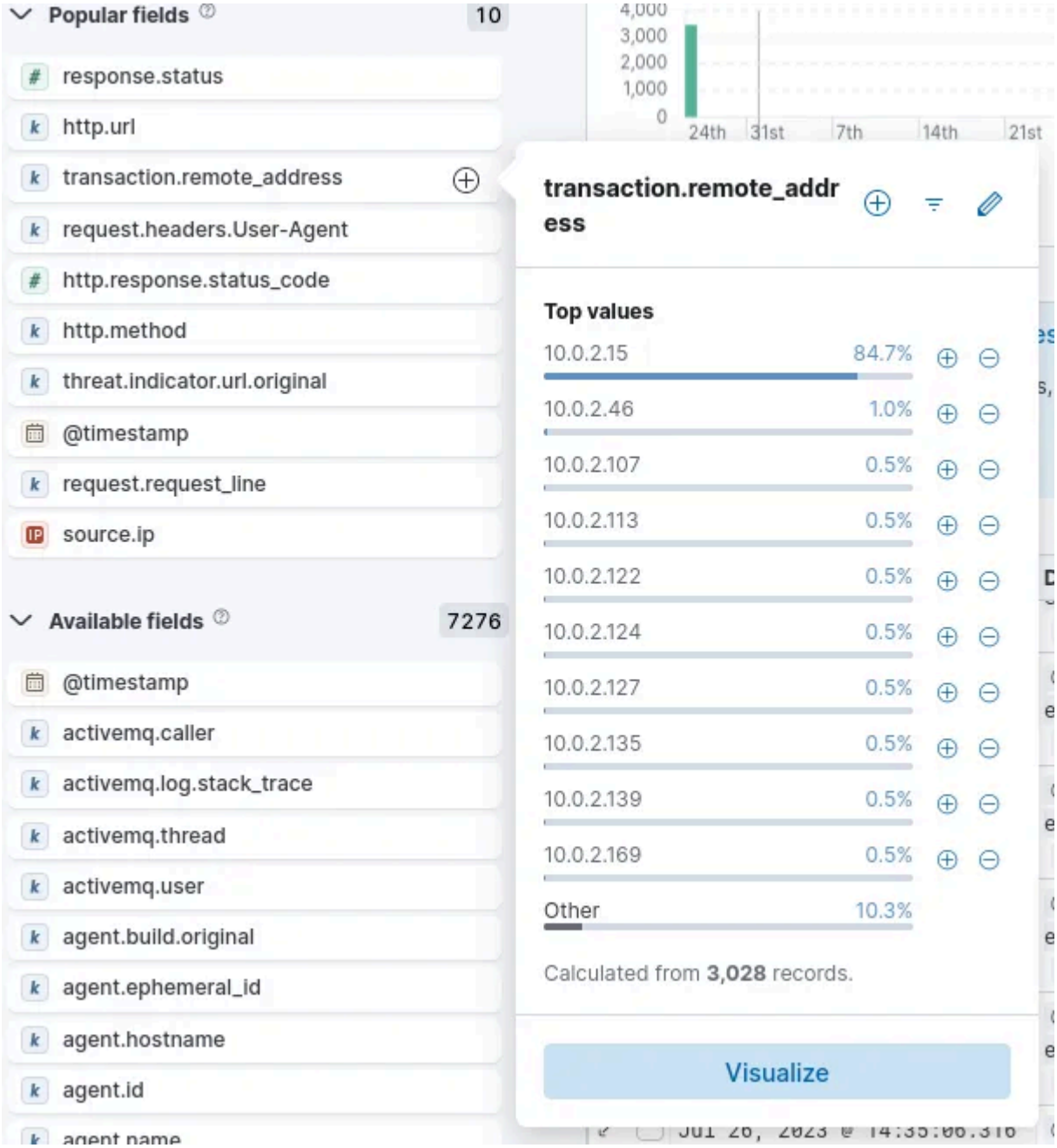
TryHackMe : Slingshot Walkthrough

M. Said Eddak · Follow
5 min read · Feb 23, 2024

In this walkthrough, I'll highlight all the method I used to respond to the question of the room. I will mainly use filters in the Kibana Query Language to get the needed information.

1. What was the attacker's IP?

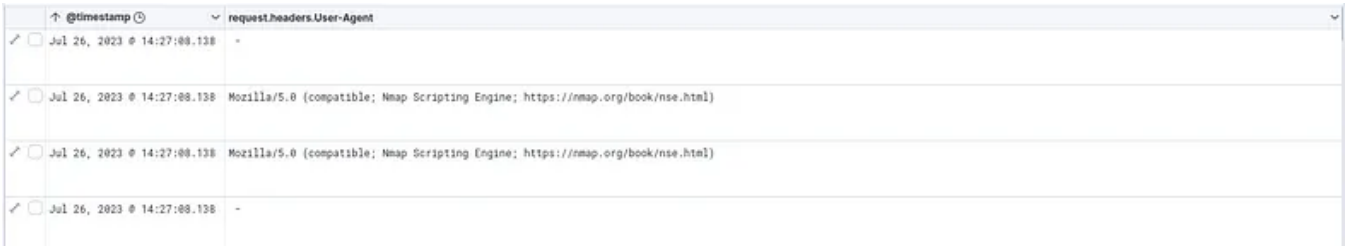
By displaying the top remote addresses, we clearly see that the IP 10.0.2.15 generated some unusual amount of traffic.



Answer : 10.0.2.15

2. What was the first scanner that the attacker ran against the web server?

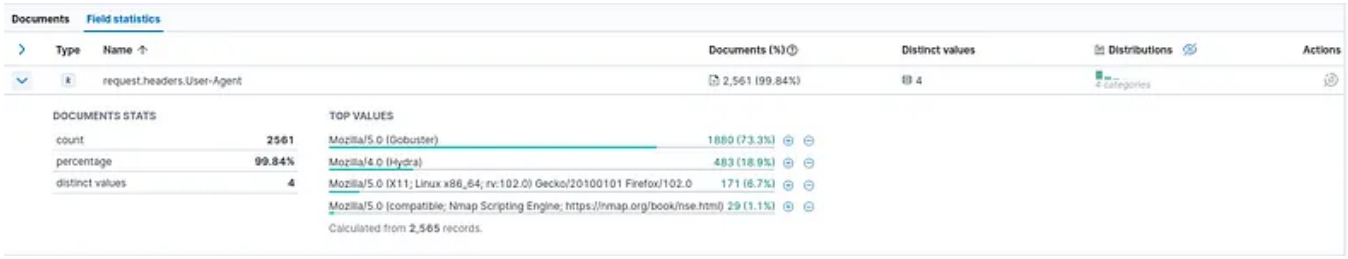
By sorting the User-Agents used by the attacker from oldest request to newest, we notice that he first started by using nmap against the server.



Answer : NMAP Scripting Engine

3. What was the User Agent of the directory enumeration tool that the attacker used on the web server?

We can display the top User Agent used by the attacker to find out that he used Gobuster to conduct the enumeration step.

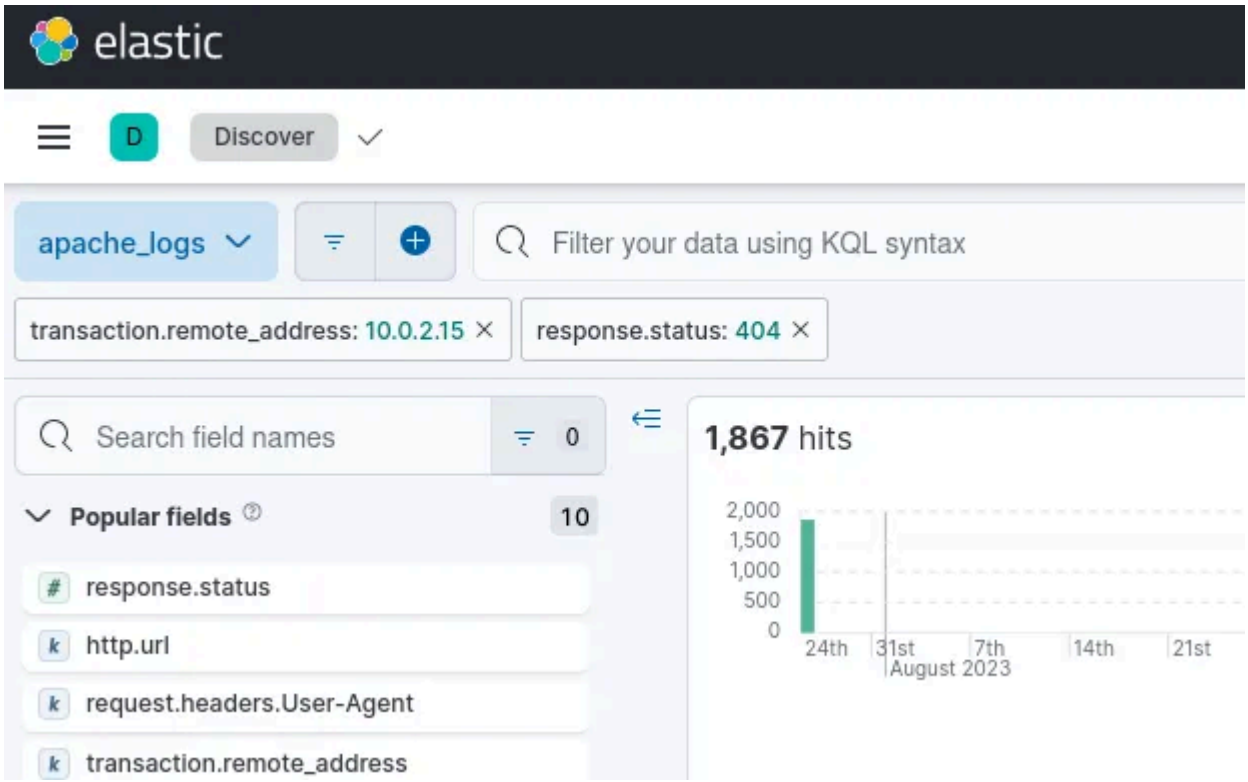


We also notice that the attacker used Hydra, in order to conduct a brute force attack (more on that later).

Answer : Mozilla/5.0 (Gobuster)

4. In total, how many requested resources on the web server did the attacker fail to find?

We can know how many requested resources failed by looking at the number of 404 response code that the server responded with.



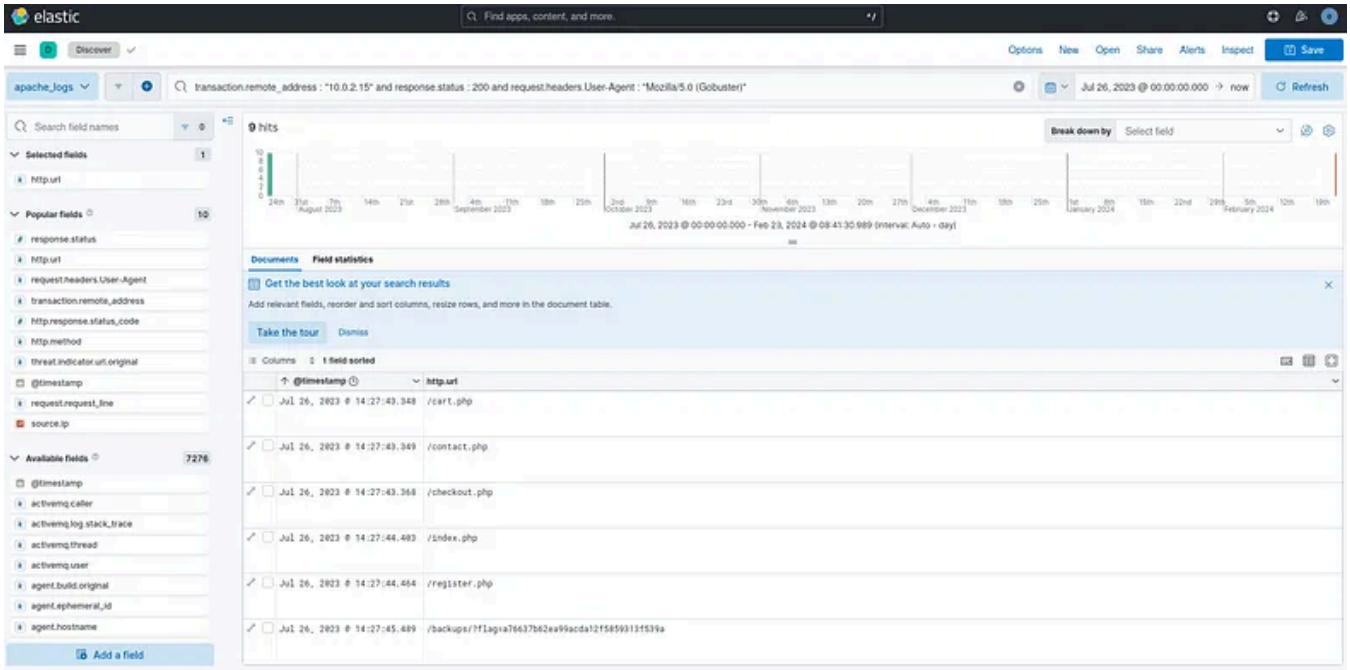
Answer : 1867

5. What is the flag under the interesting directory the attacker found?

Knowing that this is a directory that the attacker **found**, we can look at all the 200 response code to see what directory request succeeded to get the flag. For that we display all the 200 status code that appear when using the Gobuster tool.
Filter :

```
transaction.remote_address : "10.0.2.15" and response.status : 200 and request.
```

We can then show all the http.url to see the directory and the flag.



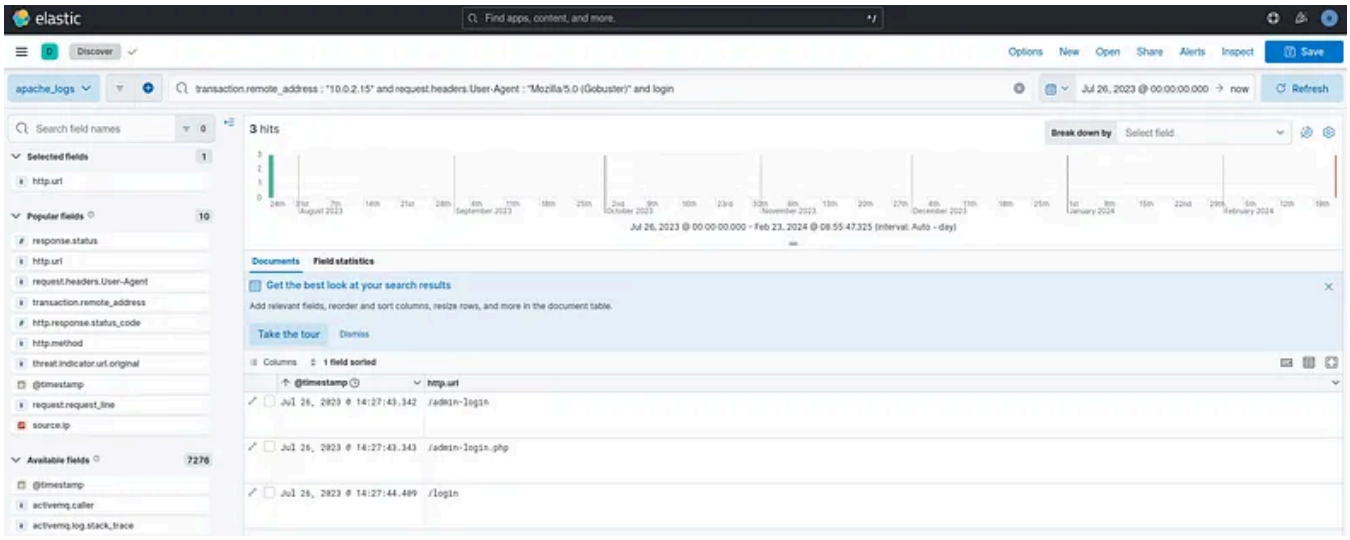
Answer : a76637b62ea99acda12f5859313f539a

6. What login page did the attacker discover using the directory enumeration tool?

We search all the URL that contain the “login” keyword used with Gobuster.

Filter :

```
transaction.remote_address : "10.0.2.15" and request.headers.User-Agent : "Mozi
```



We find the /admin-login.php login page.

Answer : /admin-login.php

7. What was the user agent of the brute-force tool that the attacker used on the admin panel?

We know from the Question 2 that the attacker used the Hydra tool to conduct the bruteforce.

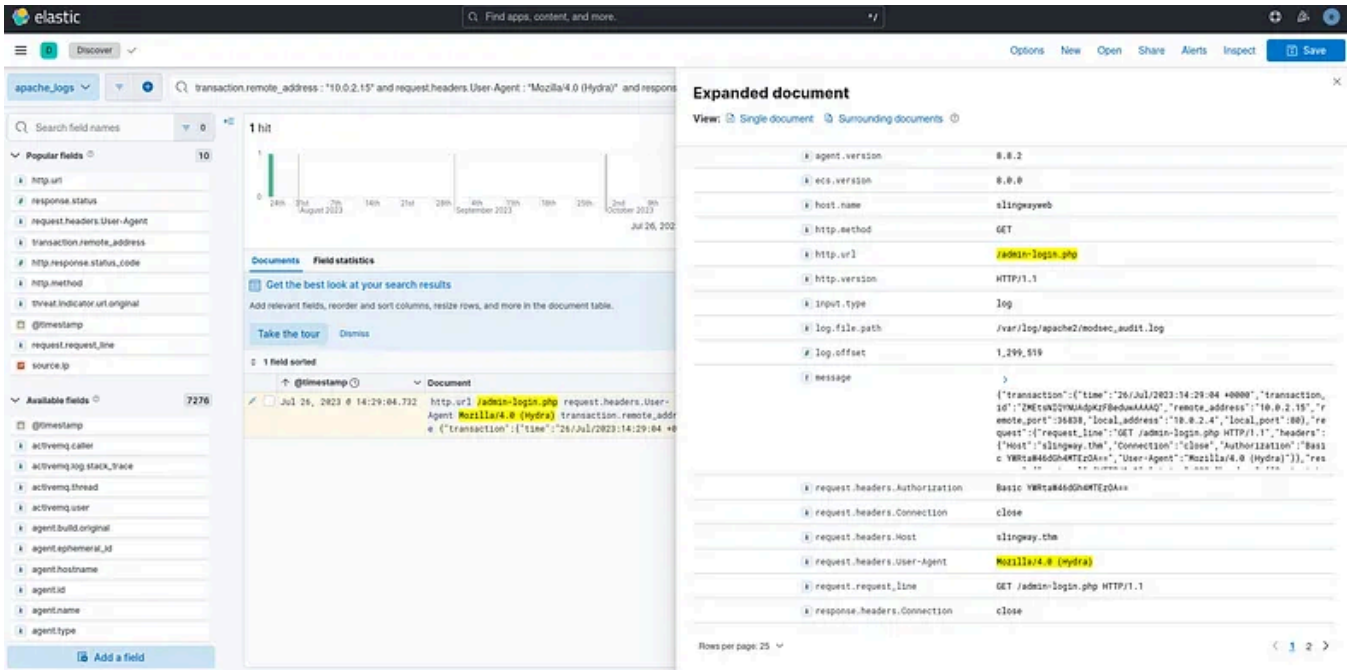
Answer : Hydra

8. What username:password combination did the attacker use to gain access to the admin page?

Since we know that the attacker did gain access to the admin page, we know that the request succeeded (status code 200) and that the User-Agent that permitted to find the username and password is the one that hydra uses.

Filter :

```
transaction.remote_address : "10.0.2.15" and request.headers.User-Agent : "Mozi
```

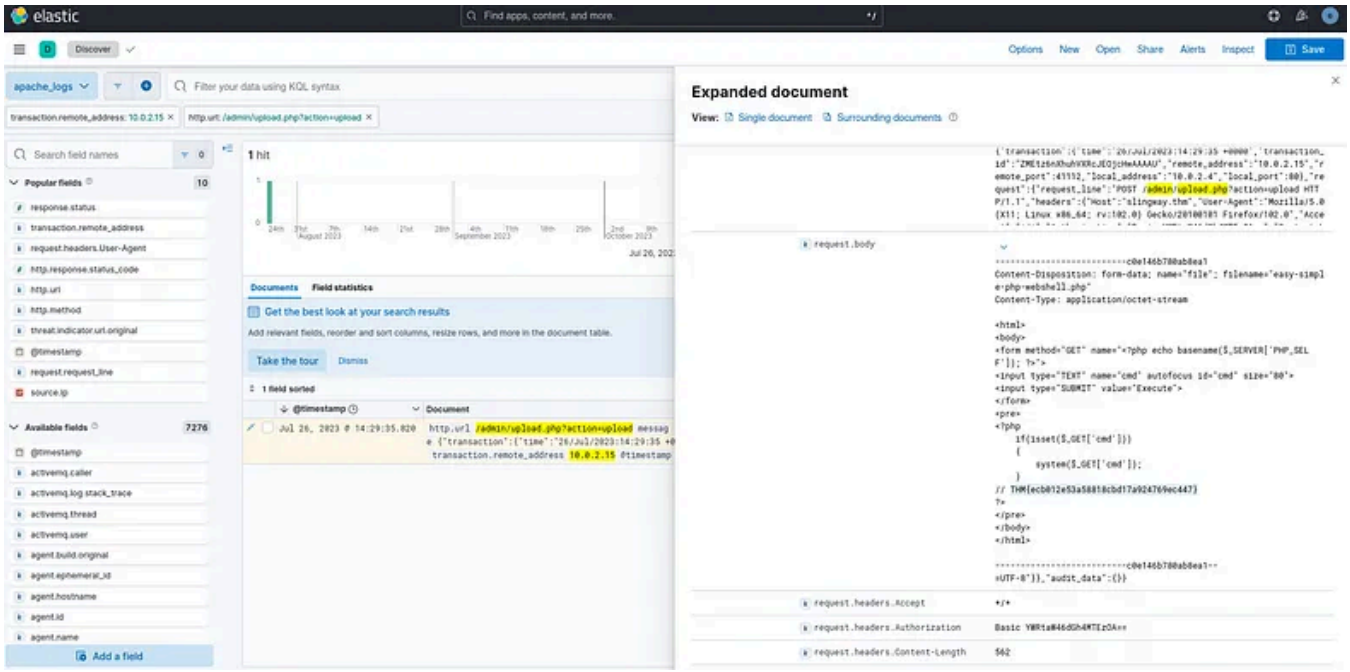


From that we find the request.headers.Authorization field that contain a base64 encoded string. After a visit on CyberChef, we find that the username and password combination found is : admin:thx1138

Answer : admin:thx1138

9. What flag was included in the file that the attacker uploaded from the admin directory?

After analyzing the URLs that the admin have access to, we find out an intresting one that allows uploads : /admin/upload.php. To find out the upload file, we search for the http.url /admin/upload.php?action=upload. From there we find the `request.body` field in the request that contains the remote web shell that the attack uploaded containing the flag.



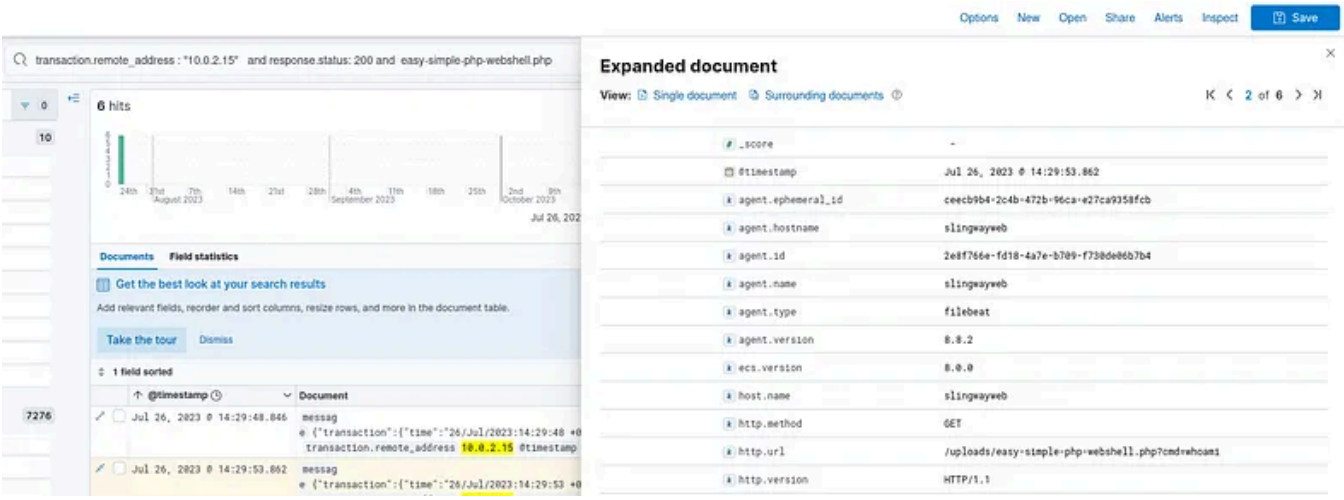
Answer : THM{ecb012e53a58818cbd17a924769ec447}

10. What was the first command the attacker ran on the web shell?

We know that the upload file is named `easy-simple-php-webshell.php`. We now display all the request that try to access this file and get the first one used.

Filter:

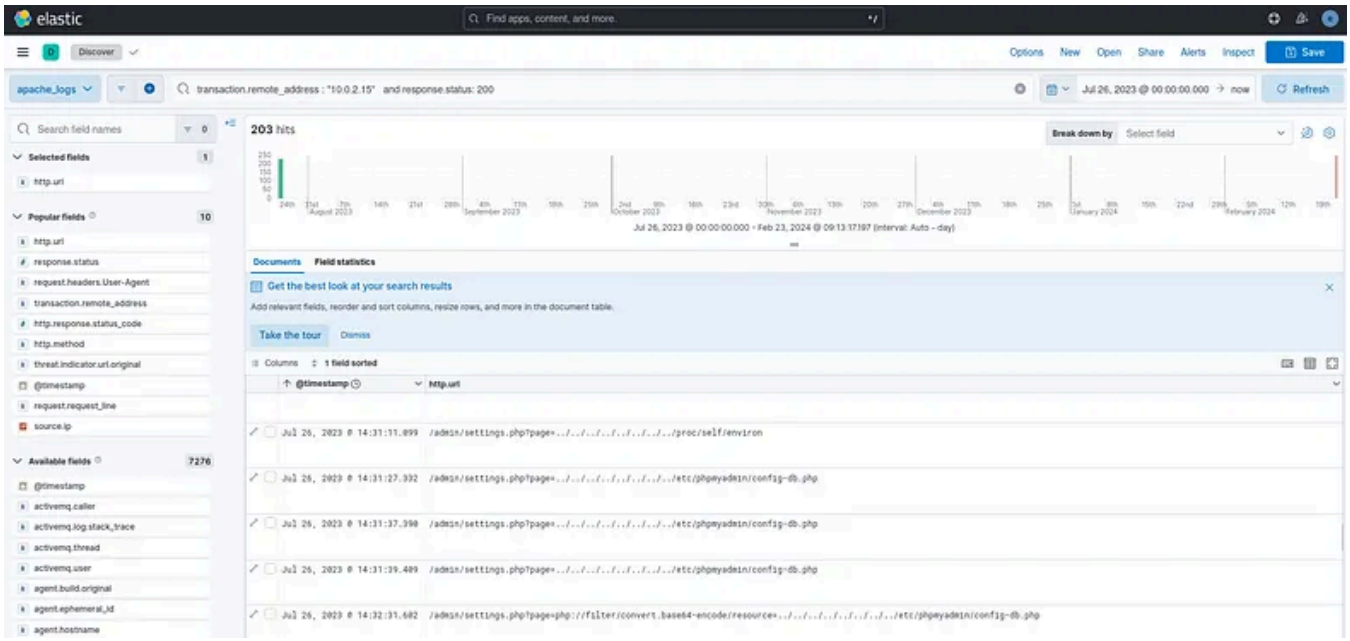
```
transaction.remote_address : "10.0.2.15"   and response.status: 200 and  easy-s
```



Answer : whoami

11. What file location on the web server did the attacker extract database credentials from using Local File Inclusion?

We know that the attack used a Local File Inclusion vulnerability to get the database credentials. To know the file location, we can look at all the URL where there is an attempt to use a local file inclusion.



From that wind find that the attacker accesses /etc/phpmyadmin/config-db.php.
Answer : /etc/phpmyadmin/config-db.php

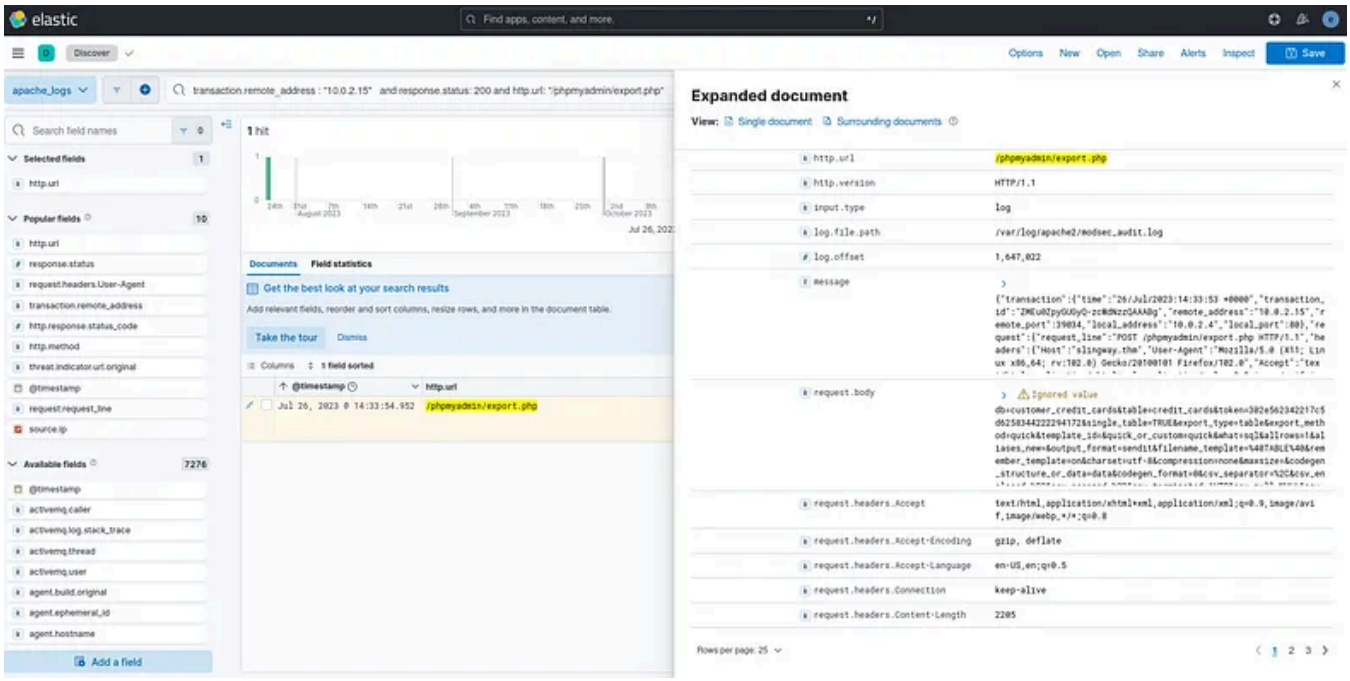
12. What directory did the attacker use to access the database manager?

From the previous question, we notice that the database manager is located in phpmyadmin.

13. What was the name of the database that the attacker exported?

To know what database the attacker exported, we can look at the phpadmin/export.php request, which contains the exported database : db:customer_credit_cards.
Filter :

```
transaction.remote_address : "10.0.2.15" and response.status: 200 and http.url:
```



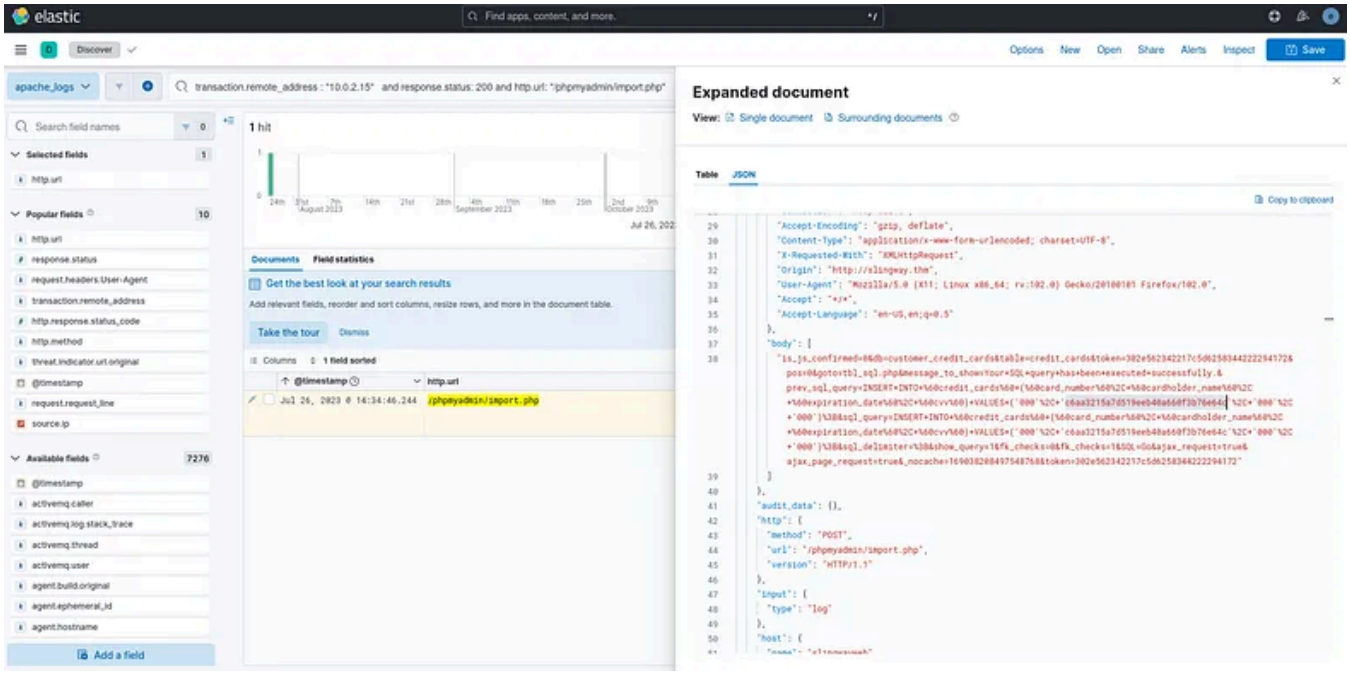
Answer : customer_credit_cards

14. What flag does the attacker insert into the database?

To know what the attacker inserted into the database, we can search usage of import.php in order to get the insert value.

Filter :

```
transaction.remote_address : "10.0.2.15"   and response.status: 200 and http.ur
```



After opening the request in the JSON format (for better readability), we can see the request as well as the inserted flag.

Answer : c6aa3215a7d519eeb40a660f3b76e64c

End of the walkthrough.

Author : Eddak Said

Cybersecurity Tryhackme Security Operation Center Hacking

Follow

Written by M. Said Eddak

8 Followers · 8 Following

Cyber Security Student | Belgium

No responses yet

What are your thoughts?

Respond

More from M. Said Eddak

M. Said Eddak

TryHackMe : SigHunt WriteUp

The SigHunt room allows us to train our writing of sigma rules. It emphasis the selection of the right IoCs in order to avoid being too...

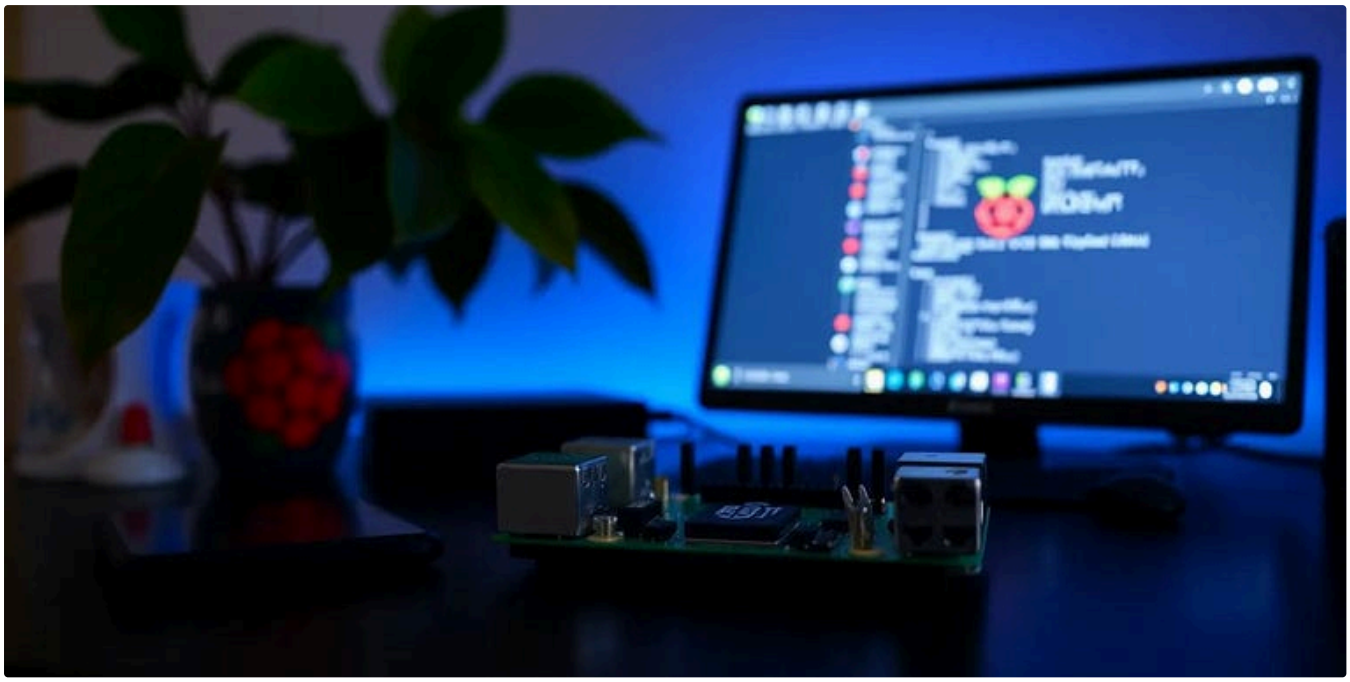
Feb 29, 2024 2

M. Said Eddak

THM : Hunt Me I: Payment Collectors Part. 2

Scenario : A Senior Finance Director from a company downloaded a malicious zip. We are called to conduct an investigation.

Mar 15, 2024 3



M. Said Eddak

Why You Should Install a Pi-hole at Home

Pi-Hole is a network-wide content blocker, offering a convenient way to track what happens on the network and to block certain content...

Sep 9, 2024 12

M. Said Eddak

Assembly : function prologue & epilogue

When using high level programming language, calling a function is straightforward : we just call it and pass it the needed arguments. For...

Feb 29, 2024 6

See all from M. Said Eddak

Recommended from Medium

In T3CH by Axoloth

TryHackMe | Vulnerability Scanner Overview | WriteUp

Learn about vulnerability scanners and how they work in a practical scenario

Nov 23, 2024 50

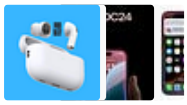
MAGESH

SigHunt-Tryhackme Writeup

You are tasked to create detection rules based on a new threat intel.

Oct 15, 2024

Lists



Tech & Tools

22 stories · 390 saves

Medium's Huge List of Publications Accepting Submissions

414 stories · 4442 saves

Staff picks

805 stories · 1593 saves

Natural Language Processing

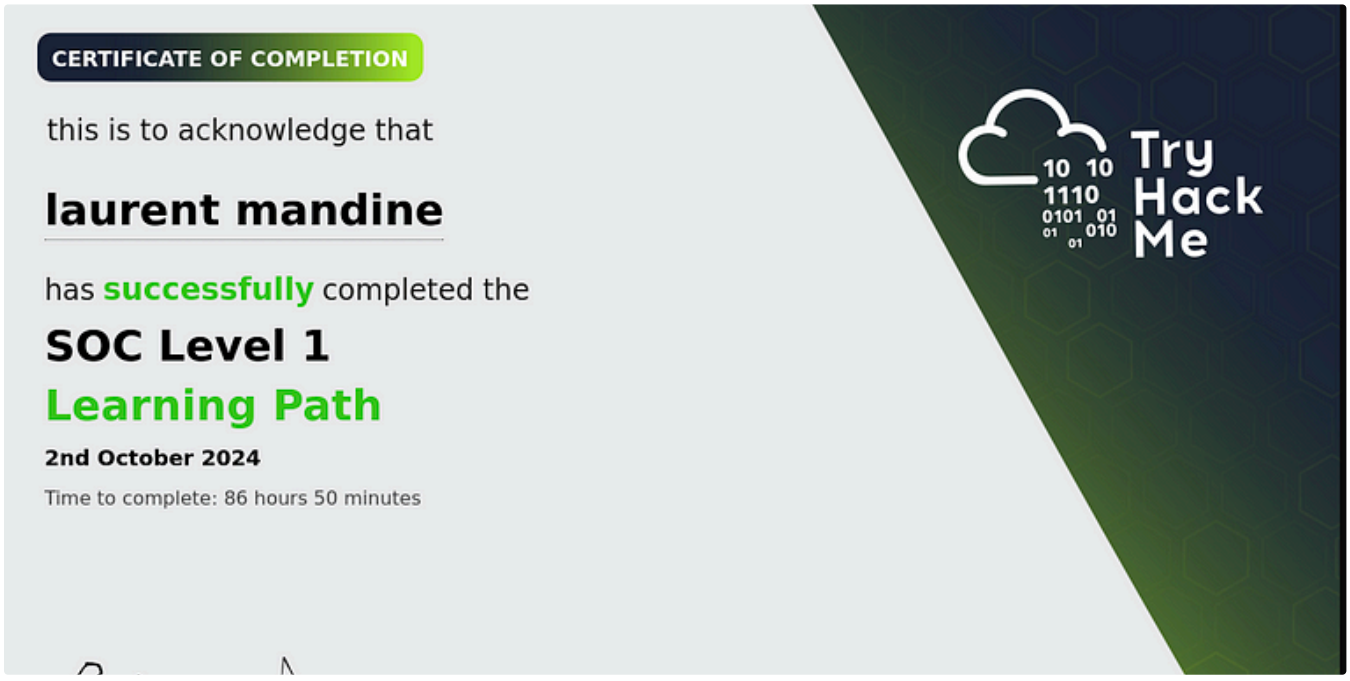
1903 stories · 1556 saves

In Twin Flame Awakening by Bensu Cangüler

Divine Feminine You Have So Much Power But How Do You Use It?

Are our thoughts about how sexy or beautiful we are stopping us?

Sep 18, 2024 188 1



Laurent Mandine

🧑‍💻 My Journey as a SOC Analyst in TryHackMe's SOC Level 1: From Clueless to Clued-in

https://tryhackme-certificates.s3-eu-west-1.amazonaws.com/THM-LSUVRFXNB3.png

Oct 2, 2024 9

nginx0

Mountaineer [THM] Writeup

Oct 19, 2024 10

Alexandros Miminas

THM Whiterose Write-Up

Whiterose is a Mr. Robot-inspired machine from the episode “409 Conflict” that mainly focuses on web exploitation and privilege escalation.

Nov 2, 2024 24