# Prince Sultan University
## College of Computer and Information Sciences
## CYS401 – Fundamentals of Cybersecurity

# Practical 4: Hacking Web Application - Perform a Brute-force Attack using Burp Suite in Kali Linux

***Disclaimer**: All the labs in this course are prepared for educational purposes. we can't harm anyone all the commands are done within our own system and network.*

## Instructions:

a. The assignment must be done individually.

b. The assignment is of 10 marks. You'll have to demonstrate the assignment on your PC OR submit a report. For each assignment, there will be an assessment.

c. The assignment should preferably be done on a laptop.

d. Required Tools: Kali- Linux, Burp Suite (available in kali Linux).

**Requirements:**

a. Select the user whose password you want to know, in order to get access to his/ her account.

b. It works only for less complex passwords (E.g., Combination of Alphanumeric, Alphabets with uppercase letters at start and end).

c. Download a word dictionary from internet or need to create your own word dictionary.

**Burp Suite:**

Burp Suite is an integrated platform for performing security testing of web applications. It has various tools that work together to support the entire testing process from the initial mapping and analysis of an application's attack surface to finding and exploiting security vulnerabilities. Burp Suite contains key

components such as an intercepting proxy, application-aware spider, advanced web application scanner, intruder tool, repeater tool, and sequencer tool.

Here, we will perform a brute-force attack on the target website using Burp Suite.

**Tasks:**

a. Download Burpsuite https://portswigger.net/burp/communitydownload. Also available in kali Linux.

b. First of all, you need to create an account on any website which you want to attack. In this case we are using demo website. "demo.testfire.net" Below you can find the details below:

1. **Create the fake website Portal.**
2. In Kali Linux, go to applications, select social engineering.
3. Type password **kali** → type 1 "Social Engineering Attack" → Type 2 "Website Attack Vectors" → Type 3 "Credential Harvester Attack Method" → Type 2 "Site Cloner".
4. It will ask for the IP Address (Copy the given IP somewhere for later use 192.168.42.129). This is the address of Kali Machine. Just Hit "ENTER".
5. Go to the browser, open http://demo.testfire.net/login.jsp
6. Paste the copied URL in "enter the URL to clone" option in the kali terminal. And hit "ENTER"
7. Go to your web browser. In the search URL type the IP address of Kali Machine and hit "ENTER".
8. You will see the fake portal has been generated successfully.

9. Now login with the “username” and “password” and click Sign in. Your credential will directly go to your Kali Machine IP address (which is acting as an attacker). (Note: Don’t close the browser window).

10. Go to your Kali Terminal and check, you will see the username and password there. Now you can use this username and password to access other accounts of this user.

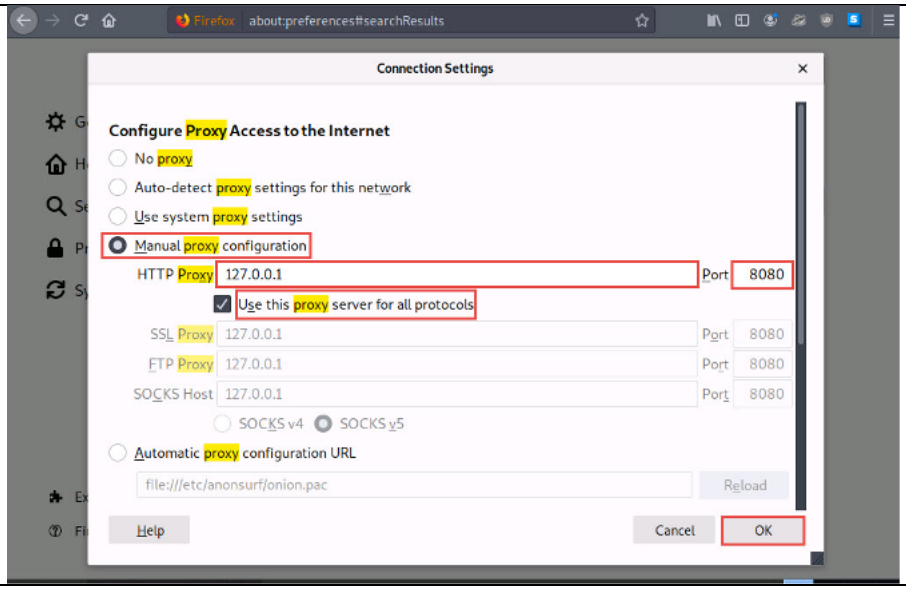
11. It looks very simply but the issue is that user will not click on this URL directly.

12. Do not Close the Previous Terminal of Kali Linux.

c. Secondly, you need to setup your Firefox proxy in order to allow it to work with burp suite.

Firefox-> settings -> options -> Proxy -> set proxy -> 127.0.0.1 and port -> 8080

Check box -> Sock 5.




d. Open your burp suite -> under proxy -> set the http connection to -> 127.0.0.1 and port 8080.

e. Whatever traffic you are sending on internet goes through burp suite. It works as sniffing tool.

f. First open your website on which you created account and go to login page.

g. Open burp suite -> go to proxy -> press intercept in off.

h. Once you press it, intercept gets on.

i. Now go back to your Firefox, enter **username** and **Password** of the user. But keep in mind the password should be incorrect. Assume you only know the user name and wants to find the password using dictionary attack.

j. Now go back to burp suite, whatever username and password you entered on web page, it is shown in burp suite.

k. On Burp suite perform the following actions:

    a. Press **action** and select **send to intruder**

    b. Go to **Intruder** tab.

    **c.** Here you need to press **$clear$**

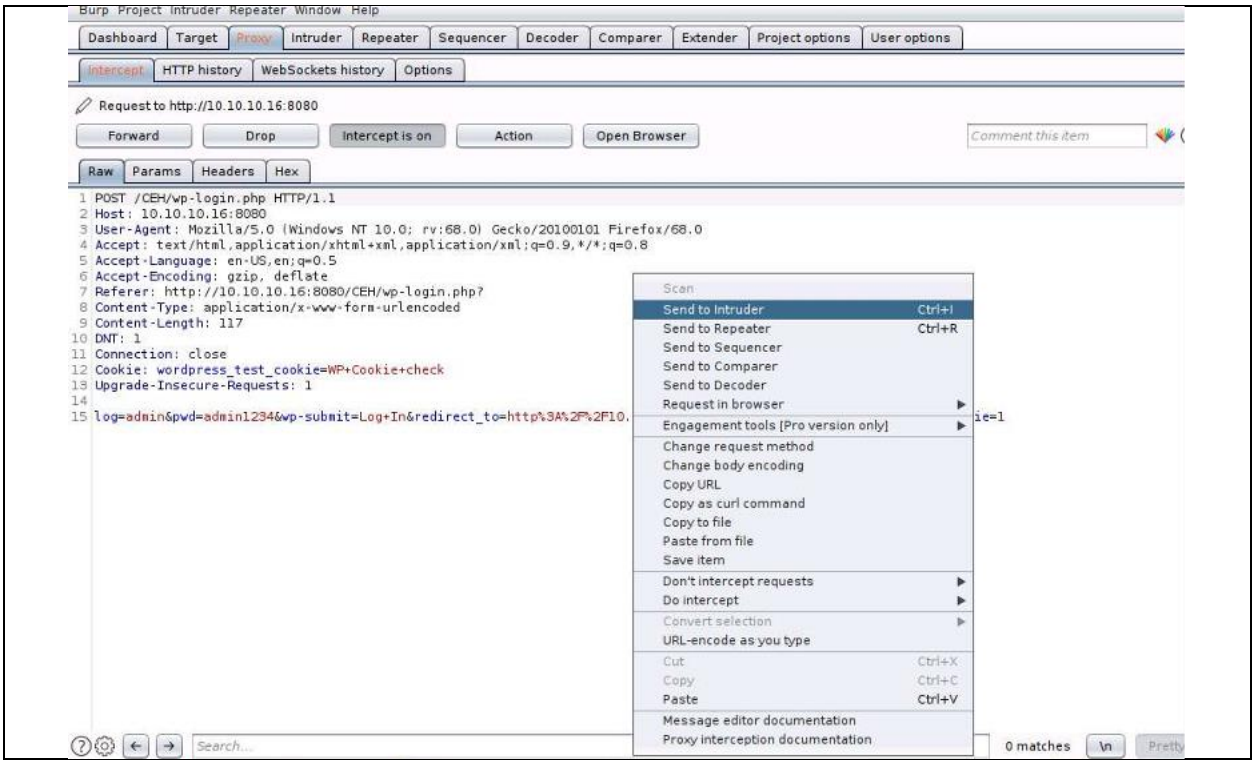
    d. Then select only **username** and **password** and click **$Add$** from right panel.

    e. Select **Cluster Bomb** from drop down menu.

    f. Choose **payload** tab -> select **payload 1** and start entering the username/ names.

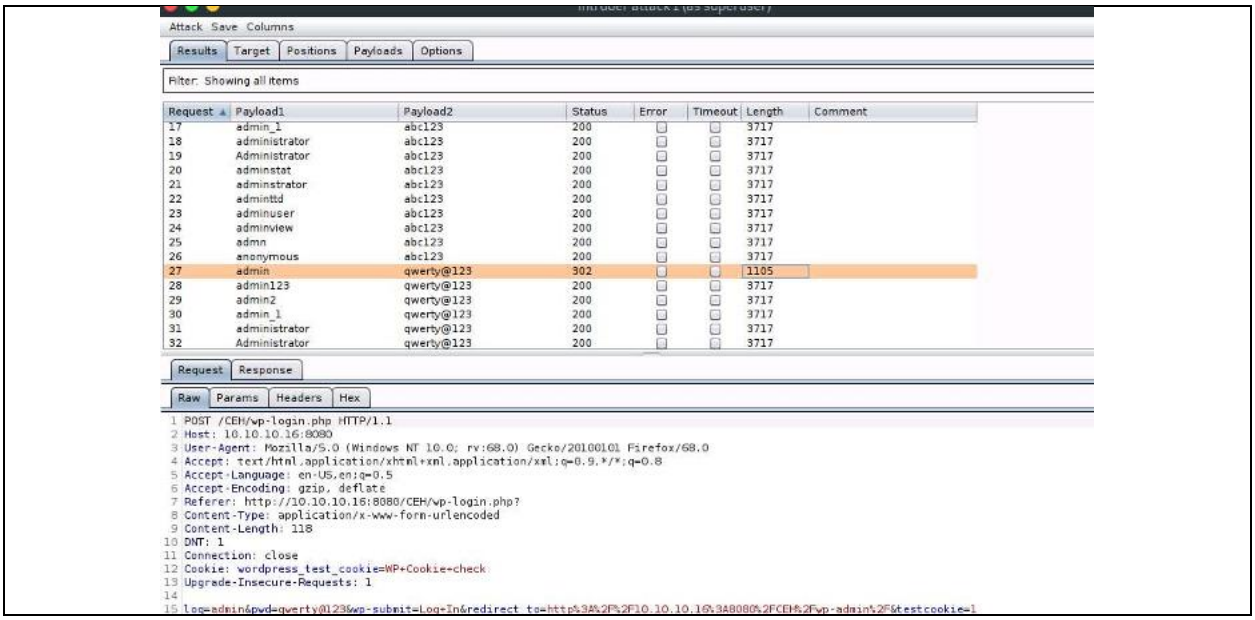
    g. Select **payload 2** and start creating your dictionary. (Note: you can also load dictionary that you have downloaded from internet, but it takes almost 10 hours to process that dictionary)

    h. Click on **Start Attack** button




l. A new Pop-up window appears that start matching your user-name and with the dictionary of passwords that you created.

m. For correct password, It shows different length & size.



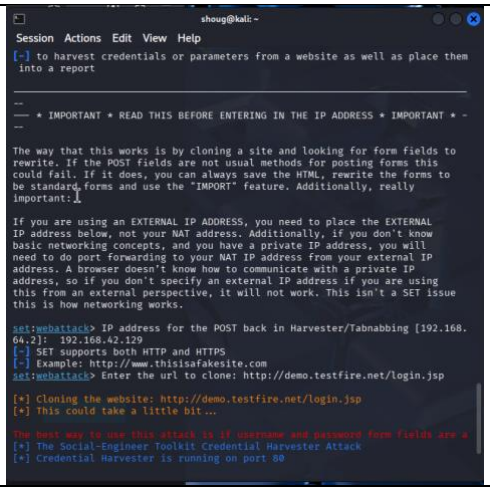
## Bonus Marks:

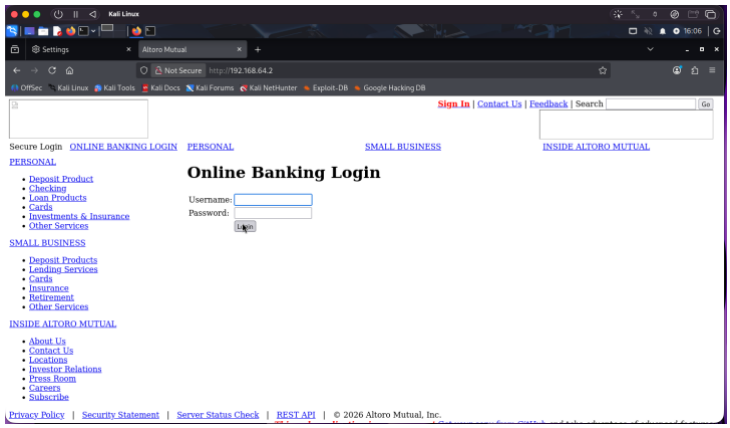
**Task:**

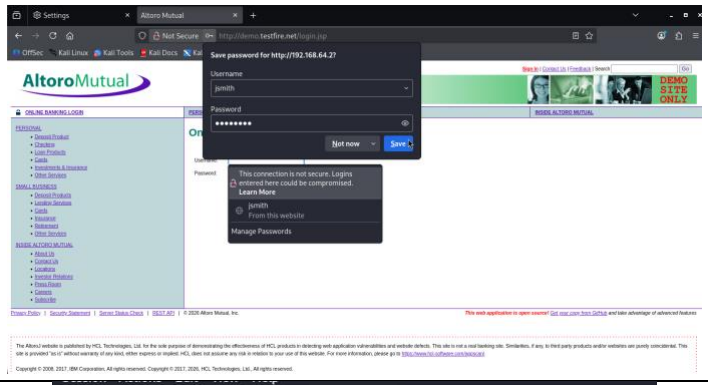
Find your own vulnerable site that runs on “http”, create account on it and perform dictionary attack on it.

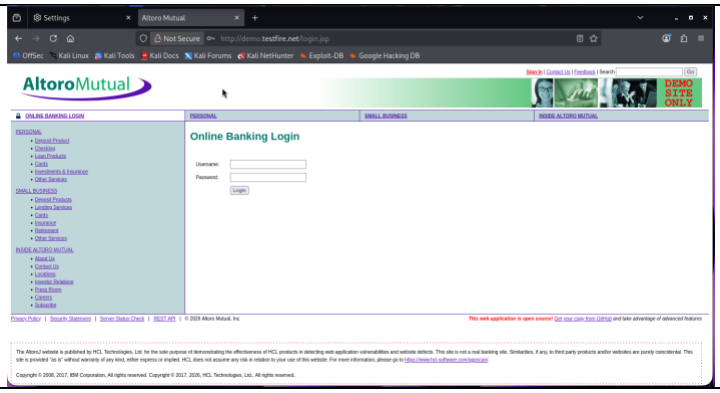
********** **Password Found Successfully** 😊**********

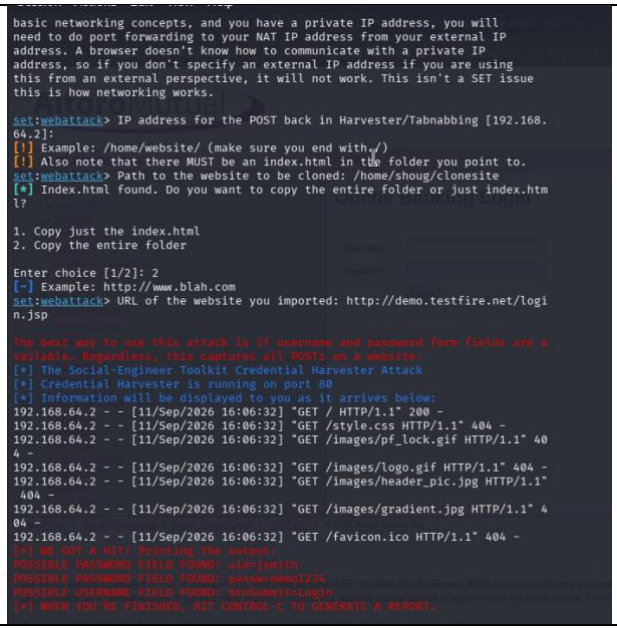
# MY SOLUTION P1



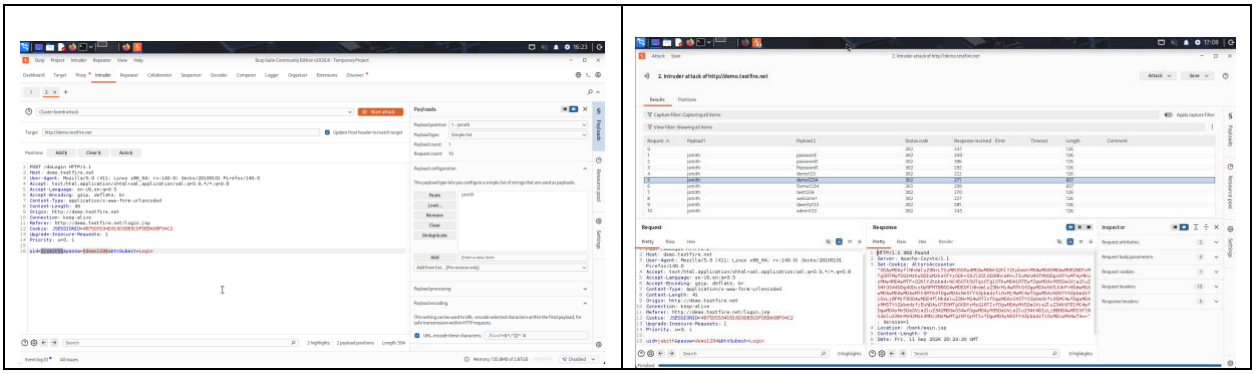



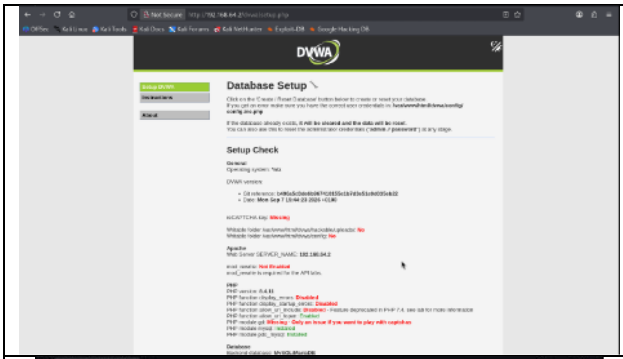

[*] WE GOT A HIT! Printing the output: POSSIBLE PASSWORD FIELD FOUND: uid=jsmith POSSIBLE PASSWORD FIELD FOUND: passw=demo1234

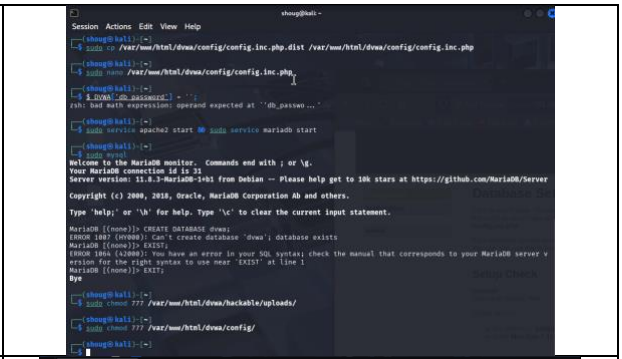
# MY SOLUTION P2

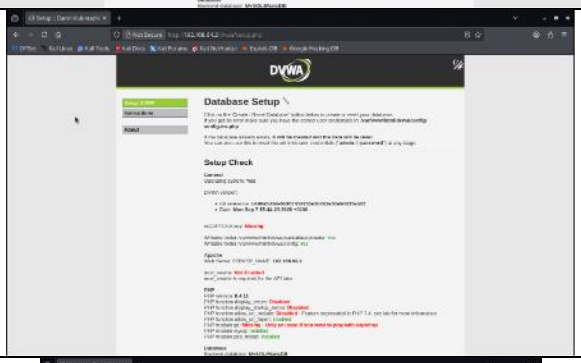


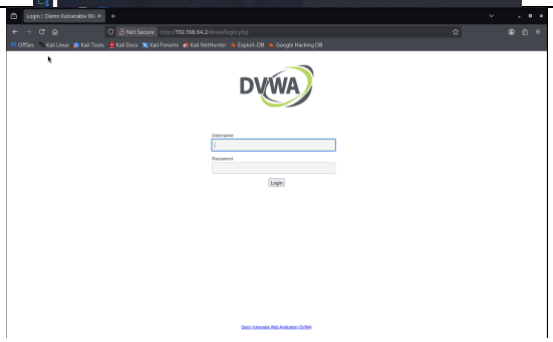
```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie:
AltoroAccounts="ODAwMDAyflNhdmluZ3N+LTIuMEU5OXw4MDAwMDN+Q2hlY2tpbmd+MS
4wMDA5MDAwMDE2NDYxMTg5RTMwfDQ1MzkwODIwMzkzOTYyODh+Q3JlZGl0IENhcmR+LTIu
MzU4OTM0ODgxNTYwMTAyMkUyMHw4MDAwMTF+Q2hlY2tpbmd+NC45OTk5OTgxOTg1OTkwMD
A1RTEwfDgwMDAxM35DaGVja2luZ34tOS44ODg4ODcxNzRFMTB8ODAwMDE0flNhdmluZ3N+
Mi4wRTk5fDgwMDAxNX5JUkF+MS4wMDAwMDAwMDAwMTI4RTE4fDgwMDAxNn5TYXZpbm
dzfi0xMjMwMC4wfDgwMDAxN35TYXZpbmdzfi0xLjBFMjF8ODAwMDE4flNhdmluZ3N+MS4w
RTIxfDgwMDAxOX5TYXZpbmdzfi05MC4wfDgwMDAyMH5TYXZpbmdzfjEuNDAyOTE0MTg0OD
YyMzQ1RTIxfDgwMDAyMX5DaGVja2luZ34tNTE1MC4wfDgwMDAyMn5DaGVja2luZ342MDQw
OS4wfDgwMDAyM35DaGVja2luZ34tNDIyLjB8ODAwMDI0flNhdmluZ3N+MS42Mzk4MDc2Nz
MwMTgzNTQyRTIxfDgwMDAyNX5TYXZpbmdzfi0xMDcwMS4wfA==";  Version=1
Location: /bank/main.jsp
Content-Length: 0
Date: Fri, 11 Sep 2026 20:23:20 GMT
```

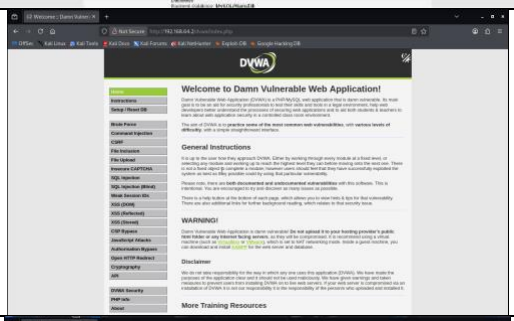
# MY SOLUTION BONUS

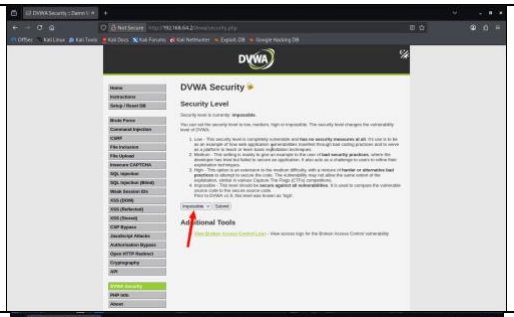


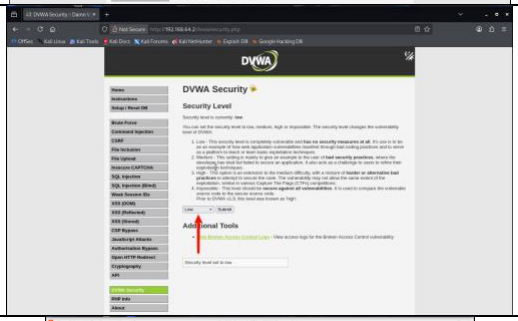



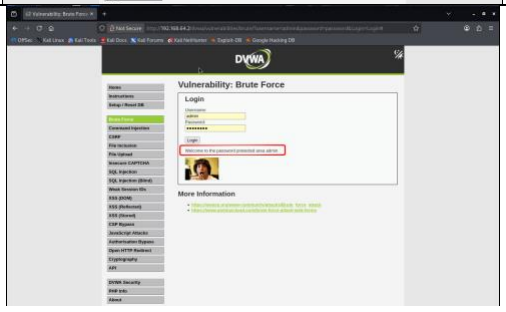



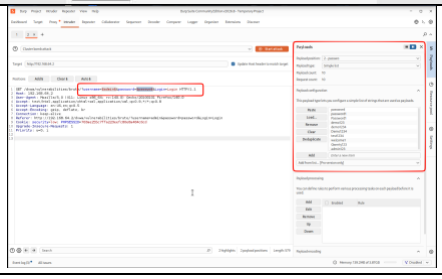



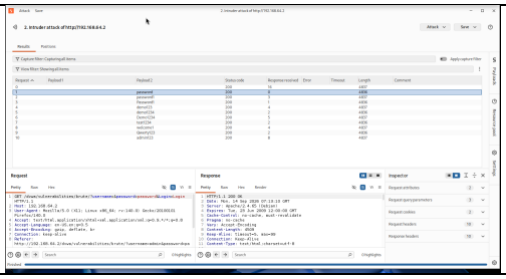





**Task 1: Credential Harvesting using SET**

A simulated attack using the Social Engineering Toolkit (SET) was performed on Kali Linux where the demo.testfire.net login page was cloned. SET was started by using the command `sudo setoolkit`, then moved to Website Attack Vectors > Credential Harvester Attack Method and Custom Import function (as the Site Cloner was unsuccessful because the page used chunked HTTP) to host an imitation of the AltoroMutual login page on the IP address of my Kali machine (192.168.64.2). When a victim accesses this web page and enters his credentials, SET will obtain this information in plain text.

**Task 2: Brute Force Attack using Burp Suite Intruder**

First, I set up Firefox to connect to Burp Suite's proxy (127.0.0.1:8080). Using the Intercept feature, I made a login attempt to `demo.testfire.net` with the known username jsmith but incorrect password. Then I sent the captured POST request to the Intruder module, selected the payload positions (username and password), defined attack type as Cluster Bomb, and added a custom password list. In the result table, I saw that `demo1234` caused the response with a significantly different length (837 bytes compared to 126 bytes for all other requests with incorrect passwords). Moreover, the server's response contained a `Set-Cookie: AltoroAccounts` session cookie, the signs of the successful login with the identified password.

**Bonus: Brute Force on the Second Target (DVWA)**

For this part, I set up DVWA on Kali with Apache, MariaDB, and PHP, configured the database, and changed the security level to Low. Then I ran the same Cluster Bomb attack using Burp Suite Intruder on the Brute

Force module of DVWA, targeting the `admin` account and determining the correct password (`password`) based on the length of the response.