All Burpsuite

Burpsuite Encoder & Decoder Tutorial

posted in[**Penetration Testing**](https://www.hackingarticles.in/category/penetration-testing/), [**Website Hacking**](https://www.hackingarticles.in/category/website-hacking/) on [**January 24, 2018**](https://www.hackingarticles.in/burpsuite-encoder-decoder-tutorial/) by [**Raj Chandel**](https://www.hackingarticles.in/author/raaz/)

SHARE

Save

Burpsuite Decoder can be said as a tool which is used for transforming encoded data into its real form, or for transforming raw data into various encoded and hashed forms. This tool is capable of recognizing several encoding formats using defined techniques. Encoding is the process of putting a sequence of character’s (letters, numbers, punctuation, and symbols) into a specialized format which is used for efficient transmission or storage. Decoding is the opposite process of encoding the conversion of an encoded format back into the original format. Encoding and decoding can be used in data communications, networking, and storage.

Today we are discussing the **Decoder** Option of ‘Burp Suite’. Burp Suite is a tool which is used for testing Web application security. 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. This tool is written in JAVA and is developed by PortSwigger Security.

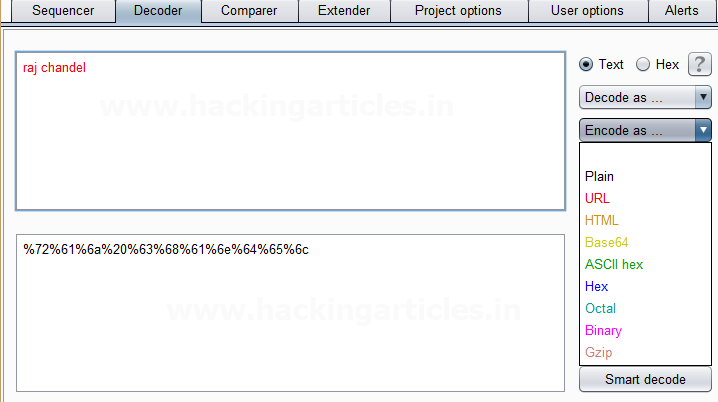
There are 9 types of decoder format in Burp Suite:

* **Plain text**
* **URL**
* **HTML**
* **Base64**
* **ASCII Hex**
* **Hex**
* **Octal**
* **Binary**
* **Gzip**

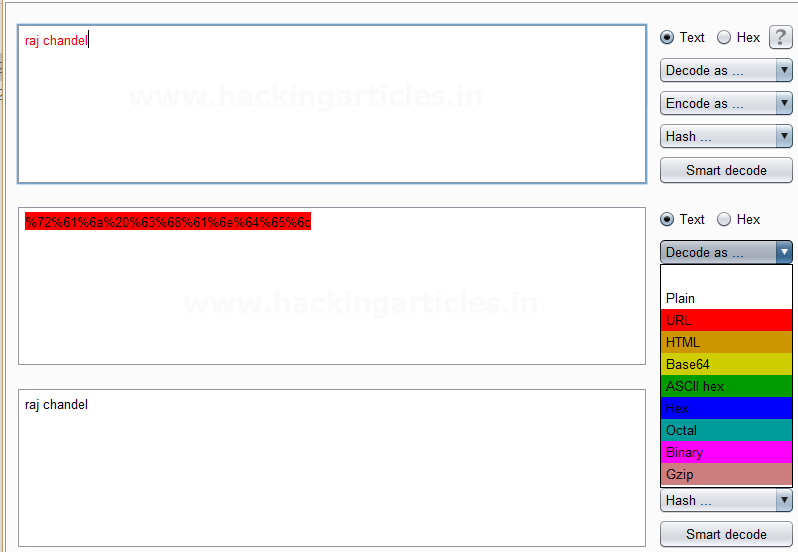
**URL Encoder & Decoder**

When you will explore decoder option in burp suite you will observe two sections left and right. The left section is further divided into two and three sections for encoding and decode option respectively. The right section contains the function tab for encoding and decodes option. And if you will observe given below image you can notice there are two radio buttons for selecting the type of content you want to encode or decode.

Enable the radio button for text option and then we can give any input in the box to be encoded, here we have given **Raj chandel** as an input as shown in the image. After that click on the **Encoded as** an option and select **URL field** from given list as shown in the image. We will get the **encoded result** in **URL format** in the second box as shown in the image.

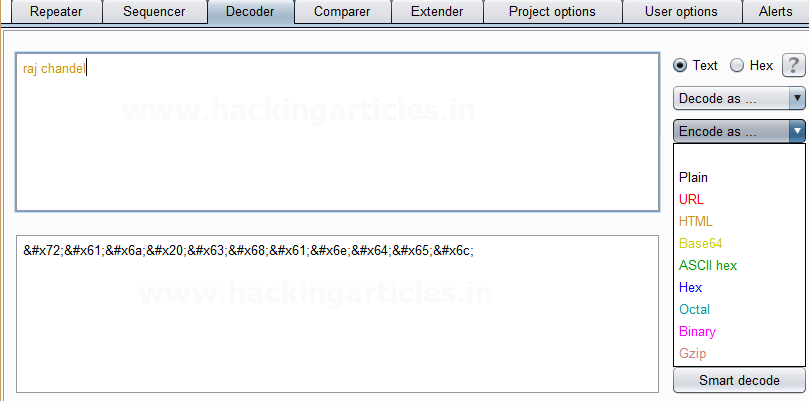


 We can directly decode the **Encoded URL Text** by clicking on the **Decoded as** an option and selecting **the URL field** from the given list of options as shown in the image.  This will **decode** the **encoded URL text** into **plain text** in the third box as shown in the image.



**HTML Encoder & Decoder**

Repeat the same and give any input in the first box to be encoded, here we have given **Raj chandel** as an input as shown in the image. After that click on the **Encoded as** an option and select **HTML field** as shown in the image. We will get the **encoded result** in **HTML format** in the second box as shown in the image.

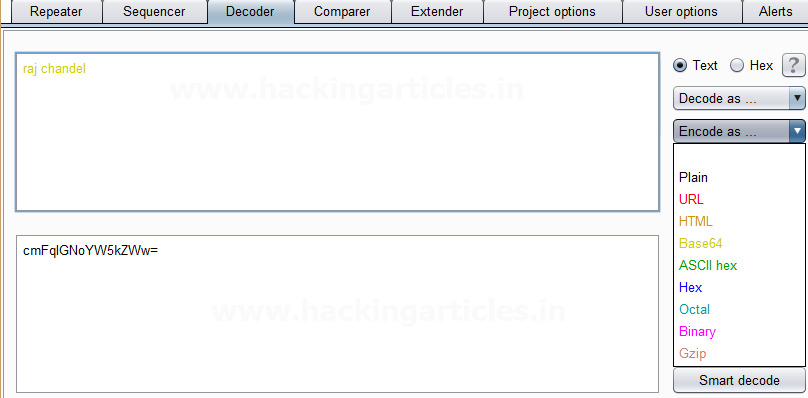


We can directly decode the **Encoded HTML Text** by clicking on the **Decoded as** an option and selecting **the HTML field** as shown in the image.  This will **decode** the **encoded HTML text** into **plain text** in the third box as shown in the image.



**Base64 Encoder & Decoder**

Repeat the same process and give any input in the first box to be encoded, here we have given **Raj chandel** as an input as shown in the image. After that click on the **Encoded as** an option and select **Base64 field** as shown in the image. We will get the **encoded result** in **Base64 format** in the second box as shown in the image.

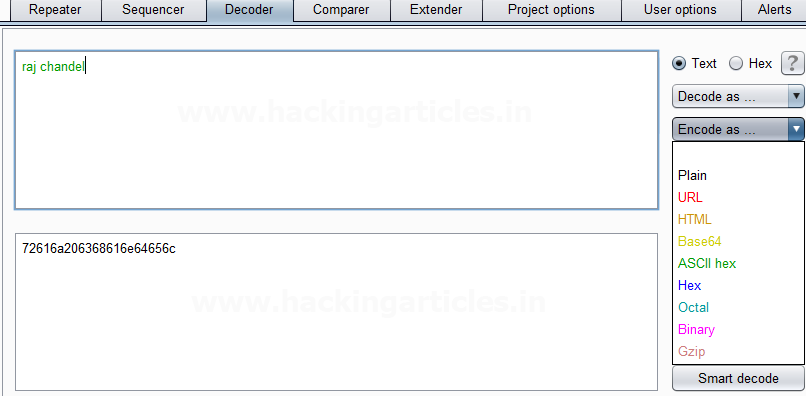


We can directly decode the **Encoded Base64 Text** by clicking on the **Decoded as** an option and selecting **the Base64 field** as shown in the image.  This will **decode** the **encoded Base64 text** into **plain text** in the third box as shown in the image.

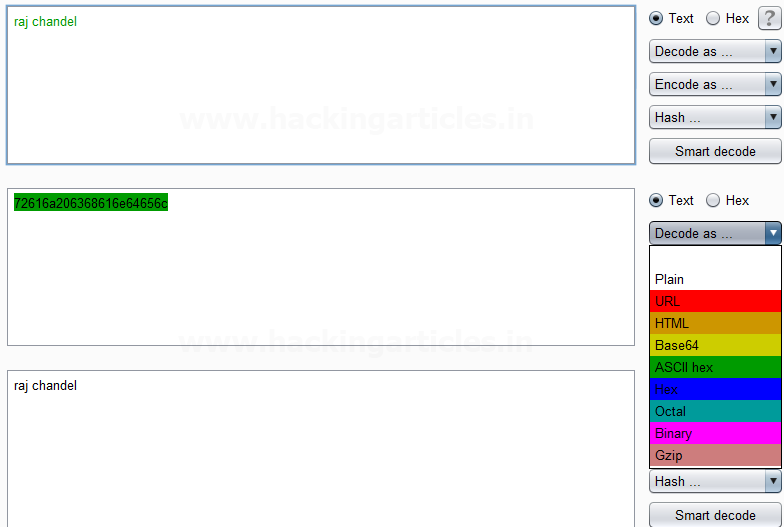


**ASCII Hex Encoder & Decoder**

Again repeat the same process and give any input in the first box to be encoded, here we have given **Raj chandel** as an input as shown in the image. After that click on the **Encoded as** an option and select **ASCII Hex field** as shown in the image. We will get the **encoded result** in **ASCII Hex format** in the second box as shown in the image.

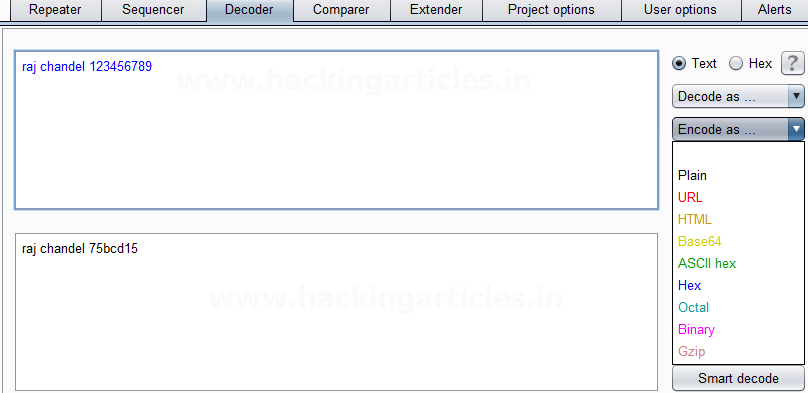


We can directly decode the **Encoded ASCII Hex Text** by clicking on the **Decoded as** the option and selecting **ASCII Hex field** as shown in the image.  This will **decode** the **encoded ASCII Hex text** into **plain text** in the third box as shown in the image.



**Hex Encoder & Decoder**

Repeat same as above and give any input in the first box to be encoded, here we have given **Raj chandel** **123456789** as an input as shown in the image. After that click on the **Encoded as** the option and select **Hex option** as shown in the image. We will get the **encoded result** in **Hex format** in the second box as shown in the image.

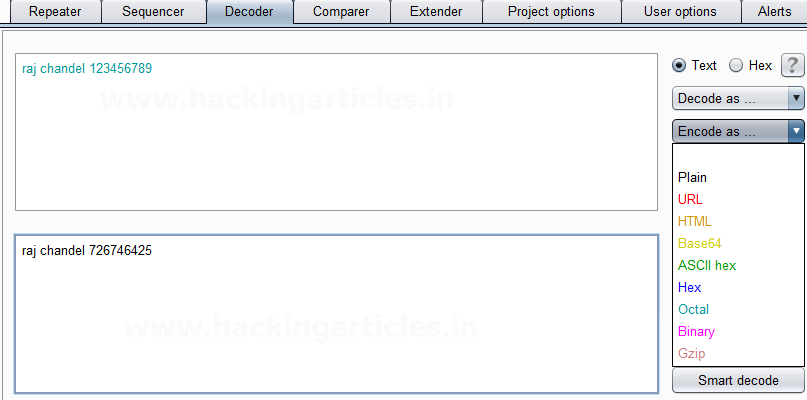


We can directly decode the **Encoded Hex Text** by clicking on the **Decoded as** the option and selecting the **Hex field** as shown in the image. This will **decode** the **encoded Hex text** into **plain text** in the third box as shown in the image.

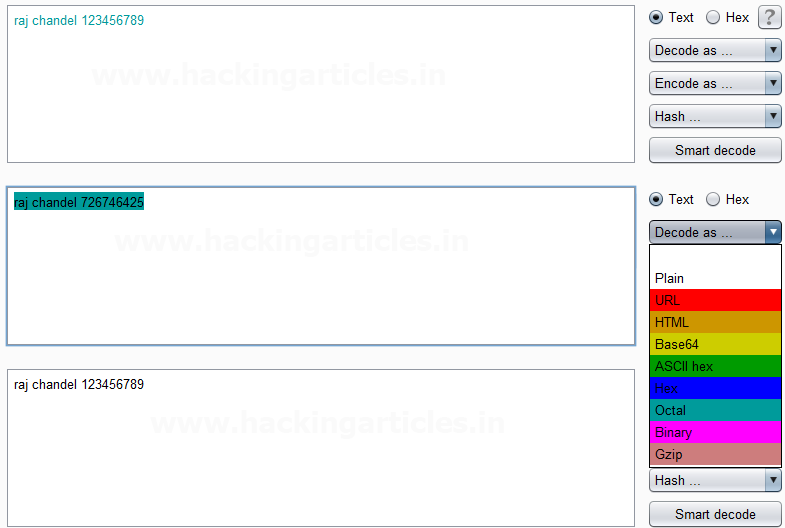


**Octal Encoder & Decoder**

Repeat again and give any input in the first box to be encoded, here we have given **Raj chandel** **123456789** as an input as shown in the image. After that click on the **Encoded as** an option and select **Octal field** as shown in the image. We will get the **encoded result** in **Octal format** in the second box as shown in the image.

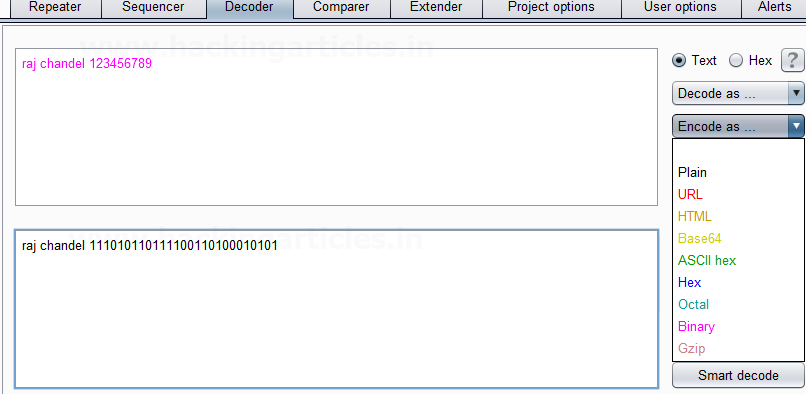


We can directly decode the **Encoded Octal Text** by clicking on the **Decoded as** the option and selecting the **Octal field** as shown in the image.  This will **decode** the **encoded Octal text** into **plain text** in the third box as shown in the image.

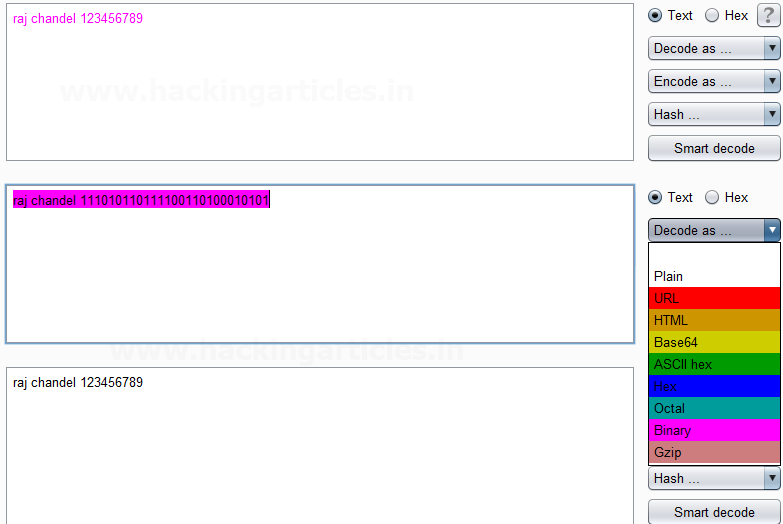


**Binary Encoder & Decoder**

Repeat the same and give any input in the first box to be encoded, here we have given **Raj chandel** **123456789** as an input as shown in the image. After that click on the **Encoded** as an option and select **Binary field** as shown in the image. We will get the **encoded result** in **Binary format** in the second box as shown in the image.

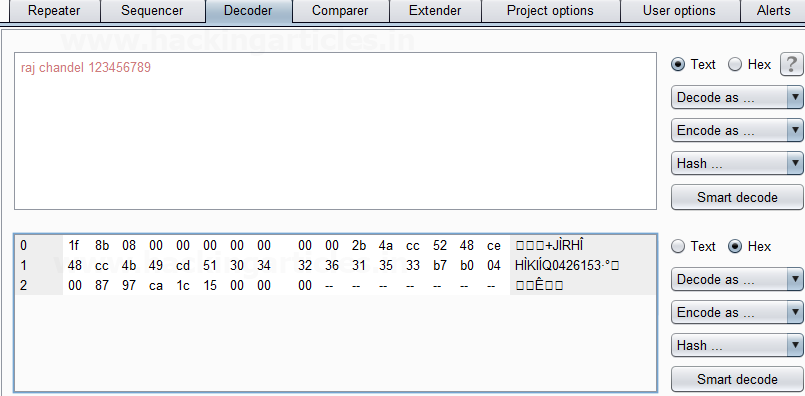


We can directly decode the **Encoded Binary Text** by clicking on the **Decoded as** an option and selecting **the Binary field** as shown in the image.  This will **decode** the **encoded Binary text** into **plain text** in the third box as shown in the image.

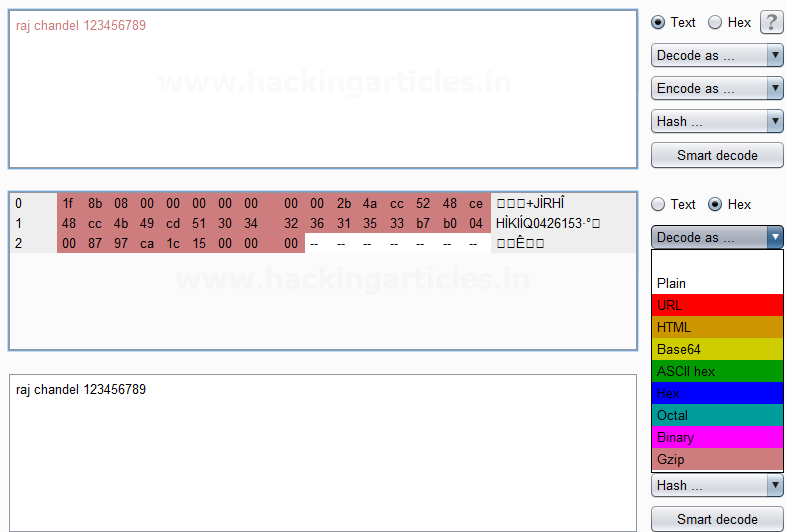


**Gzip Encoder & Decoder**

Give any input in the first box to be encoded, here we have given **Raj chandel** as an input as shown in the image. After that click on the **Encoded as** an option and select **Gzip field** as shown in the image. We will get the **encoded result** in **Gzip format** in the second box as shown in the image.



We can directly decode the **Encoded Gzip Text** by clicking on the **Decoded as** an option and selecting **the Gzip field** as shown in the image.  This will **decode** the **encoded Gzip text** into **plain text** in the third box as shown in the image.



Beginners Guide to Burpsuite Payloads (Part 1)

posted in[**Penetration Testing**](https://www.hackingarticles.in/category/penetration-testing/), [**Website Hacking**](https://www.hackingarticles.in/category/website-hacking/) on [**January 22, 2018**](https://www.hackingarticles.in/beginners-guide-burpsuite-payloads-part-1/) by [**Raj Chandel**](https://www.hackingarticles.in/author/raaz/)

SHARE

Save

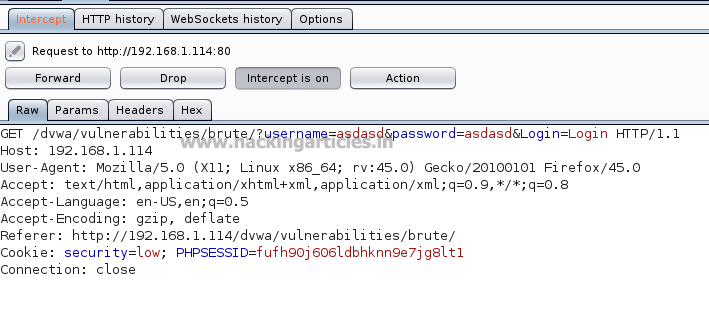
Hello friends!! Today we are discussing about the “Types of Payload in Burp Suite”. Burp Suite is an application which is used for testing Web application security. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application’s attack surface, through to finding and exploiting security vulnerabilities. This tool is written in JAVA and is developed by PortSwigger Security. We are going to use the Intruder feature of Burp Suite, it is used to brute force web applications. There are 18 types of payloads in intruder i.e.

* **Simple list**
* **Runtime File**
* **Case Modification**
* **Numbers**
* **Character substitution**
* **Custom iterator**
* **Recursive grep**
* **Illegal Unicode**
* **Character blocks**
* **Dates**
* **Brute Forcer**
* **Null Payloads**
* **Character frober**
* **Bit Flipper**
* **Username generator**
* **ECB block shuffler**
* **Extension Generated**
* **Copy other payload**

**Simple List**

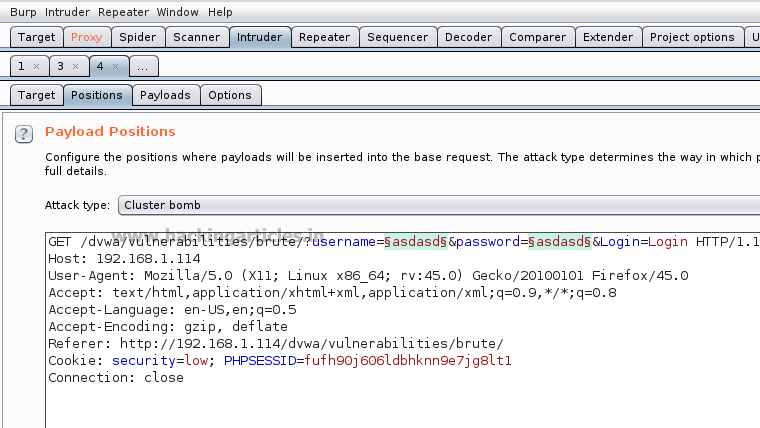
This is one of the simple types of payload, as it allows you to configure a short Dictionary of strings which are used as payload.

First, we intercept the request of the login page in the **DVWA LAB**, where we have given a random username and password. Then click on login, the burp suite will capture the request of the login page.

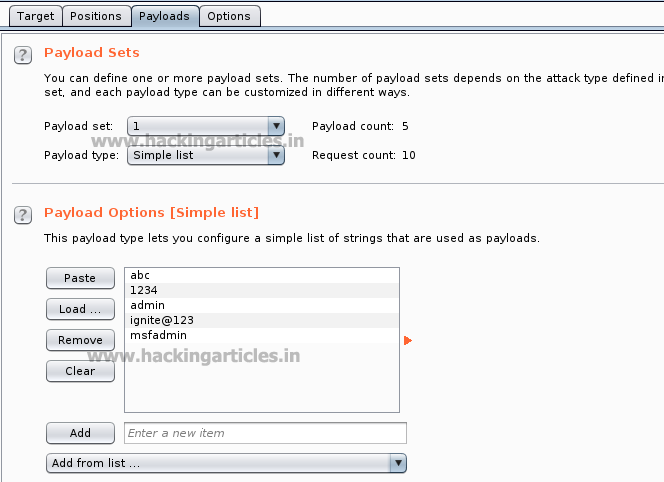


Send the captured request to the **Intruder** by clicking on the Action Tab and follow given below step. Now open the **Intruder** tab then select **positions** and you can observe the highlighted username and password and follow the given below step for selecting payload position.

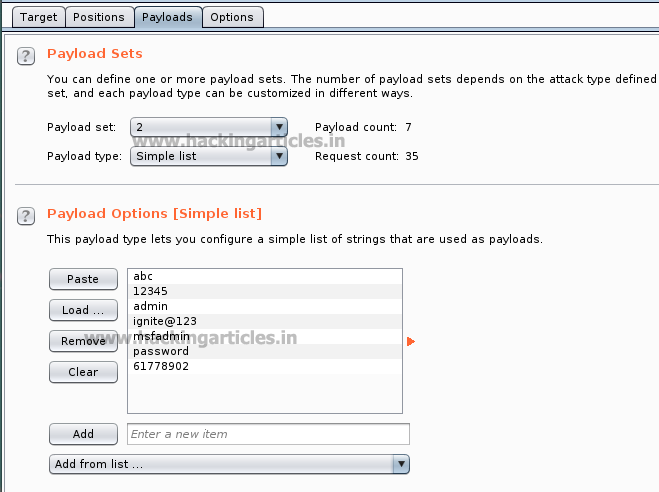
* Press on the **Clear button** given at right of window frame.
* Now we will select the fields where we want to attack which is the username and password and click on **Add button.**
* Choose the **Attack type** as **Cluster Bomb.**
* In the given below image we have selected username and password that means we will need two dictionary files i.e. one for username and second for password.



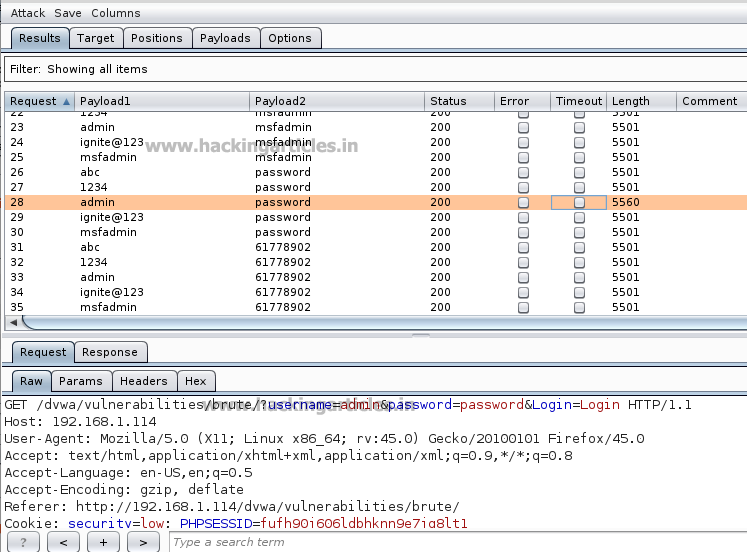
So now, go to **Payloads tab** and the select **1** from **Payload set** (this ‘1’ denotes the first file to be selected). Then click on **Load** button **and select** your dictionary file for username.



Now select **2** in the **Payload set** and again give the dictionary file for the password. Select **Start Attack** in the **Intruder menu** as shown in the image.



Now the burp suite will do its work, match the valid combination of username and password and will give you the correct password and username. The moment it will find the correct value, it will change the value of length as shown.



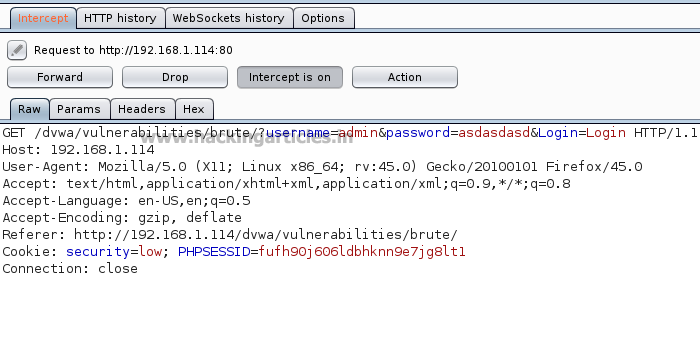
And to confirm the username and password matched, we will give the matched username and password in the **DVWA LAB login page**. We will see a message **“Welcome to the password protected area admin”** which shows are success in the simple list payload attack.



**Runtime File**

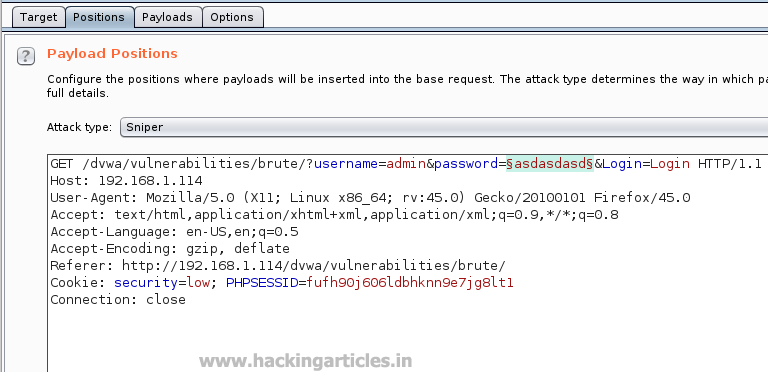
This type of payload allows you to configure a file which reads the payload strings at runtime. This type of payload is needed when we require a large list of payloads, to avoid holding the entire list in memory. This payload allows you to configure large list of strings which overcomes the simple list payload type.

First, we have intercepted the request of the login page in the **DVWA LAB**, where we have given a random username and a random password. Then click on login, the burp suite will capture the request of the login page in the intercept tab.

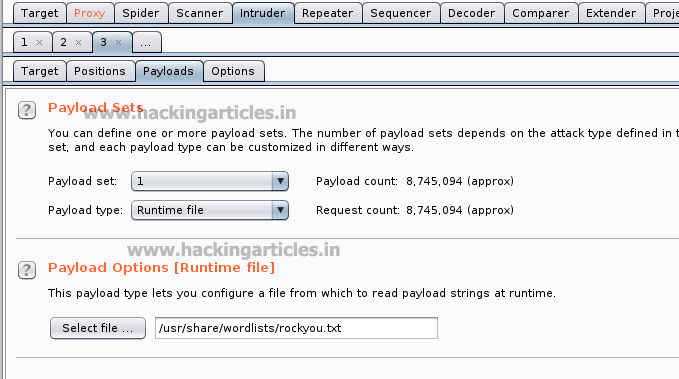


Send the captured request to the **Intruder** and follow given below step. Now open the **Intruder tab** then select **positions** and you can observe the highlighted password and follow the given below step for selecting payload position.

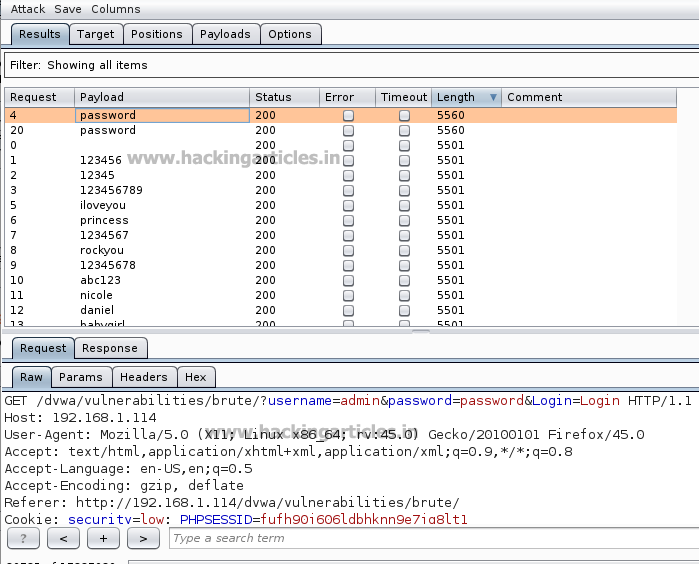
* Press on the **Clear button** given at right of window frame.
* Now we will select the fields where we want to attack and i.e. the password filed and click on **Add button.**
* Choose the **Attack type** as
* In the given below image we have selected  password that means we will need one dictionary file  for password.



Then select the “Payload type” as **Runtime File** and then give the path of dictionary in the “payload options” as **/usr/share/wordists/rockyou.txt** which is the largest dictionary in **Kali Linux**. Select **Start Attack** in the **Intruder menu**.



Now the burp suite will do its work, match the password and will give you the correct password. The moment it will find the correct value, it will change the value of length as shown.



**Case Modification**

This type of payload allows you to configure a list of strings and apply various case modifications to each item on the list. This is useful in password guessing attacks, for generating case variations on dictionary words.

The following case modification rules can be selected:

* **No change** – The item is used without being modified.
* **To lower case** – All letters in the item are converted to lower case.
* **To upper case** – All letters in the item are converted to upper case.
* **To Proper name** – The first letter in the item is converted to upper case, and the remaining letters are converted to lower case.
* **To Proper Name** – The first letter in the item is converted to upper case, and the remaining letters are not changed.

For example, if we select all the modification options, then the item “Raj Chandel” will generate the following payloads:

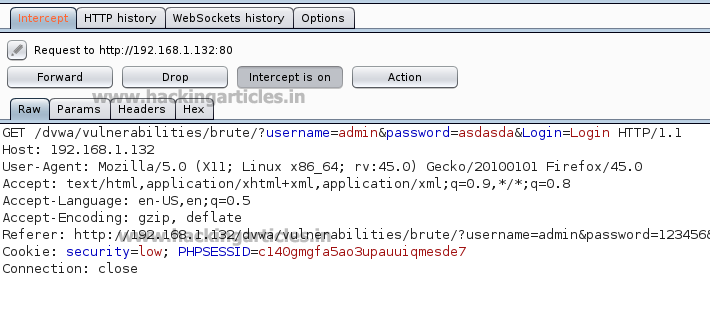
Raj Chandel

raj chandel

RAJ CHANDEL

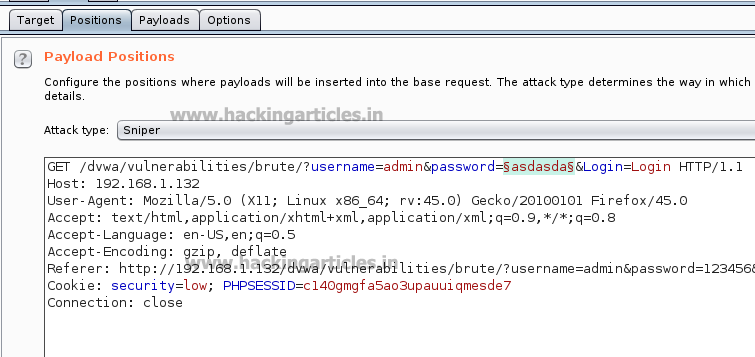
Raj chandel

First, we intercept the request of the login page in the **DVWA LAB**, where we have given a random username and a random password. Then click on login , the burp suite will capture the request of the login page in the intercept tab. Send the captured request to the **Intruder** by right clicking on the space and selecting **Send to Intruder** option or simply press **ctrl + i**.

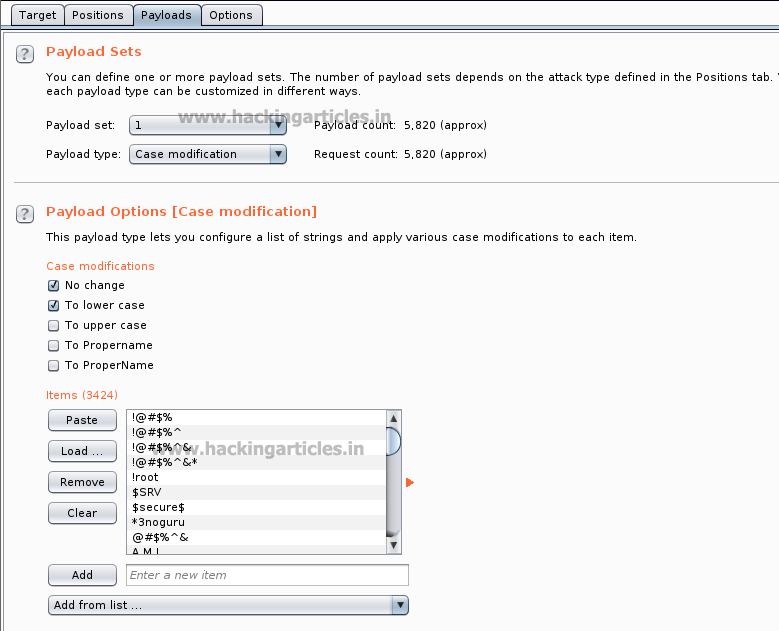


Now open the **Intruder tab** then select **positions** and you can observe the highlighted password and follow the given below step for selecting payload position.

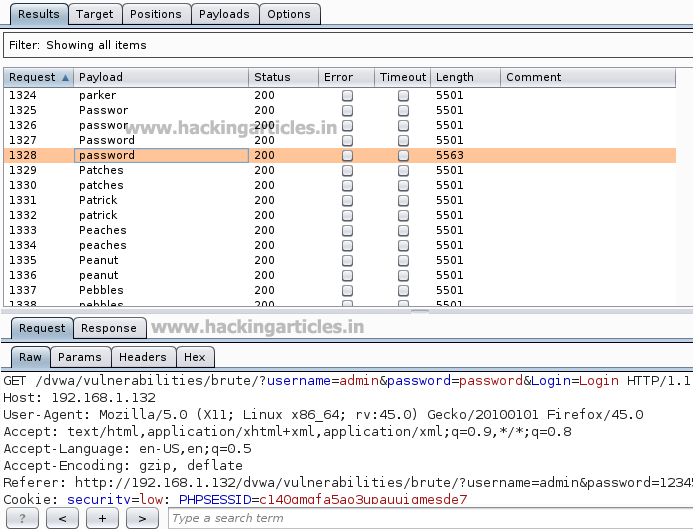
* Press on the **Clear button** given at right of window frame.
* Now we will select the fields where we want to attack and i.e. the password filed and click on **Add button.**
* Choose the **Attack type** as
* In the given below image we have selected  password that means we will need one dictionary file  for password.



Then select the “Payload” type as **Case Modification,** we have selected the **No change** and **to lower case** fields in the “payload options” of the case modification as shown in the image. We have added a default **Password dictionary** from the **Add from list** field in the payload options. Select **Start Attack** in the **Intruder menu** as shown in the image.



Now the burp suite will do its work, match the password and will give you the correct password. The moment it will find the correct value, it will change the value of length as shown.



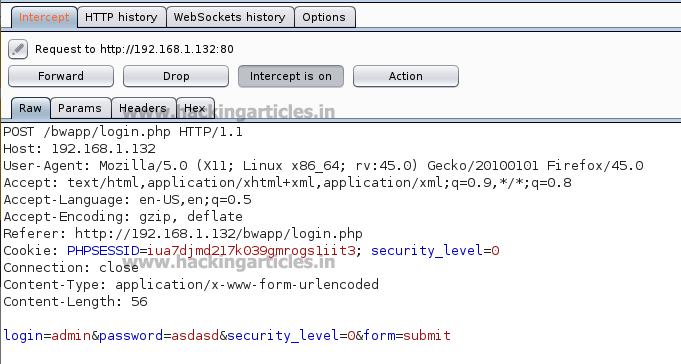
**Numbers**

This type of payload generates numeric payloads within a given range and in a specified format.

The following options are available in this payload:

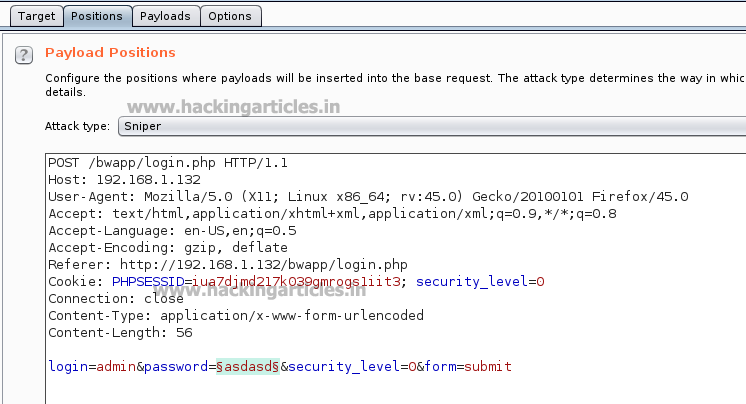
* Number range:
* **Type** – the type options describes that the numbers should be generated sequentially or randomly.
* **From** – If numbers are being generated sequentially, this is the value of the first number that will be generated.
* **To** – If numbers are being generated sequentially, this value of the last number that will be generated. It is said as the highest possible number that may be randomly generated.
* **Step** – the step option is used when numbers are being generated sequentially and specifies the increment in the successive numbers.
* **How many** – This option is available when numbers are being generated randomly, and specifies the number of payloads that will be generated

First, we intercept the request of the login page in the **Bwapp Lab**, where we have given a random username and a random password. Then click on login, the burp suite will capture the request of the login page.

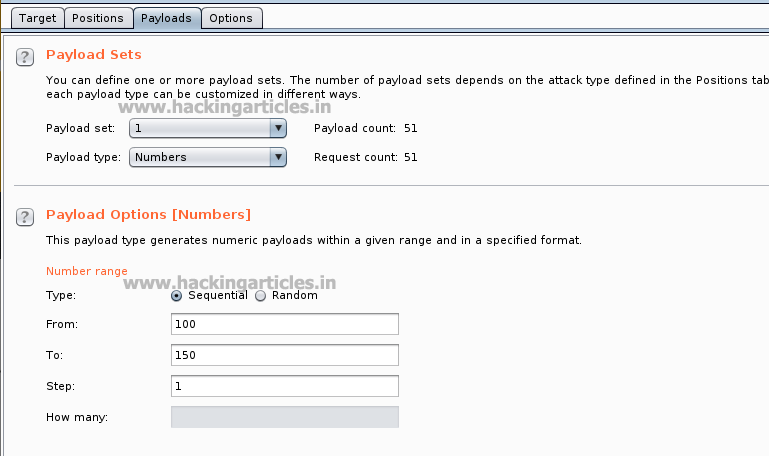


Send the captured request to the **Intruder** and follow given below step. Now open the **Intruder tab** then select **positions** and you can observe the highlighted password and follow the given below step for selecting payload position.

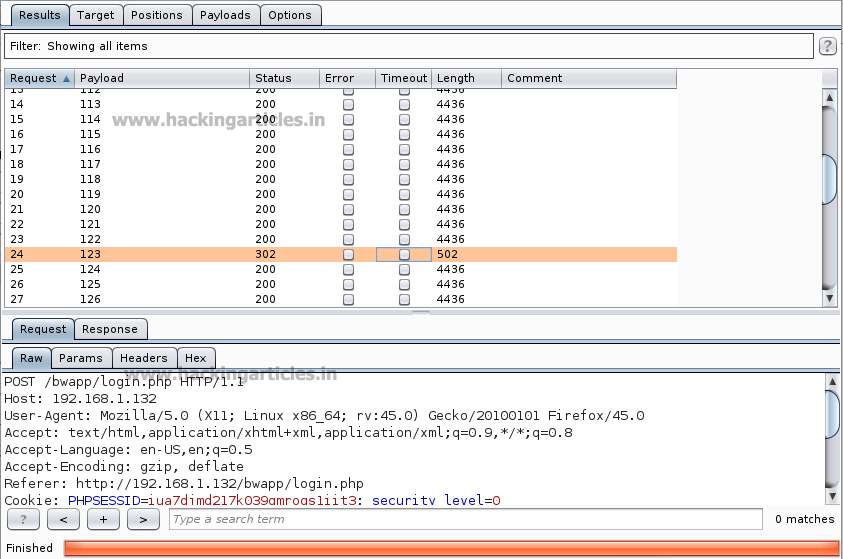
* Press on the **Clear button** given at right of window frame.
* Now we will select the fields where we want to attack and i.e. the password filed and click on **Add button.**
* Choose the **Attack type** as
* In the given below image we have selected  password that means we will need one dictionary file  for password.



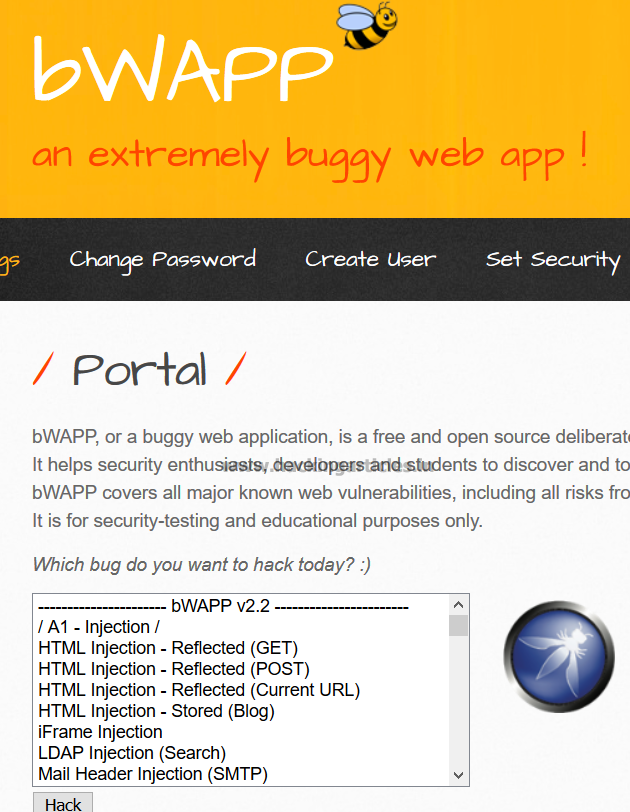
Then select the **Payload type** as **Numbers** where we have set the **number range from 100 to 150** and we have set the **step as 1** as shown in the image**,** select **Start Attack** in the **Intruder menu**.



Now the burp suite will do its work, match the password and will give you the correct password. The moment it will find the correct value, it will change the value of length as shown.



As the password matches with a number which is between the given number range. And to confirm the password matched, we will give the password in the **Bwapp LAB login page**, which will successfully log us into the **Bwapp lab**. This shows our success in the attack.



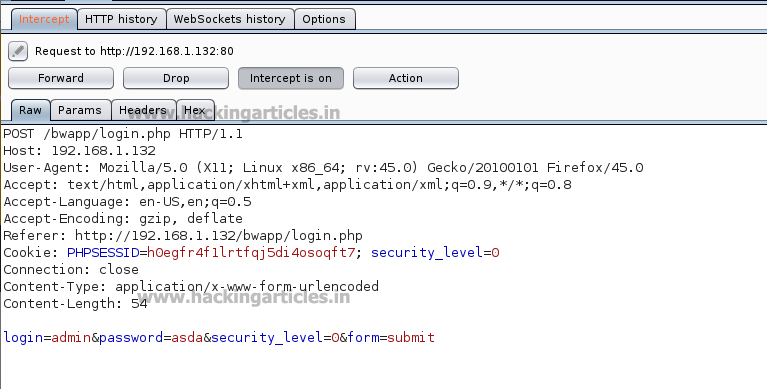
**Brute Forcer**

This type of payload generates a payload of specified lengths that contain all permutations of list of characters in the given string.

The following options are available:

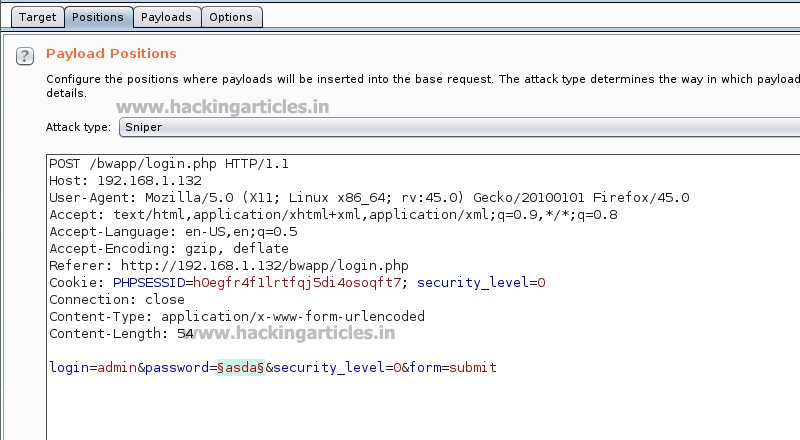
* **Character set** – The set of characters to be used in the payloads. Note that the total number of payloads increases exponentially with the size of this set.
* **Min length** – The length of the shortest payload.
* **Max length** – The length of the longest payload.

First, we intercept the request of the login page in the **Bwapp LAB**, where we have given a random username and a random password. Then click on login, the burp suite will capture the request of the login page.

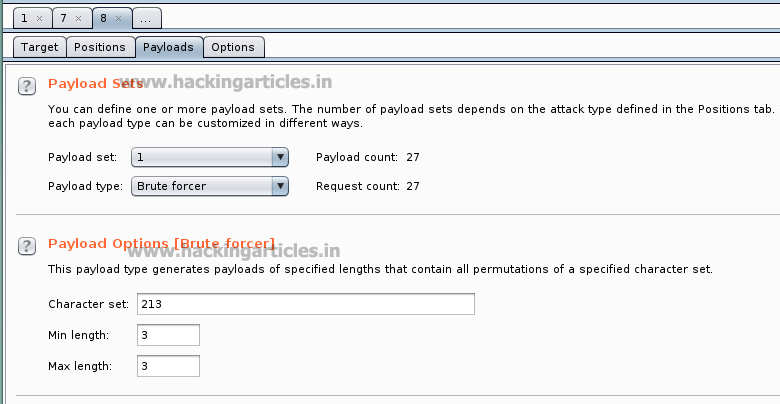


Send the captured request to the **Intruder** and follow given below step. Now open the **Intruder tab** then select **positions** and you can observe the highlighted password and follow the given below step for selecting payload position.

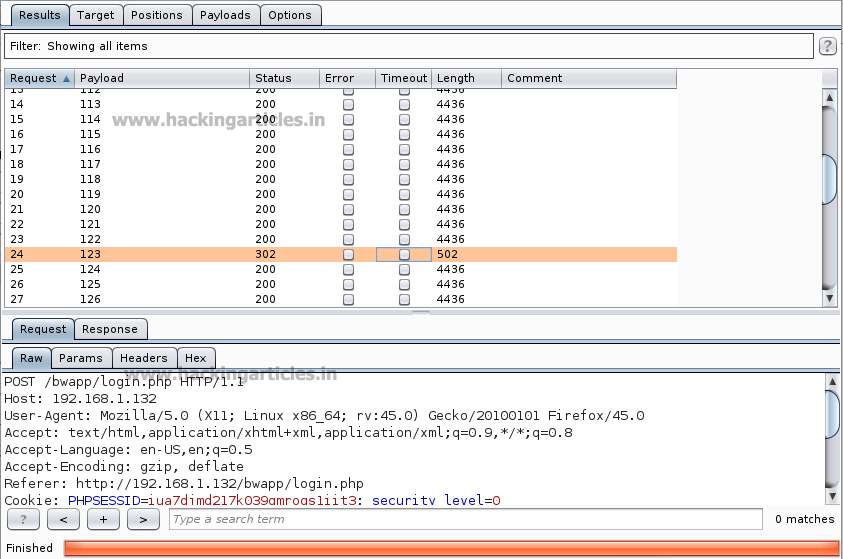
* Press on the **Clear button** given at right of window frame.
* Now we will select the fields where we want to attack and i.e. the password filed and click on **Add button.**
* Choose the **Attack type** as
* In the given below image we have selected  password that means we will need one dictionary file  for password.



Then select the “Payload type” as **Brute Forcer** where we can give any kind of input into the “character set” as shown in the figure , as we have given **213** and we have set the Min length as 3 and Max length as 3 as shown in the image. We can manually give the **Min length** and **Max length** as per your need. Select **Start Attack** in the **Intruder menu** as shown in the image.



Now the burp suite will do its work, match the password and will give you the correct password. The moment it will find the correct value, it will change the value of length as shown.



**Great!!** We have used Top 5 payloads of Burpsuite for login page brute force attack successfully.

**Note: In this articles (part-1) we will be performing top 5 payload types and the rest of the payload types will be discussed in the (part-2) of this article.**

Beginners Guide to Burpsuite Payloads (Part 2)

posted in[**Penetration Testing**](https://www.hackingarticles.in/category/penetration-testing/), [**Website Hacking**](https://www.hackingarticles.in/category/website-hacking/) on [**January 29, 2018**](https://www.hackingarticles.in/beginners-guide-burpsuite-payloads-part-2/) by [**Raj Chandel**](https://www.hackingarticles.in/author/raaz/)

SHARE

Save

In our [**previous**](https://www.hackingarticles.in/beginners-guide-burpsuite-payloads-part-1/) article part1, we had discussed how to perform a brute force attack on any web application server for making unauthorized login into it using some Payload of Burpsuite. In part 2 articles you will learn more about brute force attack with help of remaining BurpSuite payloads that might be helpful in other situation.

**Let’s Start!!**

**Character Substitution**

This type of payload allows to configure a list of strings and apply various character substitutions to each item. This type of payload is useful in password guessing attacks and generating common variations on dictionary words.

The UI of this payload allows you to configure a number of character substitutions. For each item, it will generate a number of payloads, which include all permutations of substituted characters according to the defined substitutions.

 For example, the default substitution rules states (which include **e > 4 and r > 5**), the item **“Raj Chandel”** will generate the following payloads:

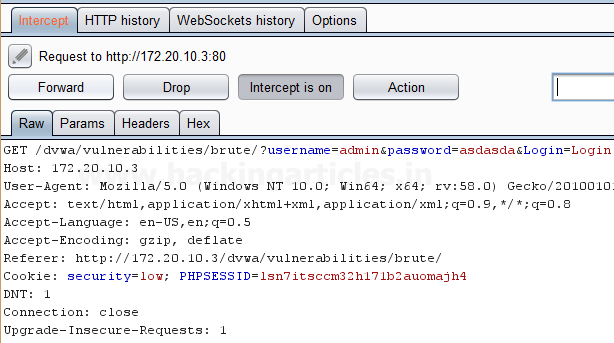
**raj chandel**

**5aj chandel**

**raj chand4l**

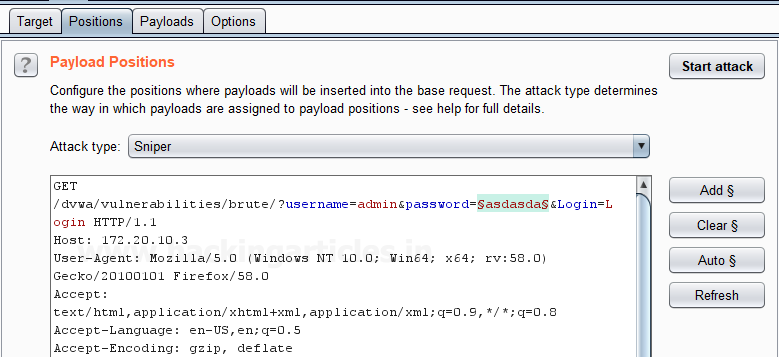
**5aj chand4l**

First, we have intercepted the request of the login page in the **DVWA LAB**, where we have given a default username and wrong password. Then click on login, the burp suite will capture the request of the login page in the intercept tab.



Send the captured request to the **Intruder** by clicking on the Action Tab and follow given below step. Now open the **Intruder tab** then select **Positions tab** and you can observe the highlighted password and follow the given below step for selecting payload position.

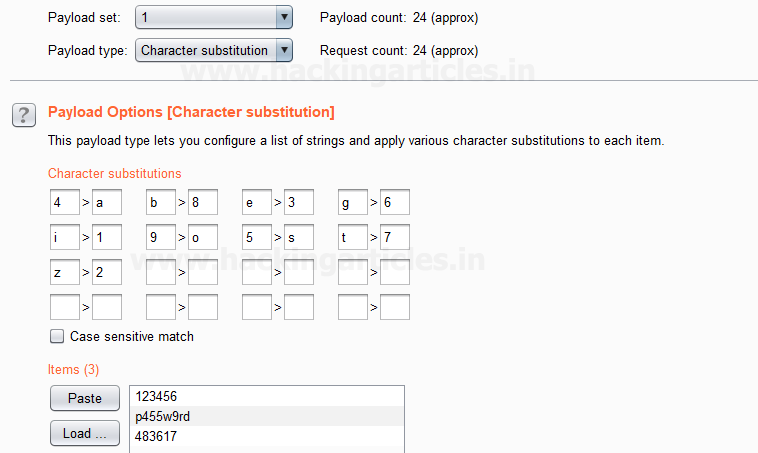
* Press on the **Clear button** given at right of the window frame.
* Now we will select the fields where we want to attack and i.e. the password filed and click on **Add button.**
* Choose the **Attack type** as
* In the given below image, we have selected a password that means we will need one dictionary files for a password.



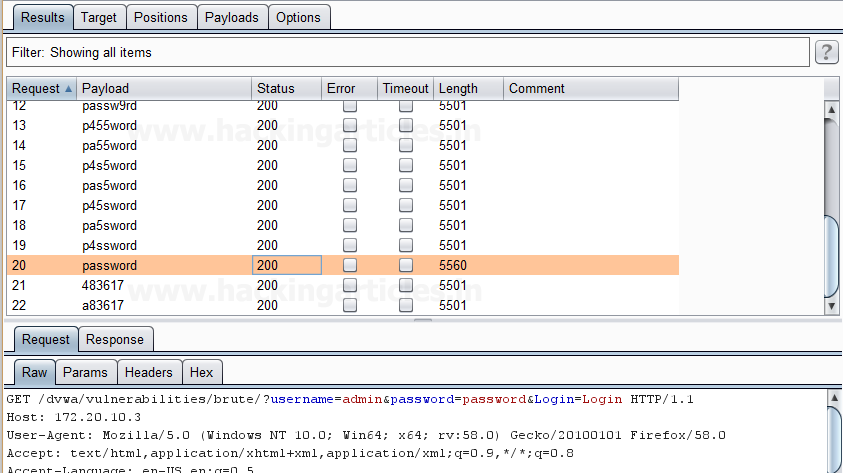
 Now click on **payloads option** after selecting payload position. Here we can add a dictionary by clicking on **Load option** or we can manually add **Strings** by clicking on the **Add option.**

Now we have substituted **4>a, 5>s, 9>o** as per our requirements to match the password and we have added the input as **p445w9rd** using the **Add option** which will substitute the character’s according to the **Defined substitution** as shown in the image.

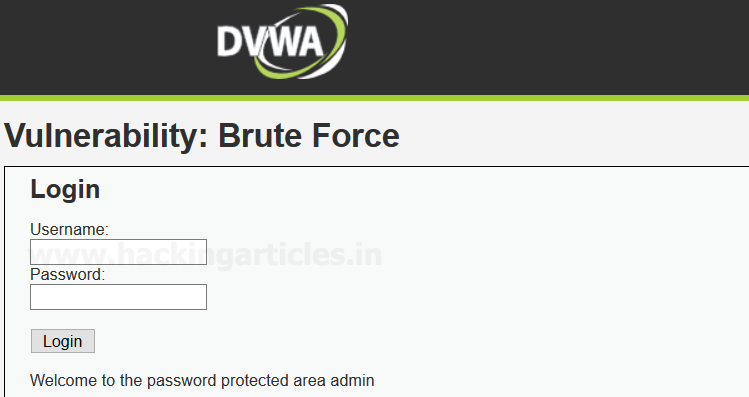
**Start Attack** in the **Intruder menu** as shown in the image.



Sit back and relax because now the burp suite will do its work, match the password and will give you the correct password. The moment it will find the correct value, it will change the value of length as shown.



 And to confirm the password matched, we will give the matched password in the **DVWA LAB login page**. We will see a message **“Welcome to the password protected area admin” which shows our success in the character substitution payload attack.**

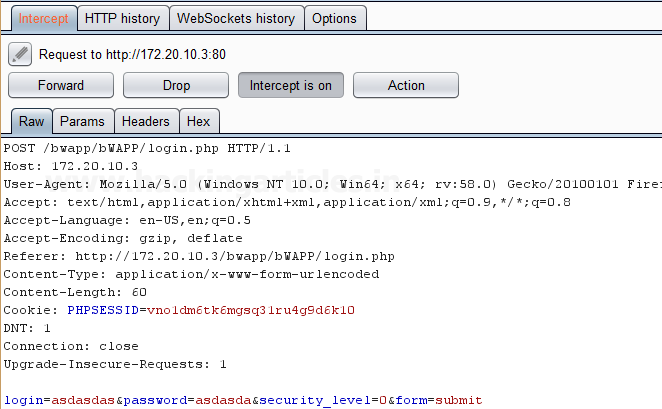


**Copy Other Payload**

This is a type of payload which can copy the value of the current payload to another payload position. It is very useful for attack types that have multiple payload sets such as cluster bomb, pitchfork, and battering ram. This payload type can be useful in various situations, for example:

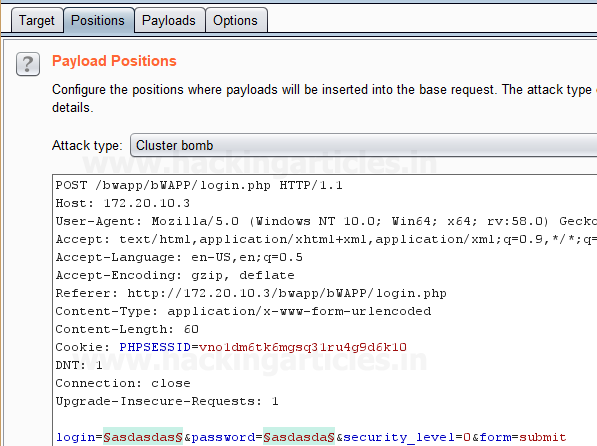
* Suppose we are using two different parameters and we want to attack at two different fields, therefore we can set different “payload types” at multiple “payload sets” inside burpsuite payload configuration as per our attack type as it allows us to simply use the same dictionary for both payloads that we have set at particular position by giving the position of the payload we want to copy. It will execute the complete payload which is set at a specific position.

First, we have intercepted the request of the login page in the **Bwapp LAB**, where we have given wrong username and password. Then click on login, the burp suite will capture the request of the login page in the intercept tab.

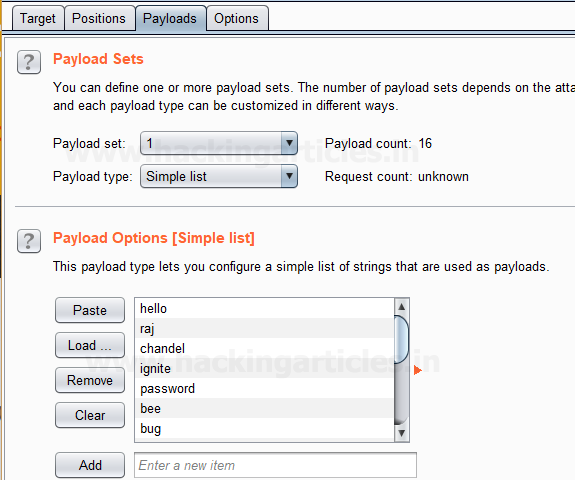


Send the captured request to the **Intruder** by clicking on the Action Tab and follow given below step. Now open the **Intruder tab** then select **Positions tab** and you can observe the highlighted username and password and follow the given below step for selecting payload position.

* Press on the **Clear button** given at right of the window frame.
* Now we will select the fields where we want to attack which is the username and password and click on **Add button.**
* Choose the **Attack type** as **Cluster Bomb.**
* In the given below image, we have selected username and password that means we will need two dictionary files i.e. one for username and second for a password.

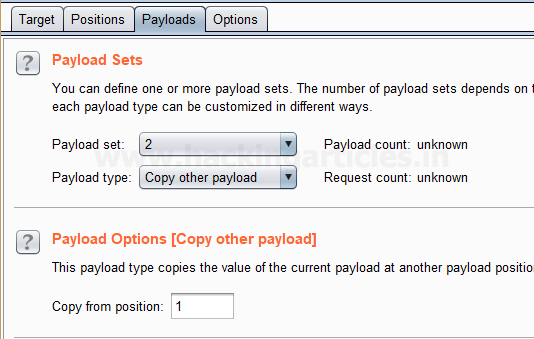


Now click on **payloads option** after selecting payload position, here we need to add a dictionary which will use for both payload set. Then select the **Payload type** as **Simple list** for **Payload Set ‘1’** which will attack at the username field**.**



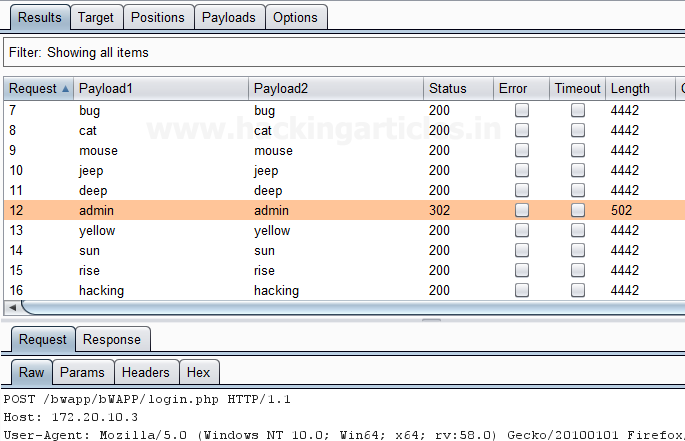
Now to attack at the password field we will select **Payload type** as **Copy other payloads** for **Payload Set ‘2’** because we want to attack the **same payload type** at payload set 2 which will **copy the dictionary** given for **payload set 1** to attack.

Select **Start Attack** in the **Intruder menu** as shown in the image.



Sit back and relax because now the burp suite will do its work, match the username and password which will give you the correct username and password. The moment it will find the correct value, it will change the value of length as shown in the image.

And to confirm the password matched, you can give the matched password in the **BWAPP LAB login page**.



**Username Generator**

This type of payload allows you to set up a list of names or email addresses and can produce usernames from given specific schemes.

For example, Let’s take a username “raj chandel” which can give results in up to 115 possible usernames, some combination is as follows :

rajchandel

raj.chandel

chandelraj

chandel.raj

chandel

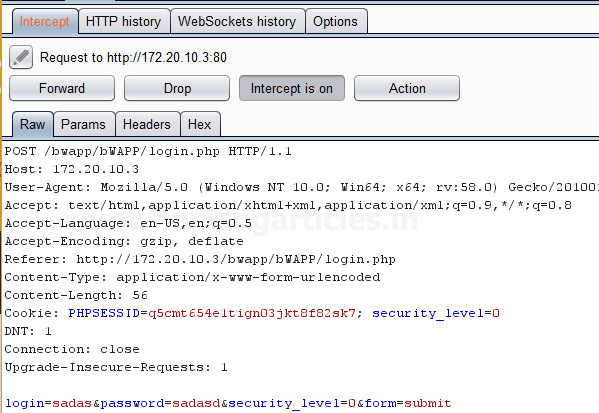
raj

rajc

etc…

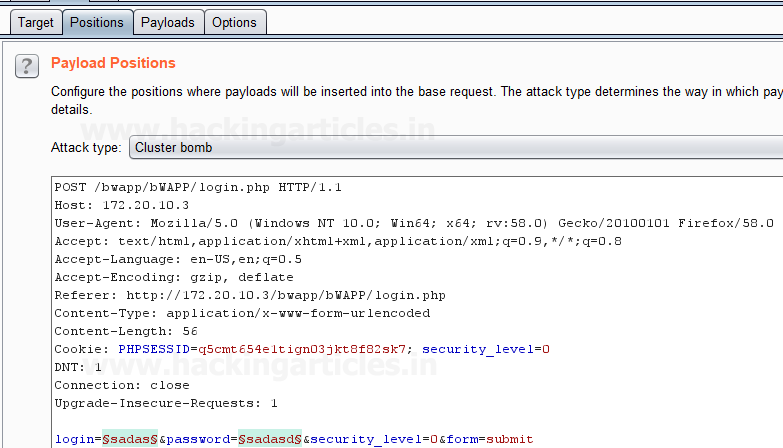
This type of payload is useful to target at a specific user, where you do not know the username or email address scheme of the user which is being used in a specific application.

First, we have intercepted the request of the login page in the **Bwapp LAB**, where we have given wrong username and password. Then click on login, the burp suite will capture the request of the login page in the intercept tab.

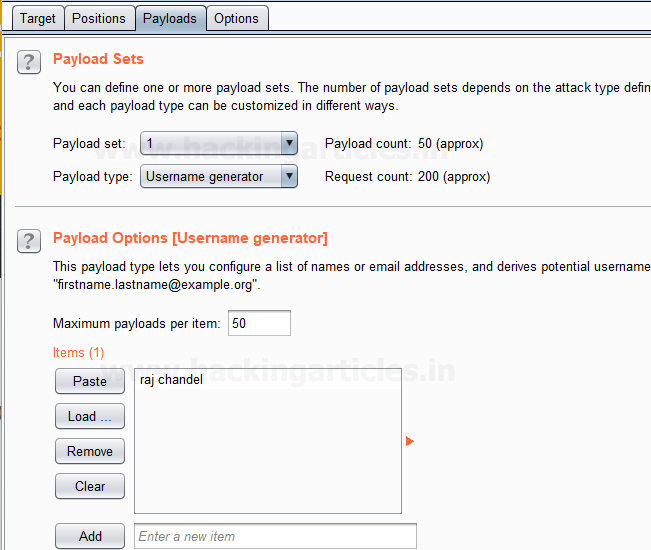


Send the captured request to the **Intruder** by clicking on the Action Tab and follow given below step. Now open the **Intruder tab** then select **Positions tab** and you can observe the highlighted username and password and follow the given below step for selecting payload position.

* Press on the **Clear button** given at right of the window frame.
* Now we will select the fields where we want to attack which is the username and password and click on **Add button.**
* Choose the **Attack type** as **Cluster Bomb.**
* In the given below image, we have selected username and password that means we will need two dictionary files i.e. one for username and second for the password.

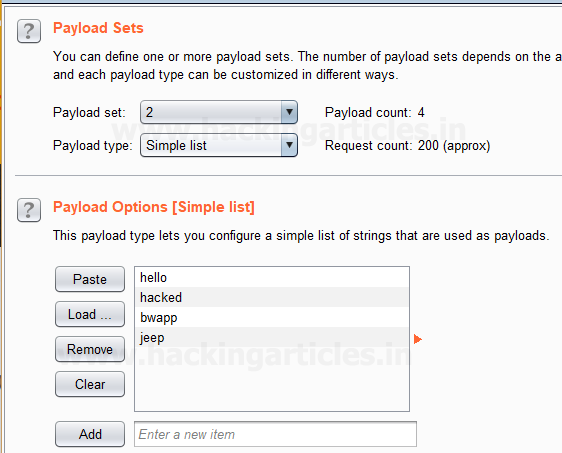


Then select the **Payload type** as “Username Generator” for **Payload Set ‘1’** which will attack at the username field, we have a given input string “raj chandel” by using the **Add option** as shown in the image, which will use different permutations on that input string given to match the correct username.

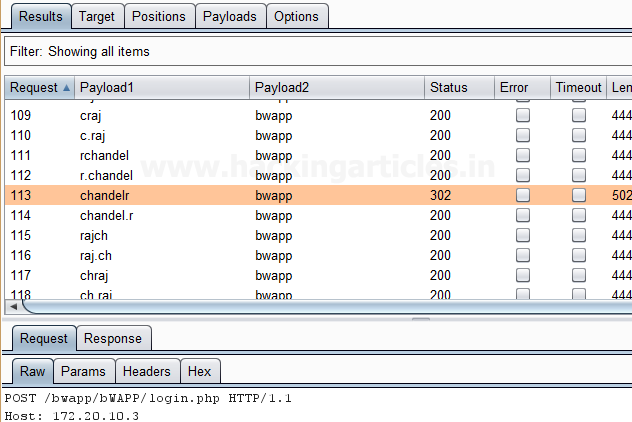


Now to attack at the password field we will select **Payload type** as **Simple list** for **Payload Set ‘2’** for which we have added a **dictionary** manually created by us by using the **Load option.**

Select **Start Attack** in the **Intruder menu** as shown in the image.



Sit back and relax because now the burp suite will do its work, match the username and password which will give you the correct username and password. The moment it will find the correct value, it will change the value of length as shown in the image.



**Dates**

This type of payload generates date payloads within a given range and in a specified format. This type of payload is can be used in data mining or brute forcing.

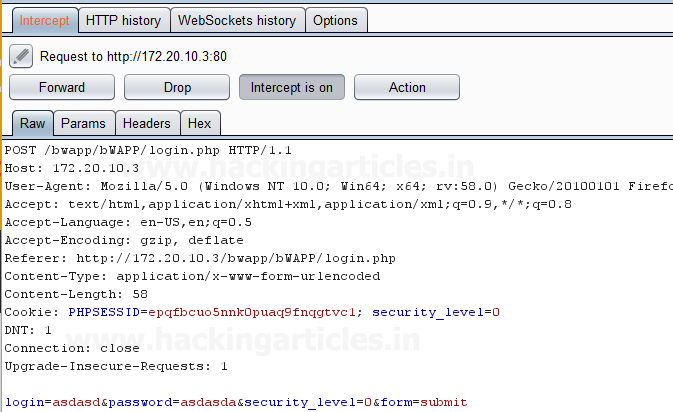
For example, it can be used to guess a user’s birth date, wedding date, anniversary date etc which can be used to brute force the security questions for an application or web applications, or it can use to brute force the password of user’s, where the user uses dates as their password.

The following options are available in this type of payload:

* **From** – This is said as the first date which will be generated.
* **To** – This is said as the last date which will be generated.
* **Step** – This is said as an increase between sequential dates, days, weeks, months or years. It should be a positive value.
* **Format** – This is said as the format in which dates can be represented. we can select from different predefined date formats, or we can make our own custom date format as per our requirement. Some example of the date format is given below:

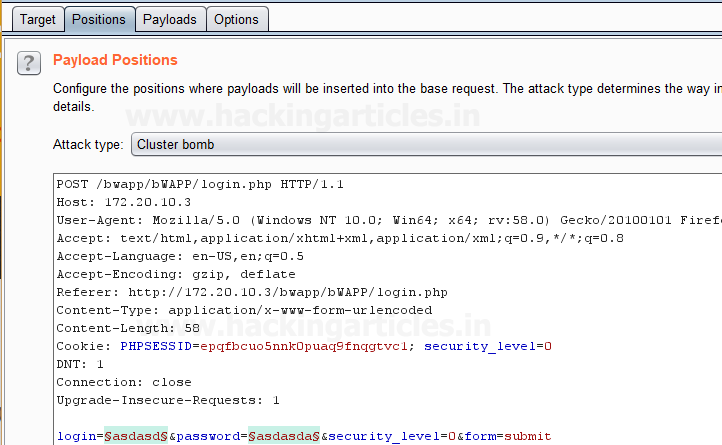
|  |  |
| --- | --- |
| E | Mon |
| EEEE | Monday |
| D | 2 |
| dd | 02 |
| M | 9 |
| MM | 09 |

Repeat the same to intercept the request of the login page in the **Bwapp LAB**, where we have given wrong username and password. Then click on login, the burp suite will capture the request of the login page in the intercept tab.

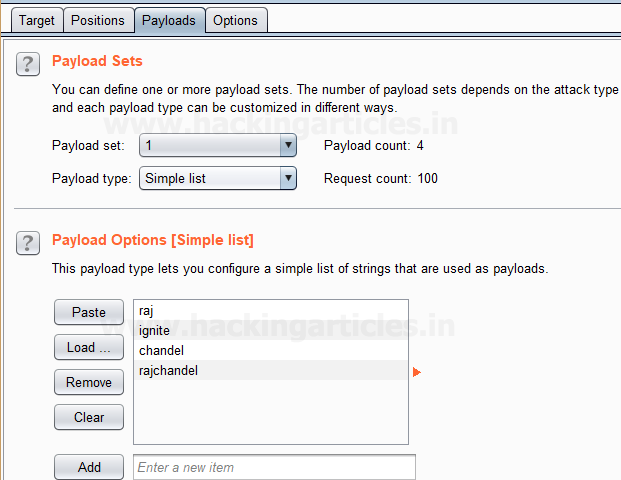


Send the captured request to the **Intruder** by clicking on the Action Tab and follow given below step. Now open the **Intruder tab** then select **Positions tab** and you can observe the highlighted username and password and follow the given below step for selecting payload position.

* Press on the **Clear button** given at right of the window frame.
* Now we will select the fields where we want to attack which is the username and password and click on **Add button.**
* Choose the **Attack type** as **Cluster Bomb.**
* In the given below image, we have selected username and password that means we will need two dictionary files i.e. one for username and second for the password.



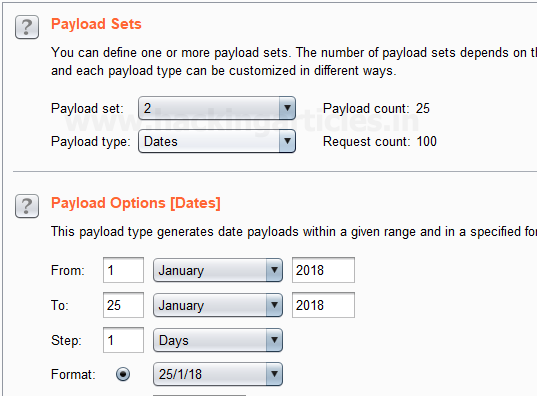
Then select the **Payload type** as **Simple list** for **Payload Set ‘1’** which will attack at the username field where we have given a dictionary as an input string as shown in given below image.



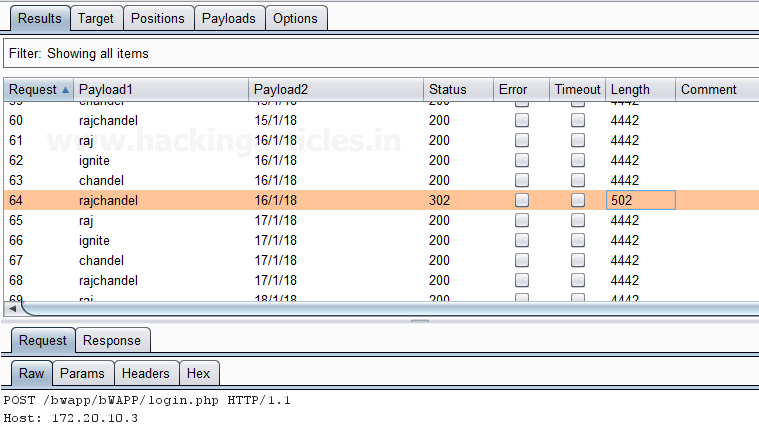
Now to attack at the password field we will select **Payload type** as **Dates** for **Payload Set ‘2’** because we are guessing the user might have its **birth date** or **any other date** as a password**.**

After this, we have set the inputs for **Payload set ‘2’** in the fields given in the payload options such as **FROM, TO, STEP and FORMAT** as shown in the image.

Now Select **Start Attack** in the **Intruder menu** for brute force attack.



Sit back and relax because now the burp suite will do its work, match the username and password which will give you the correct username and password. The moment it will find the correct value, it will change the value of length as shown in the image.



**Author**: Ashray Gupta is a Researcher and Technical Writer at Hacking Articles**.**He is a certified ethical hacker, web penetration tester and a researcher in nanotechnology. Contact [**Here**](https://www.linkedin.com/in/ashray-gupta-b77221b6/)

Payload Processing Rule in Burp suite (Part 1)

posted in[**Penetration Testing**](https://www.hackingarticles.in/category/penetration-testing/), [**Website Hacking**](https://www.hackingarticles.in/category/website-hacking/) on [**February 3, 2018**](https://www.hackingarticles.in/payload-processing-rule-burp-suite-part-1/) by [**Raj Chandel**](https://www.hackingarticles.in/author/raaz/)

SHARE

Save

Today we are going to discuss the “Payload Processing” option of Burpsuite which is advanced functionality comes under **Intruder Tab** for making brute force attack.

**Payload Processing**

Payload Processing can be defined as when payloads are generated using **payload types,** they can be further **manipulated or filtered** using various **processing rules** and **payload encoding**.

**Payload Processing Rules**

These rules are defined to perform a various processing task on each payload before it is used. These rules are executed in a sequence, and they can be used to help debug any problem with the configuration. Payload processing rules are useful in situations where you need to generate different payloads, or where we want to wrap payloads within a wider structure or encoding scheme.

There are 12 types of payload processing rules available:

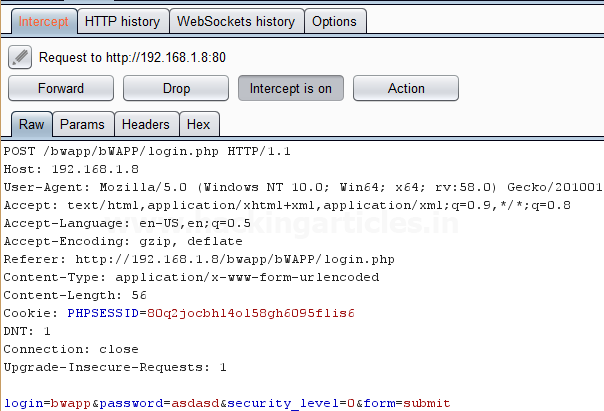
* **Add prefix**
* **Add suffix**
* **Match / Replace**
* **Substring**
* **Reverse substring**
* **Modify case**
* **Encode**
* **Decode**
* **Hash**
* **Add raw payload**
* **Skip if matches regex**
* **Invoke Burp extension**

**Let’s start!!**

**Add Prefix**

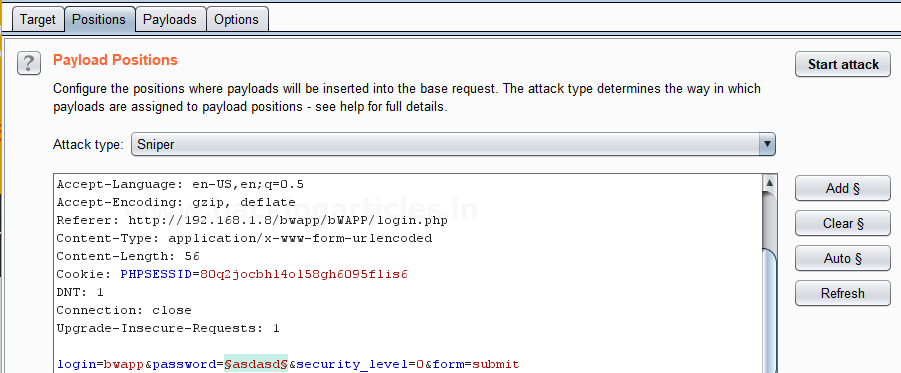
This processing rule adds up a prefix before the payload.

First, we have intercepted the request of the login page in the **Bwapp LAB**, where we have given default username and wrong password. Then click on login, the burp suite will capture the request of the login page in the intercept tab.

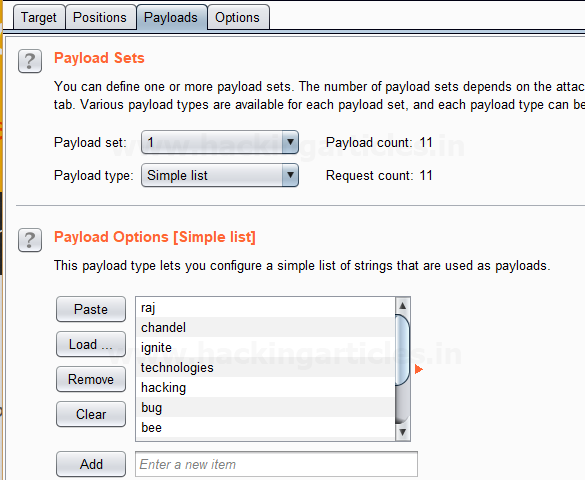


Send the captured request to the **Intruder** by clicking on the Action Tab and follow given below step. Now open the **Intruder tab** then select **Positions tab** and you can observe the highlighted password and follow the given below step for selecting payload position.

* Press on the **Clear button** given at right of the window frame.
* Now we will select the fields where we want to attack and i.e. the password filed and click on **Add button.**
* Choose the **Attack type** as **a sniper**
* In the given below image, we have selected a password that means we will need one dictionary files for a password.

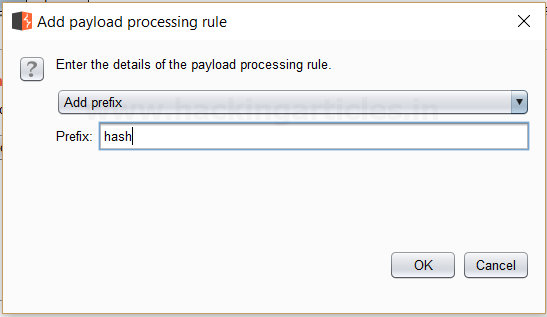


Now click on **payloads option** after selecting payload position. Then select the **Payload type** as **Simple list,** where we have added a dictionary by clicking on **Load** button. We can either load the dictionary or we can manually add input strings using the **Add button** in the **payload options** as shown in the image.

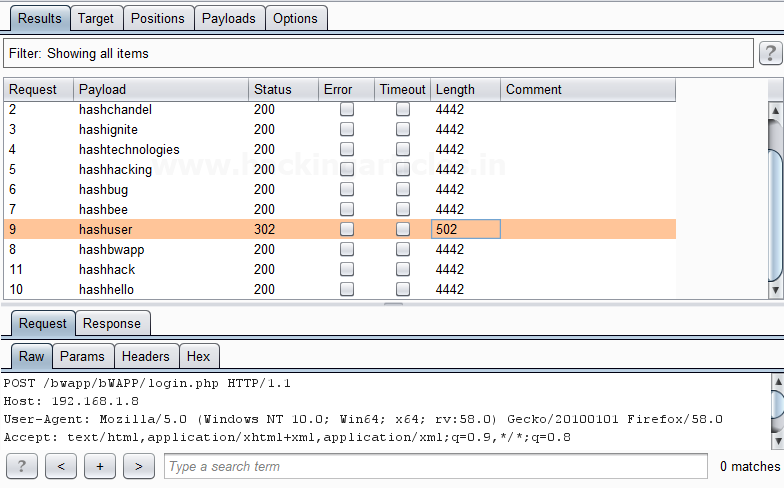


 Before executing the attack we have added a **payload processing** **rule** to the payload type which is **Add Prefix** and we have given an input string “hash” which is added as a **prefix** with every input strings in the dictionary, as shown in the **result window** of the **attack**.

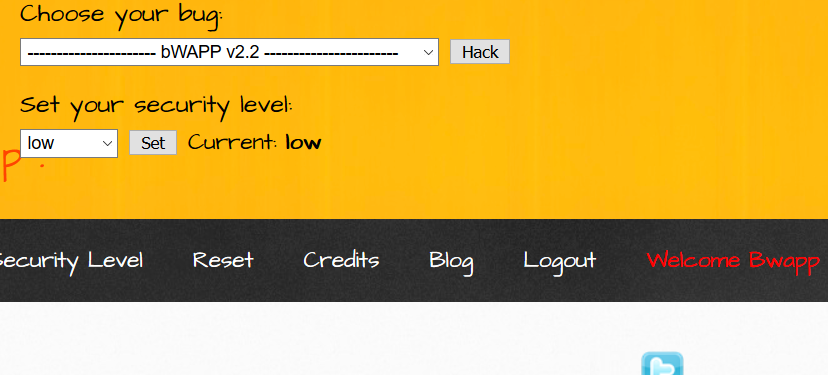
Select **Start Attack** in the **Intruder menu** as shown in the image.



Sit back and relax because now the burp suite will do its work, match the password which will give you the correct password. The moment it will find the correct value, it will change the value of length as shown in the image.



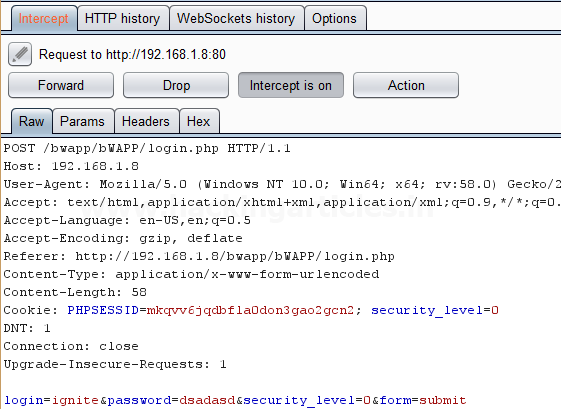
And to confirm the **password matched**, we will give the password in the **Bwapp LAB login page**, which will successfully log us into the **Bwapp lab**. This shows our success in the attack as shown in the image.



**Add Suffix**

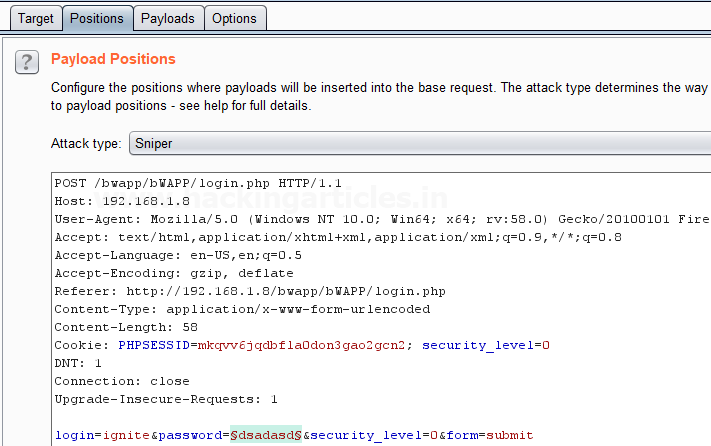
This processing rule adds up a suffix after the payload.

First, we have intercepted the request of the login page in the **Bwapp LAB**, where we have given default username and wrong password. Then click on login, the burp suite will capture the request of the login page in the intercept tab.

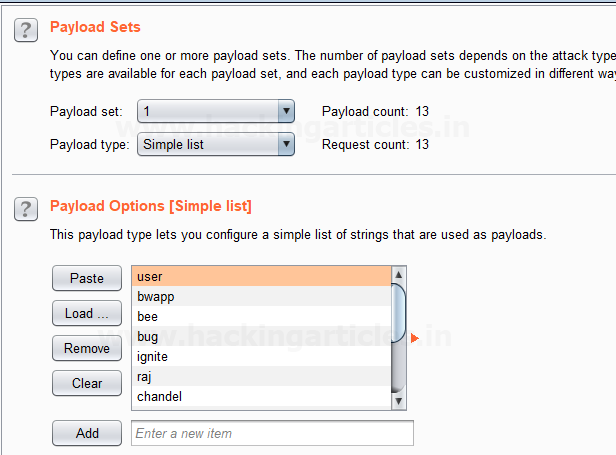


Send the captured request to the **Intruder** by clicking on the Action Tab and follow given below step. Now open the **Intruder tab** then select **Positions tab** and you can observe the highlighted password and follow the given below step for selecting payload position.

* Press on the **Clear button** given at right of the window frame.
* Now we will select the fields where we want to attack and i.e. the password filed and click on **Add button.**
* Choose the **Attack type** as a **sniper**
* In the given below image, we have selected a password that means we will need one dictionary files for a password.

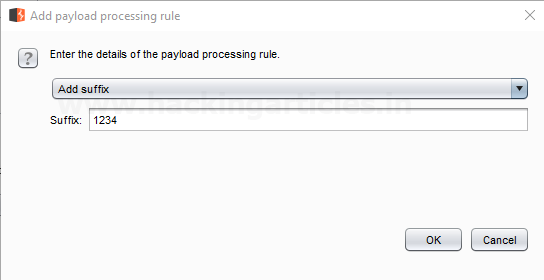


Now click on **payloads option** after selecting payload position. Then select the **Payload type** as **Simple list,** where we have added a dictionary by clicking on **Load** button. We can either load the dictionary or we can manually add input strings using the **Add button** in the **payload options** as shown in the image.



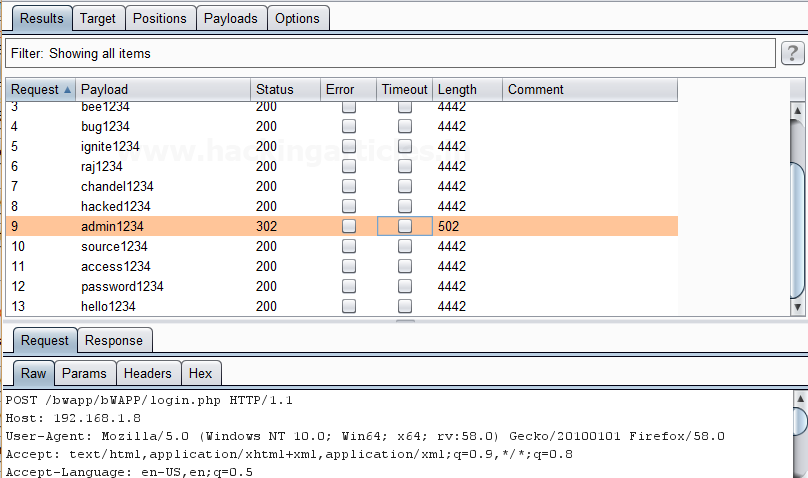
Before executing the attack we have added a **payload processing rule** to the payload type which is **Add Suffix** and we have given an input string “1234” which is added as a **suffix** with every input strings in the dictionary, as shown in the **result window** of the **attack**.

Select **Start Attack** in the **Intruder menu** as shown in the image.



Sit back and relax because now the burp suite will do its work, match the password which will give you the correct password. The moment it will find the correct value, it will change the value of length as shown in the image.

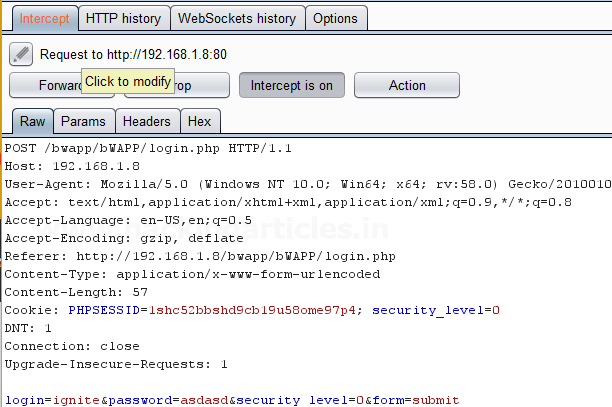
Use this combination of username and password for login to verify your brute force attack for the correct password.



**Match / Replace**

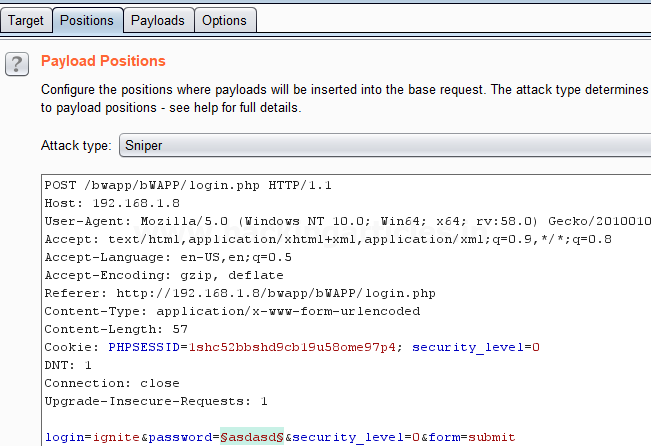
This processing rule is used to replace any part of the payload that match a specific regular expression, with a string.

First, we have intercepted the request of the login page in the **Bwapp LAB**, where we have given default username and wrong password. Then click on login, the burp suite will capture the request of the login page in the intercept tab.

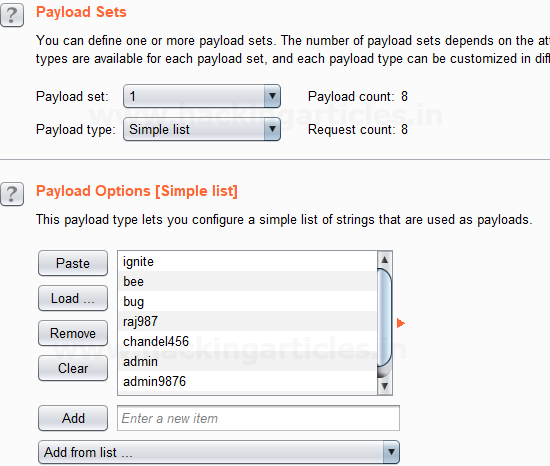


Send the captured request to the **Intruder** by clicking on the Action Tab and follow given below step. Now open the **Intruder tab** then select **Positions tab** and you can observe the highlighted password and follow the given below step for selecting payload position.

* Press on the **Clear button** given at right of the window frame.
* Now we will select the fields where we want to attack and i.e. the password filed and click on **Add button.**
* Choose the **Attack type** as **the sniper**
* In the given below image, we have selected a password that means we will need one dictionary files for the password.

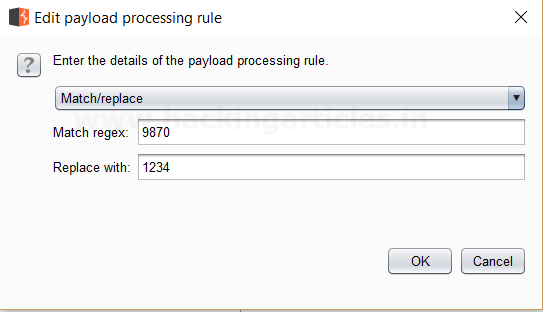


Now click on **payloads option** after selecting payload position. Then select the **Payload type** as **Simple list,** where we have added a dictionary by clicking on **Load** button. We can either load the dictionary or we can manually add input strings using the **Add button** in the **payload options** as shown in the image.



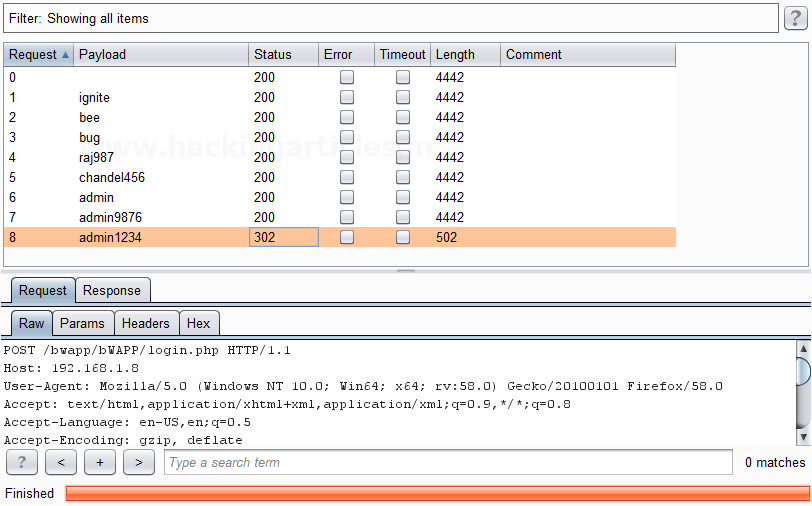
Before executing the attack we have added a **payload processing rule** to the payload type which is **Match / Replace** and we have given an input “9870” in the **Match Regex** which will match the input given with the input strings in the dictionary, if the there is a certain match than it will replace it with the input “1234” given in the **Replace with** as shown in the image.

Select **Start Attack** in the **Intruder menu**.



Sit back and relax because now the burp suite will do its work, match the password which will give you the correct password. The moment it will find the correct value, it will change the value of length as shown in the image.

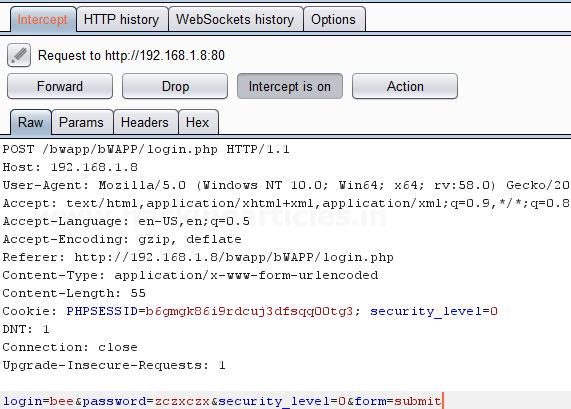
Use this combination of username and password for login to verify your brute force attack for the correct password.



**Substring**

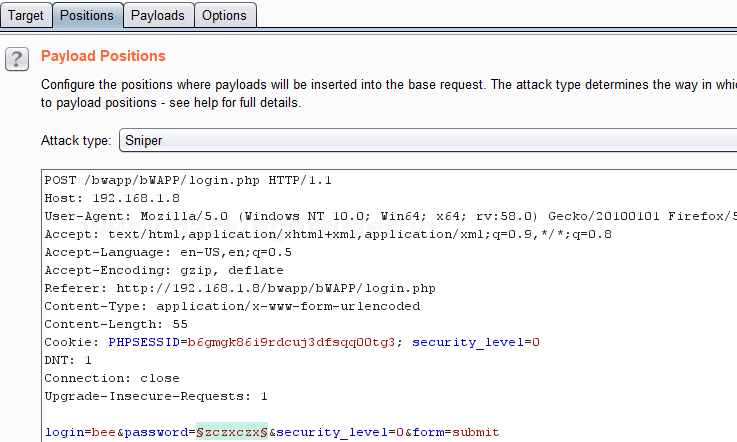
This processing rule is used to extracts a sub-portion of the payload, starting from a specified offset up to a specified length. Here the offset and length are counted from the front.

First, we have intercepted the request of the login page in the **Bwapp LAB**, where we have given default username and wrong password. Then click on login, the burp suite will capture the request of the login page in the intercept tab.

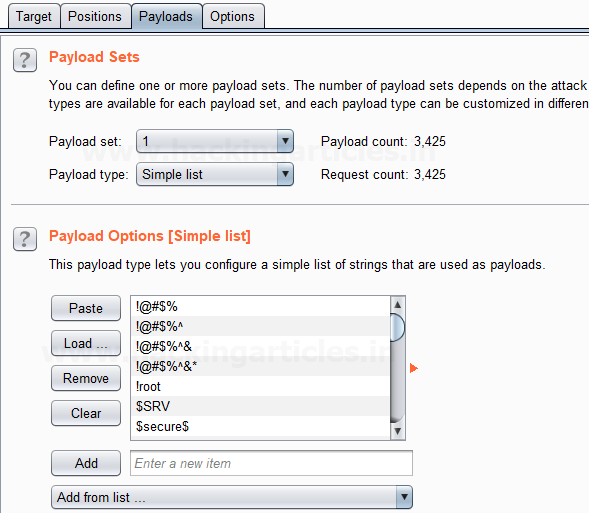


Send the captured request to the **Intruder** by clicking on the Action Tab and follow given below step. Now open the **Intruder tab** then select **Positions tab** and you can observe the highlighted password and follow the given below step for selecting payload position.

* Press on the **Clear button** given at right of the window frame.
* Now we will select the fields where we want to attack and i.e. the password filed and click on **Add button.**
* Choose the **Attack type** as **a sniper**
* In the given below image, we have selected a password that means we will need one dictionary files for the password.



Now click on **payloads option** after selecting payload position. Then select the **Payload type** as **Simple list,** where we have added a dictionary by clicking on **Load** button. Here we had added dictionary using the option “**Add from list**” as shown below in the given image.

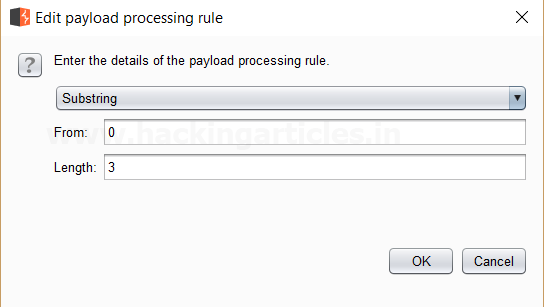


Before executing the attack we have added a **payload processing rule** to the payload type which is **Substring** and we have given an input “0” in **From option** which specifies the offset and an input “3” in the **Length option** which specifies the length of the input strings.

For example, if “password” is a word in a dictionary and we had applied above filter so it will place alphabet **p = 0; a = 1; s = 2 and s = 3** hence it will read only **pass** from whole word “password”.

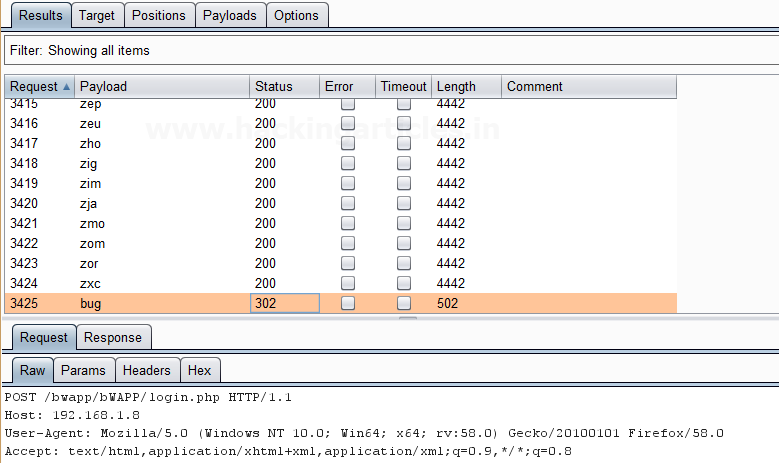
The length specified will select only those inputs having the specific length and other lower or greater length inputs are discarded as shown in the result window of the attack.

Select **Start Attack** in the **Intruder menu**.



Sit back and relax because now the burp suite will do its work, match the password which will give you the correct password. The moment it will find the correct value, it will change the value of length as shown in the image.

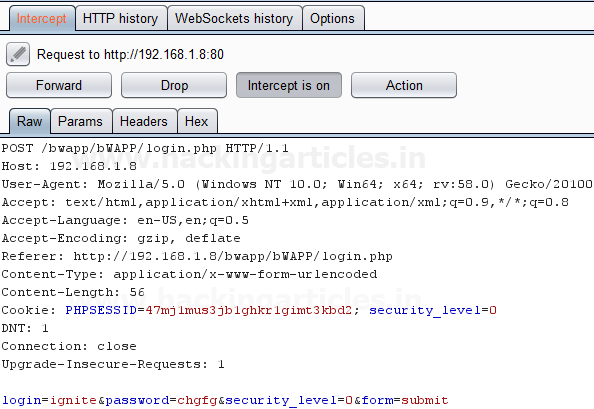
Use this combination of username and password for login to verify your brute force attack for the correct password.



**Reverse Substring**

This processing rule is used as a substring rule, but the end offset is specified counting backward from the end of the payload, and the length is counted backward from the end offset.

First, we have intercepted the request of the login page in the **Bwapp LAB**, where we have given default username and wrong password. Then click on login, the burp suite will capture the request of the login page in the intercept tab.

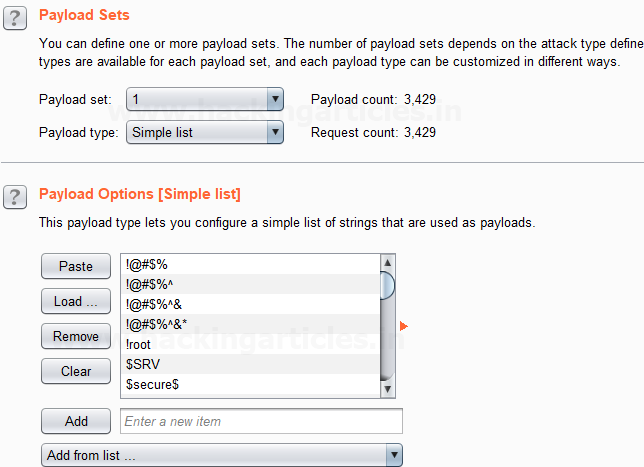


Send the captured request to the **Intruder** by clicking on the Action Tab and follow given below step. Now open the **Intruder tab** then select **Positions tab** and you can observe the highlighted password and follow the given below step for selecting payload position.

* Press on the **Clear button** given at right of the window frame.
* Now we will select the fields where we want to attack and i.e. the password filed and click on **Add button.**
* Choose the **Attack type** as the **sniper**
* In the given below image, we have selected a password that means we will need one dictionary files for a password.



 Now click on **payloads option** after selecting payload position. Then select the **Payload type** as **Simple list,** where we have added a dictionary by clicking on **Load** button. Here we had added dictionary using the option “**Add from list**” as shown below in the given image.



Before executing the attack we have added a **payload processing rule** to the payload type which is **Reverse Substring** and we have given an input “2” in **From option** which specifies the offset and an input “9” in the **Length option** which specifies the length of the input strings and they are similar to the Substring rule but it works from backward of an offset and the length is counted backward where the offset ends.

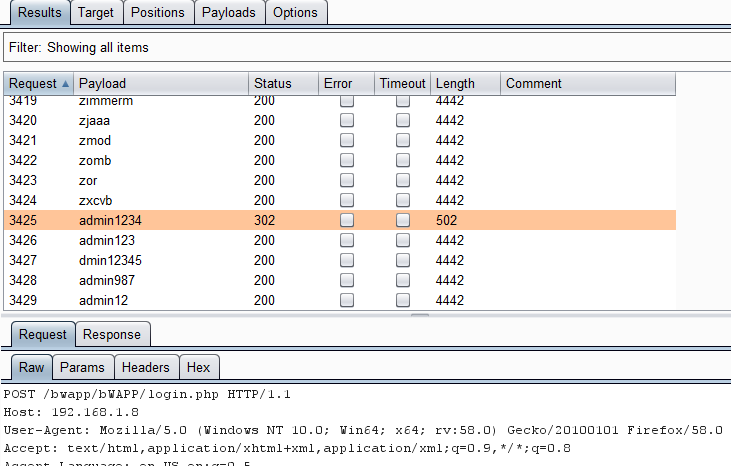
For example if “admin123456” is word in dictionary and we had applied above filter so it will place alphabet **4 = 0; 3 = 1 ; 2 = 2 ; 1 = 3 ; n = 4 ; i = 5 ; m = 6 ; d = 7 ; d = 8 ; a = 9**  hence it will read  only ‘**admin1234’** from whole word “admin123456”.

The length specified will select only those inputs having the specific length and other lower or greater length inputs are discarded as shown in the result window of the attack.

Select **Start Attack** in the **Intruder menu**.

Sit back and relax because now the burp suite will do its work, match the password which will give you the correct password. The moment it will find the correct value, it will change the value of length as shown in the image.

Use this combination of username and password for login to verify your brute force attack for the correct password.



**Modify Case**

This processing rule can be used to modify the case of the payload if needed. This rule has the same options available for the **Case Modification** payload type which we have explained in **Part-1** of the **Payload types article**.

Payload Processing Rule in Burp suite (Part 2)

posted in[**Website Hacking**](https://www.hackingarticles.in/category/website-hacking/) on [**February 6, 2018**](https://www.hackingarticles.in/payload-processing-rule-burp-suite-part-2/) by [**Raj Chandel**](https://www.hackingarticles.in/author/raaz/)

SHARE

Save

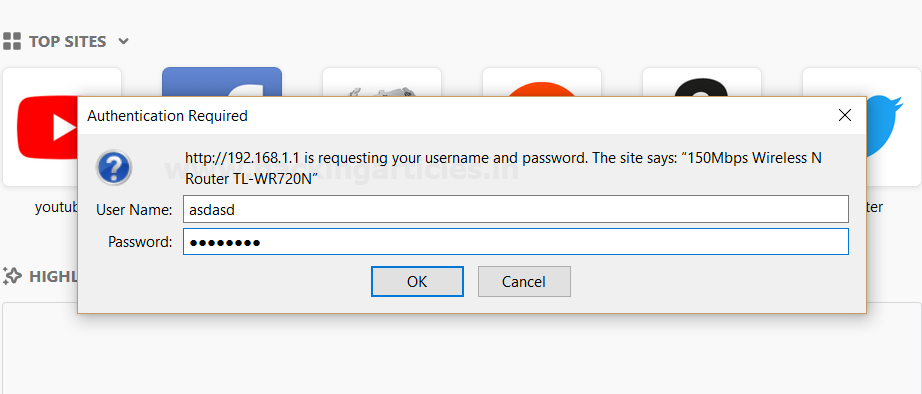
Today we are going to discuss “Payload Encoding” option followed by payload processing of Burpsuite which is advanced functionality comes under **Intruder Tab** for making brute force attack.

**Payload Encode**

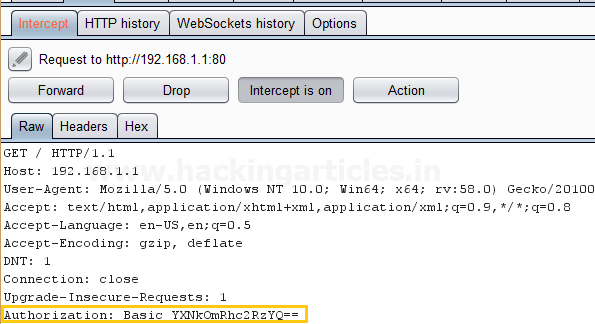
The processing rule can be used to encode the payload using various schemes such as URL, HTML, Base64, ASCII hex or constructed strings.

**Let’s start!!**

First, we have intercepted the request of the login page of the router by giving its **default IP** which is **192.168.1.1**, where we have given an invalid username and password. Then click on login, the burp suite will capture the request of the login page in the intercept tab.

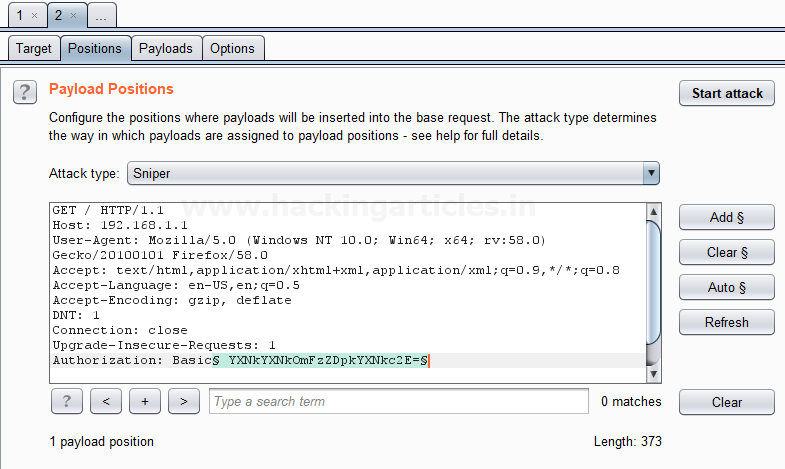


Thus the sent request will be captured by burp suite which you can see in the given below image. In the screenshot, I had highlighted some value in the last line. Here it tells the type of authentication provided by the router is **basic** and if you have read above theory of basic authentication I had described that it is **encoded** in **base 64**



Send the captured request to the **Intruder** by clicking on the Action Tab and follow given below step. Now open the **Intruder tab** then select **Positions tab** and you can observe the highlighted password and follow the given below step for selecting payload position.

* Press on the **Clear button** given at right of the window frame.
* Now **select** the **encoded value of authentication** for payload position and **click** to **ADD button** on the left side of the frame.
* Choose the **Attack type** as



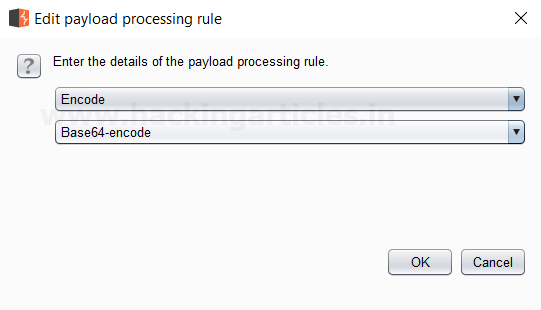
Now click on **payloads option** after selecting payload position. Then select the **Payload type** as **Simple list,** where we have added a dictionary by clicking on **Load** button. We can either load the dictionary or we can manually add input strings using the **Add button** in the **payload options** as shown in the image.

The base64 encoded value of Authentication is a combination of username and password now the scenario is to generate the same encoded value of authentication with help of user password dictionary, therefore I have made a **dictionary.**



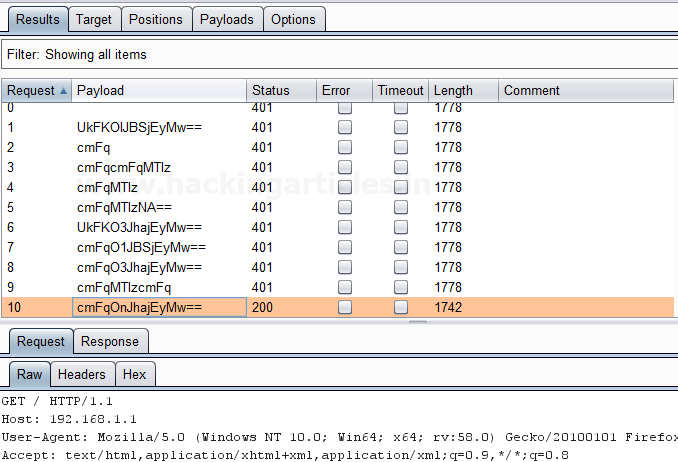
Before executing the attack we have added a **payload processing rule** to the payload type which is **Encode** and we have selected **“Base64 encode”** scheme because we know router takes the value in **Base64**.

Select **Start Attack** in the **Intruder menu** as shown in the image.



Sit back and relax because this will start brute force attack and try to match string for user authentication. In the screenshot, you can the **status** and **length**of the **highlighted value**is **different**from the rest of the values. This means we can use this encoded value to bypass the user authentication which occurs from request number 10. Now check the username and password of 10th line in the dictionary.

And to confirm the **username** and **password matched**, we will give the password in the **Router’s Login Page**, which will successfully log us into the **Router’s Configuration Page**. This shows our success in the attack as shown in the image.



**Decode**

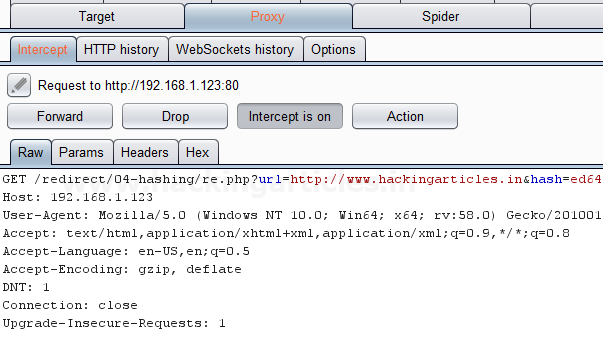
This processing rule can be used to decode the payload using various schemes: URL, HTML, Base64 or ASCII hex. As we know decoding is nothing but reversing the encoding. It can be used in the opposite way in which encoding is carried out.

**Hash**

This processing rule can be used to carry out a hashing operation on the payload. There are 7 types of hashing algorithms are available in this payload processing rule which is as follows:

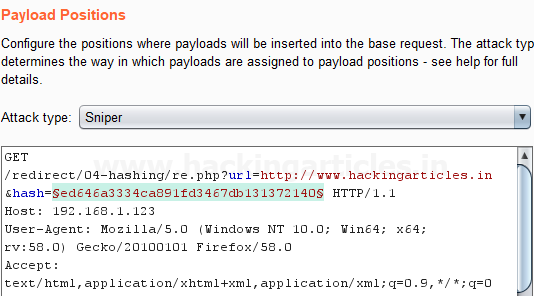
* SHA-384
* SHA-224
* SHA-256
* MD5
* MD2
* SHA
* SHA-512

First, we have intercepted the request of the **Redirection Link** designed to find **redirection vulnerabilities** in the **LAB** created by us and in the hash value of the URL we have given a wrong hash value of **HTTP://www.google.com** in place of the **actual hash value** of the **HTTP://www.hackingarticles.in** in the **URL** of the redirecting page. We have simply clicked on the Redirection link as shown in the image; the burp suite will capture the request of the redirecting page in the intercept tab.

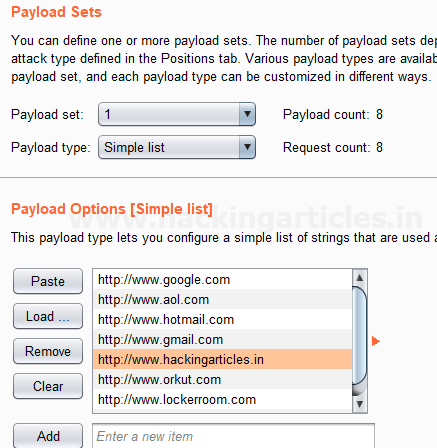


Send the captured request to the **Intruder** by clicking on the Action Tab and follow given below step. Now open the **Intruder tab** then select **Positions tab** and you can observe the highlighted password and follow the given below step for selecting payload position.

* Press on the **Clear button** given at right of the window frame.
* Now we will select the fields where we want to attack which is the **hash value** of the redirecting page and then click on **the Add button.**
* Choose the **Attack type** as a sniper.

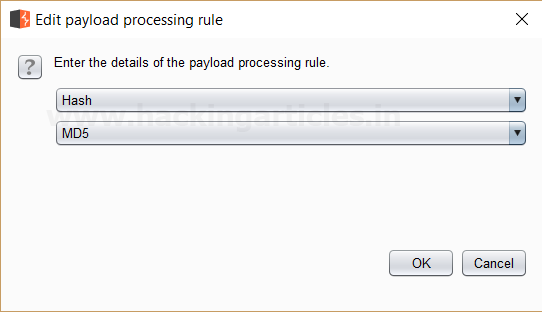


Then select the **Payload type** as **Simple list,** where we have added a dictionary by clicking on **Load** button. We can either load the dictionary or we can manually add input strings using the **Add button** in the **payload options** as shown in the image.

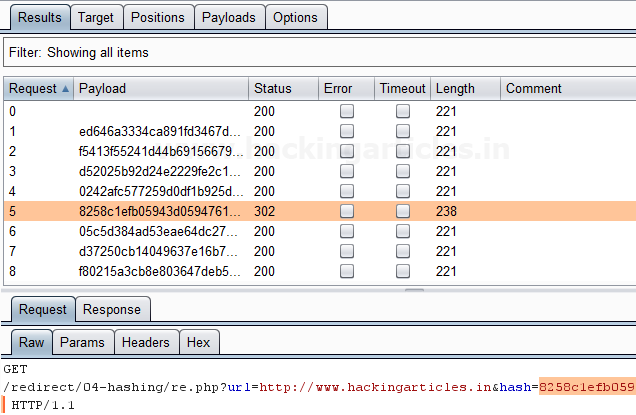


Before executing the attack we have added a **payload processing rule** to the payload type which is **Hash** and then we have selected **MD5** which is a commonly used algorithm for converting URL of the websites into a Hash MD5 value. As you can see the **input strings** of the dictionary are in a simple text form, but this processing rule converts it into Hash MD5 values which can be seen in **result window** of the **attack**.

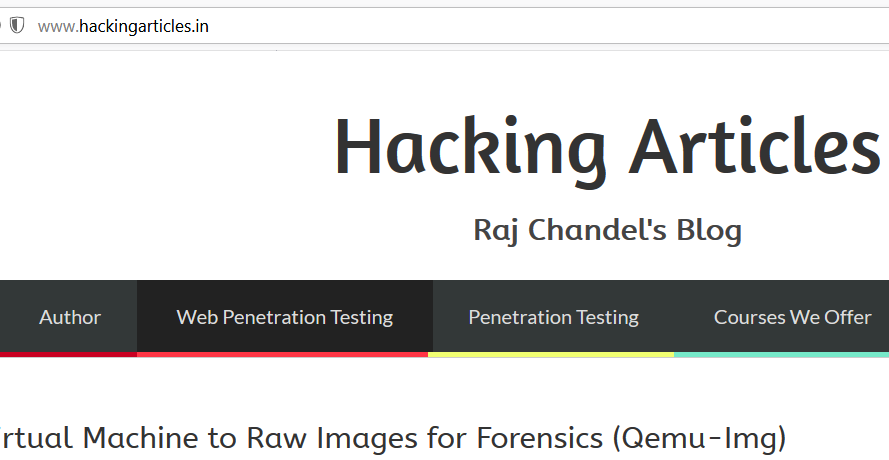
Select **Start Attack** in the **Intruder menu** as shown in the image.



Sit back and relax because now the burp suite will do its work, match the Hash MD5 of the Redirecting Page which will give you the correct MD5 value. The moment it will find the correct value, it will change the value of length as shown in the image.



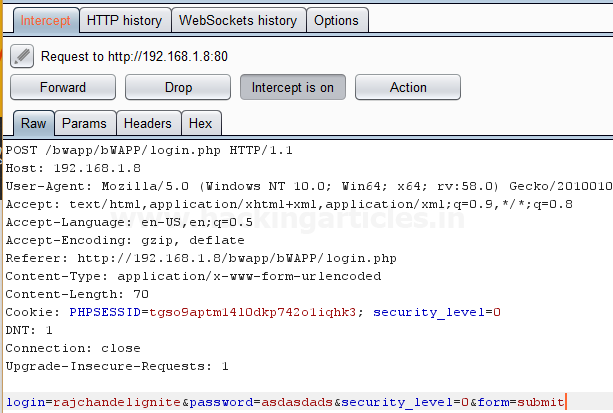
The **Hash MD5 value**, we will give the Hash value in the **URL** of the redirecting page which is **HTTP://www.hackingarticles.in**, which will successfully redirect us to **HTTP://www.hackingarticles.in**. This shows our success in the attack as shown in the image.



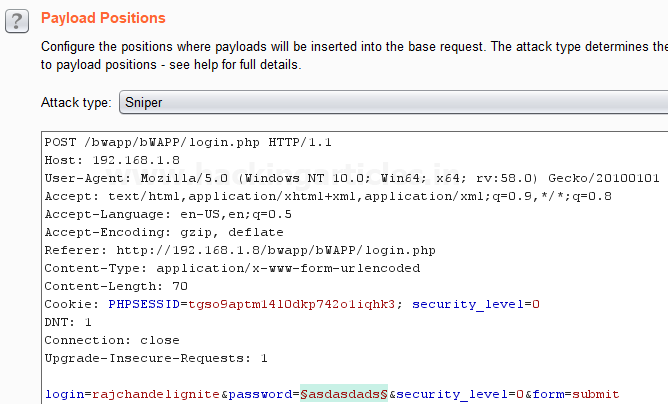
**Add Raw Payload**

This processing rule can be used to add raw payload value before or after the current processed value. For example, it can come in handy whenever we want to submit the same payload in both raw and hashed form.

First, we have intercepted the request of the login page in the **Bwapp LAB**, where we have given default username and wrong password. Then click on login, the burp suite will capture the request of the login page in the intercept tab.



Send the captured request to the **Intruder** by right-clicking on the space and selecting **Send to Intruder** option or simply press **Ctrl + i**. Now open the **Intruder tab** then select **Positions tab** and the following will be visible. Choose the **Attack type** as **Sniper.** Press on the **Clear button** as shown in the image. Now we will select the fields where we want to attack which is the password and click on **Add button.**



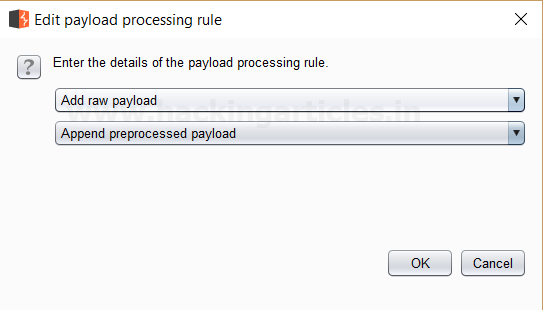
Send the captured request to the **Intruder** by clicking on the Action Tab and follow given below step. Now open the **Intruder tab** then select **Positions tab** and you can observe the highlighted password and follow the given below step for selecting payload position.

* Press on the **Clear button** given at right of the window frame.
* Now we will select the fields where we want to attack and i.e. the password filed and click on **Add button.**
* Choose the **Attack type** as
* In the given below image, we have selected a password that means we will need one dictionary files for a password.

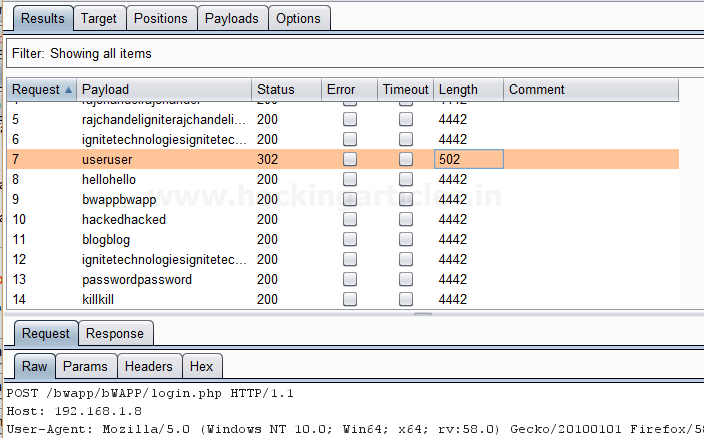


Before executing the attack we have added a payload processing rule to the payload type which is **Add Raw Payload** and then we have selected **Append Pre-processed Payload**. This adds a **raw payload value** before and after the **current processed value**. As you can see the **input strings** of the dictionary as a single input string is **repeated twice** which can be seen in **result window** of the **attack**.

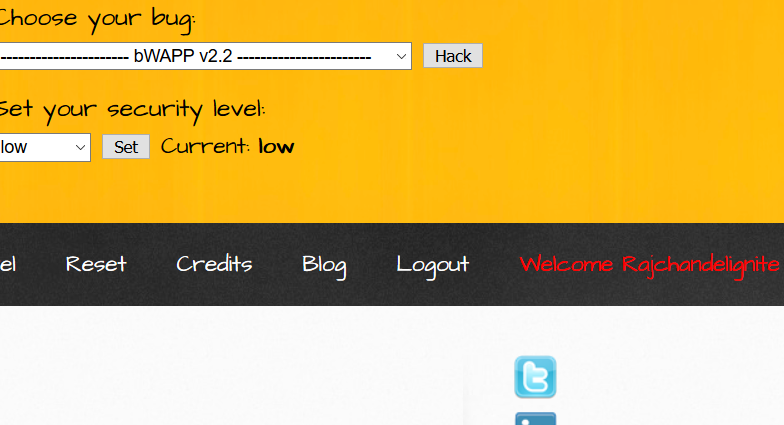
Select **Start Attack** in the **Intruder menu** as shown in the image.



Sit back and relax because now the burp suite will do its work, match the password which will give you the correct password. The moment it will find the correct value, it will change the value of length as shown in the image.



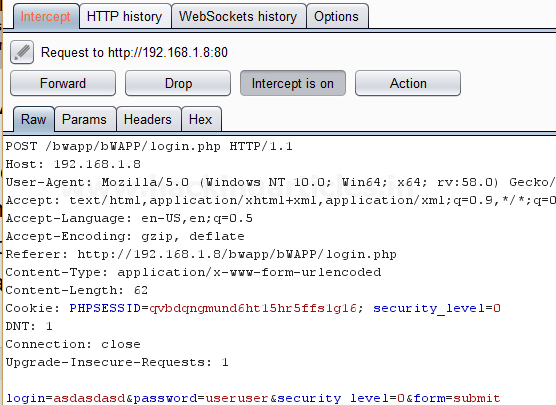
And to confirm the **password matched**, we will give the password in the **Bwapp LAB login page**, which will successfully log us into the **Bwapp lab**. This shows our success in the attack as shown in the image.



**Skip if Matches Regex**

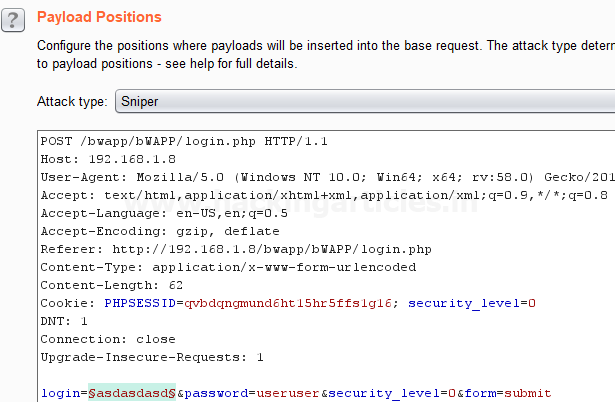
This processing rule can be used to check the current processed value matches a specified regular expression, and if it matches it will skip the payload and will move onto the next one. For example, Suppose we have a parameter value that has a minimum length and want to skip values in the list that are shorter than the minimum length defined.

First, we have intercepted the request of the login page in the **Bwapp LAB**, where we have given default username and wrong password. Then click on login, the burp suite will capture the request of the login page in the intercept tab.

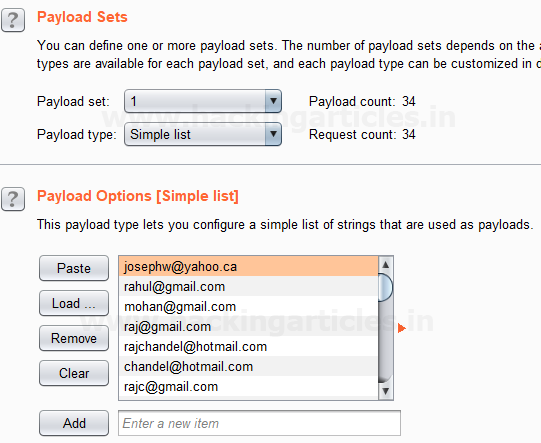


Send the captured request to the **Intruder** by clicking on the Action Tab and follow given below step. Now open the **Intruder tab** then select **Positions tab** and you can observe the highlighted password and follow the given below step for selecting payload position.

* Press on the **Clear button** given at right of the window frame.
* Now we will select the fields where we want to attack and i.e. the password filed and click on **Add button.**
* Choose the **Attack type** as
* In the given below image, we have selected a password that means we will need one dictionary files for a password.

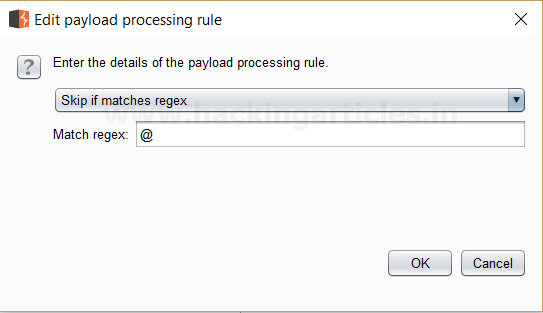


Then select the **Payload type** as **Simple list,** where we have added a dictionary by clicking on **Load** button. We can either load the dictionary or we can manually add input strings using the **Add button** in the **payload options** as shown in the image.



Before executing the attack we have added a payload processing rule to the payload type which is **Skip if Matches Regex** where we have given an input of **{@}** in the **match regex** field. Here we see that as per this rule if the input is given matches with any of the input strings in the dictionary it simply skip that value and move on to next.

Now Select **Start Attack** in the **Intruder menu** as shown in the image.



Sit back and relax because now the burp suite will do its work, match the password which will give you the correct password. The moment it will find the correct value, it will change the value of length as shown in the image.



Engagement Tools Tutorial in Burp suite

posted in[**Website Hacking**](https://www.hackingarticles.in/category/website-hacking/) on [**February 6, 2018**](https://www.hackingarticles.in/engagement-tools-tutorial-burp-suite/) by [**Raj Chandel**](https://www.hackingarticles.in/author/raaz/)

SHARE

Save

Today we are going to discuss the Importance of **Engagement tools** which is a Pro-only feature of Burp Suite. It is mainly used in information gathering and hence the analysis of any web application testing.

Its four important utilities are the following:

* Find References
* Discover Content
* Schedule Task
* Generate CSRF POC

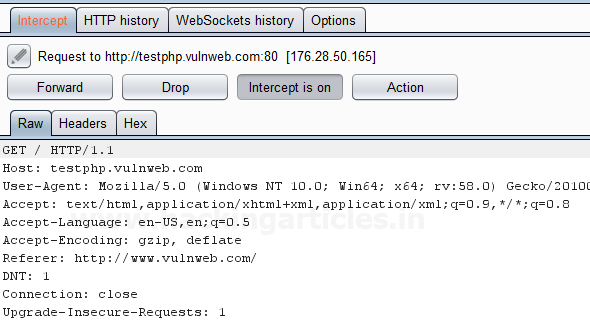
**Find References**

This function can be used to search all Burp suite tools for HTTP responses that link to a particular item. To make use of this function, select an HTTP request anywhere in Burp suite, or any part of the site map, and choose “Find references” in “Engagement tools” in the context menu which can be seen clicking Action Tab within Burp suite.

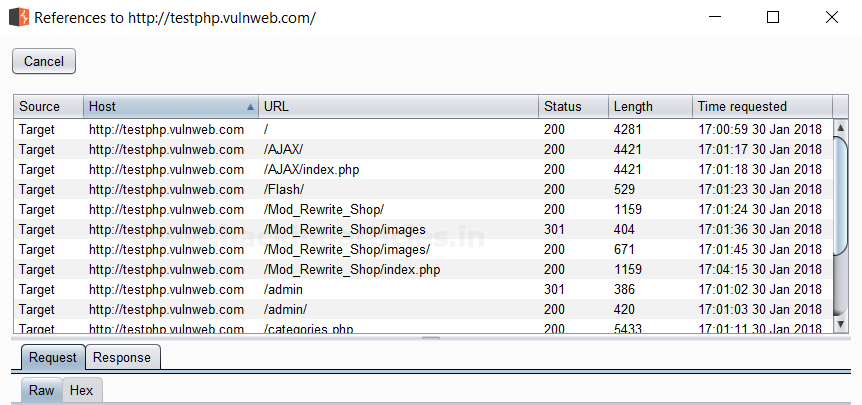
The result window of the search shows responses (from all Burp tools) that are linked to the selected item. Whenever we view an individual search result, the response will be automatically highlighted to show where the linking reference is occurring.

This function treats the original URL as a Prefix whenever we search for links, so if you select a host, you will find all references related to the host and if you select a folder, you will find all references to items inside that folder.

First, we have intercepted the request of the **Vulnweb.com** which is a **demo lab** available over the internet which can be used for testing attacks. Then click on enter after writing the URL of the Vulnerable Web in your browser, then the burp suite will capture the request of the web page in the intercept tab.



Then **click** on **Action Tab**, after that select the **Engagement tools** then click on **Find References**. This will open a result window which will show all the references related to the **URL** whose request has been captured which is the **Vulnerable Web** as shown in the image.



**Discover Content**

This function is used to discover contents and functionality which are not linked with visible content that you can browse or spider.

There are various techniques that the burp suite uses to discover content, which includes name guessing, web spidering, and extrapolation from naming conventions observed within the use of an application.

**Control**

This tab shows you the current status of the session. The **toggle button** represents whether the session is running or not, and it also allows you to pause and restart the session.

The following information is displayed about the progress of the discovery session:

* Number of requests made
* Number of bytes transferred in server responses
* Number of network errors
* Number of discovery tasks queued
* Number of spider requests queued
* Number of responses queued for analysis

**Target**

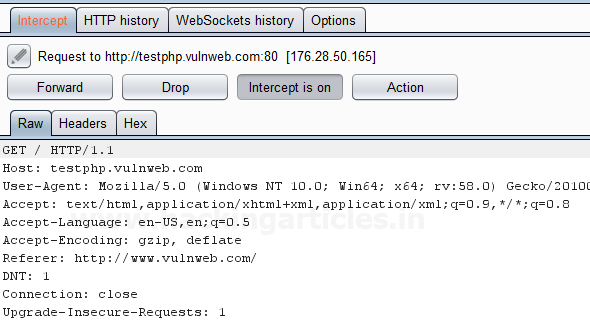
This option allows you to define or state the start directory of the content discovery session, and whether the files or directories should be targeted. The options that are available are as follows:

* **Start directory** – This is the location where Burp suite is used to look for content. The items within this path and sub-directories are requested during the session.
* **Discover** – This option can be used to determine whether the session will look for files or directories or both.

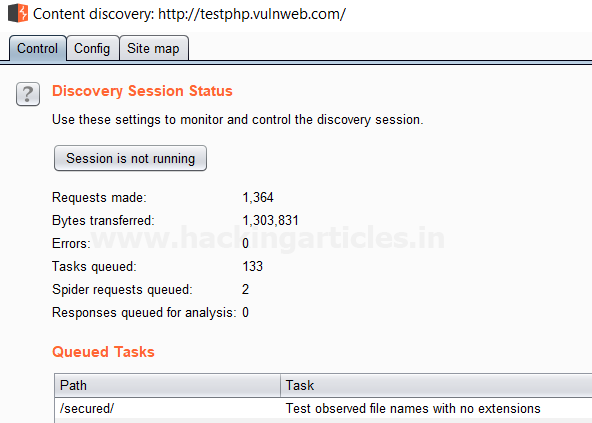
**Site Map**

The discovery session uses their own site map, showing all of the content which has been discovered within the defined scope. If you have configured your Burp suite to do so, newly discovered items can be added to Burp suite’s main site map.

First, we have intercepted the request of the **Vulnweb.com** which is a **demo lab** available over the internet which can be used for testing attacks. Then click on enter after writing the URL of the Vulnerable Web in your browser, then the burp suite will capture the request of the web page in the intercept tab.



Then **click** on **Action Tab** within the Burp suite, after that select the **Engagement tools** then click on **Content Discovery**. This will open a result window which will show the discovery session status and queued tasks which are related to the **URL** whose request has been captured which is the **Vulnerable Web** as shown in the image.



**Schedule Task**

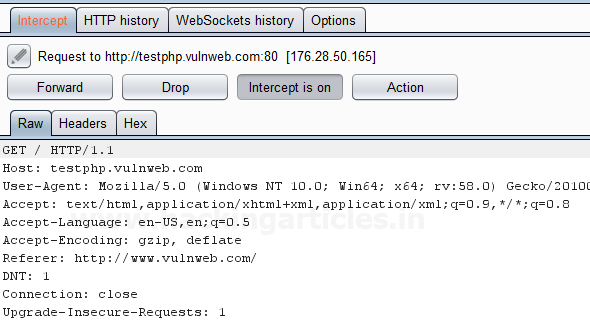
This function can be used to automatically start and stop certain tasks at defined times and intervals. We can use the task scheduler to start and stop certain automated tasks while you are not working, and to save your work periodically or at a specific time.

To make use of this function, select an HTTP request anywhere in Burp suite, or any part of the target site map, and choose “Schedule task” within “Engagement tools” in the context menu which can be seen by clicking right within Burp suite.

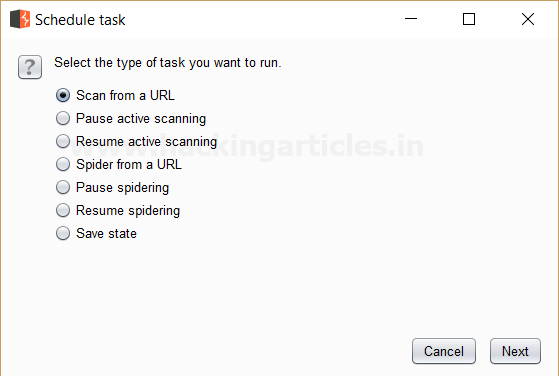
The types of task that are available within this function are as follows:

* Scan from a URL
* Pause active scanning
* Resume active scanning
* Spider from a URL
* Pause spidering
* Resume spidering
* Save state

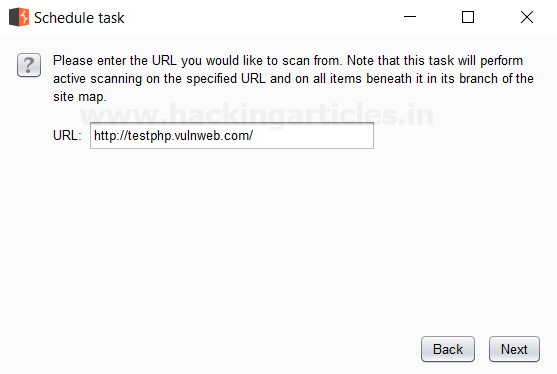
First, we have intercepted the request of the **vulnweb.com** which is a **demo lab** available over the internet which can be used for testing attacks. Then click on enter after writing the URL of the Vulnerable Web in your browser, then the burp suite will capture the request of the web page in the intercept tab.



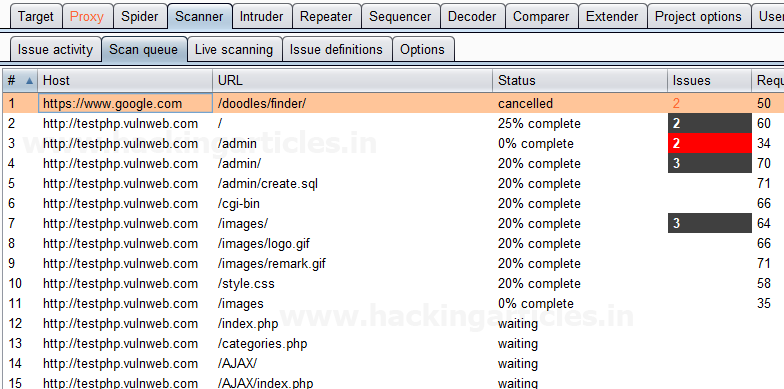
Then **click** on Action Tab within the Burp suite, after that select the **Engagement tools** then click on **Schedule Task**. This will open a window of schedule task options where we have selected **Scan from a URL** option as shown in the image.



Then Click **Next** a window will open where we have to give the **URL** we want to scan its branches from the site map.



Then Click **Next** we see that the scanner tab of the burp suite is open which **scans** all the branches beneath the site map of the given **URL** which is seen in the **scan queue tab** as shown in the image which is related to the **URL** whose request has been captured which is the **Vulnerable Web** as shown in the image.



**Generate CSRF PoC**

This function can be used to generate a proof-of-concept (PoC) cross-site request forgery (CSRF) attack for any given request.

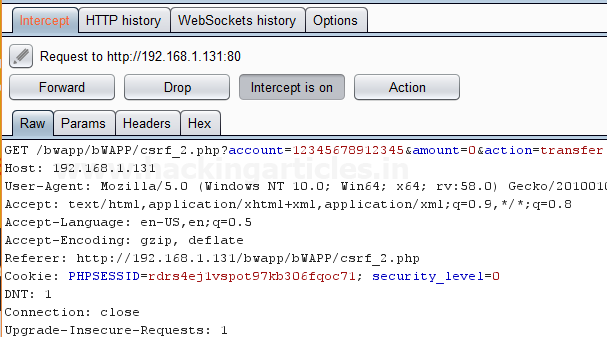
To access this function, select a URL or HTTP request anywhere in the Burp suite, and choose “Generate CSRF PoC” within “Engagement tools” in the context menu which can be seen by clicking right within Burp suite.

Let’s start!!

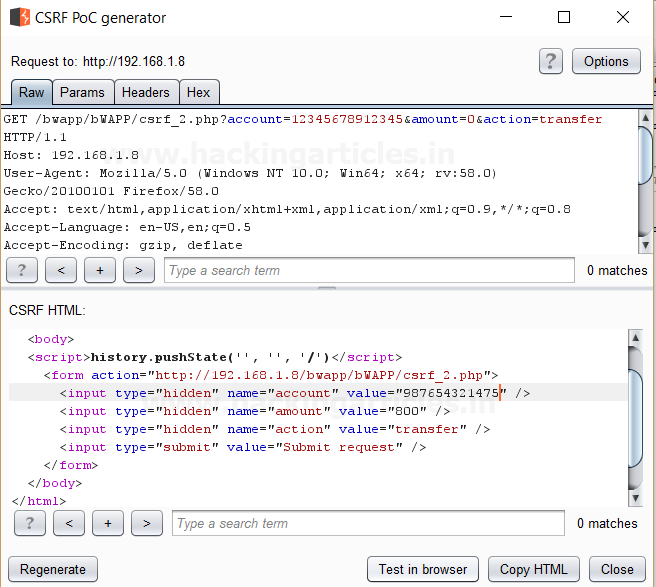
First, we have intercepted the request of the **CSRF (transfer amount)** option in the **Bwapp LAB**, where we have given an **Account Number**.



Then click on transfer, the burp suite will capture the request of the page in the intercept tab.



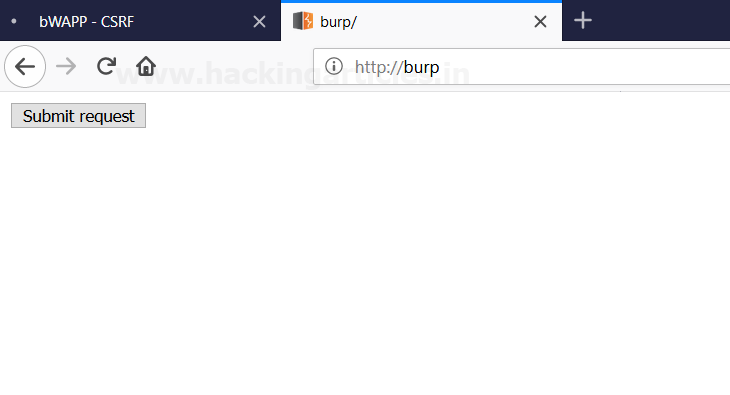
Then click on Action Tab within the Burp suite, after that select the **Engagement tools** then click on **Generate CSRF PoC**. This will open a window of the CSRF PoC where we made a change in **Account value** and **Amount value** in CSRF HTML code as shown in the image.



After making changes in the values click on **Test in Browser option** or **Copy HTML** this will open the window of Show response in the browser then click on **COPY**, and then paste it in the Browser and Press Enter as shown in the image.



We see a Submit request Button is seen in the browser after that click on it.



It appears to us that the amount is reduced as we have transferred the amount from the account by making changes in the CSRF HTML code as shown in the image.

