

Brute Force Website Login Page using Burpsuite

posted in [Kali Linux](#), [Penetration Testing](#), [Website Hacking](#) on [September 23, 2016](#) by [Raj Chandel](#)

SHARE

Hello friends!! This is a beginner guide on Brute Force attack using Burp suite. In this article, we had demonstrated the login page brute force attack on a web application “DVWA”.

Table of Content

- Introduction to Brute Force Attack
- The vector of Brute force Attack
- What is wordlist or dictionary?
- Lab Set -up Requirement
- Password Brute Force Using Sniper Attack
- Username & Password Brute Force Using Cluster Bomb Attack

Introduction to Brute Force Attack

Brute force plays a vital role in web penetration testing because is the simplest method to gain access to a site or server by checking the correct username or password by calculating every possible combination that could generate a username or password.

For example, You have 3 digits PIN for login into an account but when you forget the PIN, so you will try different values till the time you identify the right match to unlock the account.

The vector of Brute force Attack

- Using Default login credential such as admin: admin or admin: password
- Weak password or PIN such as 123
- Birth Date or Name such as raj:1111

As per Internet security, 8 letter character is considered as the standard number for the shortest length of a password because the probability of guessing complex password is much larger. For such reason, there are many software and scripts that reduce manual efforts of guessing password or PIN by generating a wordlist or dictionary.

What is wordlist or dictionary?

Wordlist or dictionary is a collection of words which are quite useful while making brute force attack. There are several tools which let you generate your own dictionary that you can use in brute force attack.

Lab Set -up Requirement

Target: DVWA

Attacking tool: Installed Burp Suite (Any Platform Windows/Kali Linux)

Password Brute Force Using Sniper Attack

Burp Suite: Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun. Importantly, it gives us another way to manage our attacks as the alternative to Metasploit.

- To make Burp Suite work, firstly, we have to turn on manual proxy and for that go to the settings and choose
- Then select an advanced option and further go to **Network** then select **Settings**.
- Now, select Manual Proxy Configuration.

Connection Settings

Configure Proxy Access to the Internet

- No proxy
- Auto-detect proxy settings for this network
- Use system proxy settings
- Manual proxy configuration 

HTTP Proxy

Use this proxy server for all protocols

SSL Proxy

FTP Proxy

SOCKS Host

SOCKS v4 SOCKS v5

No Proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

- Automatic proxy configuration URL

Do not prompt for authentication if password is saved

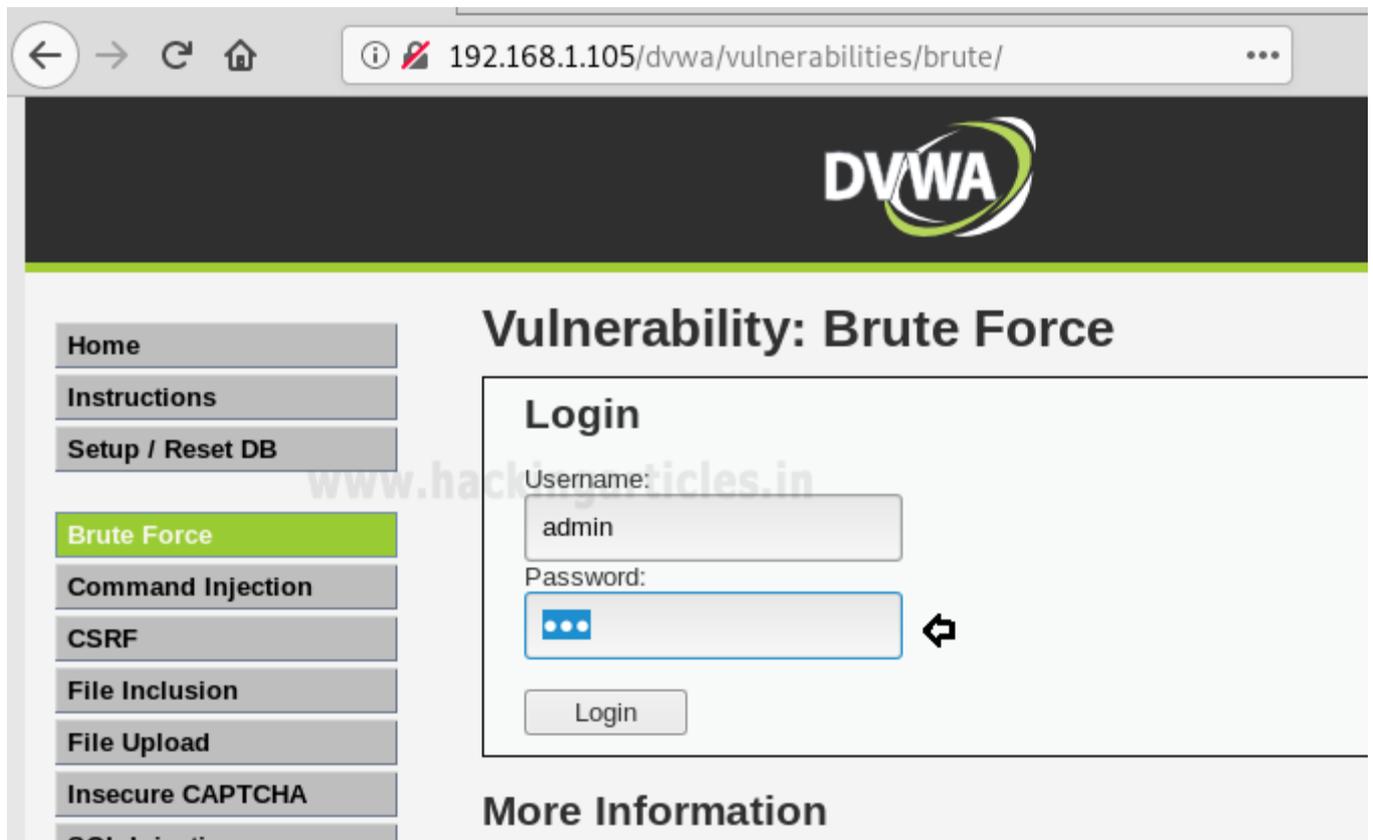
Proxy DNS when using SOCKS v5

[Help](#)

Cancel

Now, on the other hand, open DVWA and log into it using its default username and password. Once you log in, click on Brute Force. And also make sure that security is low or medium. When you click on brute force, it will ask you the username and password for login. Now suppose you don't know the password for login into an account.

To make brute force attack first you need to enter the random password and then **intercept the browser request** using burp suite as explain in the next step.



Now open burp suite and select **the Proxy** tab and turn on an interception by clicking on **Interception is on/off** the tab.

Then go back to DVWA-Brute Force page and click on login tab.

As you can observe that we have successfully intercepted browser request.

The screenshot shows a web proxy tool interface with the following elements:

- Navigation tabs: Intercept (selected), HTTP history, WebSockets history, Options.
- Request details: Request to http://192.168.1.105:80.
- Action buttons: Forward, Drop, Intercept is on, Action.
- View options: Raw (selected), Params, Headers, Hex.
- Request content:

```
GET /dvwa/vulnerabilities/brute/?username=admin&password=123&Login=Login HTTP/1.1
Host: 192.168.1.105
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: security=low; PHPSESSID=j8h31o8fsg3knkloigfs3gi7s4
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Send the captured data to the intruder by right-clicking on the space and choosing Send to Intruder option or simply press **Ctrl + i**

Then select the Positions tab and follow the below steps:

- Choose the **Attack type** as a sniper.
- Click on a **clear tab** to deselect the selected area.

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extended

1 x 2 x ...

Target Positions Payloads Options

? Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the positions.

Attack type:

```
GET /dvwa/vulnerabilities/brute/?username=$admin$&password=$123$&Login=$Login$ HTTP/1.1
Host: 192.168.1.105
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: security=$low$; PHPSESSID=$j8h31o8fsg3knkloigfs3gi7s4$
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Now select a password as shown below in the given image and then click on **add tab**.

? Payload Positions

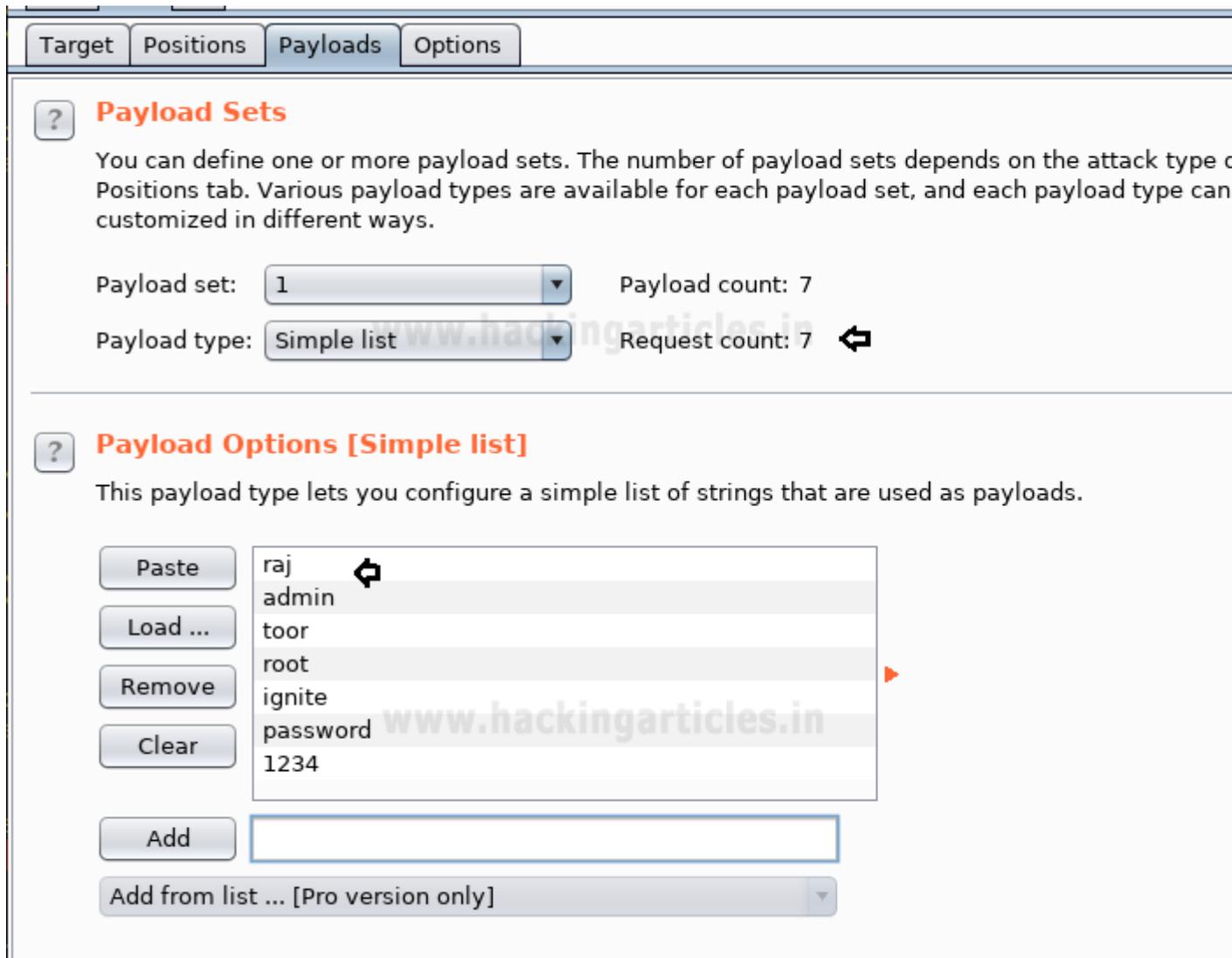
Configure the positions where payloads will be inserted into the base request. The attack type determines in which payloads are assigned to payload positions - see help for full details.

Attack type:

```
GET /dvwa/vulnerabilities/brute/?username=admin&password=$123$&Login=Login HTTP/1.1
Host: 192.168.1.105
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: security=low; PHPSESSID=j8h31o8fsg3knkloigfs3gi7s4
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

In the above image, we have selected a password that means we will need a dictionary file for the username password. Since I have ready to create a dictionary as password.txt but you can create your own dictionary as per your situation.

So now, go to **Payloads tab** and then select **1** from **Payload set** (this '1' denotes the password file). Then click on **Load** button and **browse and select** your dictionary file for a password.



Now all you have to do is go to the **Intruder menu** and select **Start attack** to launch the brute force attack.

Sit back and relax because now the burp suite will do its work and match the username and password and to give you the correct password for the given username.

The moment it will find the correct value, it will have larger the value of length as shown:

Intruder attack 4

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comments
0		200	<input type="checkbox"/>	<input type="checkbox"/>	4700	
1	raj	200	<input type="checkbox"/>	<input type="checkbox"/>	4700	
2	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	4700	
3	toor	200	<input type="checkbox"/>	<input type="checkbox"/>	4700	
4	root	200	<input type="checkbox"/>	<input type="checkbox"/>	4700	
5	ignite	200	<input type="checkbox"/>	<input type="checkbox"/>	4700	
6	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4738	
7	1234	200	<input type="checkbox"/>	<input type="checkbox"/>	4700	

Request Response

Raw Headers Hex HTML Render

Username:

Password:

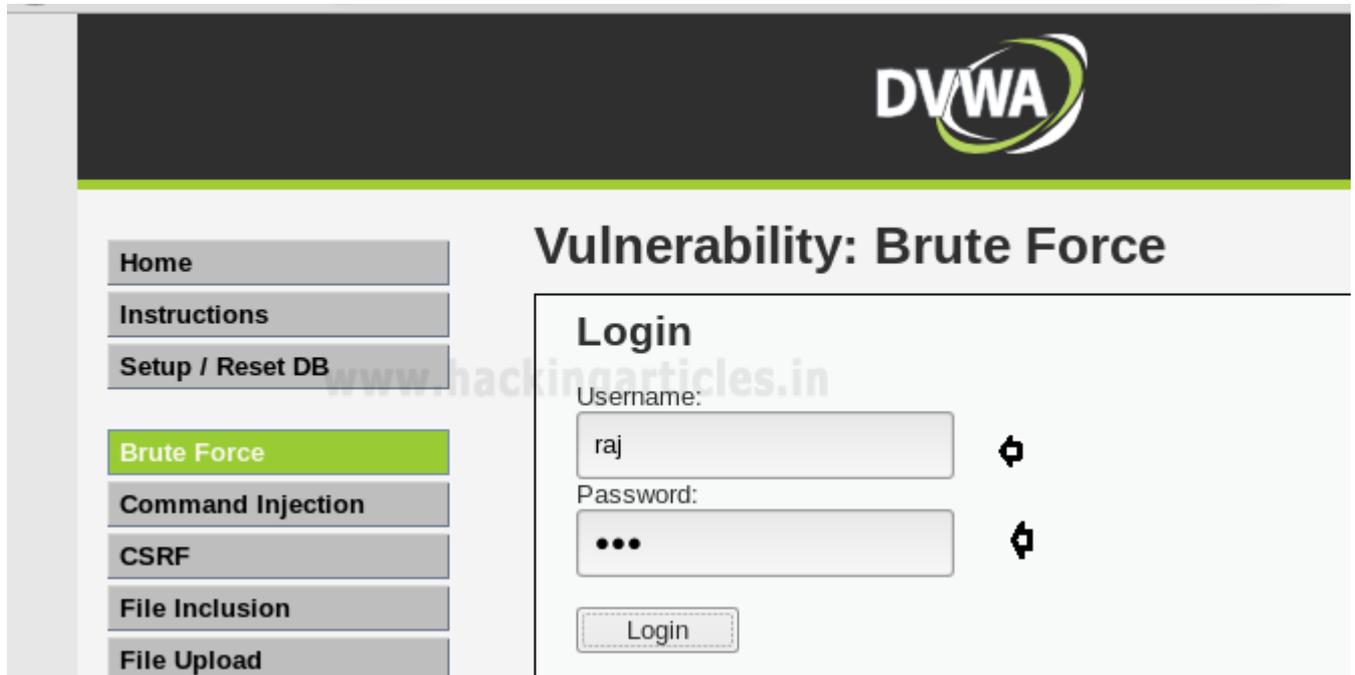
Welcometo the passwordprotected area admin

Username & Password Brute Force Using Cluster Bomb Attack

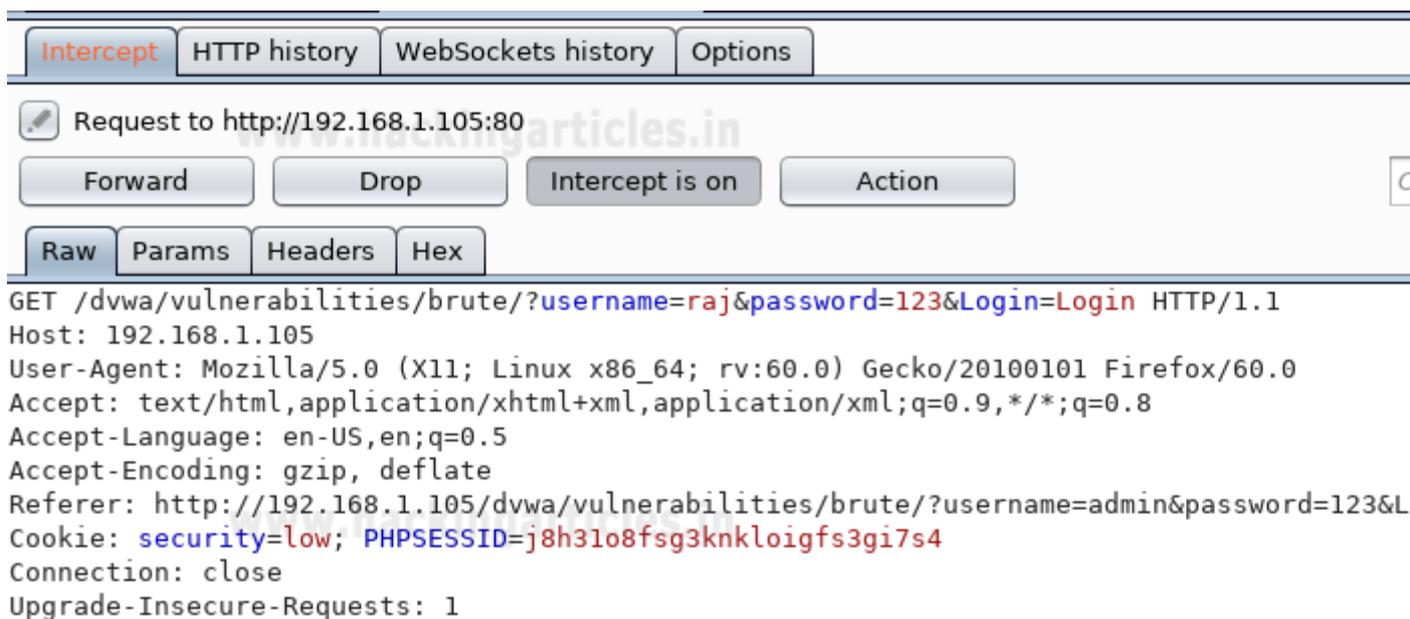
In the above scenario, you saw, how easily we were able to guess the correct password when we knew the username. But what you will do when you don't know anything, neither username nor password?

So don't anxiety while facing such scenario, because Burp suite has many options to shoot brute force attack in various situation, similarly "Cluster Bomb" is the attack type which will help us in brute forcing the username and password filed simultaneously.

Now once again repeat the above steps to capture the browser request and this time enter random credential and do not forget to configure burp suite setting before hitting on login tab.

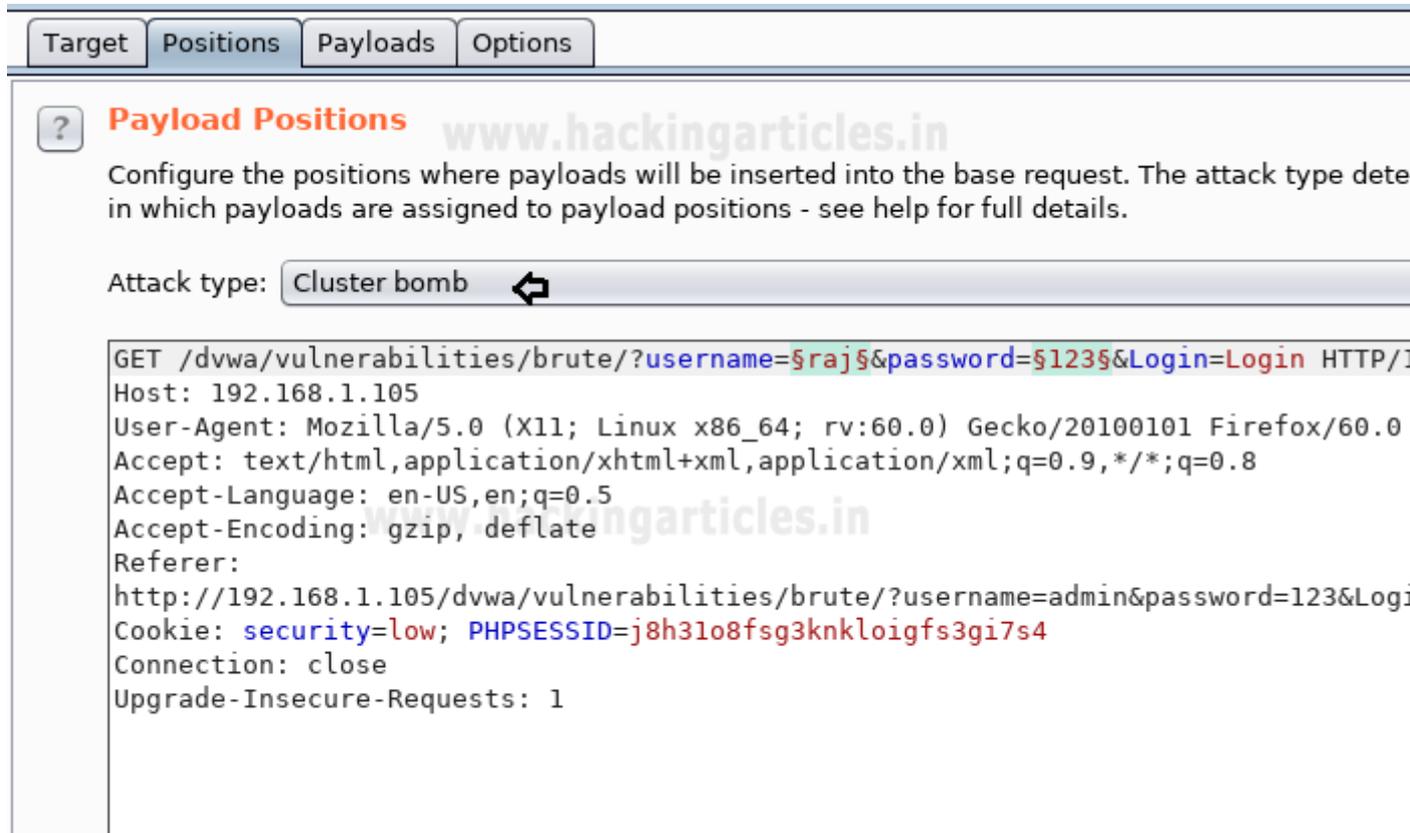


As you can observe that we have successfully intercepted browser request and then send the captured data to the intruder.



Then select the **Positions** tab and follow the below steps:

- Choose the **Attack type** as “cluster bomb”.
- Click on a **clear** tab to deselect the selected area.
- Then select username and password as shown below in the given image and then click on **add**



Target **Positions** **Payloads** **Options**

? **Payload Positions** www.hackingarticles.in

Configure the positions where payloads will be inserted into the base request. The attack type determines in which payloads are assigned to payload positions - see help for full details.

Attack type: **Cluster bomb** ↩

```
GET /dwa/vulnerabilities/brute/?username=$raj$&password=$123$&Login=Login HTTP/1.1
Host: 192.168.1.105
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.105/dwa/vulnerabilities/brute/?username=admin&password=123&Login=Login
Cookie: security=low; PHPSESSID=j8h31o8fsg3knkloigfs3gi7s4
Connection: close
Upgrade-Insecure-Requests: 1
```

Since in above situation we were making brute force attack on the single password field, therefore, we had uploaded one dictionary for guessing correct password but this we selected two payload position, therefore, we have you upload two dictionaries for username and password respectively.

Therefore set payload 1 along with simple list as payload type and upload username wordlist.

Target Positions Payloads Options

? Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type of the selected Position 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: 5

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.

Paste Load ... Remove Clear Add

- raj
- admin
- root
- ignite
- toor

www.hackingarticles.in

And set payload 2 along with simple list as payload type and upload password wordlist.

Target Positions Payloads Options

? Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type of the selected Position 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: 7 ↺

Payload type: Simple list Request count: 35

? Payload Options [Simple list]

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

Paste ↺

Load ...

Remove ▶

Clear

Add

- raj ↺
- admin
- root
- ignite ▶
- toor
- password
- abcd

www.hackingarticles.in

Now all you have to do is go to the **Intruder menu** and select **Start attack** to launch the brute force attack.

Sit back and relax because now the burp suite will do its work and match the username and password and to give you the correct username and password.

The moment it will find the correct value, it will have larger the value of length as shown:

Intruder attack 3

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload1	Payload2	Status	Error
16	raj	ignite	200	<input type="checkbox"/>
17	admin	ignite	200	<input type="checkbox"/>
18	root	ignite	200	<input type="checkbox"/>
19	ignite	ignite	200	<input type="checkbox"/>
20	toor	ignite	200	<input type="checkbox"/>
21	raj	toor	200	<input type="checkbox"/>
22	admin	toor	200	<input type="checkbox"/>
23	root	toor	200	<input type="checkbox"/>
24	ignite	toor	200	<input type="checkbox"/>
25	toor	toor	200	<input type="checkbox"/>
26	raj	password	200	<input type="checkbox"/>
27	admin	password	200	<input type="checkbox"/>
28	root	password	200	<input type="checkbox"/>
29	ignite	password	200	<input type="checkbox"/>
30	toor	password	200	<input type="checkbox"/>
31	raj	abcd	200	<input type="checkbox"/>
32	admin	abcd	200	<input type="checkbox"/>
33	root	abcd	200	<input type="checkbox"/>
34	ignite	abcd	200	<input type="checkbox"/>

Request Response

Raw Headers Hex HTML Render

• XSS (DOM

• XSS (Refl

• XSS (Stor

• CSP Bypass

Login

Welcome to the password protected area admin