	Regex	mail	winter@example.com
☑	Regex	first	Peter
☑	Regex	last	Winter
☑	Regex	surname	Winter
☑	Regex	name	Peter Winter
☑	Regex	comp	Winter Consulting
☑	Regex	addr	1 Main Street
☑	Regex	city	Winterville

☑ Set unmatched fields to: 555-555-0199@example.com

☑ Iterate all values of submit fields - max submissions per form: 10

Figure 3.5 – Spider settings: form submission


Burp Suite Professional v1.7.37 - Temporary Project - licensed to CERT.be [single user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Control Options

☑ Iterate all values of submit fields - max submissions per form: 10

Application Login

These settings control how the Spider submits login forms.

○ Don't submit login forms
● Prompt for guidance
○ Handle as ordinary forms
○ Automatically submit these credentials:

Username:

Password:

Figure 3.6 – Spider settings: application login

4. Interception and crawling

In the tab **Proxy**-> **Intercept,** the proxy interception function must be turned on by clicking on the button “Intercept is off” (fig. 3.7).

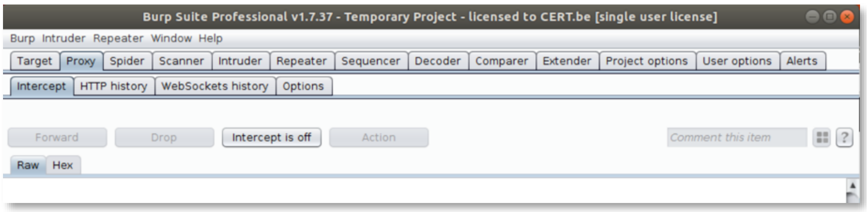

Burp Suite Professional v1.7.37 - Temporary Project - licensed to CERT.be [single user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is off
Action
Comment this item
Raw Hex

Figure 3.7 – Proxy interception

Then go on the targeted website using the web browser (fig. 3.8).

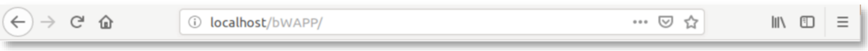
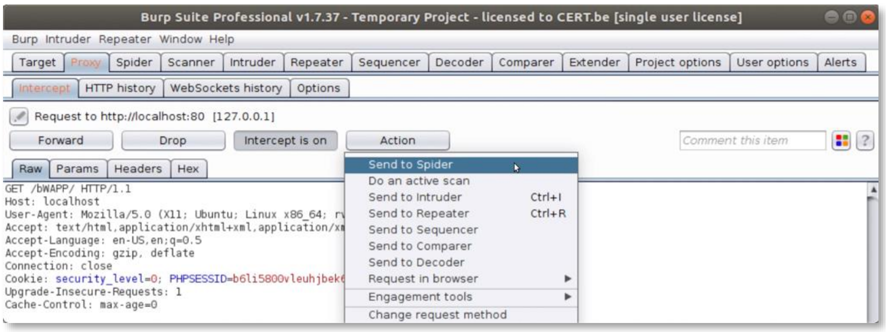


Figure 3.8 – Enter the URL in the web browser

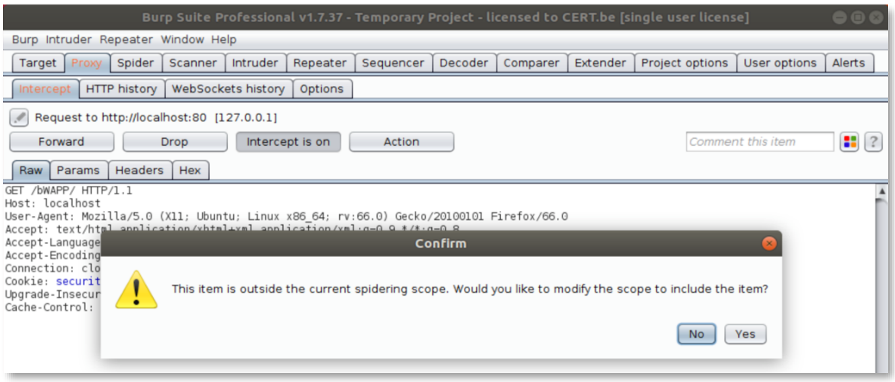
Now you can observe the request originating from the web browser in the tab **Proxy**-> **Intercept**. Click on the Action tab and send the request to the Spider (fig. 3.9). Then add the targeted website to the scope by clicking on “Yes” (fig. 3.10). Finally, stop sending out-of-scope requests (originating from other websites) by clicking on “Yes” again (fig. 3.11).


Burp Suite Professional v1.7.37 - Temporary Project - licensed to CERT.be [single user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Comment this item
Raw Params Headers Hex
Send to Spider
Do an active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools
Change request method

Request to http://localhost:80 [127.0.0.1]

```
GET /bWAPP/ HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv
Accept: text/html,application/xhtml+xml,application/xm
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: security_level=0; PHPSESSID=b6li5800vleuhjbek
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Figure 3.9 – Sending the request to Spider


Burp Suite Professional v1.7.37 - Temporary Project - licensed to CERT.be [single user license]

Request to http://localhost:80 [127.0.0.1]

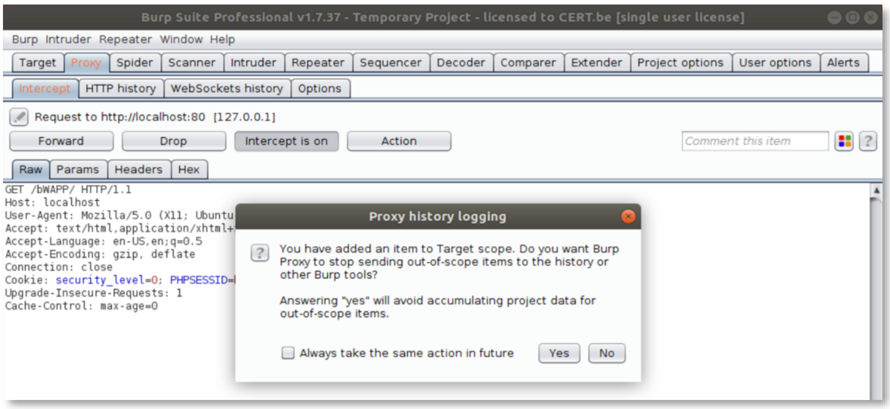
```
GET /bWAPP/ HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:66.0) Gecko/20100101 Firefox/66.0
Accept: text/ht
Accept-Language
Accept-Encoding
Connection: clo
Cookie: securit
Upgrade-Insecur
Cache-Control:
```

Confirm

This item is outside the current spidering scope. Would you like to modify the scope to include the item?

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Comment this item
?
Raw Params Headers Hex
No
Yes

Figure 3.10 – Adding the targeted website to the scope


Burp Suite Professional v1.7.37 - Temporary Project - licensed to CERT.be [single user license]

Request to http://localhost:80 [127.0.0.1]

```
GET /bWAPP/ HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu
Accept: text/html,application/xhtml+
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: security_level=0; PHPSESSID=
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Proxy history logging

You have added an item to Target scope. Do you want Burp Proxy to stop sending out-of-scope items to the history or other Burp tools?

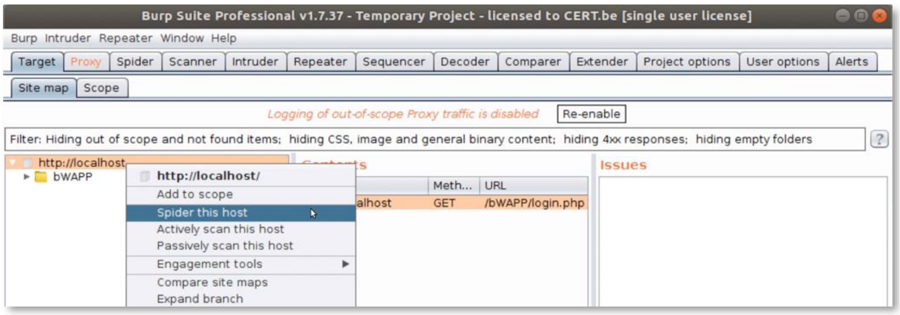
Answering "yes" will avoid accumulating project data for out-of-scope items.

□ Always take the same action in future

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Comment this item
?
Raw Params Headers Hex
Yes
No

Figure 3.11 – Stop sending out-of-scope requests

In the tab **Target** -> **Site map**, the website has been added to the site map. Right click on the URL and select "Spider this host" to start the automatic crawling of the website (fig. 3.12). All the content discovered on the website by the Spider is now added and shown on the site map (fig. 3.13). The site map shows a visualization of the entire website structure. Note that Burp will also include contents that are linked to the targeted website.

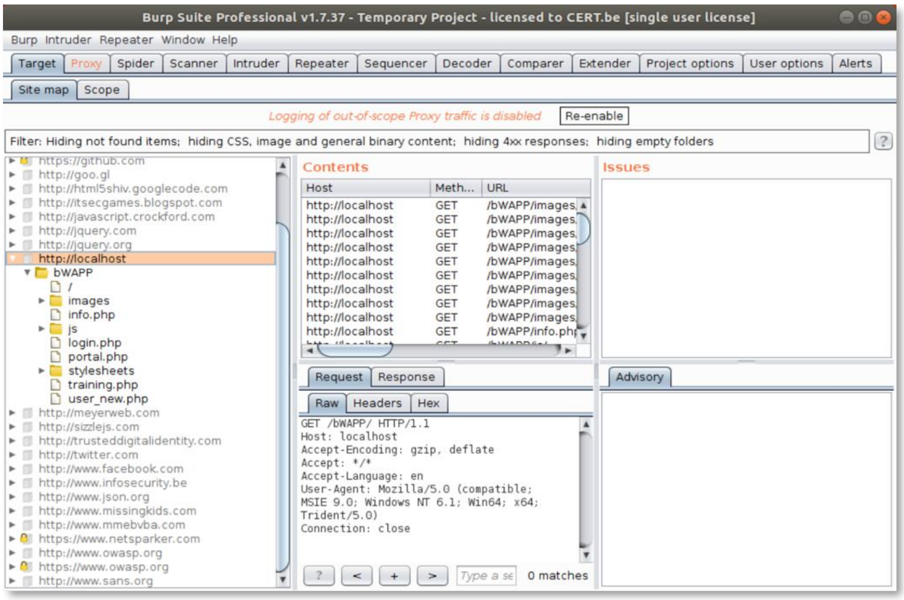

Burp Suite Professional v1.7.37 - Temporary Project - licensed to CERT.be [single user license]

Logging of out-of-scope Proxy traffic is disabled

Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

	Meth...	URL
alhost	GET	/bWAPP/login.php

Figure 3.12 – Using the Spider to crawl automatically a host


Burp Suite Professional v1.7.37 - Temporary Project - licensed to CERT.be [single user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
Re-enable
Contents
Issues
Request Response
Raw Headers Hex
Advisory
? < + > Type a se 0 matches

Logging of out-of-scope Proxy traffic is disabled

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

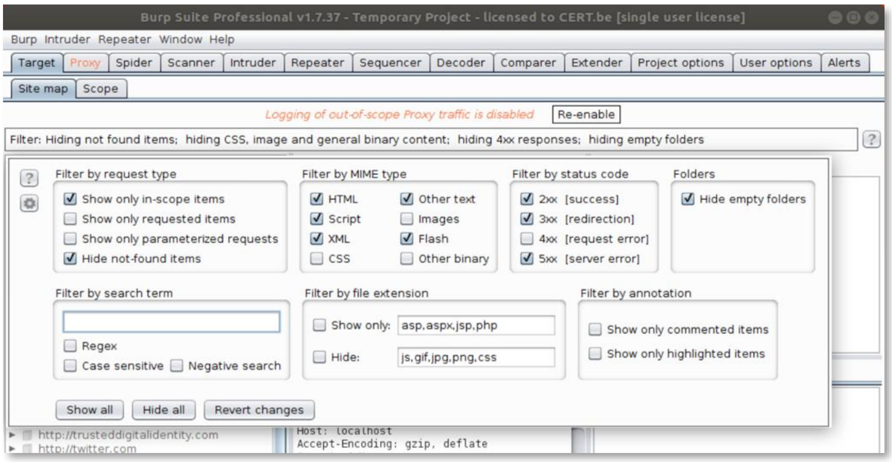
```
https://github.com
http://goo.gl
http://html5shiv.googlecode.com
http://itsecgames.blogspot.com
http://javascript.crockford.com
http://jquery.com
http://jquery.org
http://localhost
  bWAPP
    /
    images
    info.php
    js
    login.php
    portal.php
    stylesheets
    training.php
    user_new.php
http://meyerweb.com
http://sizzlejs.com
http://trusteddigitalidentity.com
http://twitter.com
http://www.facebook.com
http://www.infosecurity.be
http://www.json.org
http://www.missingkids.com
http://www.mmebvba.com
https://www.netsparker.com
http://www.owasp.org
https://www.owasp.org
http://www.sans.org
```

Host	Meth...	URL
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/info.php

```
GET /bWAPP/ HTTP/1.1
Host: localhost
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible;
MSIE 9.0; Windows NT 6.1; Win64; x64;
Trident/5.0)
Connection: close
```

Figure 3.13 – Site map of the website

To filter out the out-of-scope pages, click on the Filter section above the display and select “Show only in-scope items” (fig. 3.14).


Burp Suite Professional v1.7.37 - Temporary Project - licensed to CERT.be [single user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
Re-enable
Show all
Hide all
Revert changes

Logging of out-of-scope Proxy traffic is disabled

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Filter by request type
☑ Show only in-scope items
☐ Show only requested items
☐ Show only parameterized requests
☑ Hide not-found items

Filter by MIME type
☑ HTML ☑ Other text
☑ Script ☐ Images
☑ XML ☑ Flash
☐ CSS ☐ Other binary

Filter by status code
☑ 2xx [success]
☑ 3xx [redirection]
☐ 4xx [request error]
☑ 5xx [server error]

Folders
☑ Hide empty folders

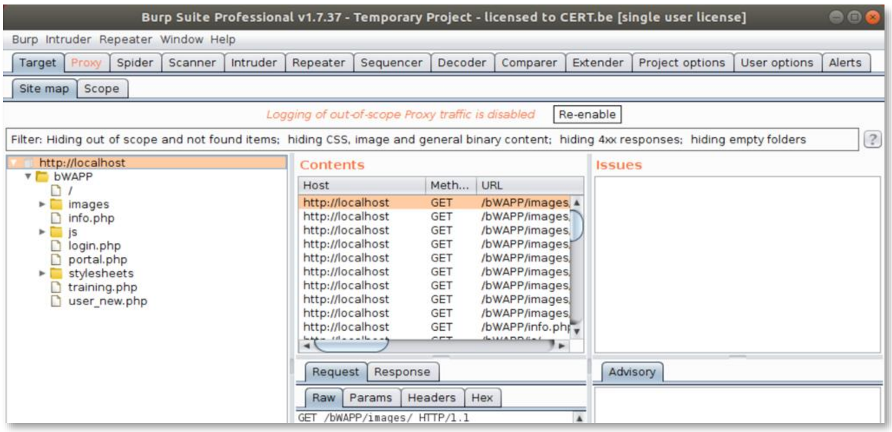
Filter by search term
☐ Regex
☐ Case sensitive ☐ Negative search

Filter by file extension
☐ Show only: asp,aspx,jsp,php
☐ Hide: js,gif,jpg,png,css

Filter by annotation
☐ Show only commented items
☐ Show only highlighted items

Figure 3.14 – Site map of the website

Now, in the tab **Target** -> **Site map**, the content related specifically to the targeted website is shown on the site map (fig. 3.15).


Burp Suite Professional v1.7.37 - Temporary Project - licensed to CERT.be [single user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
Re-enable
Contents
Issues
Request Response
Raw Params Headers Hex
Advisory

Logging of out-of-scope Proxy traffic is disabled

Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

```
http://localhost
  bWAPP
    /
    images
    info.php
    js
    login.php
    portal.php
    stylesheets
    training.php
    user_new.php
```

Host	Meth...	URL
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/info.ph

```
GET /bWAPP/images/ HTTP/1.1
```

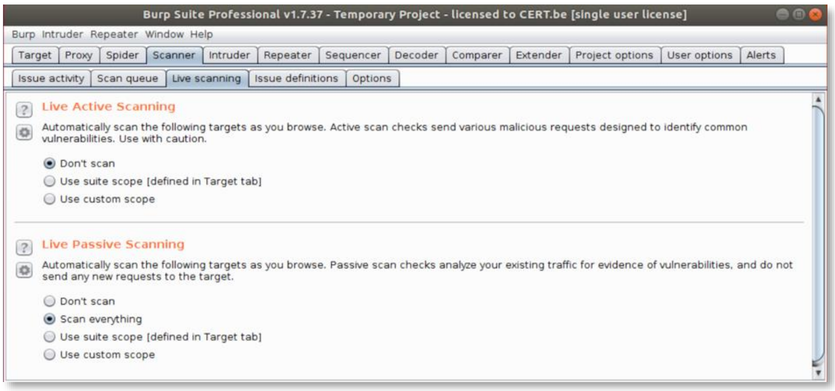
Figure 3.15 – Site map of the website

5. Scanning configuration

Set up the scan type in the tab **Scanner** -> **Live Scanning**.

There are two types of scanning: active scanning that sends malicious requests and may harm the web application, and passive scanning that just analyzes traffic to find vulnerabilities.

Use the default configuration (passive scanning) for a scan in “safe mode” or change it to active scanning by switching to “Use suite scope (defined in Target tab)” in Live Active Scanning section (fig. 3.16).


Burp Suite Professional v1.7.37 - Temporary Project - licensed to CERT.be [single user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Issue activity Scan queue Live scanning Issue definitions Options

Live Active Scanning

Automatically scan the following targets as you browse. Active scan checks send various malicious requests designed to identify common vulnerabilities. Use with caution.

● Don't scan
○ Use suite scope [defined in Target tab]
○ Use custom scope

Live Passive Scanning

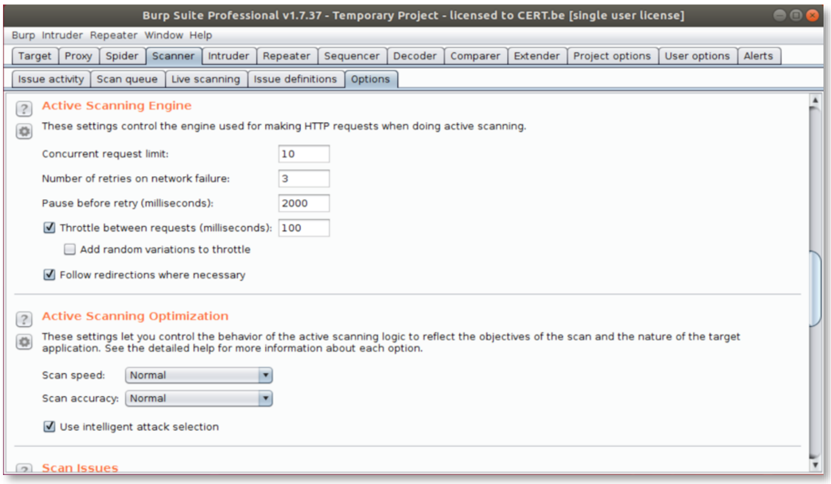
Automatically scan the following targets as you browse. Passive scan checks analyze your existing traffic for evidence of vulnerabilities, and do not send any new requests to the target.

○ Don't scan
● Scan everything
○ Use suite scope [defined in Target tab]
○ Use custom scope

Figure 3.16 – Configure the scanner: scan types

Set up the scan options in the tab **Scanner** -> **Options**.

Scroll down to the “Active Scanning Engine” section. It may be useful to add a waiting time (throttle) between requests such that a slower web server will be able to handle Burp sending cadence (fig. 3.17). The “Active Scanning Optimization” section should be left unchanged. However, the user can adapt the scan speed and the accuracy if needed.


Burp Suite Professional v1.7.37 - Temporary Project - licensed to CERT.be [single user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Issue activity Scan queue Live scanning Issue definitions Options

Active Scanning Engine

These settings control the engine used for making HTTP requests when doing active scanning.

Concurrent request limit: 10

Number of retries on network failure: 3

Pause before retry (milliseconds): 2000

☑ Throttle between requests (milliseconds): 100

☐ Add random variations to throttle

☑ Follow redirections where necessary

Active Scanning Optimization

These settings let you control the behavior of the active scanning logic to reflect the objectives of the scan and the nature of the target application. See the detailed help for more information about each option.

Scan speed: Normal

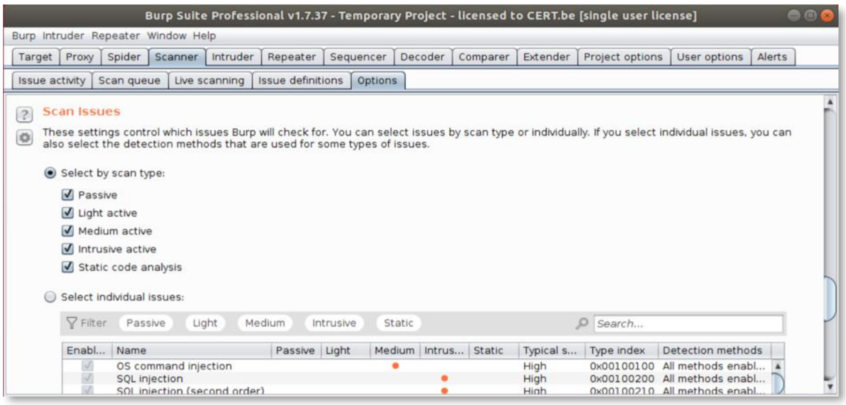
Scan accuracy: Normal

☑ Use intelligent attack selection

Scan Issues

Figure 3.17 – Active Scanning Engine: throttle between requests

Burp allows a fine control over the testing of security issues. The user can select simply by scan type (fig. 3.18) or select individually the desired types of issue to be checked (fig. 3.19). In this case, the user may uncheck, for example, issues related to ASP.NET if the web server doesn't rely on this technology.


Burp Suite Professional v1.7.37 - Temporary Project - licensed to CERT.be [single user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Issue activity Scan queue Live scanning Issue definitions Options
Filter Passive Light Medium Intrusive Static
Search...

Scan Issues

These settings control which issues Burp will check for. You can select issues by scan type or individually. If you select individual issues, you can also select the detection methods that are used for some types of issues.

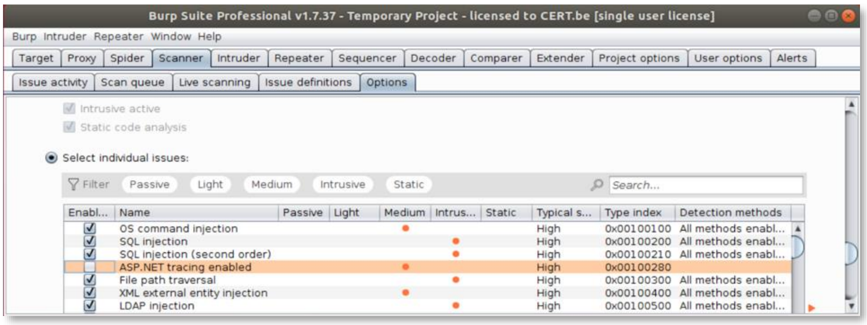
● Select by scan type:

☑ Passive
☑ Light active
☑ Medium active
☑ Intrusive active
☑ Static code analysis

○ Select individual issues:

Enabl...	Name	Passive	Light	Medium	Intrus...	Static	Typical s...	Type index	Detection methods
☑	OS command injection			●			High	0x00100100	All methods enabl...
☑	SQL injection				●		High	0x00100200	All methods enabl...
☑	SQL injection (second order)				●		High	0x00100210	All methods enabl...

Figure 3.18– Scan issues: select by scan type


Burp Suite Professional v1.7.37 - Temporary Project - licensed to CERT.be [single user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Issue activity Scan queue Live scanning Issue definitions Options
Filter Passive Light Medium Intrusive Static
Search...

☑ Intrusive active
☑ Static code analysis

● Select individual issues:

Enabl...	Name	Passive	Light	Medium	Intrus...	Static	Typical s...	Type index	Detection methods
☑	OS command injection			●			High	0x00100100	All methods enabl...
☑	SQL injection				●		High	0x00100200	All methods enabl...
☑	SQL injection (second order)				●		High	0x00100210	All methods enabl...
☐	ASP.NET tracing enabled			●			High	0x00100280	
☑	File path traversal				●		High	0x00100300	All methods enabl...
☑	XML external entity injection			●			High	0x00100400	All methods enabl...
☑	LDAP injection				●		High	0x00100500	All methods enabl...

Figure 3.19 – Scan issues: select individual issues

At some points, the user may want to restore the default configuration of a section. Right click on the little wheel icon on the left and select "Restore defaults" (fig. 3.20).

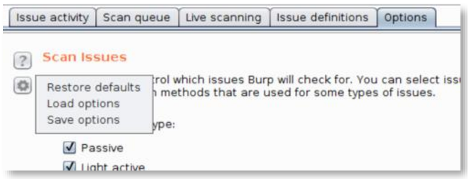


Figure 3.20 – Restore defaults

All other options can be left as default.

6. Vulnerability Scanning

In the tab **Target** -> **Site map,** right click on the target and select "Actively scan this host" (fig. 3.21). When the wizard appears, click on "Next" and then "Ok".

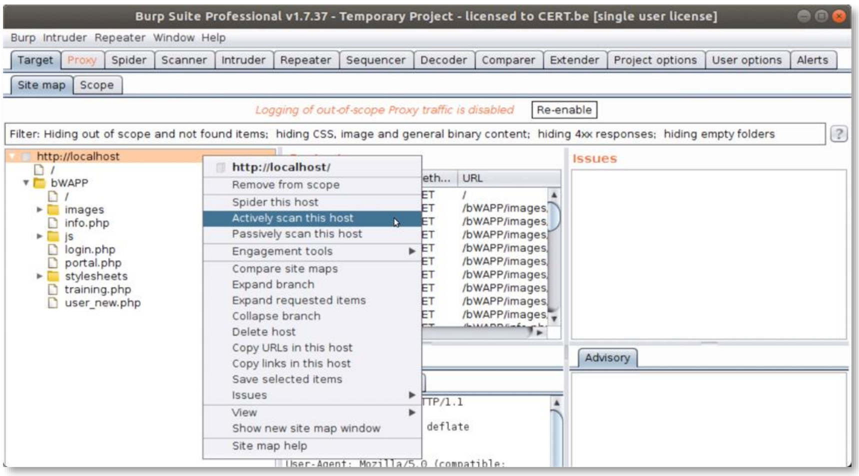
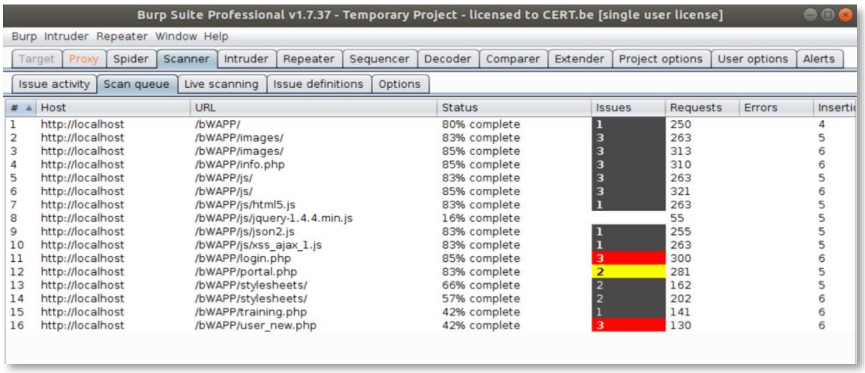


Figure 3.21 – Actively scan this branch/host

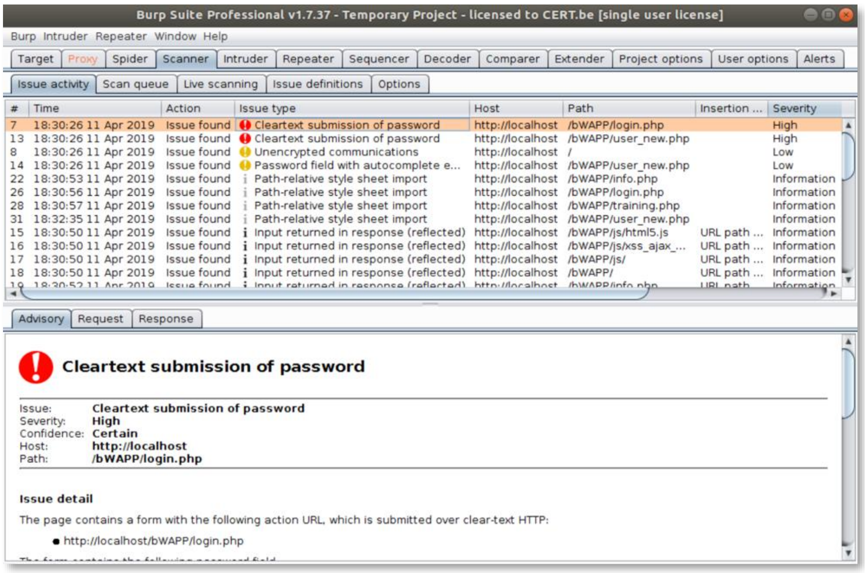
In the tab **Scanner** -> **Scan queue**, you can follow the status of the scanning process (fig. 3.22).



# ▲	Host	URL	Status	Issues	Requests	Errors	Inserti
1	http://localhost	/bWAPP/	80% complete	1	250		4
2	http://localhost	/bWAPP/images/	83% complete	3	263		5
3	http://localhost	/bWAPP/images/	85% complete	3	313		6
4	http://localhost	/bWAPP/info.php	85% complete	3	310		6
5	http://localhost	/bWAPP/js/	83% complete	3	263		5
6	http://localhost	/bWAPP/js/	85% complete	3	321		6
7	http://localhost	/bWAPP/js/html5.js	83% complete	1	263		5
8	http://localhost	/bWAPP/js/jquery-1.4.4.min.js	16% complete		55		5
9	http://localhost	/bWAPP/js/json2.js	83% complete	1	255		5
10	http://localhost	/bWAPP/js/xss_ajax_1.js	83% complete	1	263		5
11	http://localhost	/bWAPP/login.php	85% complete	3	300		6
12	http://localhost	/bWAPP/portal.php	83% complete	2	281		5
13	http://localhost	/bWAPP/stylesheets/	66% complete	2	162		5
14	http://localhost	/bWAPP/stylesheets/	57% complete	2	202		6
15	http://localhost	/bWAPP/training.php	42% complete	1	141		6
16	http://localhost	/bWAPP/user_new.php	42% complete	3	130		6

Figure 3.22 – Scan queue

When the vulnerability scan is finished, Burp reports the issues identified in the tab **Scanner** -> **Issue activity** (fig. 3.23). Sorting is achieved by clicking on the title of the column.


Burp Suite Professional v1.7.37 - Temporary Project - licensed to CERT.be [single user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Issue activity Scan queue Live scanning Issue definitions Options
Advisory Request Response

#	Time	Action	Issue type	Host	Path	Insertion ...	Severity
7	18:30:26 11 Apr 2019	Issue found	Cleartext submission of password	http://localhost	/bWAPP/login.php		High
13	18:30:26 11 Apr 2019	Issue found	Cleartext submission of password	http://localhost	/bWAPP/user_new.php		High
8	18:30:26 11 Apr 2019	Issue found	Unencrypted communications	http://localhost	/		Low
14	18:30:26 11 Apr 2019	Issue found	Password field with autocomplete e...	http://localhost	/bWAPP/user_new.php		Low
22	18:30:53 11 Apr 2019	Issue found	Path-relative style sheet import	http://localhost	/bWAPP/info.php		Information
26	18:30:56 11 Apr 2019	Issue found	Path-relative style sheet import	http://localhost	/bWAPP/login.php		Information
28	18:30:57 11 Apr 2019	Issue found	Path-relative style sheet import	http://localhost	/bWAPP/training.php		Information
31	18:32:35 11 Apr 2019	Issue found	Path-relative style sheet import	http://localhost	/bWAPP/user_new.php		Information
15	18:30:50 11 Apr 2019	Issue found	Input returned in response (reflected)	http://localhost	/bWAPP/js/html5.js	URL path ...	Information
16	18:30:50 11 Apr 2019	Issue found	Input returned in response (reflected)	http://localhost	/bWAPP/js/xss_ajax_...	URL path ...	Information
17	18:30:50 11 Apr 2019	Issue found	Input returned in response (reflected)	http://localhost	/bWAPP/js/	URL path ...	Information
18	18:30:50 11 Apr 2019	Issue found	Input returned in response (reflected)	http://localhost	/bWAPP/	URL path ...	Information
19	18:30:52 11 Apr 2019	Issue found	Input returned in response (reflected)	http://localhost	/bWAPP/info.php	URL path	Information

Cleartext submission of password

Issue: **Cleartext submission of password**
Severity: **High**
Confidence: **Certain**
Host: **http://localhost**
Path: **/bWAPP/login.php**

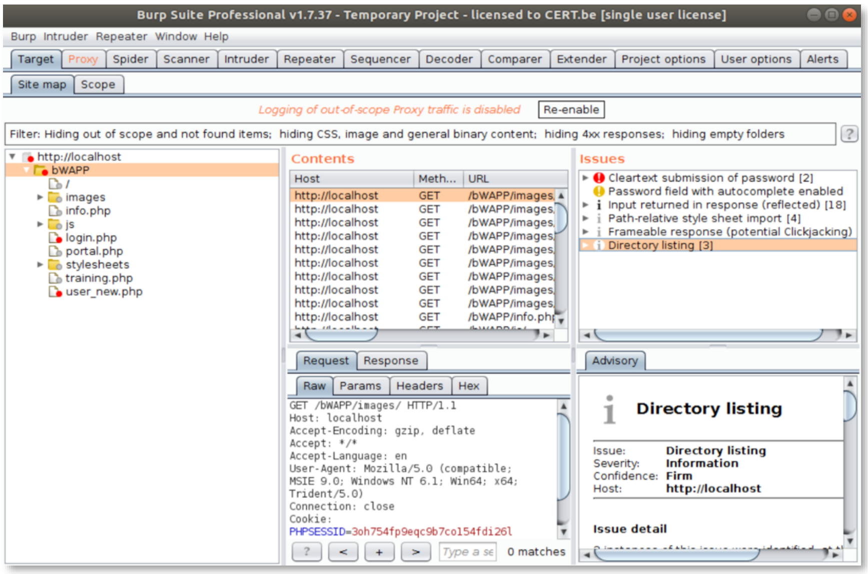
Issue detail

The page contains a form with the following action URL, which is submitted over clear-text HTTP:

- http://localhost/bWAPP/login.php

Figure 3.23 – Issues reported

An overview is displayed in the tab **Target** -> **Site map** (fig. 3.24).


Burp Suite Professional v1.7.37 - Temporary Project - licensed to CERT.be [single user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
Logging of out-of-scope Proxy traffic is disabled
Re-enable
http://localhost
bWAPP
/
images
info.php
js
login.php
portal.php
stylesheets
training.php
user_new.php
Contents
Issues
Request Response
Raw Params Headers Hex
? < + > Type a se 0 matches
Advisory

Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Meth...	URL
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/images
http://localhost	GET	/bWAPP/info.php

- Cleartext submission of password [2]
- Password field with autocomplete enabled
- Input returned in response (reflected) [18]
- Path-relative style sheet import [4]
- Frameable response (potential Clickjacking)
- Directory listing [3]

```
GET /bWAPP/images/ HTTP/1.1
Host: localhost
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible;
MSIE 9.0; Windows NT 6.1; Win64; x64;
Trident/5.0)
Connection: close
Cookie:
PHPSESSID=3oh754fp9eqc9b7co154fdi26l
```

Directory listing

Issue: **Directory listing**
Severity: **Information**
Confidence: **Firm**
Host: **http://localhost**

Issue detail

Figure 3.24 – Overview

Warning: You might need the help of a security professional to fully understand Burp’s results.

OWASP ZAP [Windows-Linux-macOS]

Skill level needed

From beginner to advanced.

Description

Zap (https://www.zaproxy.org/) is an easy-to-use tool to help you find vulnerabilities on your web application, it is completely free and open source, it is a good alternative to Burp Suite.

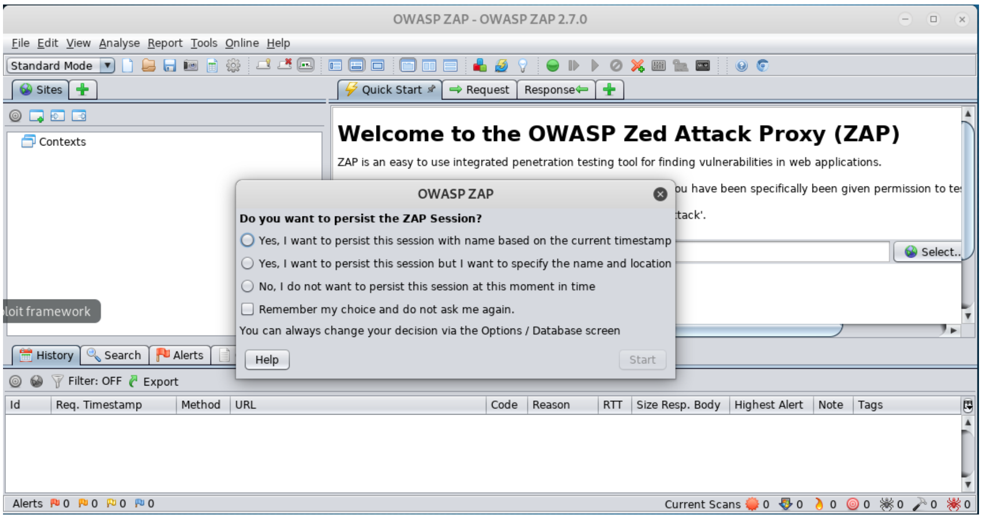
It is cross platform and can be used on Linux (already installed in the Kali Linux distribution), Windows and Mac. It needs Java to run.

Zap uses an intercepting proxy just like Burp Suite, it also features passive and active scanners. The passive scanner is safe to use at any time as it doesn't alter the traffic, the active scanner on the other hand can be used to performs attacks. The spider crawls the website for hidden pages or directory and can be used in combination with dictionaries to run brute force attacks.

Zap also has the possibility to add extensions with new functionalities.

How to use ZAP?

Below is an example of the starting page on a Linux version (Figure 4), Zap lets you choose if you want to persist this session.



Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

ou have been specifically been given permission to te

tack'.

OWASP ZAP

Do you want to persist the ZAP Session?

○ Yes, I want to persist this session with name based on the current timestamp

○ Yes, I want to persist this session but I want to specify the name and location

○ No, I do not want to persist this session at this moment in time

□ Remember my choice and do not ask me again.

You can always change your decision via the Options / Database screen

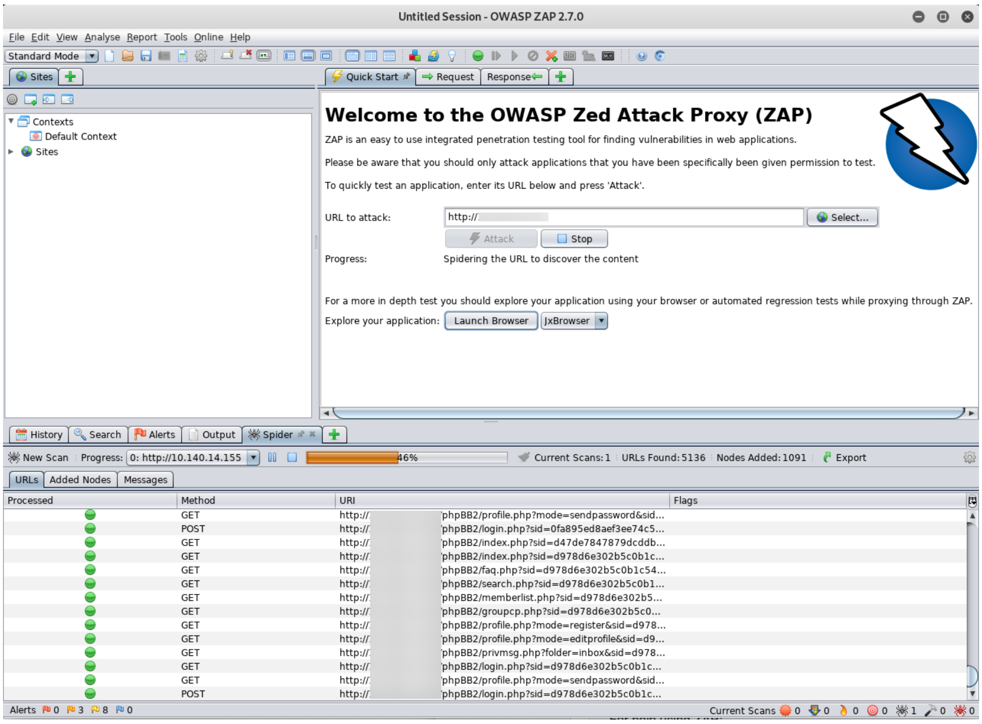
Help | Start

Id	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags

Alerts 0 0 0 0 Current Scans 0 0 0 0 0 0 0

Figure 4 - Zap start page

We will perform an active scanning on a vulnerable virtual machine from the Owasp project, we just have to enter the target address in the 'URL to attack' search bar and click on the 'Attack' button. Zap will use the spider to crawl (discover) the complete website in his http & https versions and make an active vulnerability scan.



Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://[redacted]

Progress: Spidering the URL to discover the content

For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.

Explore your application:

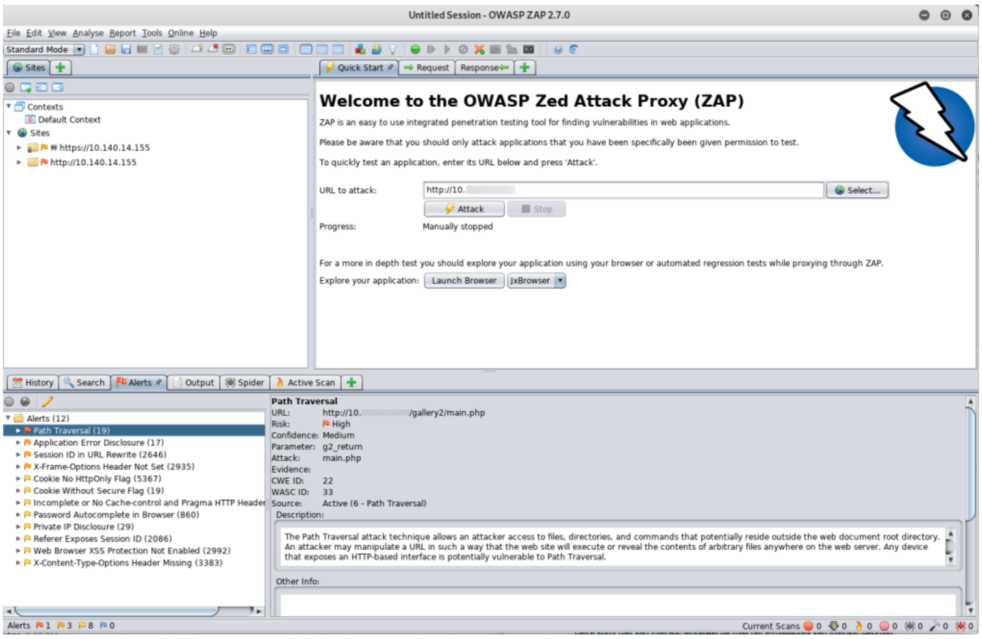
Progress: 0: http://10.140.14.155 46% Current Scans: 1 URLs Found: 5136 Nodes Added: 1091

Processed	Method	URI	Flags
●	GET	http://[redacted]phpBB2/profile.php?mode=sendpassword&sid...	
●	POST	http://[redacted]phpBB2/login.php?sid=0fa895ed8aef3ee74c5...	
●	GET	http://[redacted]phpBB2/index.php?sid=d47de7847879dcddb...	
●	GET	http://[redacted]phpBB2/index.php?sid=d978d6e302b5c0b1c...	
●	GET	http://[redacted]phpBB2/faq.php?sid=d978d6e302b5c0b1c54...	
●	GET	http://[redacted]phpBB2/search.php?sid=d978d6e302b5c0b1...	
●	GET	http://[redacted]phpBB2/memberlist.php?sid=d978d6e302b5...	
●	GET	http://[redacted]phpBB2/groupcp.php?sid=d978d6e302b5c0...	
●	GET	http://[redacted]phpBB2/profile.php?mode=register&sid=d978...	
●	GET	http://[redacted]phpBB2/profile.php?mode=editprofile&sid=d9...	
●	GET	http://[redacted]phpBB2/privmsg.php?folder=inbox&sid=d978...	
●	GET	http://[redacted]phpBB2/login.php?sid=d978d6e302b5c0b1c...	
●	GET	http://[redacted]phpBB2/profile.php?mode=sendpassword&sid...	
●	POST	http://[redacted]phpBB2/login.php?sid=d978d6e302b5c0b1c...	

Alerts 0 3 8 0 Current Scans 0 0 0 0 1 0 0

Figure 5 - ZAP in action

When done, the results are shown in the Alerts tab, classified by risk importance with the higher risks at the top (from high to low).



https://10.140.14.155
http://10.140.14.155

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://10.[redacted]

Progress: Manually stopped

For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.

Explore your application:

- Alerts (12)
  - Path Traversal (19)
  - Application Error Disclosure (17)
  - Session ID in URL Rewrite (2646)
  - X-Frame-Options Header Not Set (2935)
  - Cookie No HttpOnly Flag (5367)
  - Cookie Without Secure Flag (19)
  - Incomplete or No Cache-control and Pragma HTTP Header
  - Password Autocomplete in Browser (860)
  - Private IP Disclosure (29)
  - Referer Exposes Session ID (2086)
  - Web Browser XSS Protection Not Enabled (2992)
  - X-Content-Type-Options Header Missing (3383)

Path Traversal
URL: http://10.[redacted]/gallery2/main.php
Risk: High
Confidence: Medium
Parameter: g2_return
Attack: main.php
Evidence:
CWE ID: 22
WASC ID: 33
Source: Active (6 - Path Traversal)

Description:

The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any device that exposes an HTTP-based interface is potentially vulnerable to Path Traversal.

Other Info:

Alerts 1 3 8 0 Current Scans 0 0 0 0 0 0 0

Figure 6 - Zap results

To go deeper with Zap:
https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

3.3 Network Vulnerability scanners

Nessus [Windows-Linux-macOS]

Description

Nessus started as a free tool. But in 2005, it became a proprietary product. Nowadays, it is one of the most well-known and used security vulnerability scanning tool. Nessus helps to identify a large variety of vulnerabilities such as software flaws, missing patches, malware, and misconfigurations.

Nessus will run on most systems (Windows, Linux, Mac) and comes with a graphical user interface to perform the scans.

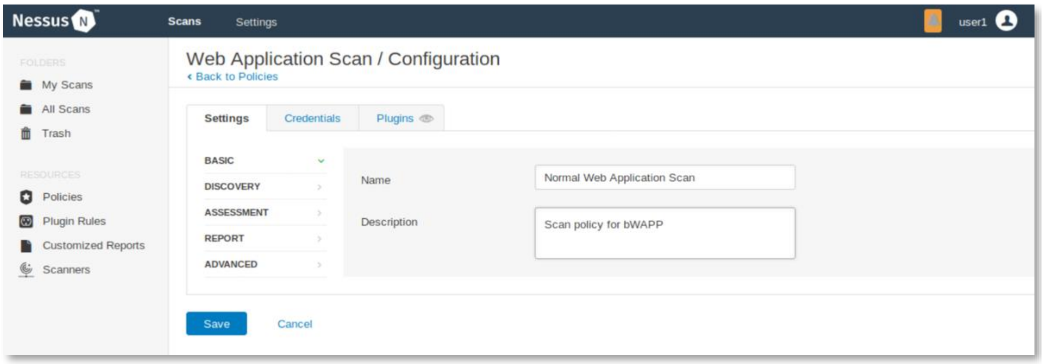
Nessus Pro costs +/- 4000€ per year but tenable also provides an essential version (formerly Nessus Home) which will allow you to scan your environment up to 16 IP addresses per scanner for free.

How to use Nessus?

1. Policy set up

When performing a scan, the first step is to create a scan policy. Different plugins come by default with Nessus such as Host Discovery, Basic Network Scan, or Web Application Tests. Many others are also available.

For a Vulnerability testing of web applications, we will use the Web Application Tests policy. On the left menu choose **Policies**, then create a new policy. Add a name (i.e "Normal Web Application Scan") and a description (fig. 7.1). With the Assessment settings, choose the scan type (i.e. Scan for all web vulnerabilities (complex)) and save it (fig 7.2). The other settings can be left unchanged.

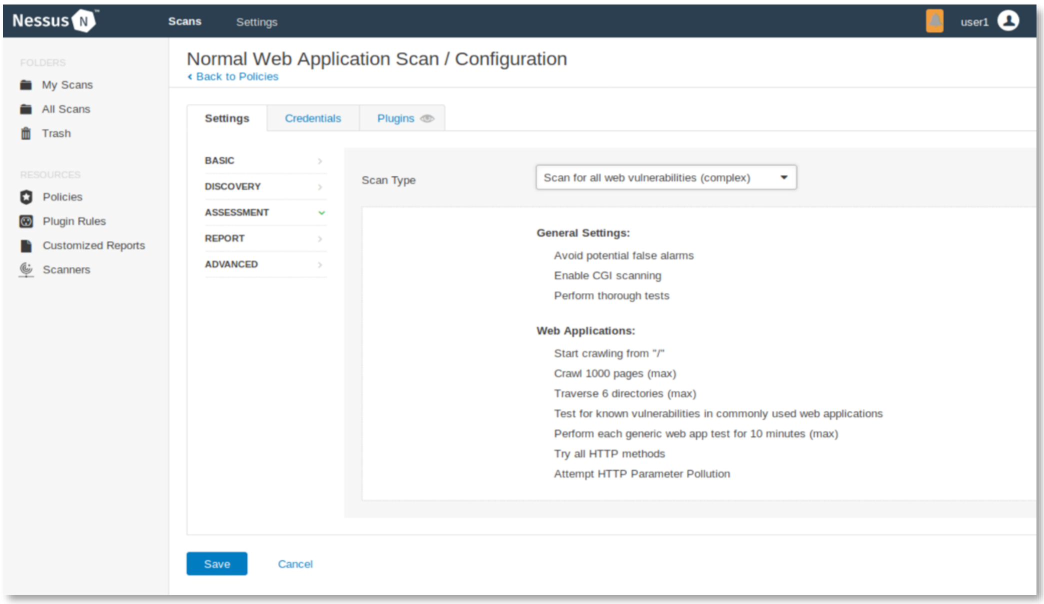


Web Application Scan / Configuration

Name: Normal Web Application Scan

Description: Scan policy for bWAPP

Figure 7.1 – Policies/Settings/Basic



Normal Web Application Scan / Configuration
‹ Back to Policies

Scan Type: Scan for all web vulnerabilities (complex)

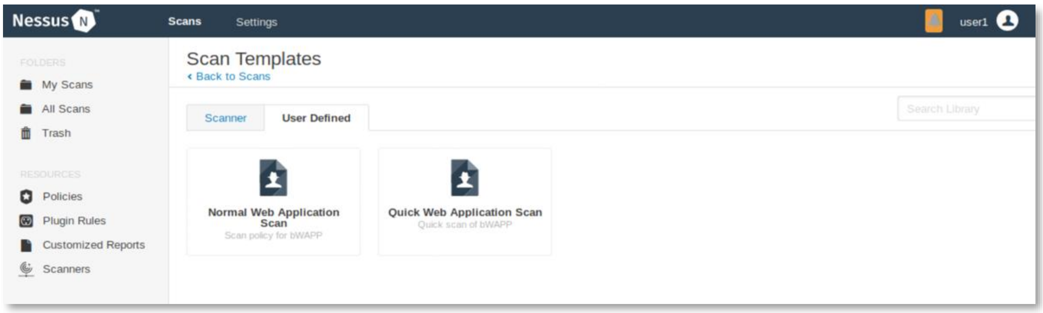
General Settings:
Avoid potential false alarms
Enable CGI scanning
Perform thorough tests

Web Applications:
Start crawling from "/"
Crawl 1000 pages (max)
Traverse 6 directories (max)
Test for known vulnerabilities in commonly used web applications
Perform each generic web app test for 10 minutes (max)
Try all HTTP methods
Attempt HTTP Parameter Pollution

Figure 7.2 – Policies/Settings/Assessment

2. Scanning set up

Having set the policy, on the left menu choose **My Scans** and then Create a new scan. In the tab “User defined”, from the created policy, choose the appropriate one (i.e. “Normal Web Application Scan”) (fig 7.3). Note that if you haven’t created a policy previously, it is also possible to set up the scan policy during the setup of a new scan.



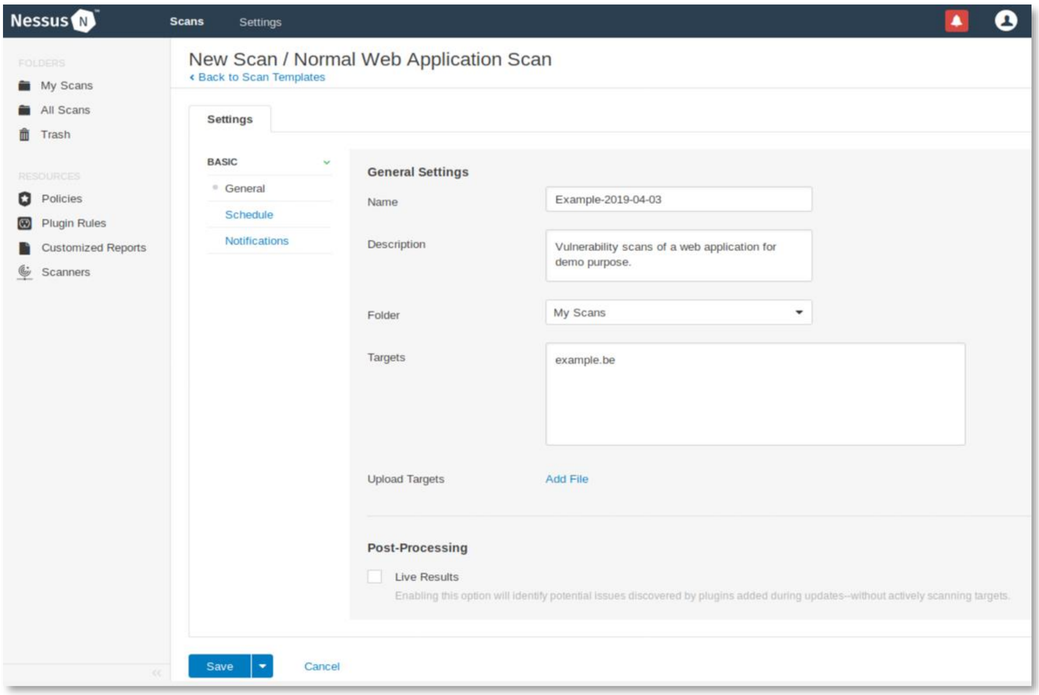
Scan Templates
‹ Back to Scans

Normal Web Application Scan
Scan policy for bWAPP

Quick Web Application Scan
Quick scan of bWAPP

Figure 7.3 – My Scans/User Defined

Now specify the general settings of your scan such as Name, Description, Folder, and Targets, and save them (fig. 7.4).



New Scan / Normal Web Application Scan

General Settings

Name: Example-2019-04-03

Description: Vulnerability scans of a web application for demo purpose.

Folder: My Scans

Targets: example.be

Upload Targets: Add File

Post-Processing

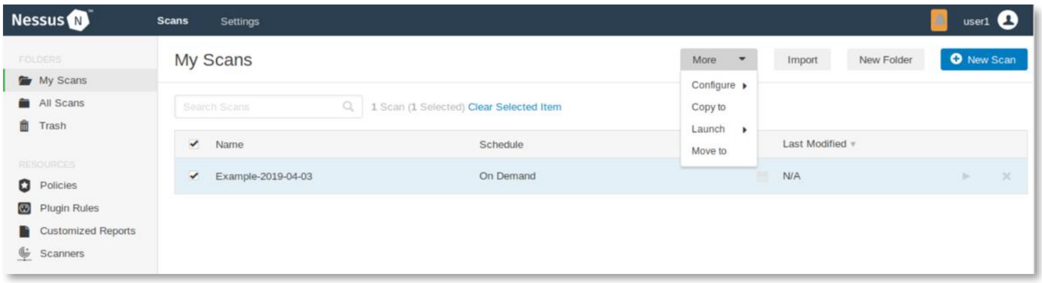
□ Live Results

Enabling this option will identify potential issues discovered by plugins added during updates–without actively scanning targets.

Figure 7.4 – New Scan/Settings/General

Step 3. Scanning & Report

Choose the scan to be performed and launch it using the menu at the top of the page (**More** -> **Launch**) or by clicking on the arrow ▶ (fig. 7.5).



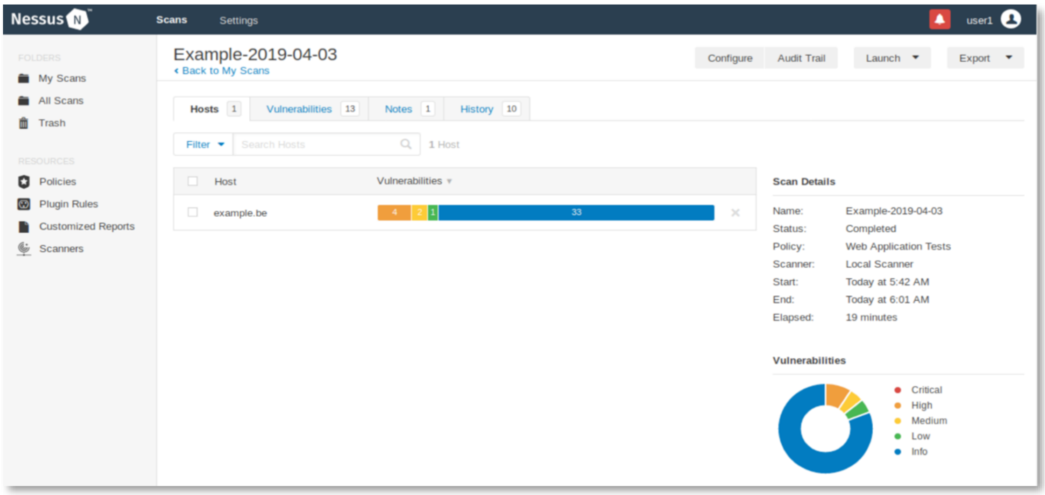
My Scans

1 Scan (1 Selected) Clear Selected Item

✓	Name	Schedule	Last Modified
✓	Example-2019-04-03	On Demand	N/A

Figure 7.5 – My Scans

When the scan is finished, click on the name of the scan to see the scan report. The report displays a horizontal bar chart and a pie chart, both showing the percentage of each type of vulnerability identified (fig. 7.6).



Example-2019-04-03
‹ Back to My Scans

Host	Vulnerabilities
example.be	4 2 1 33

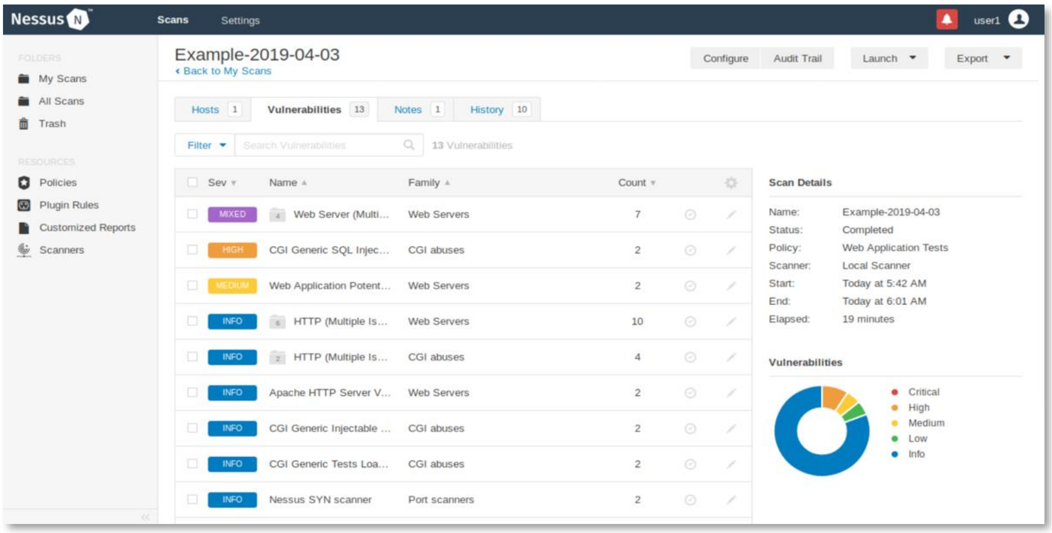
Scan Details

Name:	Example-2019-04-03
Status:	Completed
Policy:	Web Application Tests
Scanner:	Local Scanner
Start:	Today at 5:42 AM
End:	Today at 6:01 AM
Elapsed:	19 minutes

Vulnerabilities

Figure 7.6 – My Scans/Hosts

To see the detailed report, click on the tab **Vulnerabilities**. A list of all vulnerabilities is displayed (fig. 7.7). Some of them may group several vulnerabilities (i.e. MIXED – Apache HTTP Server). Click it to show the elements composing that particular group (fig. 7.8).



Example-2019-04-03
‹ Back to My Scans

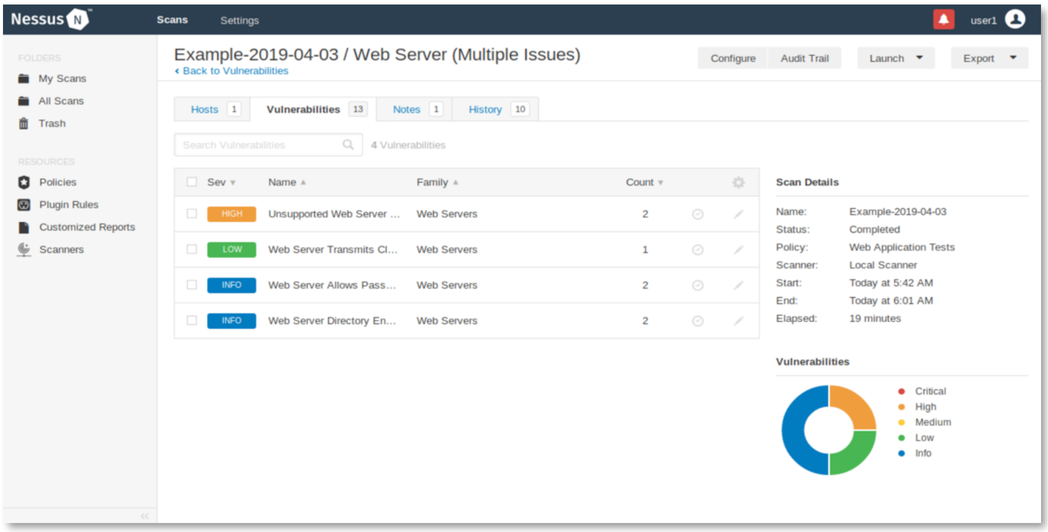
Sev	Name	Family	Count
MIXED	4 Web Server (Multi...	Web Servers	7
HIGH	CGI Generic SQL Injec...	CGI abuses	2
MEDIUM	Web Application Potent...	Web Servers	2
INFO	6 HTTP (Multiple Is...	Web Servers	10
INFO	2 HTTP (Multiple Is...	CGI abuses	4
INFO	Apache HTTP Server V...	Web Servers	2
INFO	CGI Generic Injectable ...	CGI abuses	2
INFO	CGI Generic Tests Loa...	CGI abuses	2
INFO	Nessus SYN scanner	Port scanners	2

Scan Details

Name:	Example-2019-04-03
Status:	Completed
Policy:	Web Application Tests
Scanner:	Local Scanner
Start:	Today at 5:42 AM
End:	Today at 6:01 AM
Elapsed:	19 minutes

Vulnerabilities

Figure 7.7 – My Scans/Vulnerabilities



Example-2019-04-03 / Web Server (Multiple Issues)

‹ Back to Vulnerabilities

4 Vulnerabilities

	Sev	Name	Family	Count
□	HIGH	Unsupported Web Server ...	Web Servers	2
□	LOW	Web Server Transmits Cl...	Web Servers	1
□	INFO	Web Server Allows Pass...	Web Servers	2
□	INFO	Web Server Directory En...	Web Servers	2

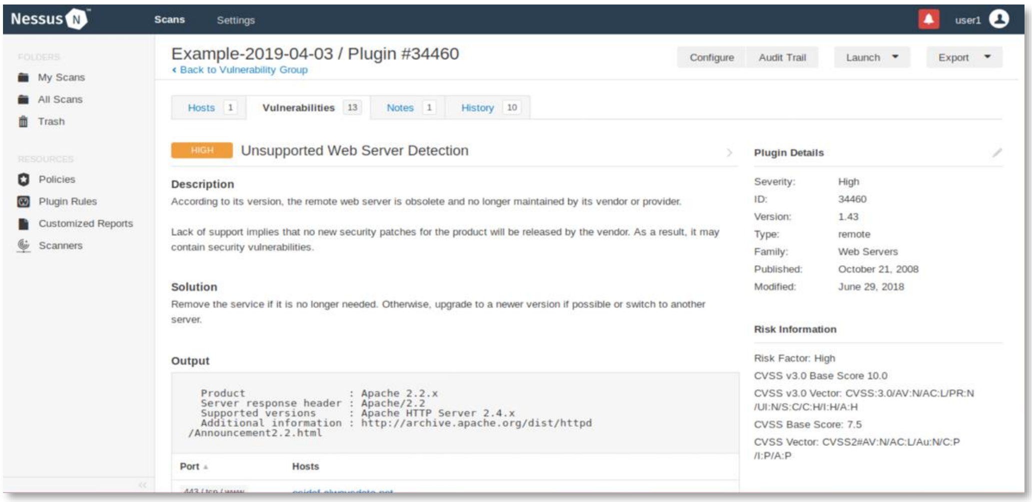
Scan Details

Name:	Example-2019-04-03
Status:	Completed
Policy:	Web Application Tests
Scanner:	Local Scanner
Start:	Today at 5:42 AM
End:	Today at 6:01 AM
Elapsed:	19 minutes

Vulnerabilities

Figure 7.8 – My Scans/Vulnerabilities/Mixed (vulnerability group)

When clicking on a vulnerability, Nessus will show its description and the corresponding solution/remediation (fig. 7.9).



Example-2019-04-03 / Plugin #34460

‹ Back to Vulnerability Group

HIGH Unsupported Web Server Detection

Description

According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Remove the service if it is no longer needed. Otherwise, upgrade to a newer version if possible or switch to another server.

Output

```
    Product                : Apache 2.2.x
    Server response header : Apache/2.2
    Supported versions     : Apache HTTP Server 2.4.x
    Additional information : http://archive.apache.org/dist/httpd
  /Announcement2.2.html
```

Port ▲	Hosts

Plugin Details

Severity:	High
ID:	34460
Version:	1.43
Type:	remote
Family:	Web Servers
Published:	October 21, 2008
Modified:	June 29, 2018

Risk Information

Risk Factor: High

CVSS v3.0 Base Score 10.0

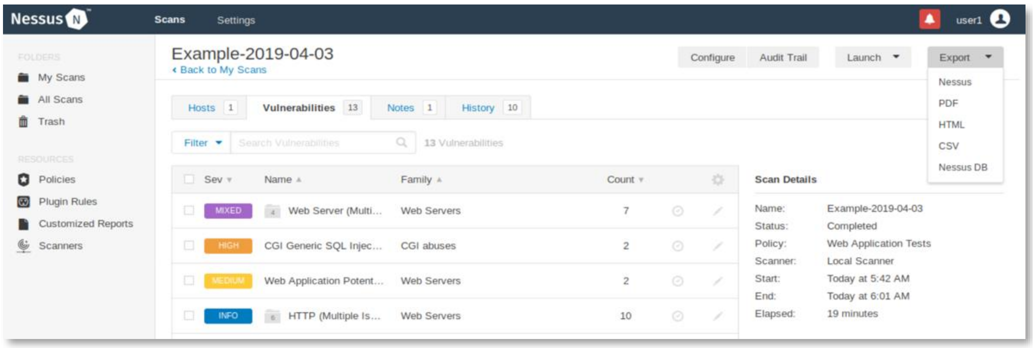
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS Base Score: 7.5

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

Figure 7.9 – My Scans/Vulnerabilities/Mixed/Apache 2.4.x < 2.4.35 Dos

At any time, a report can be printed out (exported) using the menu at the top of the page (fig. 7.10).



Example-2019-04-03

Sev	Name	Family	Count
MIXED	4 Web Server (Multi…	Web Servers	7
HIGH	CGI Generic SQL Injec…	CGI abuses	2
MEDIUM	Web Application Potent…	Web Servers	2
INFO	6 HTTP (Multiple Is…	Web Servers	10

Scan Details

Name: Example-2019-04-03
Status: Completed
Policy: Web Application Tests
Scanner: Local Scanner
Start: Today at 5:42 AM
End: Today at 6:01 AM
Elapsed: 19 minutes

Figure 7.10 – My Scans/Vulnerabilities/Export

Nessus is a very powerful tool but may require the help of a cybersecurity professional to understand the report results and mitigate the vulnerabilities found.

OpenVas [~~Windows~~-Linux-~~macOS~~]

Skill level needed

Intermediate.

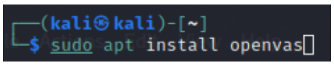
Description

Open VAS (https://openvas.org/) stands for Open Vulnerability Assessment Scanner, it is a full-featured open-source vulnerability scanner. The project was created as a reaction to the discontinuation of the Open-Source version of Nessus.

How to use Open VAS?

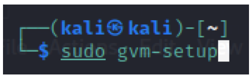
An already configured VM with a trial version of the tool is available on the website of Greenbone, the company supporting the project.

Installation is also easily done through Kali Linux just run the following command:



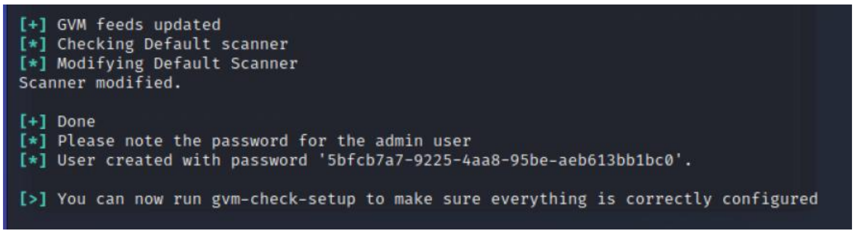
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install openvas
```

Once the first part of the installation is over, run the following command to set up Open Vas:



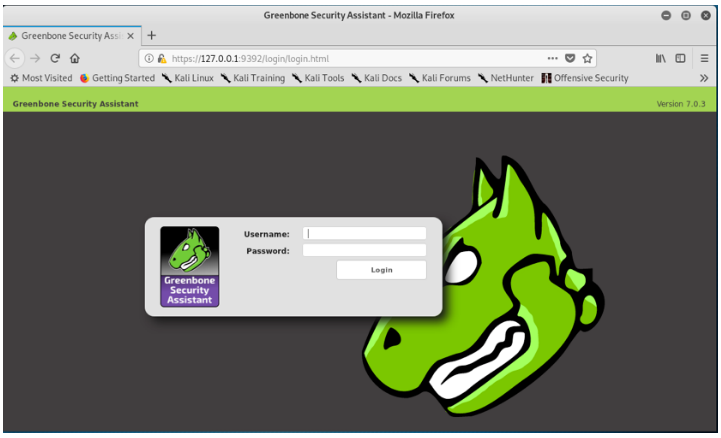
```
┌──(kali㉿kali)-[~]
└─$ sudo gvm-setup
```

When done you will see the following message:

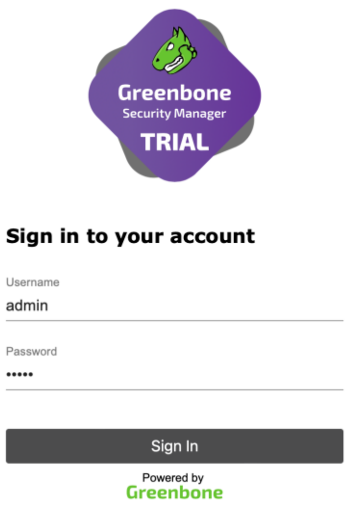


```
[+] GVM feeds updated
[*] Checking Default scanner
[*] Modifying Default Scanner
Scanner modified.

[+] Done
[*] Please note the password for the admin user
[*] User created with password '5bfcb7a7-9225-4aa8-95be-aeb613bb1bc0'.

[>] You can now run gvm-check-setup to make sure everything is correctly configured
```

You have to run the gvm-check-setup command and Open Vas will check your configuration. If the configuration is successful, Open Vas install will automatically launch your web browser and open a web page with an interface where you can login using ‘admin’ as the user in combination with the generated password from the script (see above screenshot) in our case it is '5bfcb7a7-9225-4aa8-95be-aeb613bb1bc0'.



If you used the virtual machine from Greenbone's website instead of the command line install you will see the logging screen. After you defined a new admin user via the console you will be able to log in with the web interface:

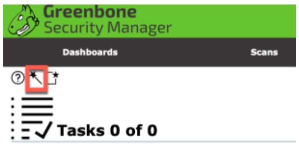


Sign in to your account

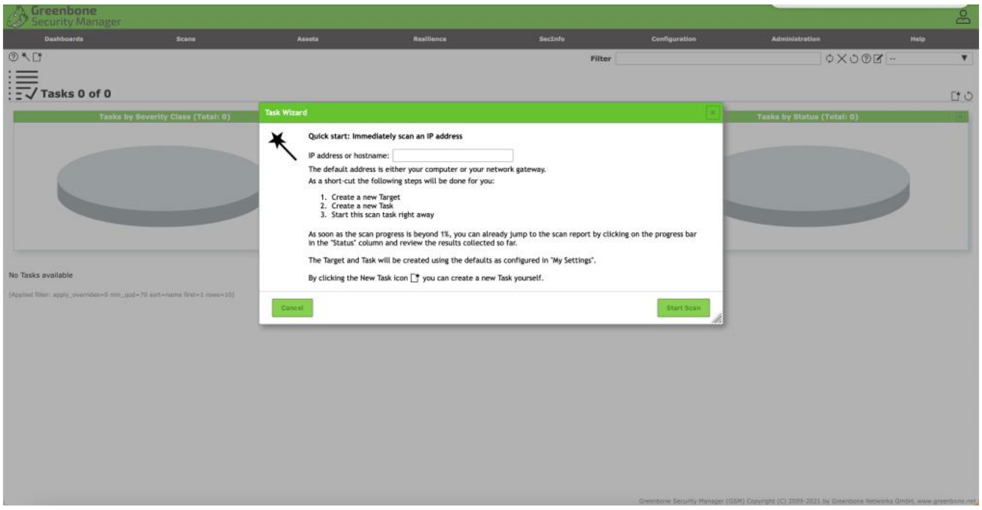
Username
admin

Password
•••••

Once logged in, go into the Scans menu at the top and click on the small magic wand in the upper left corner to use the Task Wizard to launch our first scan.



For the purpose of this report, we will use a vulnerable virtual machine (Metasploitable VM) with a private IP address, we just have to fill in the field "IP address or hostname".



Tasks 0 of 0

Task Wizard

Quick start: Immediately scan an IP address

IP address or hostname:

The default address is either your computer or your network gateway.

As a short-cut the following steps will be done for you:

1. Create a new Target
2. Create a new Task
3. Start this scan task right away

As soon as the scan progress is beyond 1%, you can already jump to the scan report by clicking on the progress bar in the "Status" column and review the results collected so far.

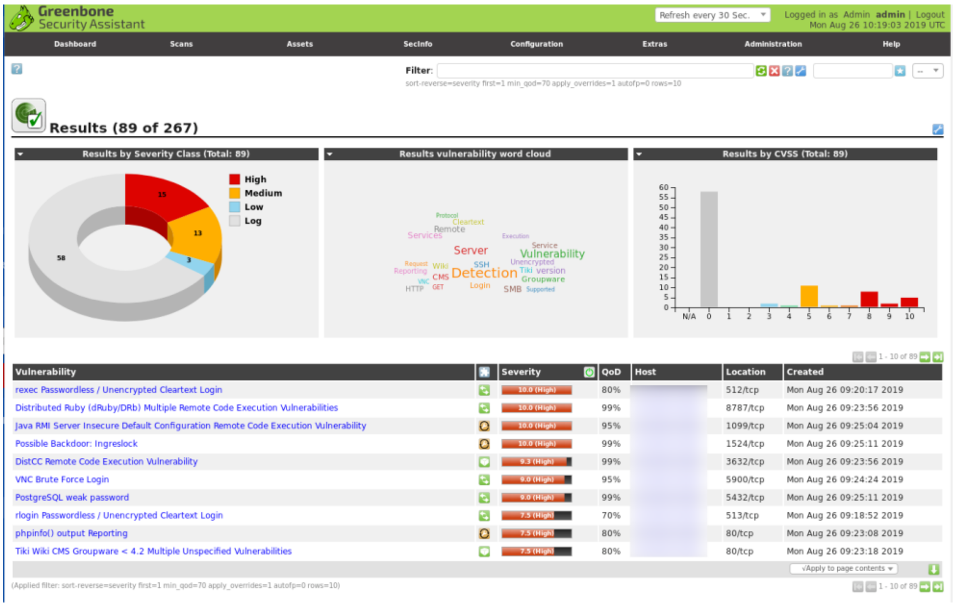
The Target and Task will be created using the defaults as configured in "My Settings".

By clicking the New Task icon you can create a new Task yourself.

No Tasks available

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Since the virtual machine we are testing is vulnerable, after the scan has been completed, a lot of vulnerabilities can be seen in the result tab:



sort-reverse=severity first=1 min_qod=70 apply_overrides=1 autofp=0 rows=10

Results (89 of 267)

Vulnerability		Severity	QoD	Host	Location	Created
rexec Passwordless / Unencrypted Cleartext Login		10.0 (High)	80%	[redacted]	512/tcp	Mon Aug 26 09:20:17 2019
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities		10.0 (High)	99%	[redacted]	8787/tcp	Mon Aug 26 09:23:56 2019
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability		10.0 (High)	95%	[redacted]	1099/tcp	Mon Aug 26 09:25:04 2019
Possible Backdoor: Ingreslock		10.0 (High)	99%	[redacted]	1524/tcp	Mon Aug 26 09:25:11 2019
DistCC Remote Code Execution Vulnerability		9.3 (High)	99%	[redacted]	3632/tcp	Mon Aug 26 09:23:56 2019
VNC Brute Force Login		9.0 (High)	95%	[redacted]	5900/tcp	Mon Aug 26 09:24:24 2019
PostgreSQL weak password		9.0 (High)	99%	[redacted]	5432/tcp	Mon Aug 26 09:25:11 2019
rlogin Passwordless / Unencrypted Cleartext Login		7.5 (High)	70%	[redacted]	513/tcp	Mon Aug 26 09:18:52 2019
phpinfo() output Reporting		7.5 (High)	80%	[redacted]	80/tcp	Mon Aug 26 09:23:08 2019
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities		7.5 (High)	80%	[redacted]	80/tcp	Mon Aug 26 09:23:18 2019

(Applied filter: sort-reverse=severity first=1 min_qod=70 apply_overrides=1 autofp=0 rows=10)

The vulnerabilities can be classified by severity, a score is automatically attributed by the scanner, Open Vas will also test web vulnerabilities.

More information about Open Vas and also a live demo can be found on the website of Greenbone, the company supporting the project.

3.4 Encryption configuration validation tools

Qualys SSL/TLS scanner [Cloud-based]

Skill level needed

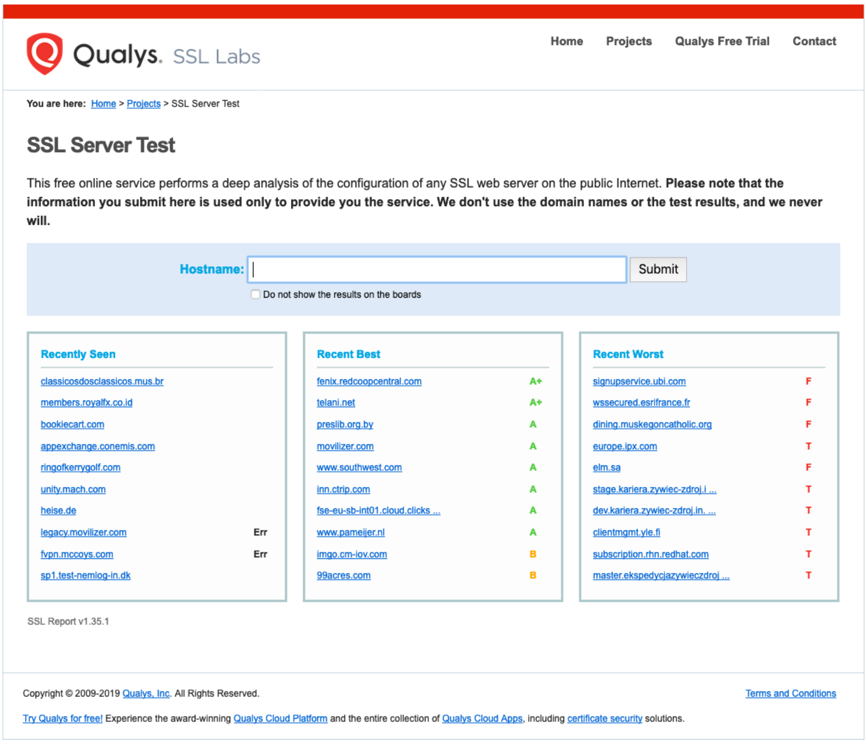
Beginner.

Description

SSL stands for Secure Socket Layer; its purpose is to establish a secure and encrypted link between two points on the internet. It has been updated to TLS which stands for Transport Layer Security. When a website uses the https acronym it means it is using hypertext transfer protocol through a secured connection (TLS).

It can be interesting to evaluate the SSL/TLS configuration of your website, companies like Qualys gives you the possibility to assess it for free.

Just enter your website address in the 'Hostname' field to test your website.



You are here: Home > Projects > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Hostname: | Submit

□ Do not show the results on the boards

Recently Seen	
classicosdosclassicos.mus.br	
members.royalfx.co.id	
bookiecart.com	
appexchange.conemis.com	
ringofkerrygolf.com	
unity.mach.com	
heise.de	
legacy.movilizer.com	Err
fvpn.mccoys.com	Err
sp1.test-nemlog-in.dk	

Recent Best	
fenix.redcoopcentral.com	A+
telani.net	A+
preslib.org.by	A
movilizer.com	A
www.southwest.com	A
inn.ctrip.com	A
fse-eu-sb-int01.cloud.clicks ...	A
www.pameijer.nl	A
imgo.cm-iov.com	B
99acres.com	B

Recent Worst	
signupservice.ubi.com	F
wssecured.esrifrance.fr	F
dining.muskegoncatholic.org	F
europe.ipx.com	T
elm.sa	F
stage.kariera.zywiec-zdroj.i ...	T
dev.kariera.zywiec-zdroj.in. ...	T
clientmgmt.yle.fi	T
subscription.rhn.redhat.com	T
master.ekspedycjazywieczdroj ...	T

SSL Report v1.35.1

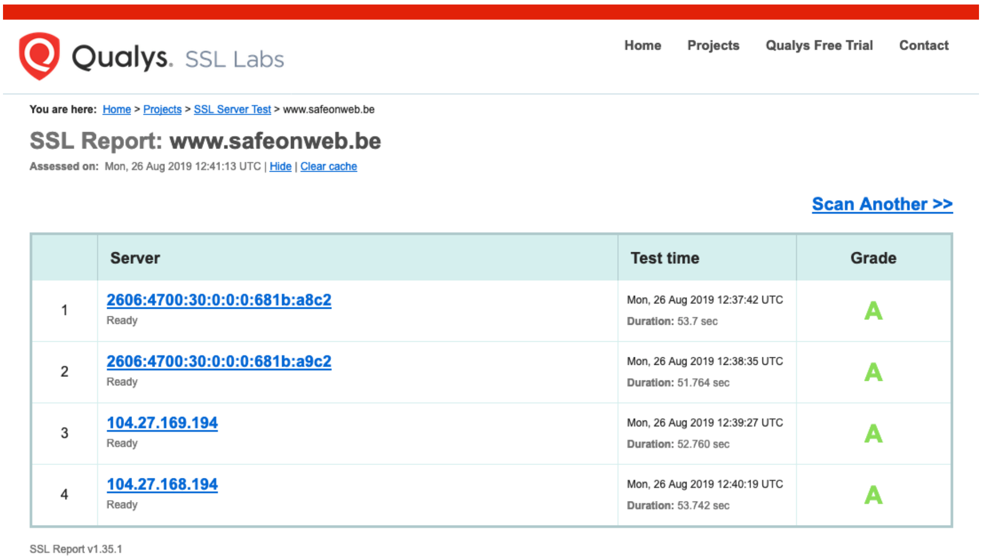
Copyright © 2009-2019 Qualys, Inc. All Rights Reserved. Terms and Conditions

Try Qualys for free! Experience the award-winning Qualys Cloud Platform and the entire collection of Qualys Cloud Apps, including certificate security solutions.

Figure 7 - Qualys SSL host scanning page

After analysis your website will be graded from 'A' to 'F', the scanner will check different parameters to attribute the grade like certificate validity, protocol used, key exchange support, cipher support etc.

Here is an example of a scan result with a ‘A’ grade:



You are here: Home > Projects > SSL Server Test > www.safeonweb.be

SSL Report: www.safeonweb.be

Assessed on: Mon, 26 Aug 2019 12:41:13 UTC | Hide | Clear cache

Scan Another >>

	Server	Test time	Grade
1	2606:4700:30:0:0:0:681b:a8c2 Ready	Mon, 26 Aug 2019 12:37:42 UTC Duration: 53.7 sec	A
2	2606:4700:30:0:0:0:681b:a9c2 Ready	Mon, 26 Aug 2019 12:38:35 UTC Duration: 51.764 sec	A
3	104.27.169.194 Ready	Mon, 26 Aug 2019 12:39:27 UTC Duration: 52.760 sec	A
4	104.27.168.194 Ready	Mon, 26 Aug 2019 12:40:19 UTC Duration: 53.742 sec	A

SSL Report v1.35.1

Figure 8 - SSL Scan results

3.5 Website’s CMS (Content Management System) Vulnerability assessment tools

Droopescan [~~Windows~~-Linux-~~macOS~~]

Skill level needed

Intermediate.

Description

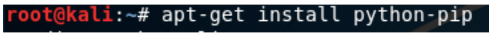
Droopescan (https://github.com/SamJoan/droopescan) is a plugin-based scanner, it can help you identify issues with several CMS.

Supported CMS are Silver Stripe and WordPress.

Some partial functionality for Joomla, Moodle and Drupal.

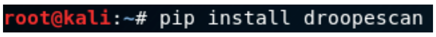
Droopescan is easy to install from a Kali Linux operating system, just use PIP (Package Installer for Python).

In the terminal just type the following command to install PIP:



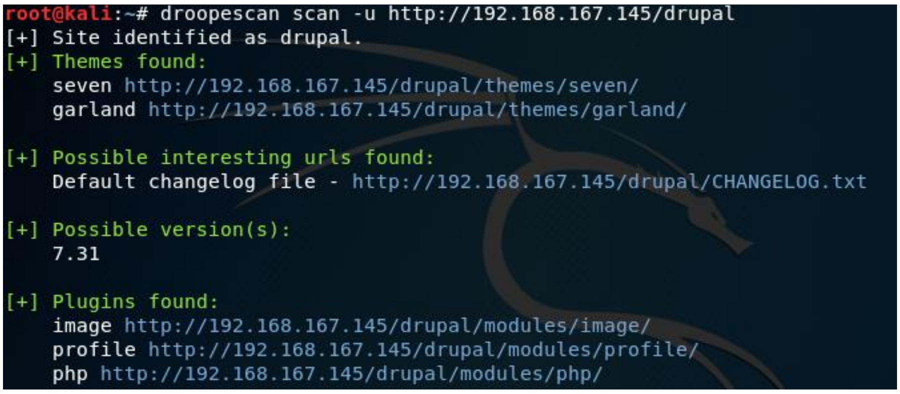
```
root@kali:~# apt-get install python-pip
```

Once PIP is installed it is time to install DroopeScan:



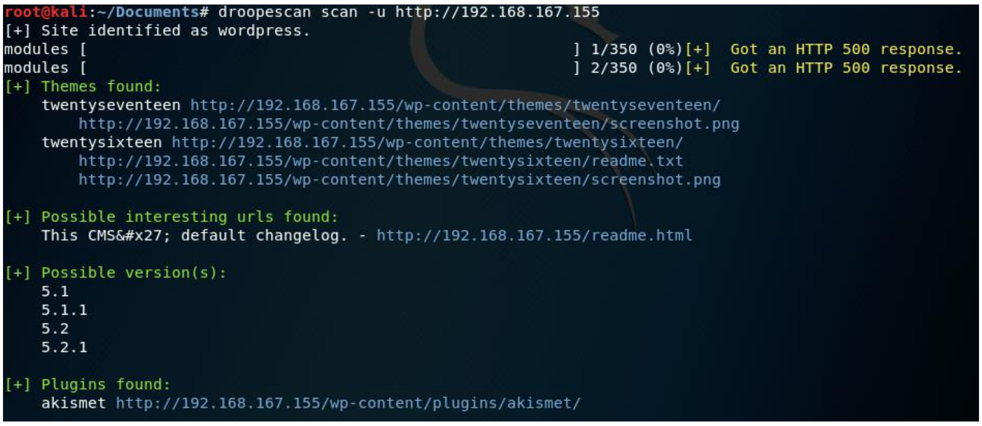
```
root@kali:~# pip install droopescan
```

Next step is to try a scan on a Drupal website, when the Droopescan scan command is executed against your target, the installed plugins are detected. It might be a good idea to make sure that they are updated to the latest version:



```
root@kali:~# droopescan scan -u http://192.168.167.145/drupal
[+] Site identified as drupal.
[+] Themes found:
    seven http://192.168.167.145/drupal/themes/seven/
    garland http://192.168.167.145/drupal/themes/garland/

[+] Possible interesting urls found:
    Default changelog file - http://192.168.167.145/drupal/CHANGELOG.txt

[+] Possible version(s):
    7.31

[+] Plugins found:
    image http://192.168.167.145/drupal/modules/image/
    profile http://192.168.167.145/drupal/modules/profile/
    php http://192.168.167.145/drupal/modules/php/
```

Let’s also scan a WordPress site:



```
root@kali:~/Documents# droopescan scan -u http://192.168.167.155
[+] Site identified as wordpress.
modules [                                                    ] 1/350 (0%)[+]  Got an HTTP 500 response.
modules [                                                    ] 2/350 (0%)[+]  Got an HTTP 500 response.
[+] Themes found:
    twentyseventeen http://192.168.167.155/wp-content/themes/twentyseventeen/
        http://192.168.167.155/wp-content/themes/twentyseventeen/screenshot.png
    twentysixteen http://192.168.167.155/wp-content/themes/twentysixteen/
        http://192.168.167.155/wp-content/themes/twentysixteen/readme.txt
        http://192.168.167.155/wp-content/themes/twentysixteen/screenshot.png

[+] Possible interesting urls found:
    This CMS&#x27; default changelog. - http://192.168.167.155/readme.html

[+] Possible version(s):
    5.1
    5.1.1
    5.2
    5.2.1

[+] Plugins found:
    akismet http://192.168.167.155/wp-content/plugins/akismet/
```

The program has found the Themes installed, an interesting URL, the possible versions and an installed plugin.

Drupwn [Windows-Linux-macOS]

Skill level needed

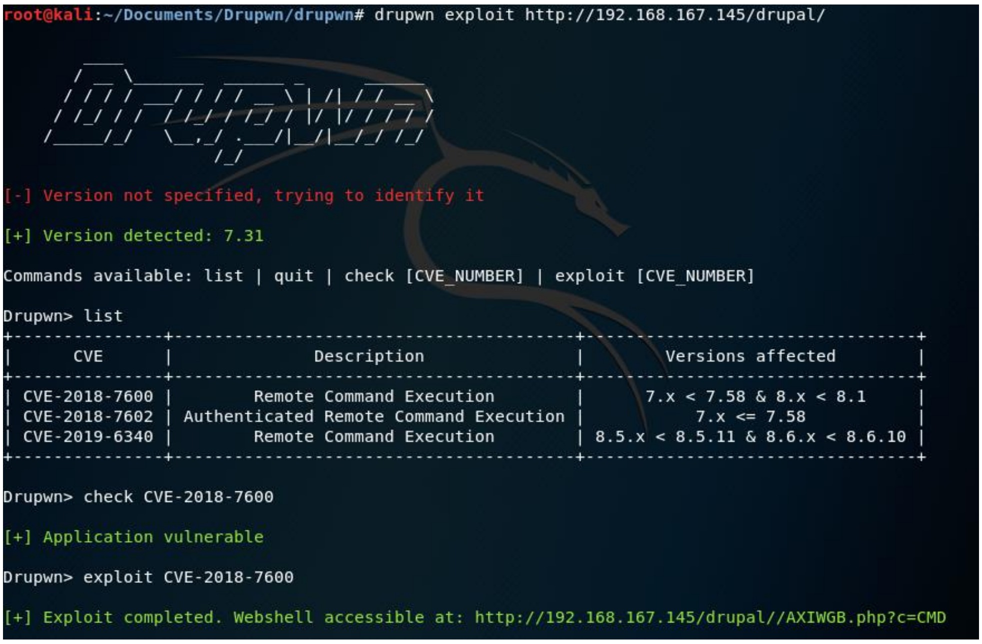
Intermediate.

Description

Drupwn is a utility tool used to test exploit and weaknesses in Drupal, it is available on GitHub.

The tool can test the website for vulnerabilities (CVE's) and exploit some of them automatically.

An enumeration mode is also available. To demonstrate its functionality, we quickly exploited a vulnerable website using it:

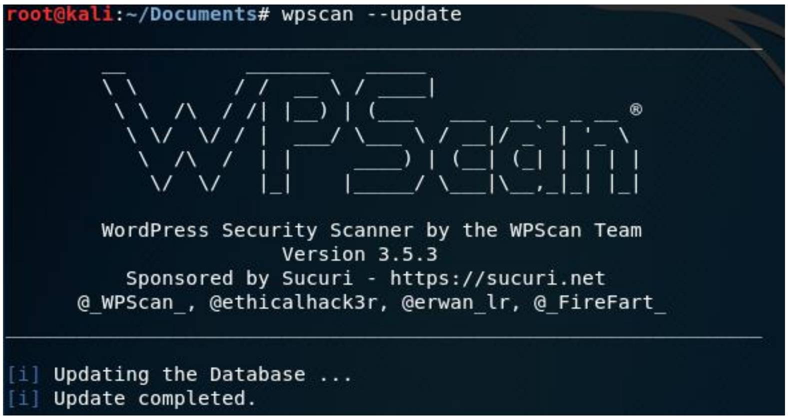


```
root@kali:~/Documents/Drupwn/drupwn# drupwn exploit http://192.168.167.145/drupal/

        ____
       / __ \_______  ______ _      ______
      / / / / ___/ / / / __ \ | /| / / __ \
     / /_/ / /  / /_/ / /_/ / |/ |/ / / / /
    /_____/_/   \__,_/ .___/|__/|__/_/ /_/
                    /_/

[-] Version not specified, trying to identify it

[+] Version detected: 7.31

Commands available: list | quit | check [CVE_NUMBER] | exploit [CVE_NUMBER]

Drupwn> list
+---------------+-----------------------------------------+---------------------------------+
|      CVE      |               Description               |        Versions affected        |
+---------------+-----------------------------------------+---------------------------------+
| CVE-2018-7600 |         Remote Command Execution        |      7.x < 7.58 & 8.x < 8.1     |
| CVE-2018-7602 | Authenticated Remote Command Execution  |           7.x <= 7.58           |
| CVE-2019-6340 |         Remote Command Execution        | 8.5.x < 8.5.11 & 8.6.x < 8.6.10 |
+---------------+-----------------------------------------+---------------------------------+

Drupwn> check CVE-2018-7600

[+] Application vulnerable

Drupwn> exploit CVE-2018-7600

[+] Exploit completed. Webshell accessible at: http://192.168.167.145/drupal//AXIWGB.php?c=CMD
```

WPScan [Windows-Linux-macOS]

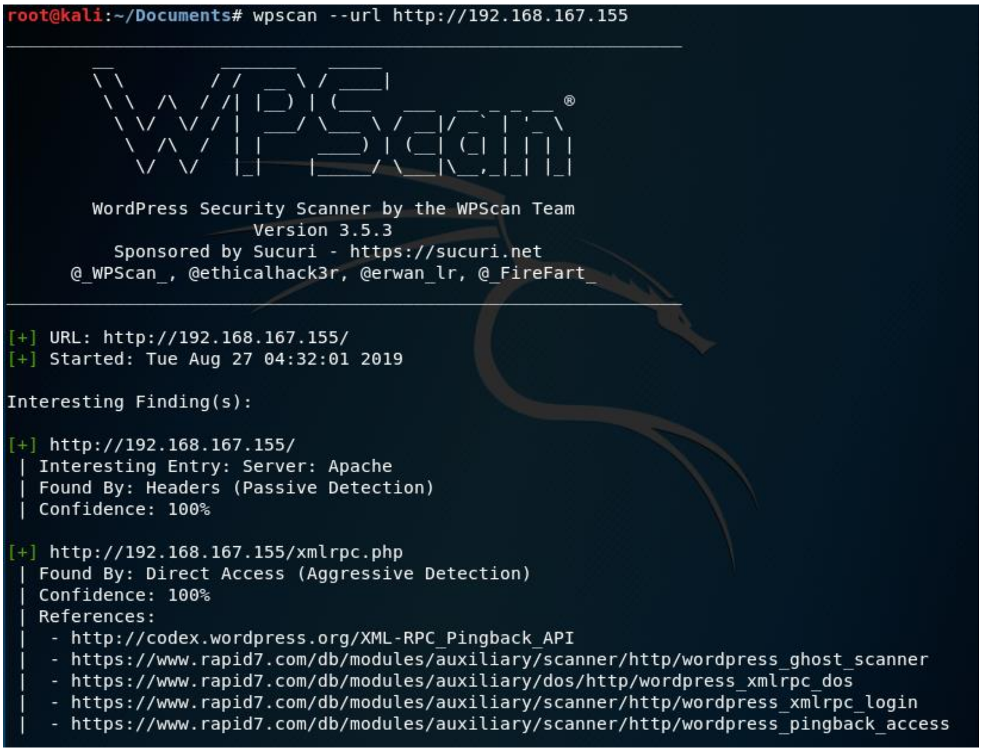
Description

WPScan is a free, for non-commercial use, black box vulnerability scanner to test the security of a Wordpress site, it is already preinstalled in Kali Linux. First let's update its vulnerability database:



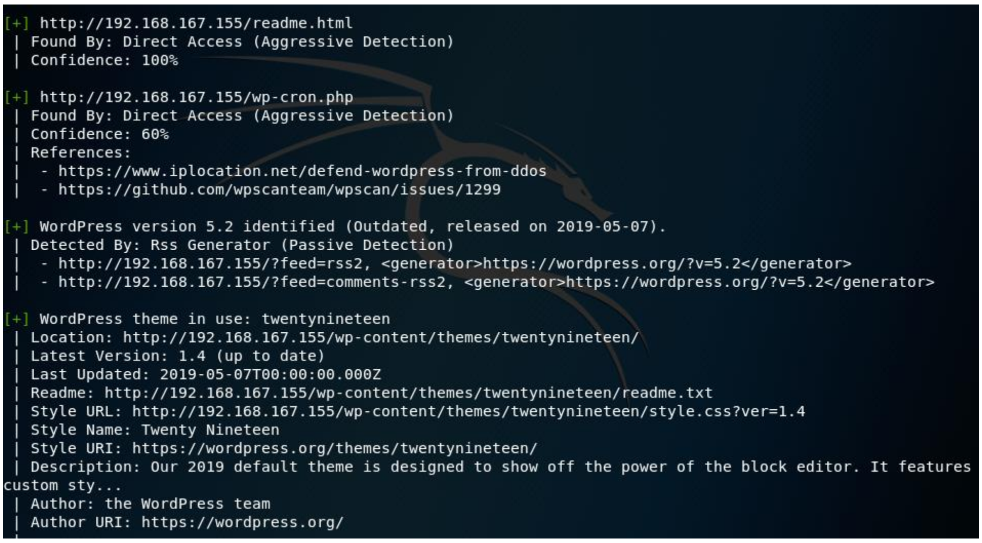
```
root@kali:~/Documents# wpscan --update
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.5.3
           Sponsored by Sucuri - https://sucuri.net
       @_WPScan_, @ethicalhack3r, @erwan_lr, @_FireFart_
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.
```

Now that we are up-to-date, let's try to scan a test website to see what information we can retrieve:



```
root@kali:~/Documents# wpscan --url http://192.168.167.155
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.5.3
           Sponsored by Sucuri - https://sucuri.net
       @_WPScan_, @ethicalhack3r, @erwan_lr, @_FireFart_
_______________________________________________________________

[+] URL: http://192.168.167.155/
[+] Started: Tue Aug 27 04:32:01 2019

Interesting Finding(s):

[+] http://192.168.167.155/
 | Interesting Entry: Server: Apache
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] http://192.168.167.155/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access
```

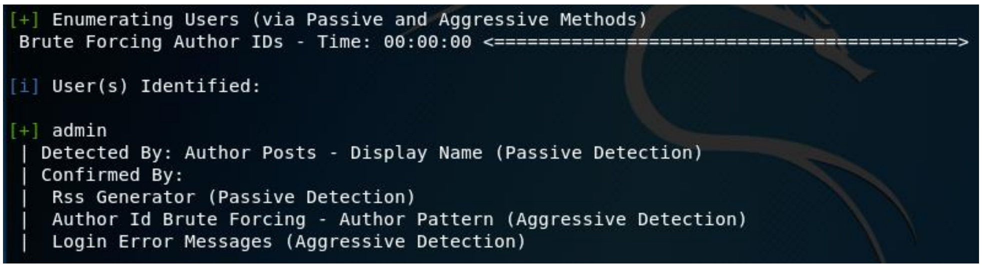
The program gathers interesting information like web server type, Apache in this case. Xmlrpc is also enabled on the website, this could lead to brute force attack attempts.



```
[+] http://192.168.167.155/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] http://192.168.167.155/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.2 identified (Outdated, released on 2019-05-07).
 | Detected By: Rss Generator (Passive Detection)
 |  - http://192.168.167.155/?feed=rss2, <generator>https://wordpress.org/?v=5.2</generator>
 |  - http://192.168.167.155/?feed=comments-rss2, <generator>https://wordpress.org/?v=5.2</generator>

[+] WordPress theme in use: twentynineteen
 | Location: http://192.168.167.155/wp-content/themes/twentynineteen/
 | Latest Version: 1.4 (up to date)
 | Last Updated: 2019-05-07T00:00:00.000Z
 | Readme: http://192.168.167.155/wp-content/themes/twentynineteen/readme.txt
 | Style URL: http://192.168.167.155/wp-content/themes/twentynineteen/style.css?ver=1.4
 | Style Name: Twenty Nineteen
 | Style URI: https://wordpress.org/themes/twentynineteen/
 | Description: Our 2019 default theme is designed to show off the power of the block editor. It features
custom sty...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
```

The wp-cron.php file could also lead to DDOS (Distributed Denial Of Service) attacks that could disrupt the availability of the website. WPScan also finds the installed theme and the outdated WordPress's version.

We can also try to identify the users:



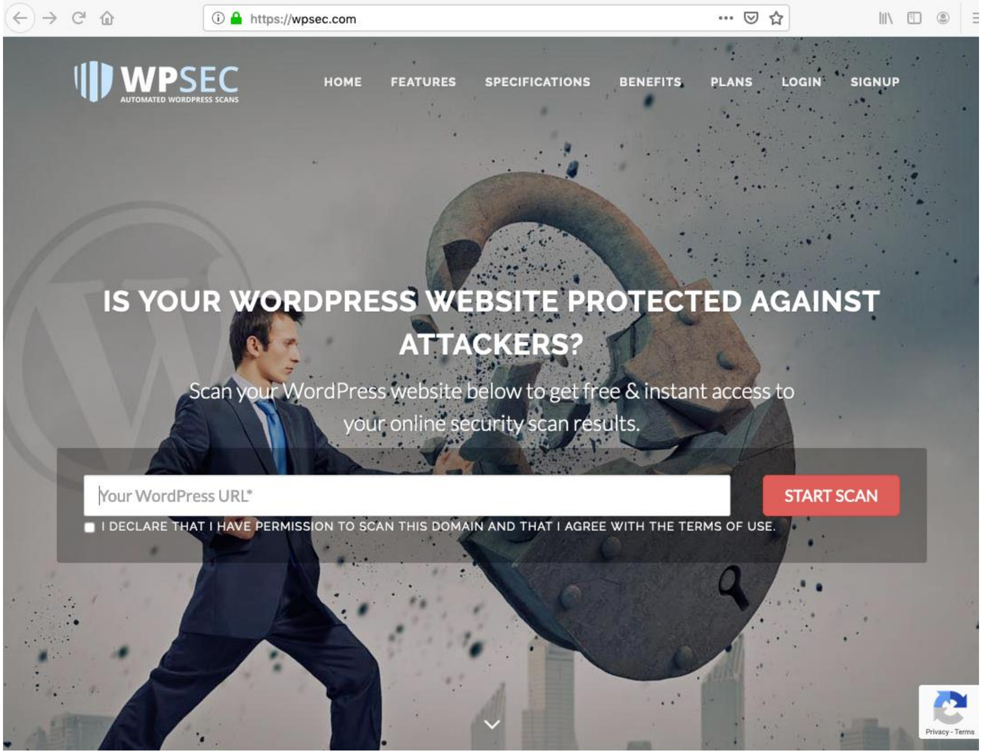
```
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <============================================>

[i] User(s) Identified:

[+] admin
 | Detected By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```

WPScan has a lot of parameters that can be used to fine tune our research on a WordPress website's vulnerabilities it is a free and easy to install tool.

WPSEC [Cloud-based]

Description

WPSec is an online tool that will scan your WordPress website for vulnerabilities and delivers a report. You will have to register to review your scan results though. The company provides different paid plans which will give you the ability to scan more than just one web site.



IS YOUR WORDPRESS WEBSITE PROTECTED AGAINST ATTACKERS?

Scan your WordPress website below to get free & instant access to your online security scan results.

Your WordPress URL*

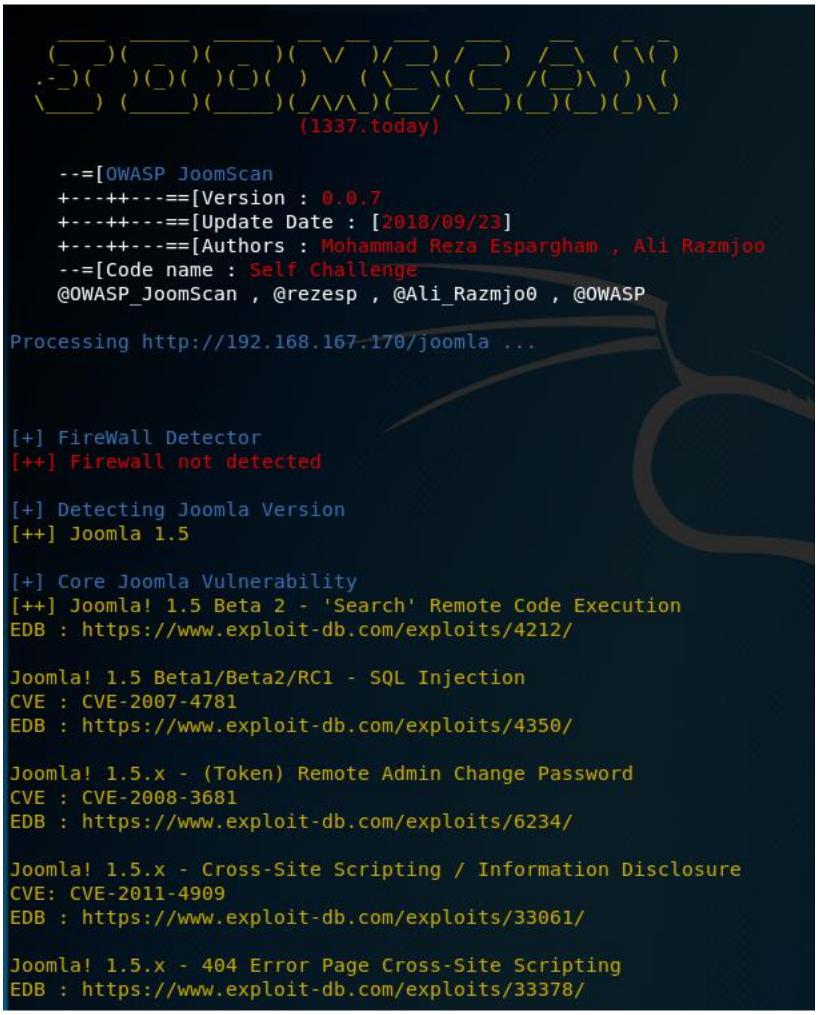
□ I DECLARE THAT I HAVE PERMISSION TO SCAN THIS DOMAIN AND THAT I AGREE WITH THE TERMS OF USE.

JoomScan [Windows-Linux-macOS]

Description

JoomScan is a free vulnerability scanner for Joomla based websites, it comes also preinstalled in Kali Linux Pen Testing distribution.

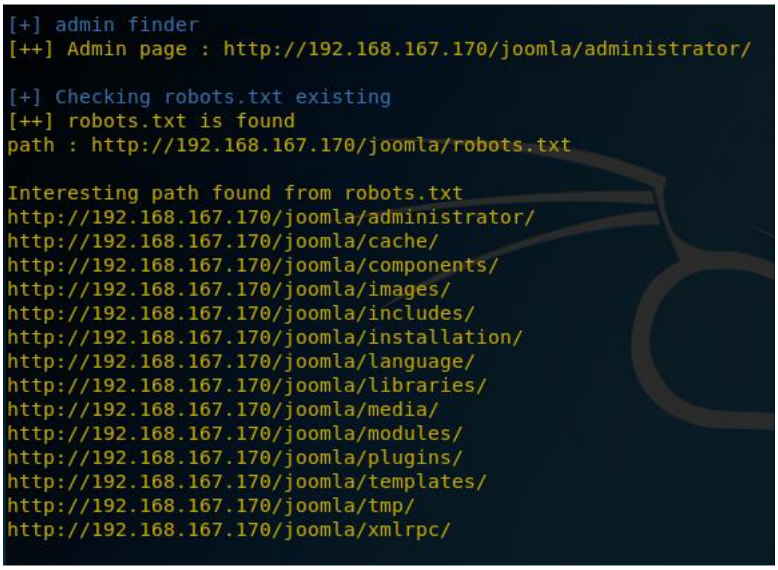
We have run the tool against a vulnerable Joomla installation and here are the results.



```
    ____  _____  _____  __  __  ___   ___    __    _  _
   (_  _)(  _  )(  _  )(  \/  )/ __) / __)  /__\  ( \( )
  .-_)(   )(_)(  )(_)(  )    ( \__ \( (__  /(__)\  )  (
  \____) (_____)(_____)(_/\/\_)(___/ \___)(__)(__)(_)\_)
                        (1337.today)

    --=[OWASP JoomScan
    +---++---==[Version : 0.0.7
    +---++---==[Update Date : [2018/09/23]
    +---++---==[Authors : Mohammad Reza Espargham , Ali Razmjoo
    --=[Code name : Self Challenge
    @OWASP_JoomScan , @rezesp , @Ali_Razmjo0 , @OWASP

Processing http://192.168.167.170/joomla ...


[+] FireWall Detector
[++] Firewall not detected

[+] Detecting Joomla Version
[++] Joomla 1.5

[+] Core Joomla Vulnerability
[++] Joomla! 1.5 Beta 2 - 'Search' Remote Code Execution
EDB : https://www.exploit-db.com/exploits/4212/

Joomla! 1.5 Beta1/Beta2/RC1 - SQL Injection
CVE : CVE-2007-4781
EDB : https://www.exploit-db.com/exploits/4350/

Joomla! 1.5.x - (Token) Remote Admin Change Password
CVE : CVE-2008-3681
EDB : https://www.exploit-db.com/exploits/6234/

Joomla! 1.5.x - Cross-Site Scripting / Information Disclosure
CVE: CVE-2011-4909
EDB : https://www.exploit-db.com/exploits/33061/

Joomla! 1.5.x - 404 Error Page Cross-Site Scripting
EDB : https://www.exploit-db.com/exploits/33378/
```

As you may have noticed, JoomScan automatically finds the vulnerabilities present on the website with a link to the exploit database giving you more information about this specific exploit.

The tool also locates the admin login page and the robots.txt file containing sensitive information about the website:



```
[+] admin finder
[++] Admin page : http://192.168.167.170/joomla/administrator/

[+] Checking robots.txt existing
[++] robots.txt is found
path : http://192.168.167.170/joomla/robots.txt

Interesting path found from robots.txt
http://192.168.167.170/joomla/administrator/
http://192.168.167.170/joomla/cache/
http://192.168.167.170/joomla/components/
http://192.168.167.170/joomla/images/
http://192.168.167.170/joomla/includes/
http://192.168.167.170/joomla/installation/
http://192.168.167.170/joomla/language/
http://192.168.167.170/joomla/libraries/
http://192.168.167.170/joomla/media/
http://192.168.167.170/joomla/modules/
http://192.168.167.170/joomla/plugins/
http://192.168.167.170/joomla/templates/
http://192.168.167.170/joomla/tmp/
http://192.168.167.170/joomla/xmlrpc/
```

3.6 DMARC (Domain-based Message Authentication, Reporting & Conformance) online checker

MXToolbox [Cloud-based]

Skill level needed

Beginner.

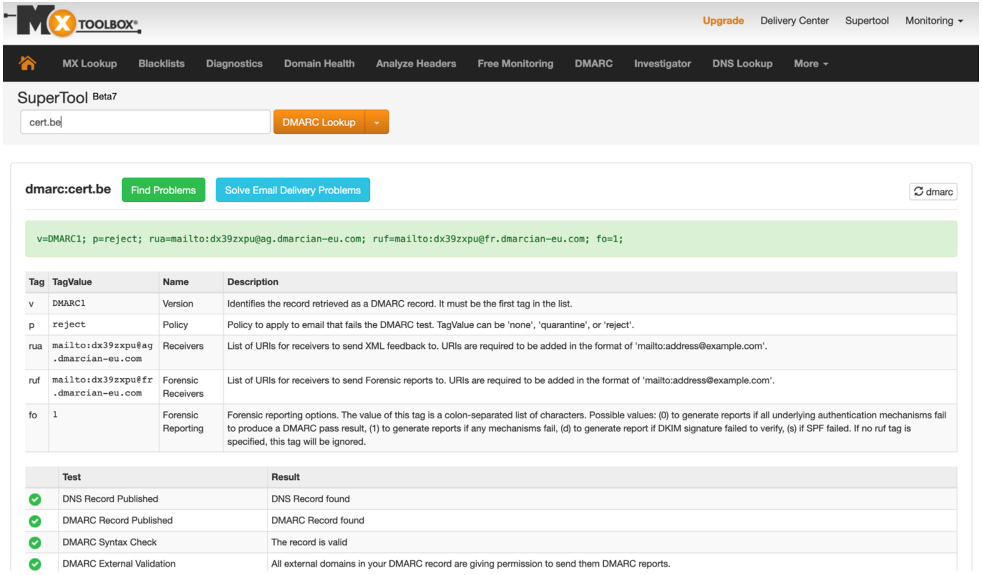
Description

DMARC is a must have in email authentication for your mail server, its role is to check that a legitimate email is properly authenticated against DKIM (Domain Keys Identified Mail) and SPF (Sender Policy Framework) standards.

For a SPF check, the “header from” domain name must match with the “enveloper from” domain name and for a DKIM signature check the “header from” domain name must match with the “d=domain name” in the signature.

Some websites provide free tools to assess your DMARC installation, MXToolbox is one of them but there are numerous tools online (Sercurius.net or DMARC Analyzer cloud-based solutions are proposing this service too).

Here is a screenshot of the result from a DMARC check done on the CERT.be domain with MXToolBox:



cert.be

dmarc:cert.be

```
v=DMARC1; p=reject; rua=mailto:dx39zxpu@ag.dmarcian-eu.com; ruf=mailto:dx39zxpu@fr.dmarcian-eu.com; fo=1;
```

Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	reject	Policy	Policy to apply to email that fails the DMARC test. TagValue can be 'none', 'quarantine', or 'reject'.
rua	mailto:dx39zxpu@ag.dmarcian-eu.com	Receivers	List of URIs for receivers to send XML feedback to. URIs are required to be added in the format of 'mailto:address@example.com'.
ruf	mailto:dx39zxpu@fr.dmarcian-eu.com	Forensic Receivers	List of URIs for receivers to send Forensic reports to. URIs are required to be added in the format of 'mailto:address@example.com'.
fo	1	Forensic Reporting	Forensic reporting options. The value of this tag is a colon-separated list of characters. Possible values: (0) to generate reports if all underlying authentication mechanisms fail to produce a DMARC pass result, (1) to generate reports if any mechanisms fail, (d) to generate report if DKIM signature failed to verify, (s) if SPF failed. If no ruf tag is specified, this tag will be ignored.

	Test	Result
✓	DNS Record Published	DNS Record found
✓	DMARC Record Published	DMARC Record found
✓	DMARC Syntax Check	The record is valid
✓	DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.

This free tool can be interesting to check the configuration of your DMARC setup and be assured that everything is working fine and well configured.

3.7 Active Directory Security Audit Tool

PingCastle [Windows-~~Linux~~-~~macOS~~]

Skill level needed

Beginner.

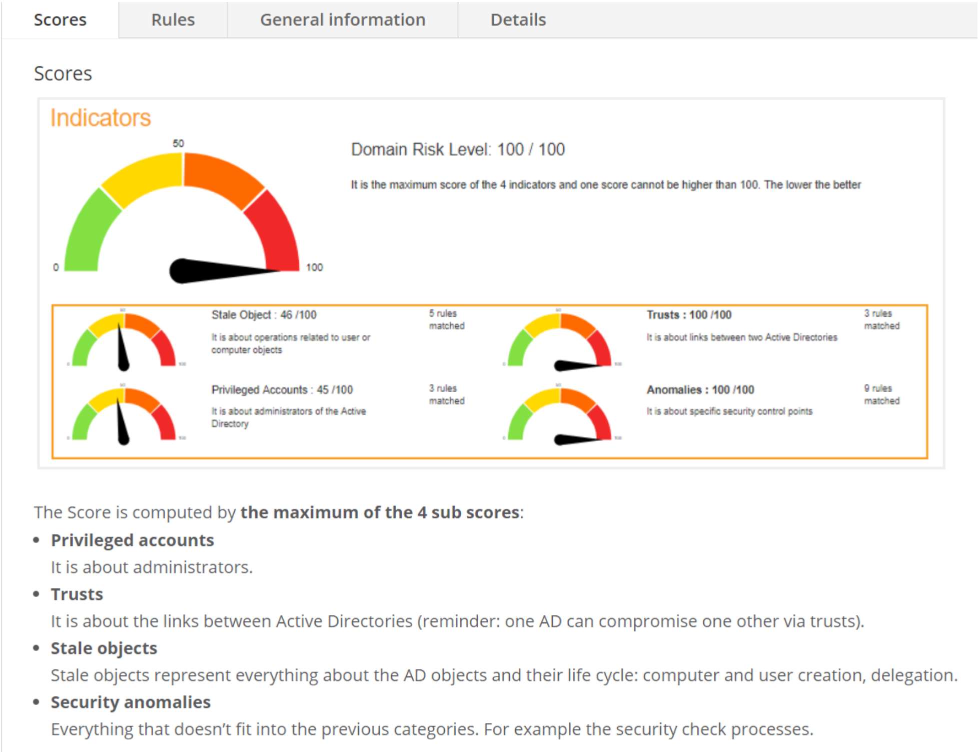
Description

PingCastle is a free, Windows-based Active Directory Security Assessment Tool designed to quickly assess the Active Directory security level with a methodology based on a risk assessment and maturity framework.

PingCastle once executed as a simple user can provide you with various deliverables: a detailed HTML report, PowerPoint presentations of the data and spreadsheets.

If you use it with the default Healthcheck mode it will quickly collect the most important information of the Active Directory to establish an overview on it. Based on a model and rules it will evaluate the score of the sub-processes of the Active Directory and proceed with a risk evaluation.

The report is divided in 4 parts: Scores, Rules, General information & Details.



Scores

Domain Risk Level: 100 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

Stale Object : 46 /100 — 5 rules matched
It is about operations related to user or computer objects

Trusts : 100 /100 — 3 rules matched
It is about links between two Active Directories

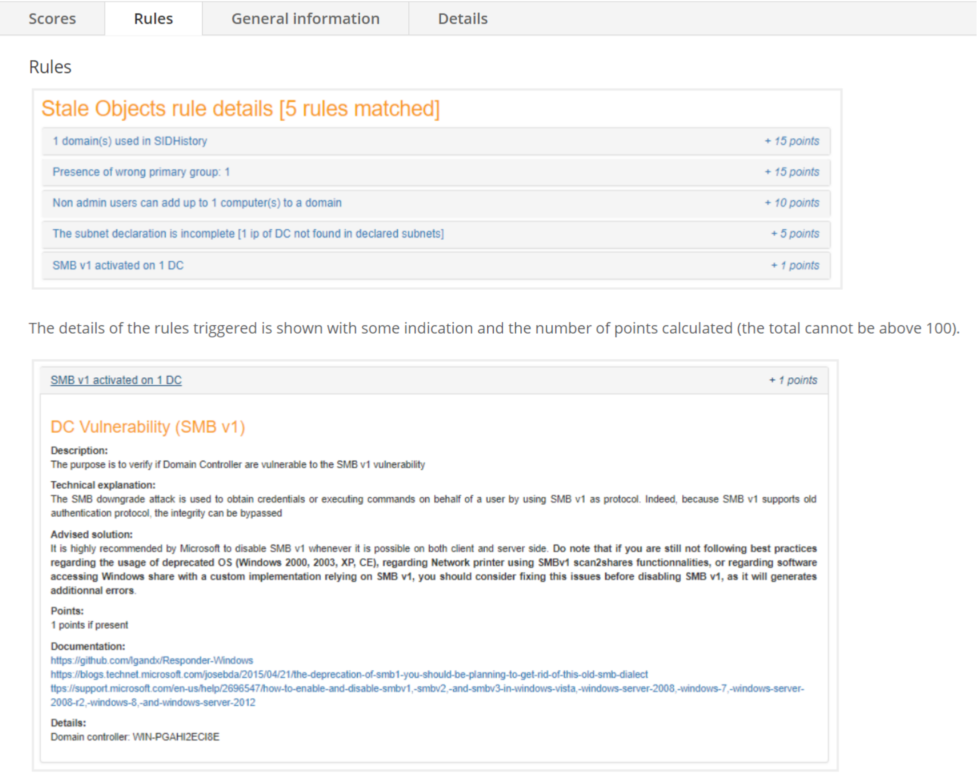
Privileged Accounts : 45 /100 — 3 rules matched
It is about administrators of the Active Directory

Anomalies : 100 /100 — 9 rules matched
It is about specific security control points

The Score is computed by **the maximum of the 4 sub scores**:

- **Privileged accounts**
  It is about administrators.
- **Trusts**
  It is about the links between Active Directories (reminder: one AD can compromise one other via trusts).
- **Stale objects**
  Stale objects represent everything about the AD objects and their life cycle: computer and user creation, delegation.
- **Security anomalies**
  Everything that doesn't fit into the previous categories. For example the security check processes.

Figure 9 Score Tab



Rules

Stale Objects rule details [5 rules matched]

1 domain(s) used in SIDHistory	*+ 15 points*
Presence of wrong primary group: 1	*+ 15 points*
Non admin users can add up to 1 computer(s) to a domain	*+ 10 points*
The subnet declaration is incomplete [1 ip of DC not found in declared subnets]	*+ 5 points*
SMB v1 activated on 1 DC	*+ 1 points*

The details of the rules triggered is shown with some indication and the number of points calculated (the total cannot be above 100).

SMB v1 activated on 1 DC *+ 1 points*

DC Vulnerability (SMB v1)

Description:
The purpose is to verify if Domain Controller are vulnerable to the SMB v1 vulnerability

Technical explanation:
The SMB downgrade attack is used to obtain credentials or executing commands on behalf of a user by using SMB v1 as protocol. Indeed, because SMB v1 supports old authentication protocol, the integrity can be bypassed

Advised solution:
It is highly recommended by Microsoft to disable SMB v1 whenever it is possible on both client and server side. **Do note that if you are still not following best practices regarding the usage of deprecated OS (Windows 2000, 2003, XP, CE), regarding Network printer using SMBv1 scan2shares functionnalities, or regarding software accessing Windows share with a custom implementation relying on SMB v1, you should consider fixing this issues before disabling SMB v1, as it will generates additionnal errors**.

Points:
1 points if present

Documentation:
https://github.com/lgandx/Responder-Windows
https://blogs.technet.microsoft.com/josebda/2015/04/21/the-deprecation-of-smb1-you-should-be-planning-to-get-rid-of-this-old-smb-dialect
ttps://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012

Details:
Domain controller: WIN-PGAHI2ECI8E

Figure 10 Rules Tab

PingCastle can also generate two different types of Active Directory maps based on existing health check reports or via a special mode collecting the required information.

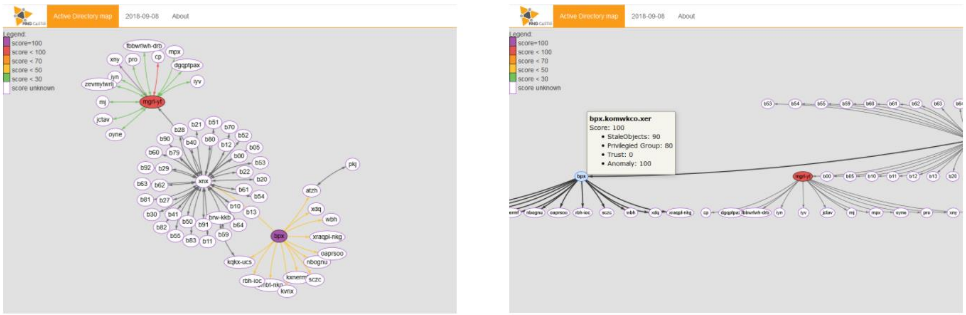


Figure 11 AD maps

More information about PingCastle and the link to download the program itself can be found on the company website: https://www.pingcastle.com/

4 CONCLUSION

With this report, CCB (CERT.be) has tried to give you a general overview of some of the most popular vulnerability assessment tools available on the market.

Of course, this list is far from being complete: new tools and features are added every day and it is practically impossible to list them all. All these tools have full books dedicated to them that can help you go deeper should you want to improve your skills in a particular field or with a particular tool.

The aim of this report is to be a good reference starting guide if you want to try to learn how to assess your infrastructure by yourself and have no idea which tool to use and where to start.

This guide's purpose is not to replace the experience and the expertise of a professional vulnerability assessor, but we hope it will raise your cybersecurity awareness and introduce you to some of the tools you need to test your infrastructure.

5 CONTACT

CERT.be
Federal Cyber Emergency Team
Rue de la Loi, 16/ Wetstraat 16
1000 Bruxelles/ Brussel
info@certbe

Centre for Cybersecurity Belgium
Rue de la Loi, 16/ Wetstraat 16
1000 Bruxelles/ Brussel
info@ccb.belgium.be

Disclaimer

This document and its annexes have been prepared by the Centre for Cybersecurity Belgium (CCB), a federal administration created by the Royal Decree of 10 October 2014 and under the authority of the Prime Minister.

All texts, layouts, designs and other elements of any nature in this document are subject to copyright law. Reproduction of extracts from this document is authorised for non-commercial purposes only and provided the source is acknowledged.

The CCB accepts no responsibility for the content of this document.

The information provided:

- are exclusively of a general nature and do not intend to take into consideration all particular situations;

- are not necessarily exhaustive, precise or up to date on all points

Responsible editor

Centre for Cybersecurity Belgium
Mr. De Bruycker, Director
Rue de la Loi, 16
1000 Brussels

Legal deposit

D/2022/14828/001