**Name: Varun Salgarkar**

**Reg No: 19BCE1435**

## **Burp Suite Bruteforce Attack & Cluster Bomb Attack**

**Aim:** To create a login page and then perform Brute force attack on that page using Cluster Bomb technique in Burp Suite and gather potential information.

Step 1: Creating a simple login page and home page in PHP, with the necessary authentication

**Login.php**

<?php try {

$db = new PDO('mysql:host=localhost;dbname=lab7','','');

$db->setAttribute(PDO::ATTR\_ERRMODE,PDO::ERRMODE\_EXCEPTION);

}

catch (PDOException $e) {

die('<h4 style="color:red">Incorrect Connection Details</h4>');

} ?>

<!DOCTYPE html>

<html>

<head>

<title>LAB 7 (9-3-22)</title>

<link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.5.2/css/bootstrap.min.css">

<link href="https://fonts.googleapis.com/css2?family=Quicksand:wght@500&display=swap" rel="stylesheet">

<style>

html {

font-family: 'Quicksand', sans-serif;

height: 100%;

}

body{

background: #3CF78D;

/\* background: linear-gradient(to right, #2a5298, #1e3c72); \*/

}

.main{

width: 290px;

height: 250px;

position:absolute;

top:0; bottom:0;

left:0;right:0;

margin: auto;

text-align: center;

box-shadow: 0 0 20px 0 rgba(0, 0, 0, 0.2), 0 5px 5px 0 rgba(0, 0, 0, 0.24);

}

.main input{

outline: 0;

background: #f2f2f2;

width: 75%;border: 0;

margin: 0 0 15px;

padding: 12px;

box-sizing: border-box;

}

.main button{

outline: 0;

background: #4CAF50;

width: 80%;border: 0;

padding: 10px;color: #FFFFFF;

cursor: pointer;

}

.main p {

color:white;

font:'Quicksand';

font-size: 20px;

}

</style>

</head>

<body>

<?php

if (isset($\_POST['submit']))

{ $uname = trim($\_POST['unm']);$pass = $\_POST['pass'];

$q = $db->query("SELECT \* FROM user WHERE username = '$uname' AND password = '$pass' ");

$count = $q->rowCount();$rows = $q->fetchAll(PDO::FETCH\_OBJ);

if($count > 0){ foreach($rows as $row){ header('location: home.php'); } }

else{ echo '<script type="text/javascript">alert("Incorrect Login Credentials...")</script>'; }

} ?>

<center><h3 style="color:white;">ISM LAB <br>Varun Salgarkar - 19BCE1435</h3>

</center>

<div class="main">

<p>Login Page</p>

<form action="" method="POST">

<input type="text" name="unm" placeholder="Username">

<input type="password" name="pass" placeholder="Password">

<button type="submit" name="submit">Sign In</button><br>

</form>

</div>

</body>

</html>

home.php

<!DOCTYPE html>

<html>

<head>

<title>ISM LAB 7</title>

<link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.5.2/css/bootstrap.min.css">

<link href="https://fonts.googleapis.com/css2?family=Quicksand:wght@500&display=swap" rel="stylesheet">

<style>

html {

font-family: 'Quicksand', sans-serif;

height: 100%;

}

body{

background: #1e3c72;

background: linear-gradient(to right, #2a5298, #1e3c72);

}

button{

outline: 0;

background: #4CAF50;

width: 10%;

border: 0;

padding: 10px;

color: #FFFFFF;

cursor: pointer;

}

</style>

</head>

<body>

<center> <h3 style="color:white;">Homepage</h3>

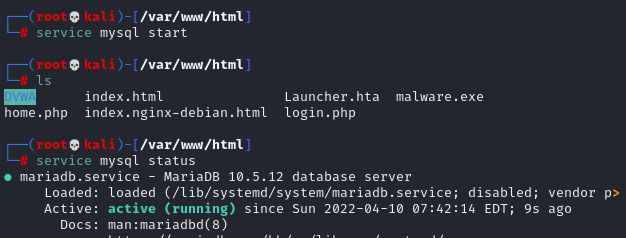
<a href="login.php"><button>Log Out</button></a>

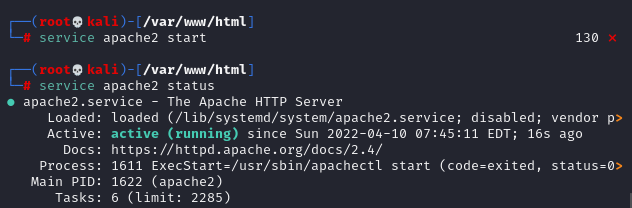
</center>

</body>

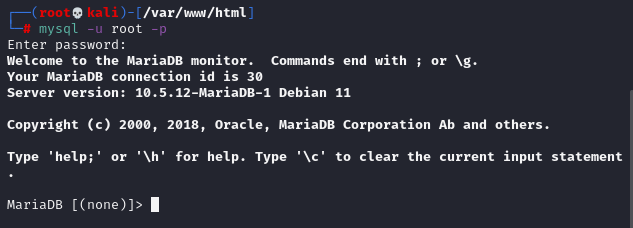
</html>

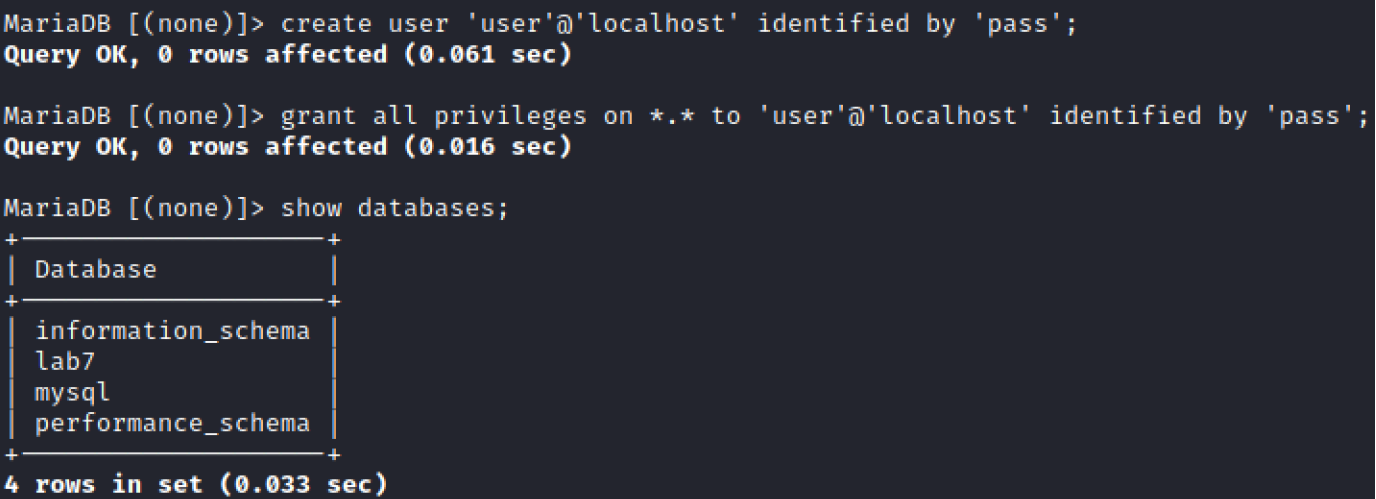
**MYSQL**

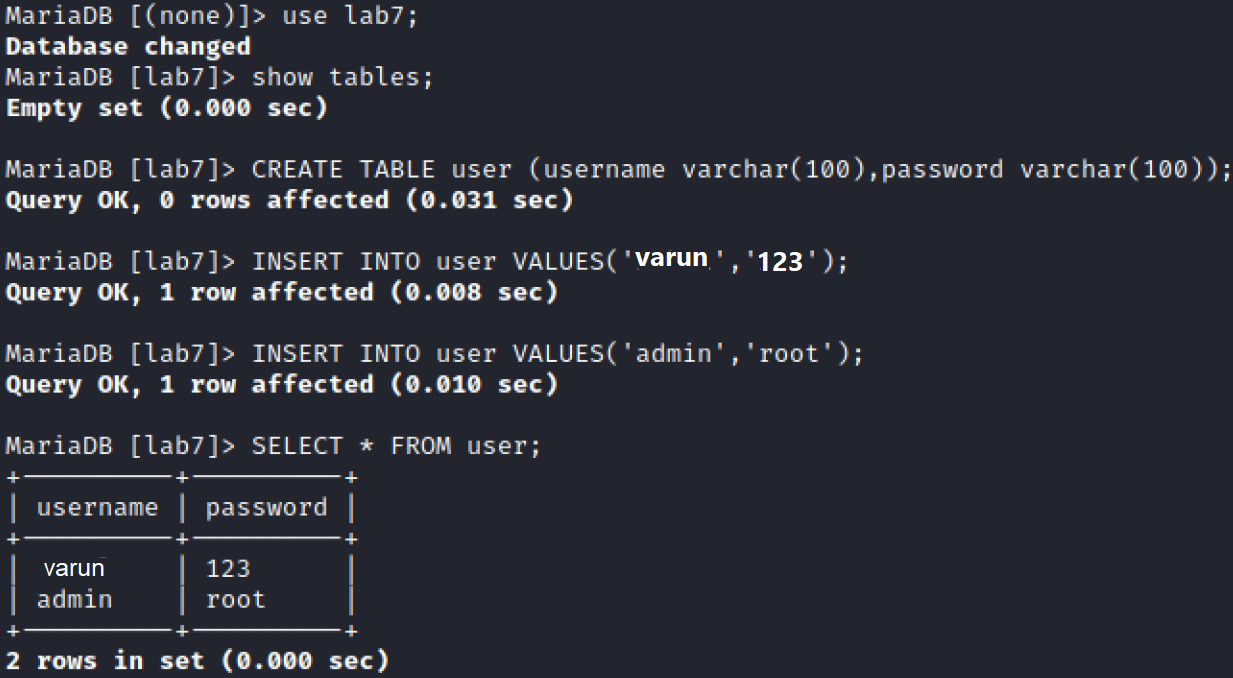




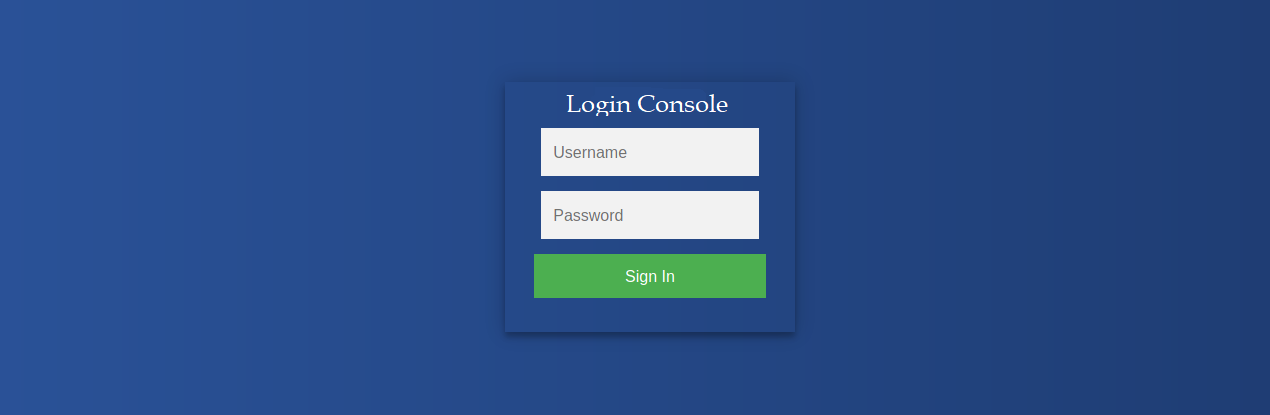
Step 2: Starting the Apache and MySQL server in Kali Linux and creating the necessary database and table for the authentication.



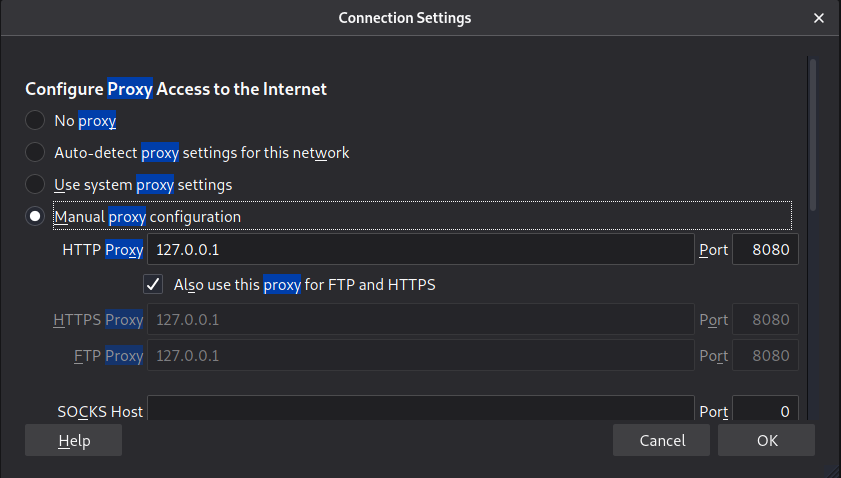
Creating a user in the MySQL schema and then granting all the privileges to that user.



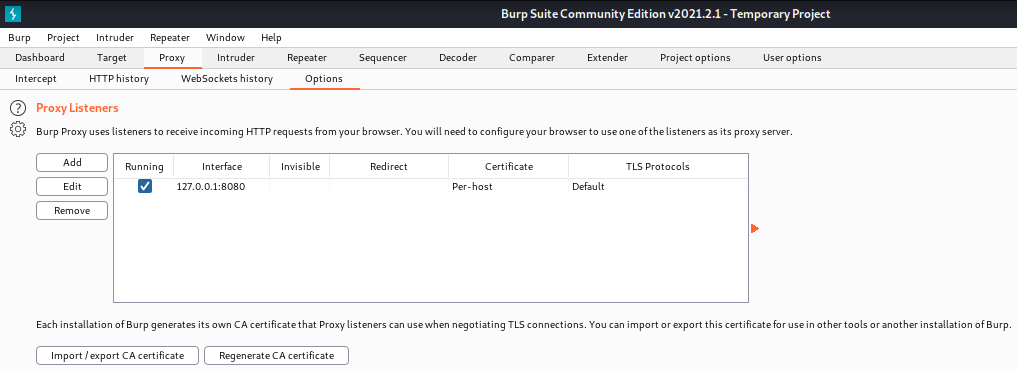
Step 3: Accessing the login page by typing the URL http://localhost/login.php in the browser



Step 4: Configuring Firefox’s proxy settings

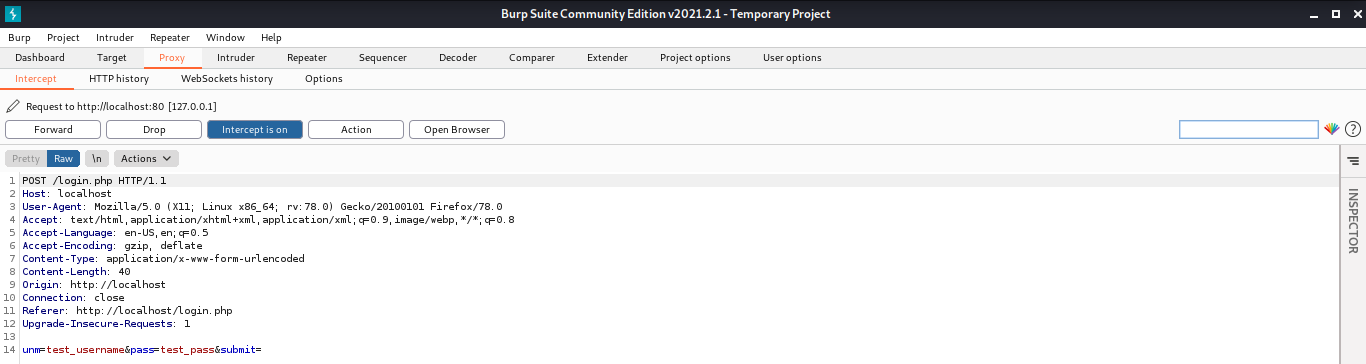


Step 5: Configuring Burp Suite’s proxy setting in the Proxy tab

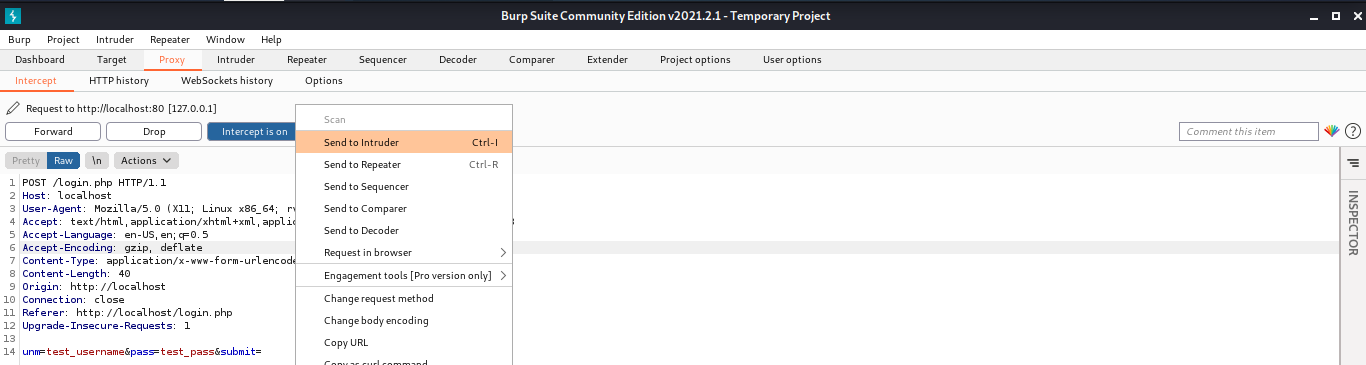


Step 6: Turn the Intercept on by heading to Proxy tab and Intercept sub tab. Now type some credentials in the login page, so that the request gets intercepted in Burp Suite.

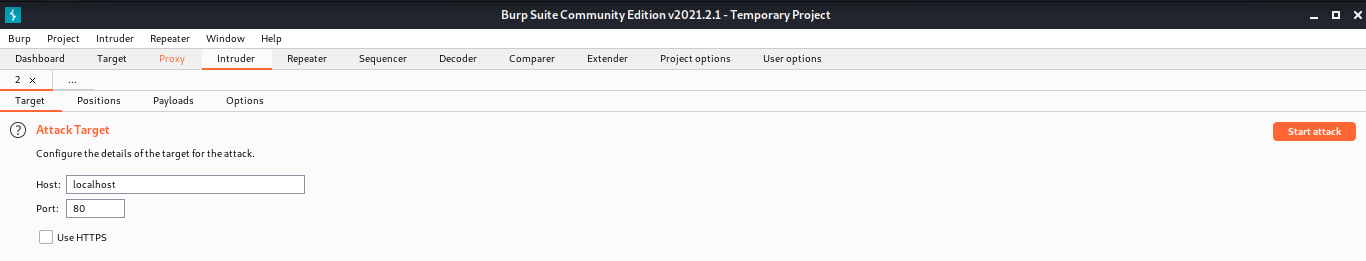
Step 7: Intercepting the login request in Proxy tab of Burp Suite



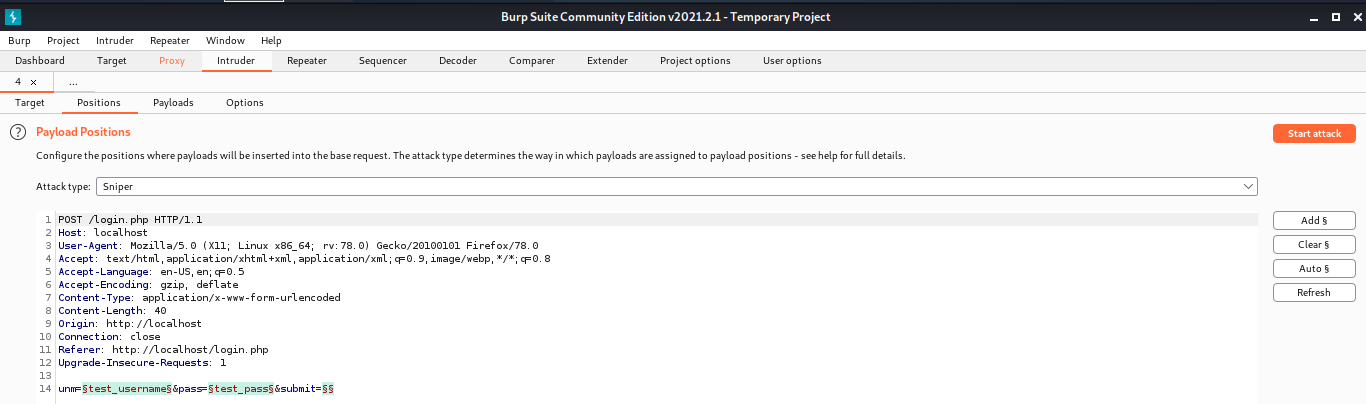
Step 8: Sending the intercepted request to the Intruder tool in Burp



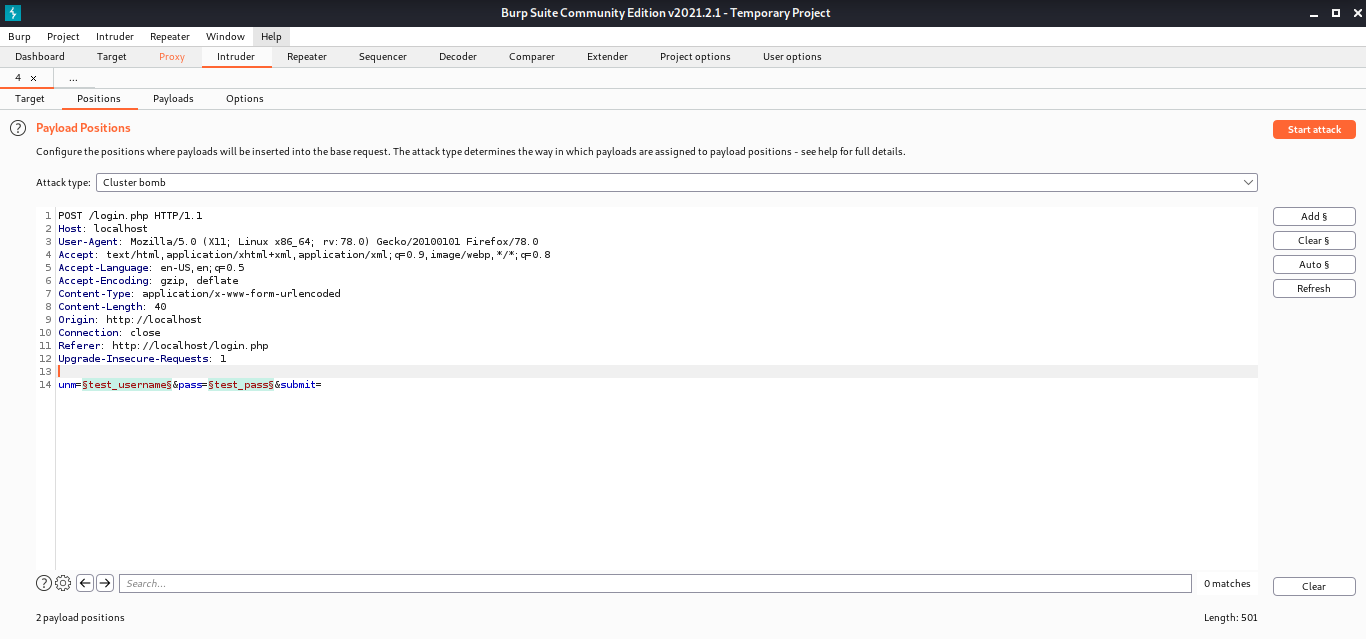
Step 9: Viewing the request in Intruder tab



Step 10: Removing the existing 3 pre-defined payload positions using the Clear button in Positions subtab

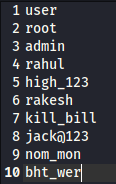
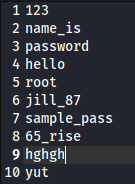


Step 11: Configuring the attack type as ‘Cluster Bomb’ and setting the user and pass parameters as the payload positions for the brute-force attack

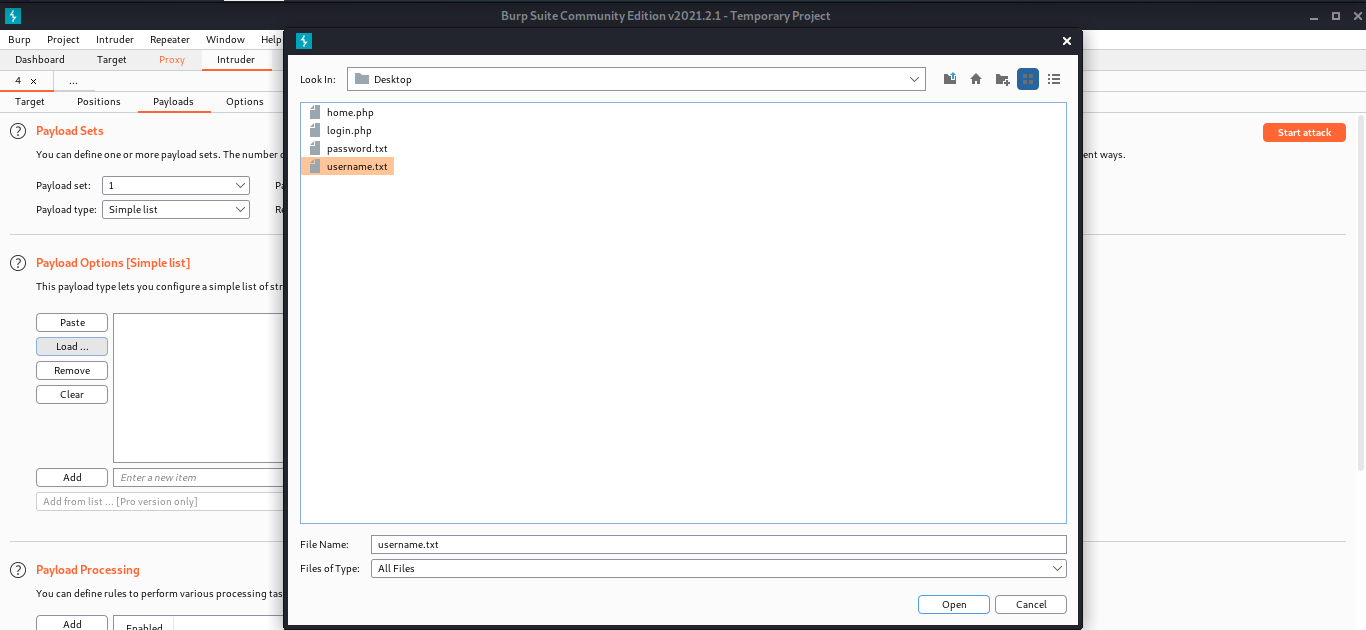


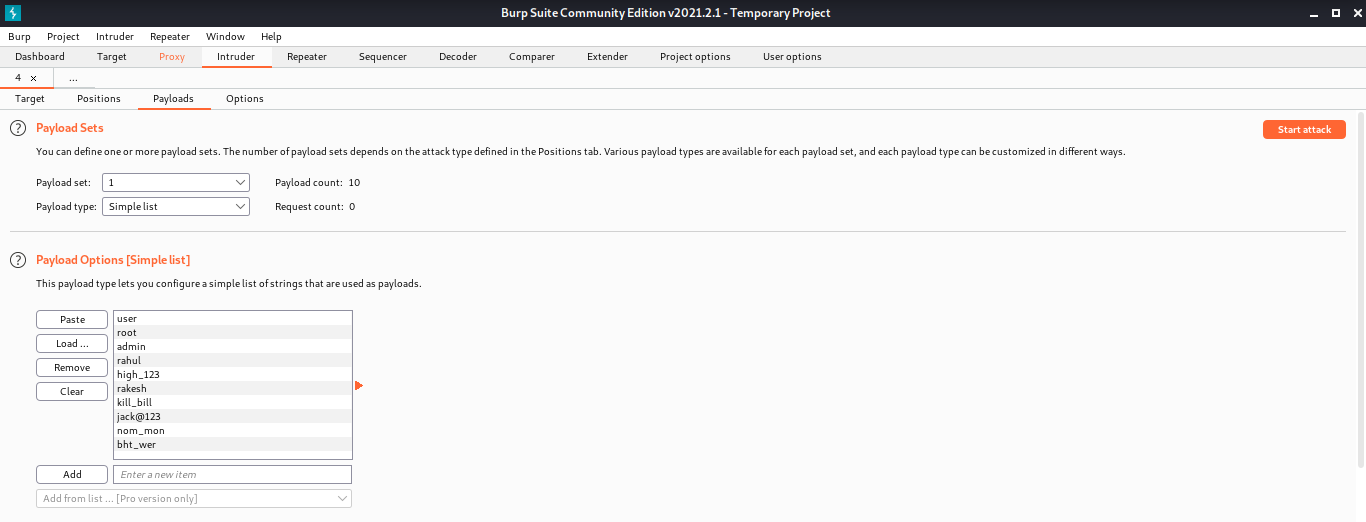
Step 12: Loading the payload for the first payload position (i.e. user parameter) and the second payload position (i.e. pass parameter) with the help of text files that contains some usernames and passwords.

username.txt passwords.txt

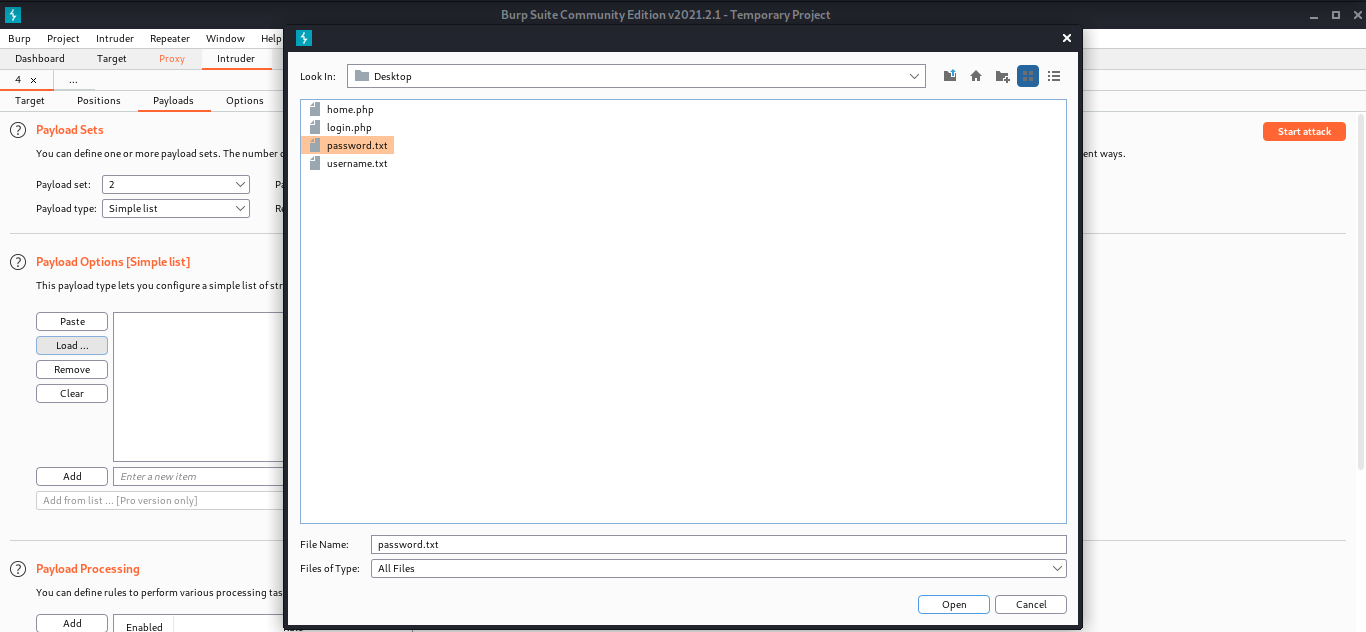
 

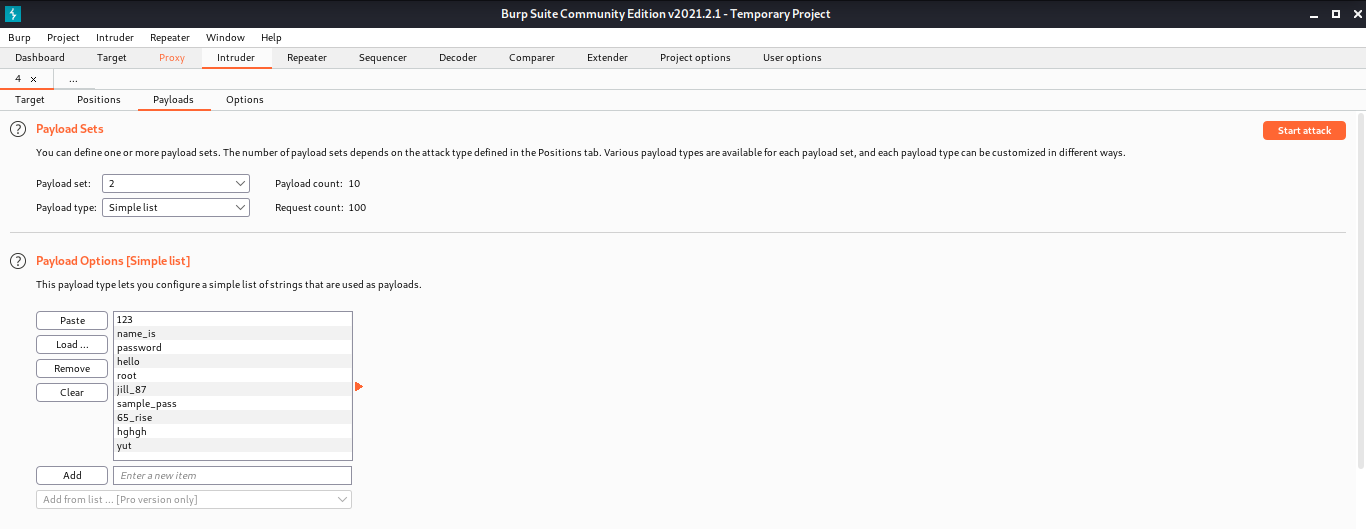
Loading the payload for the first payload position





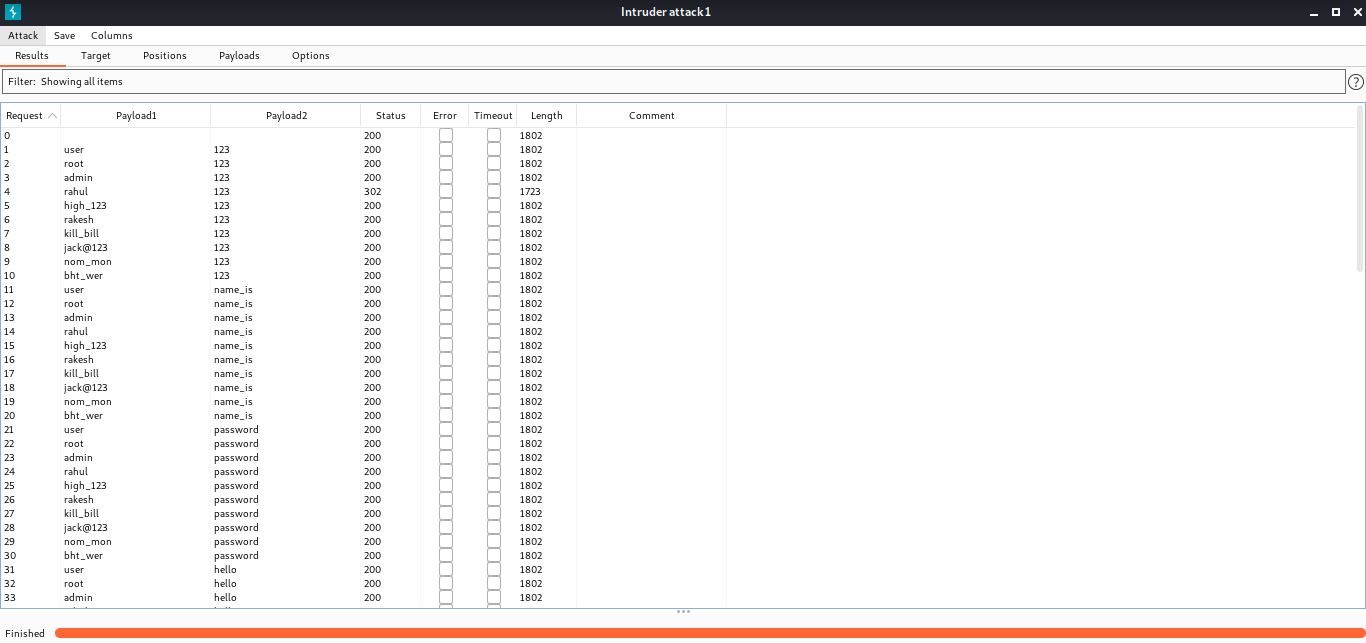
Loading the second payload position

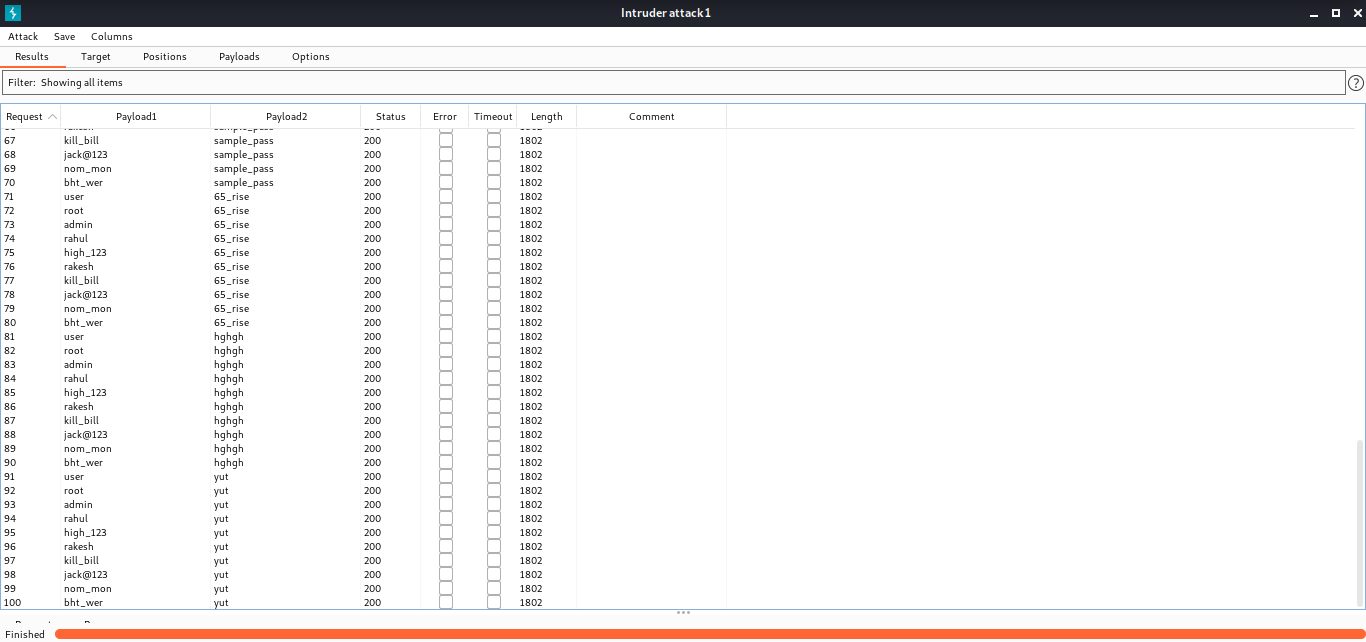




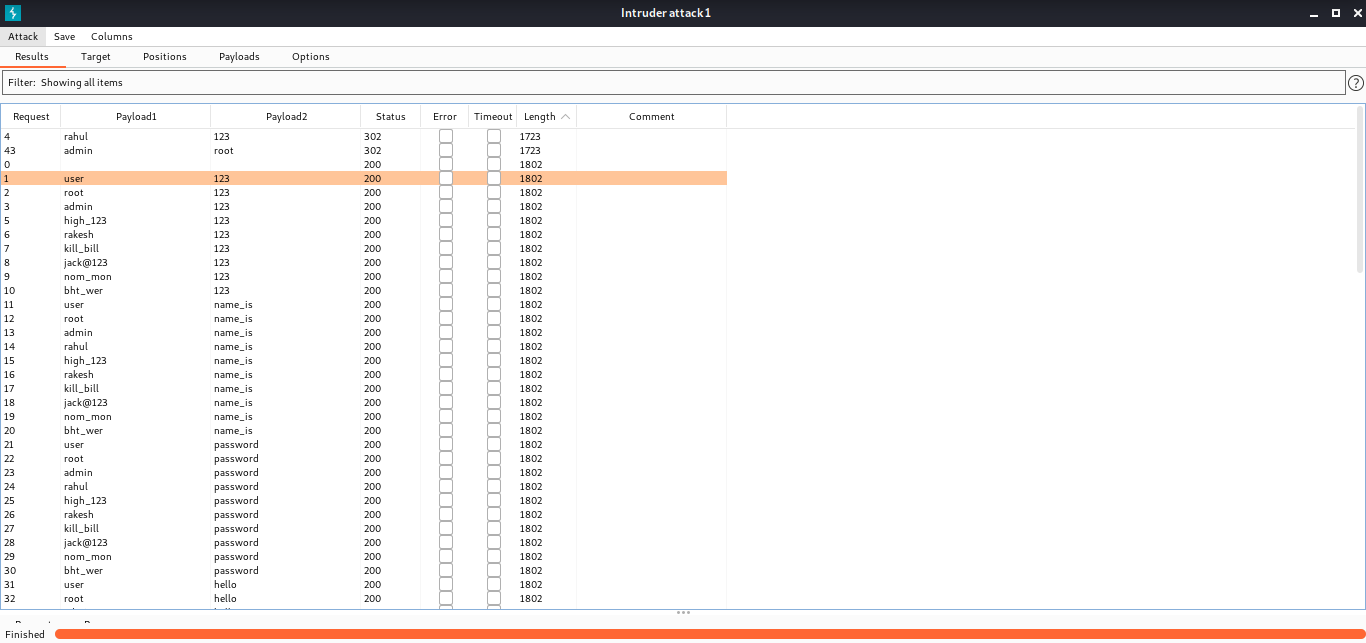
Step 13: Starting the Cluster Bomb Attack by clicking on the ‘Start Attack’

A total of 100 requests would be sent because each payload list has 10 entries for username and password each, hence 10\*10=100 request. Thus trying out all the possible combinations



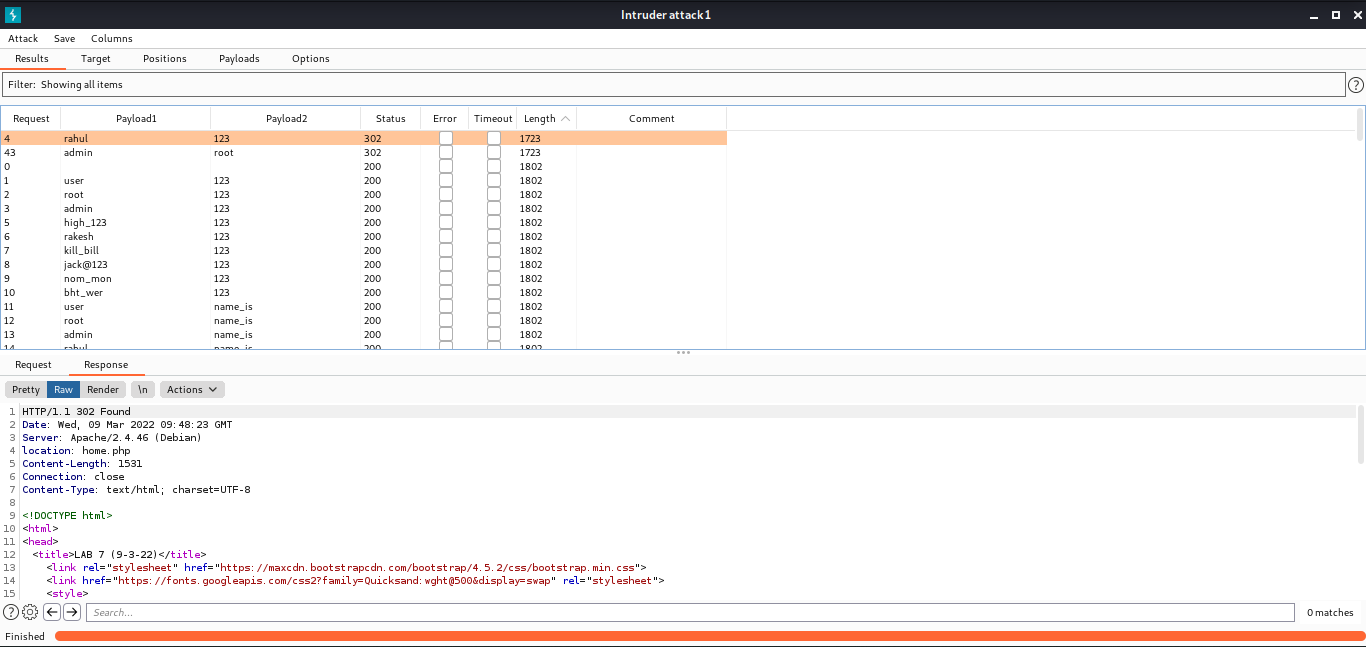


Step 14: Sorting the requests based on their length to see for any abnormal packets, which might have sensitive information

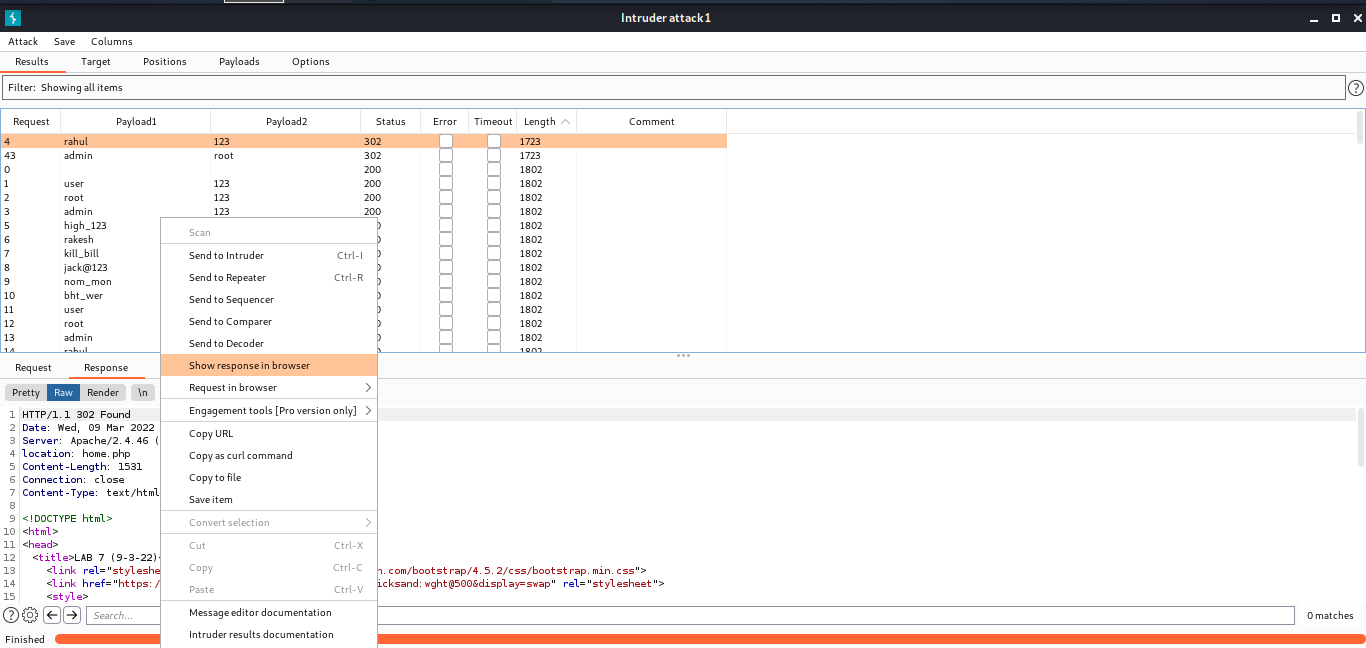


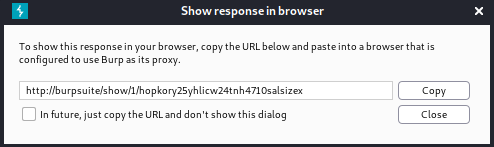
So we have two packets with different length and also different status code, so these might be the correct credentials but to check if they’re valid credentials we have to check their response.

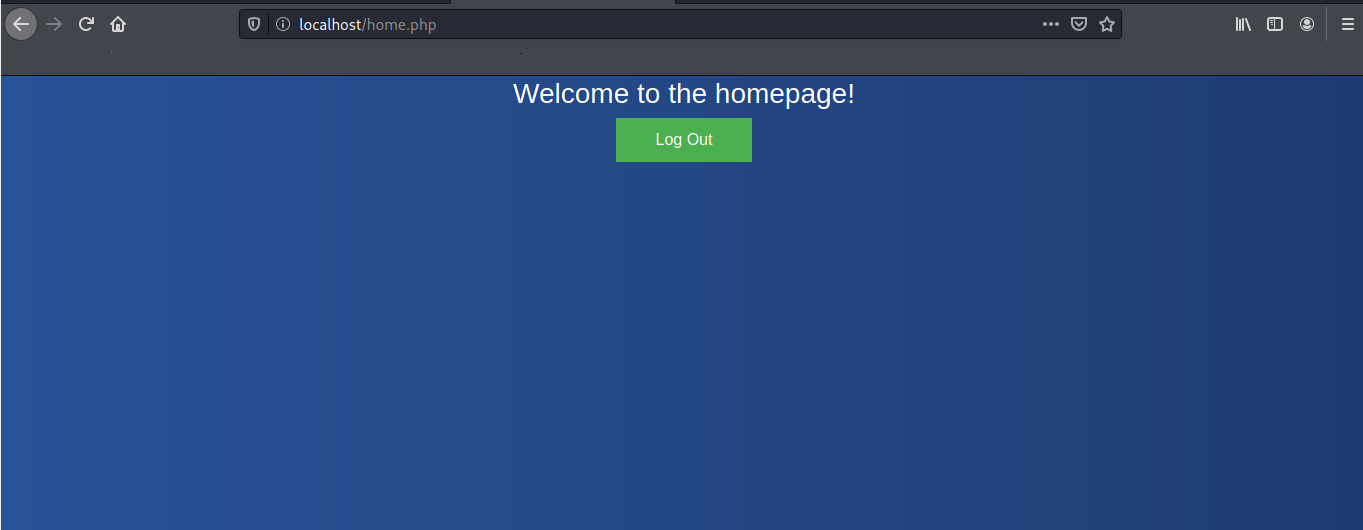
Checking the Request No. 4 response



Viewing the response in the browser

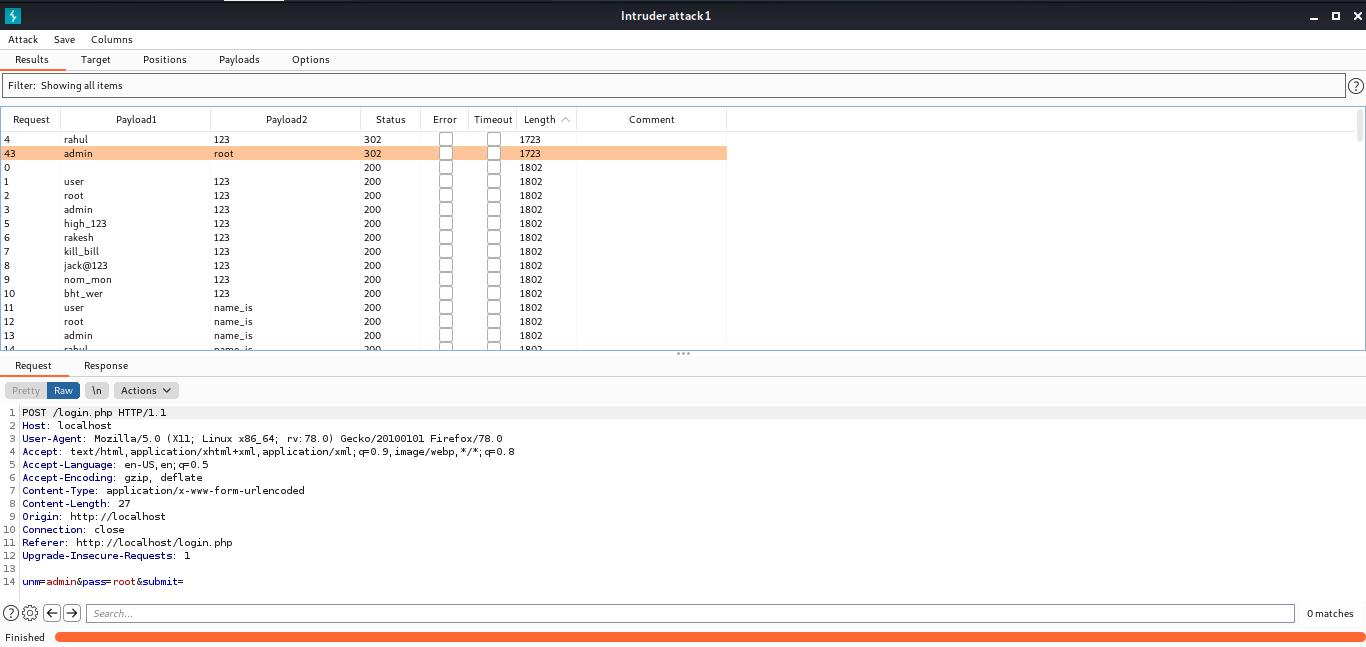


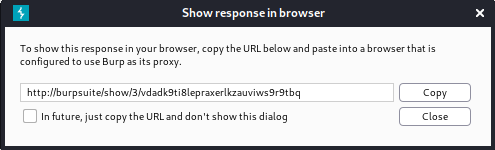


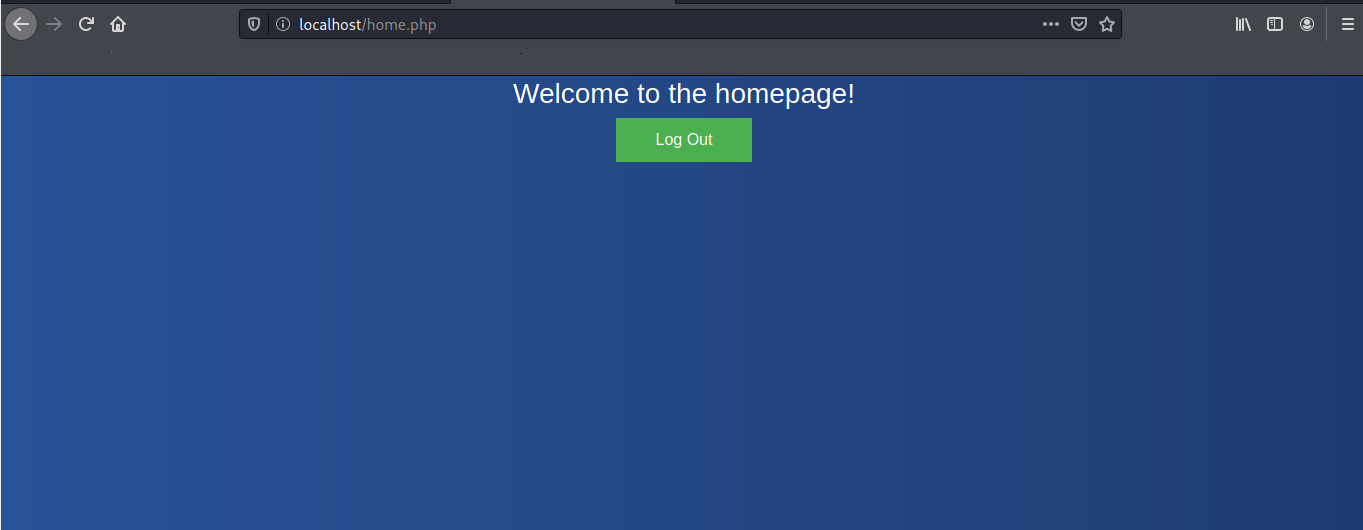


So, this has request has the correct credentials, that is Username=varun & Password=123

Similarly, by viewing the Response of Request 43 we can get other set of valid credentials

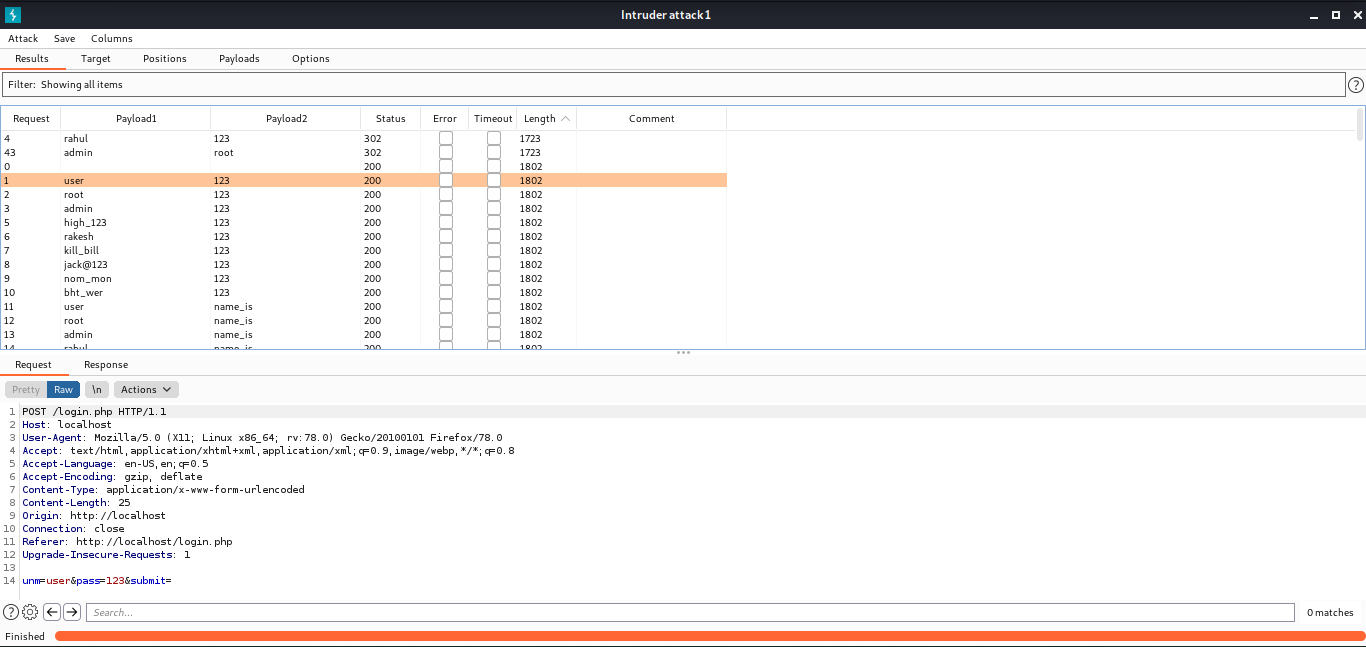


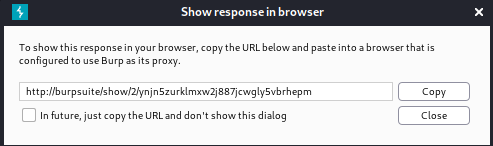


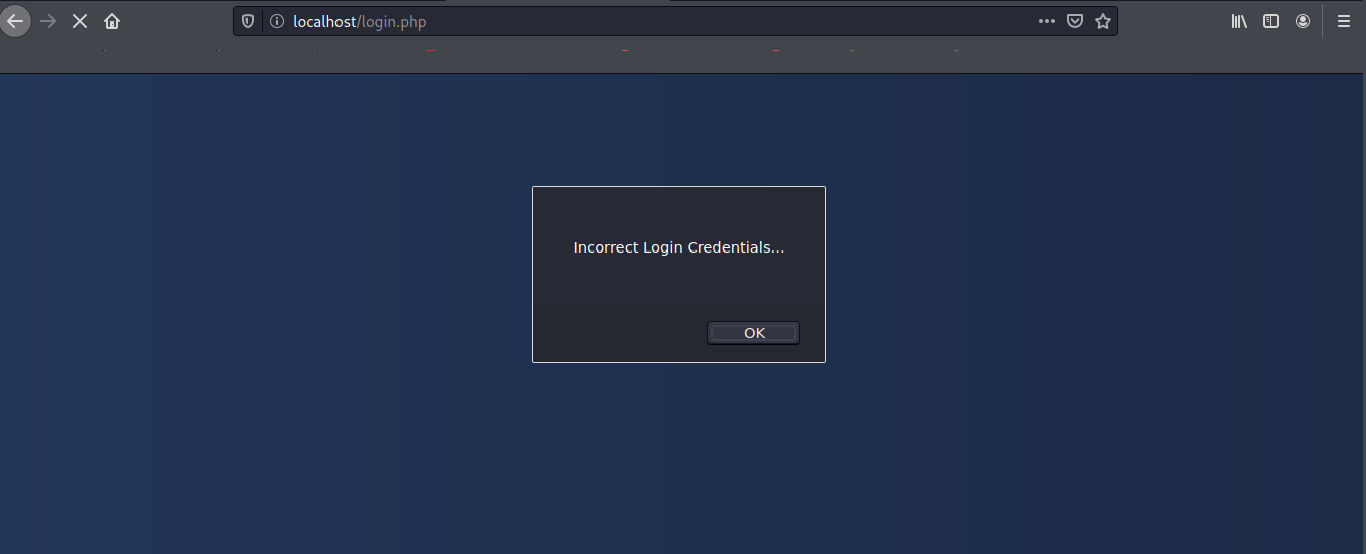


So, this has request has the correct credentials, that is Username=admin & Password=root

Viewing a response with the same packet length and status code, thus indicating that these requests might have invalid credentials

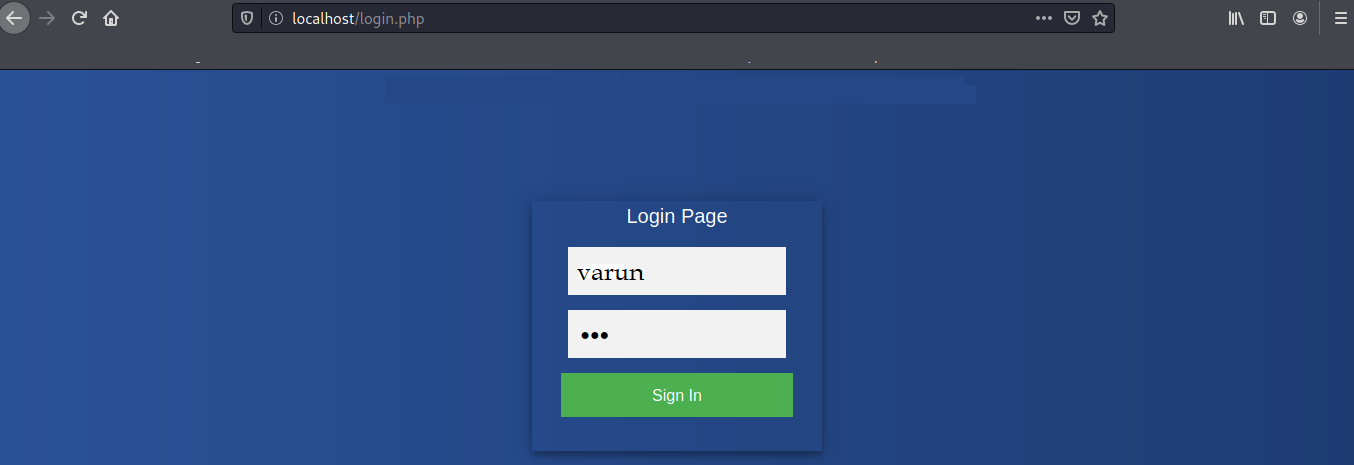


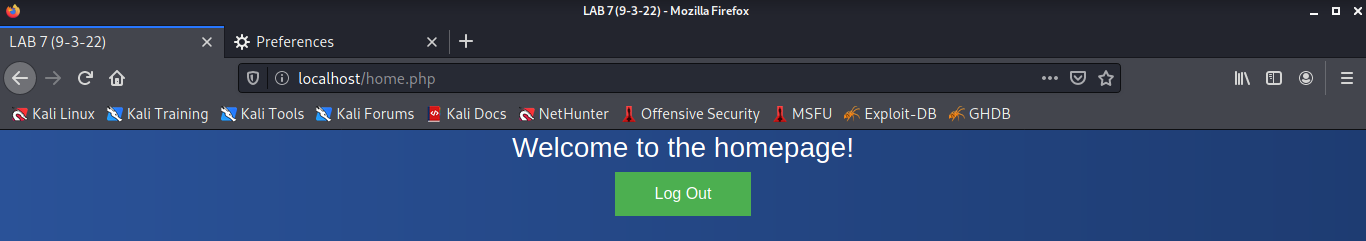




Step 15: By the information gathered from the Intruder tool, let’s see if can login with those credentials

Username: varun & Password:123





Username: admin & Password: root

