TITLE:(WORD PRESS EXPLOITATION REPORT FOR KREATIVSTORM)

DATE:2ND OCTOBER,2023

PREPARED BY: WENDELL AKUBIA NYARKO

Table of Contents

Objective

The objective of the report is to find two usernames of this website and with the permission to exploit and gain access into the login page of the website.

Executive Summary

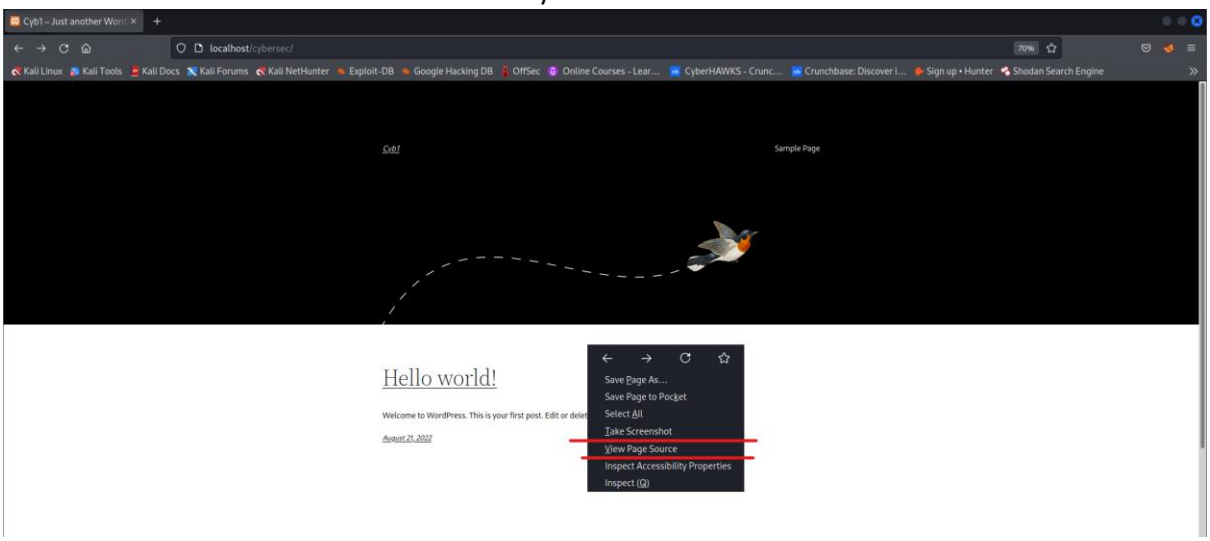
Provide the processes and methodologies involved in exploiting the website and some recommendations to help prevent such an attack.

Introduction

The scope of the target is a website where I am permitted to hack into the login page of the website. The login page is said to have a weakness and I am to find the weakness and gain access into the admin webpage of the website. There is also a set of passwords that was leaked and this information that will help in this exploitation .

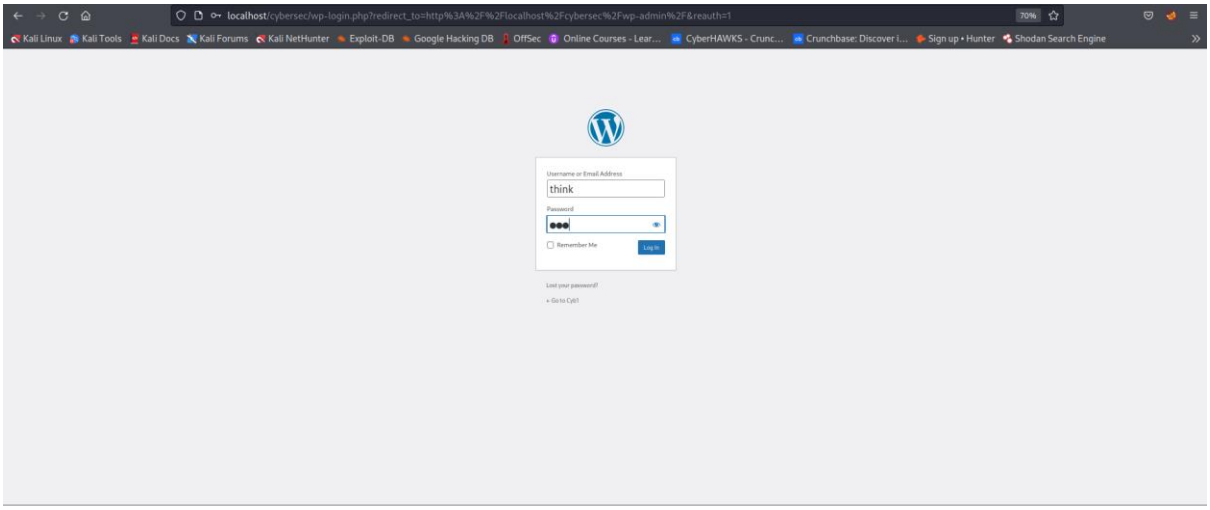
Methodology

- I first visited the webpage of the website that I was to exploit and also visited the page source of the website to see if I could find any useful information.

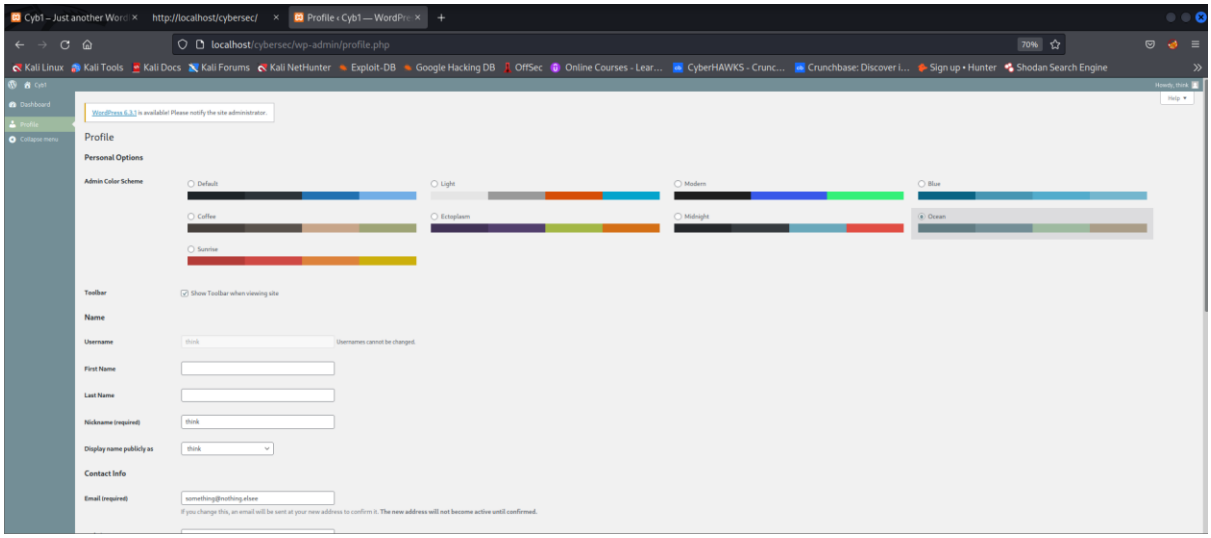


- And on line 106, I found a commented part of the code which revealed one of the usernames and it's respective password. The username was **think** and the password was just a simple **123.**

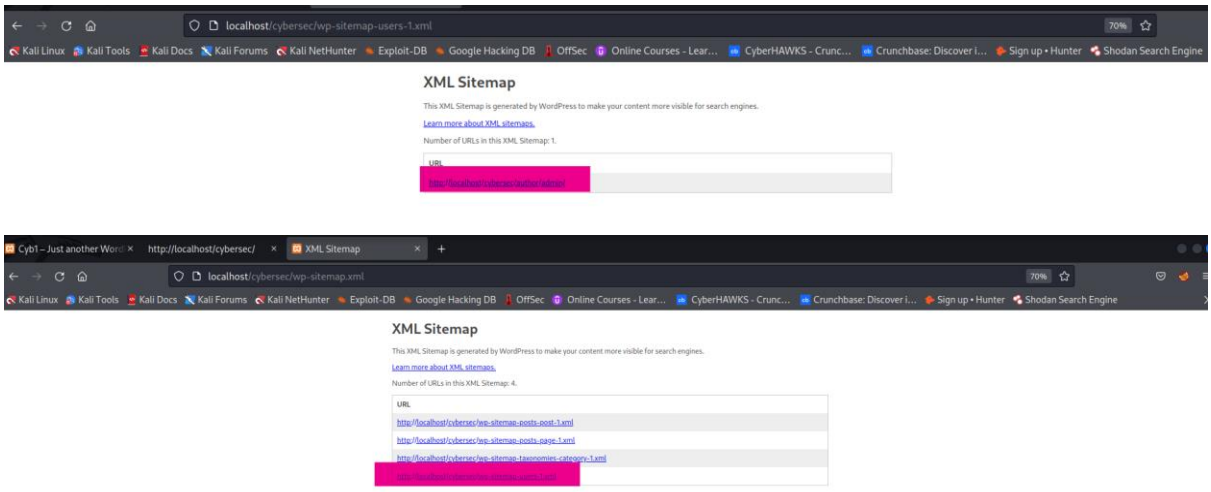
- Since it was a wordpress website, I had to visit the wordpress admin page where I could use the credentials found to gain access into the admin page of that particular website.



- Gaining access into admin webpage gave me some administrative control of the website where I could update the website, manage posts of the website, install plugins and themes, add usernames and even do some privilege escalation by adding a user as an administrator.



- To be able to find the second username, I visited the sitemap of the website. A sitemap is an XML file which provides information about the pages, videos and other files that can be found on the website. I found the file that contains the users in the website and the username that was found was **admin.**



- After finding the username, I now needed to find the password of the username **admin.** To be able to carry this task out , I need to brute force the admin page with the leaked passwords that I have and with the help of Burp Suite I will be able to intercept the login page and manipulate the response that will be sent to the website.

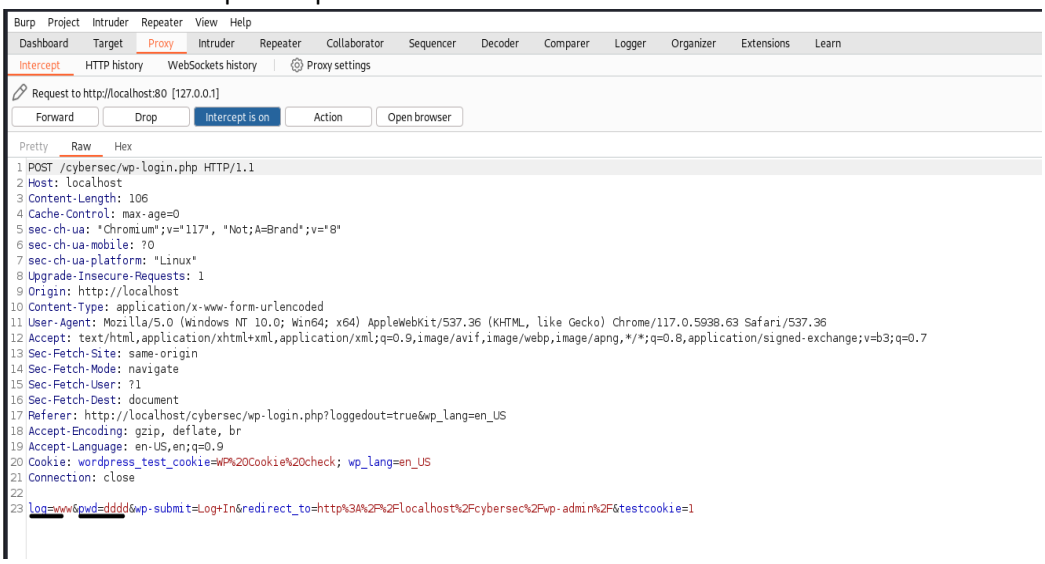
- The website has some number of limits that when you don't enter the correct password , it starts blocking you for some minutes and eventually blocks you from accessing the website

because it has detected you are trying to gain unauthorized access into the admin login page.

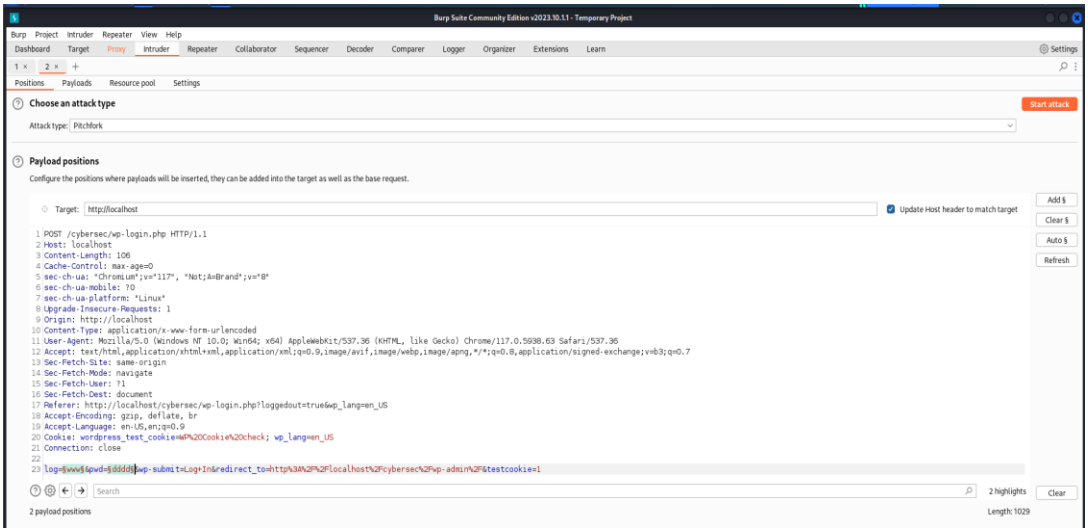
- And since I don't want that scenario to happen, I have already found one of the username and it's password, so I can use that whiles performing the brute force attack to prevent me from being blocked by into gaining access.
- Using burpsuite I manipulated both the username payload of the and the password payload of the website to help find the password of the admin username.

The process I used to perform this attack in the burpsuite are as follows:

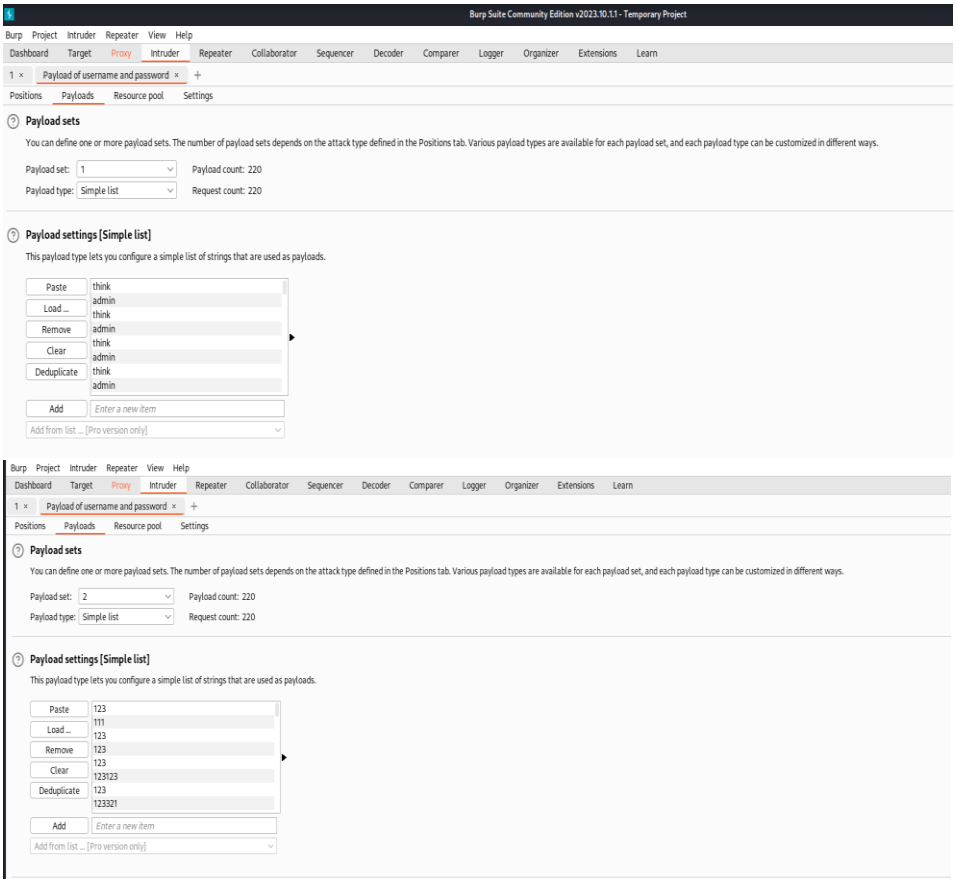
1. On proxy tab I turned on the intercept and opened the website in the burpsuite browser to intercept or capture the website.



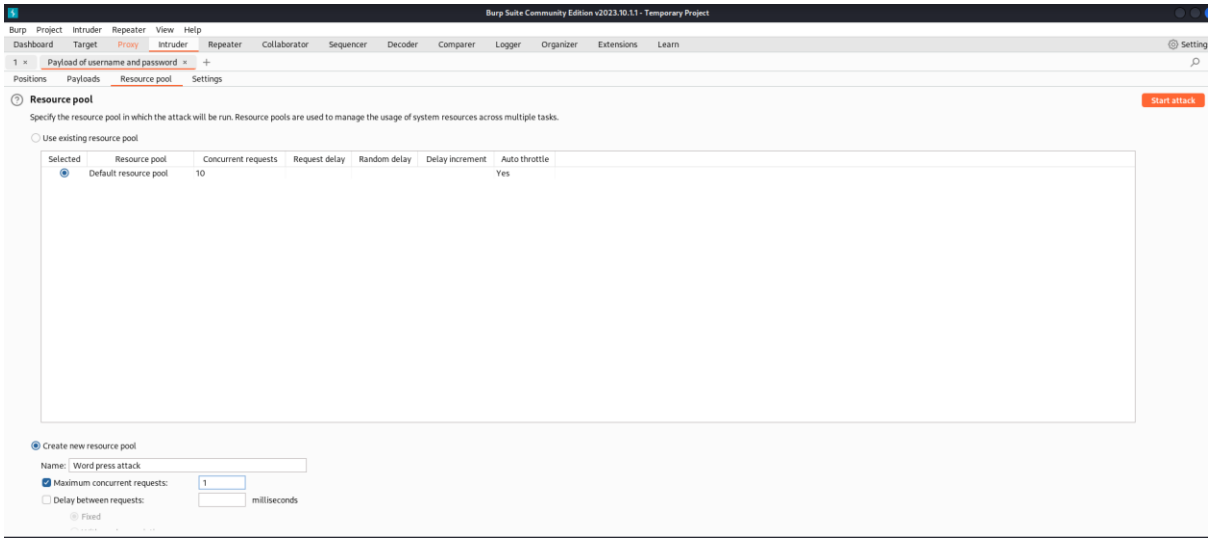
2. From the captured information, I sent the response the intruder tab of burpsuite where the attack is going to take place. I changed the attack type to pitchfork because I was going to manipulate more than one payload which was the username payload and the password payload.



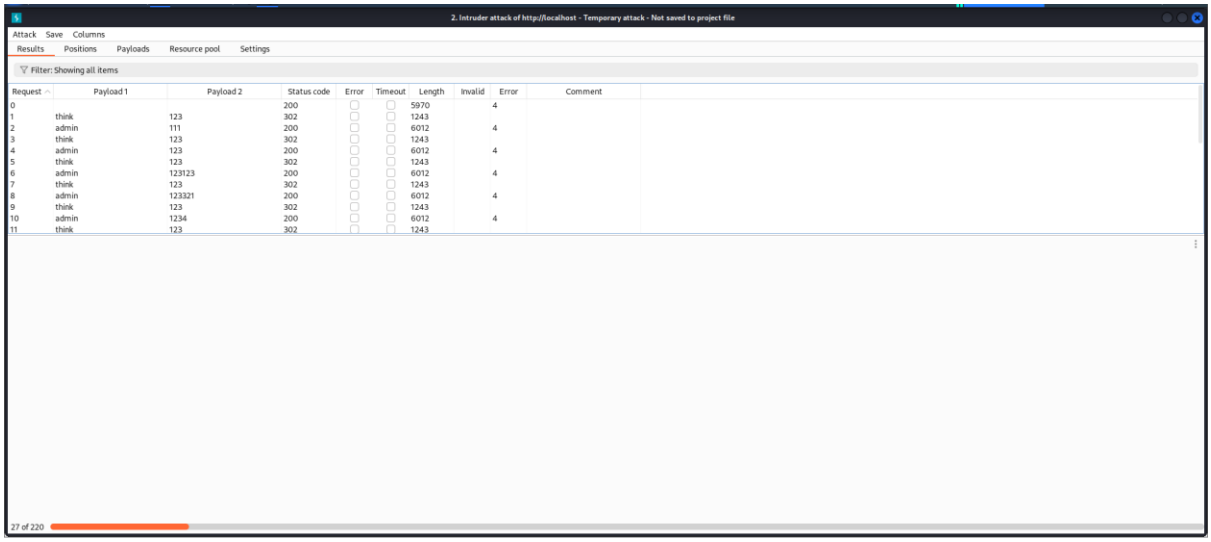
3. I then went to the payload section and added the different payloads both in the username section and password section.

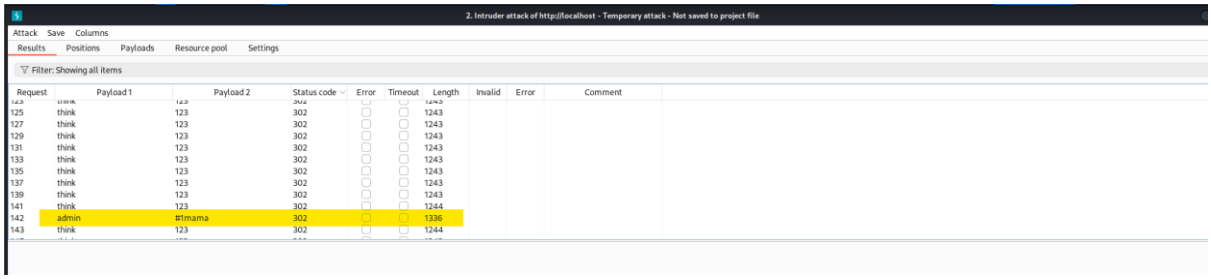


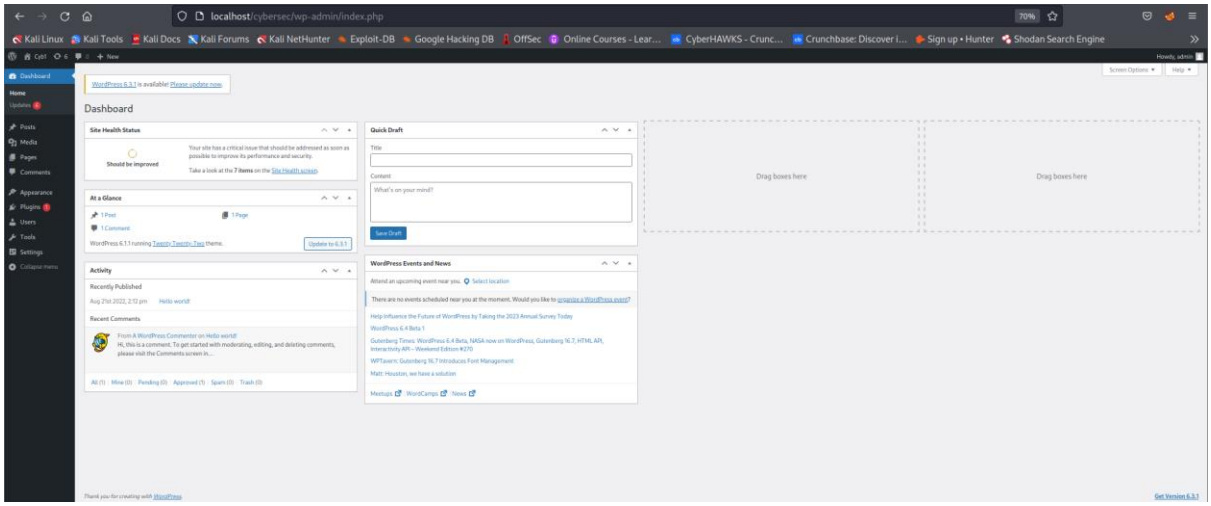
4.I visited the Resource pool to create a new resource pool because I wanted a maximum 1 request per time so the attack will not flood the website with too many requests or payloads simultaneously.



5.After all this settings were done, I started the attack and the at the end of this attack, I wanted to find a particular payload of admin which gave a status code of 302 which meant there was a redirection to another webpage meaning the access to the admin page was successful. Looking at the results below I was able to find the password of the username admin to be **#1mama .**







Vulnerability Assessment

- From this project work, the use of commented credentials in the page source of the website made it vulnerable to attacks. And based on this vulnerability found I was able to leverage this information to help me escalate the privilege of the other username to gain access using that credentials as well.
- Very poor passwords and no proper encryption method to protect it.
- The site-map of the website is easily accessible to the general public.

Recommendations

- I will recommend that developers should avoid putting important credentials in the source code of the program but in this case since it has been done, they should immediately remove the credentials and change the respective passwords of the usernames.
- The use of strong passwords and encryption or hashing of passwords that when fallen into the hands of an attacker cannot easily decrypt the particular password.
- The use of very good security programs that can hide your sitemap file, along with other vulnerable files and path where hackers and spammers cannot not make use of.

Conclusion

- I successfully exploited the web page and gave some recommendations to help prevent such an attack in the future.

References

Burpsuite.