Assignment - 4

What to do:

→ What is burp suite?
→ Why burp suite?
→ What are the features of burp suite?
→ Test the vulnerabilities of testfire.net

What is Burp Suite?

Burp Suite is a comprehensive cybersecurity toolset designed for web application security testing. Developed by PortSwigger, it is widely used by security professionals and developers to identify and fix vulnerabilities in web applications.

Why Burp Suite?

Burp Suite is used for several reasons:

1. **Vulnerability Assessment:** It helps identify and assess vulnerabilities in web applications, including SQL injection, cross-site scripting (XSS), and more.
2. **Penetration Testing:** Security professionals use Burp Suite to simulate attacks, assess an application's security posture, and find weaknesses.
3. **Proxy Functionality:** It acts as an intercepting proxy, allowing users to monitor and manipulate HTTP requests and responses, making it an invaluable tool for understanding how web applications work.
4. **Automation:** Burp Suite provides automated scanning capabilities to quickly identify common vulnerabilities.
5. **Integration:** It integrates with various tools and extensions, making it adaptable for different testing scenarios and extending its functionality.

Features of Burp Suite:

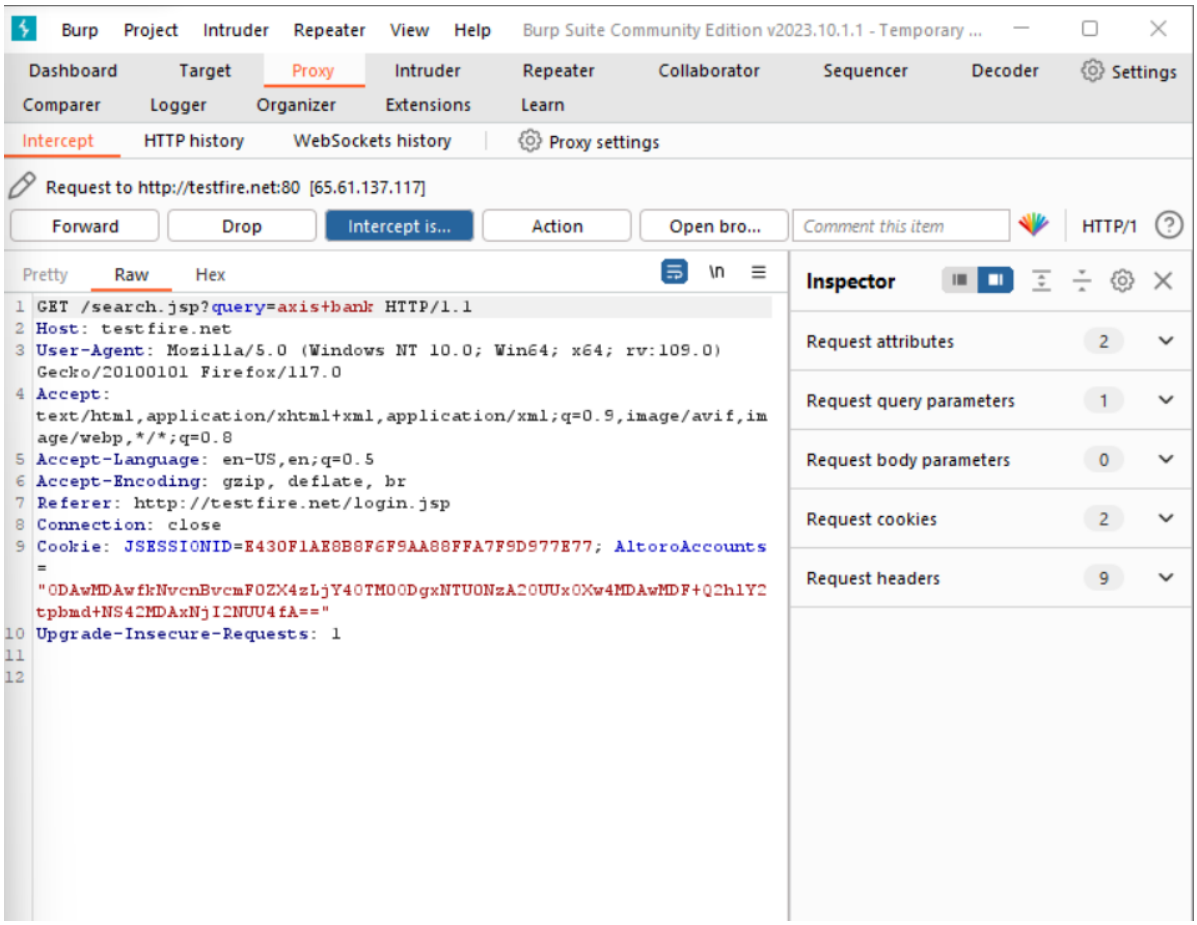
Burp Suite offers a wide range of features and tools for web application security testing:

1. **Proxy:** Intercept, inspect, and modify HTTP requests and responses.
2. **Scanner:** Automated scanning to detect vulnerabilities like XSS, SQL injection, and more.
3. **Spider:** Crawl web applications to discover and map their structure.
4. **Intruder:** Perform automated attacks, such as brute-force and injection attacks.
5. **Repeater:** Manually modify and re-send HTTP requests for testing.
6. **Sequencer:** Analyze the randomness of tokens and session identifiers.
7. **Decoder:** Decode and encode various data formats.
8. **Comparer:** Compare two requests or responses to find differences.
9. **Extender:** Add custom extensions and plugins to enhance functionality.

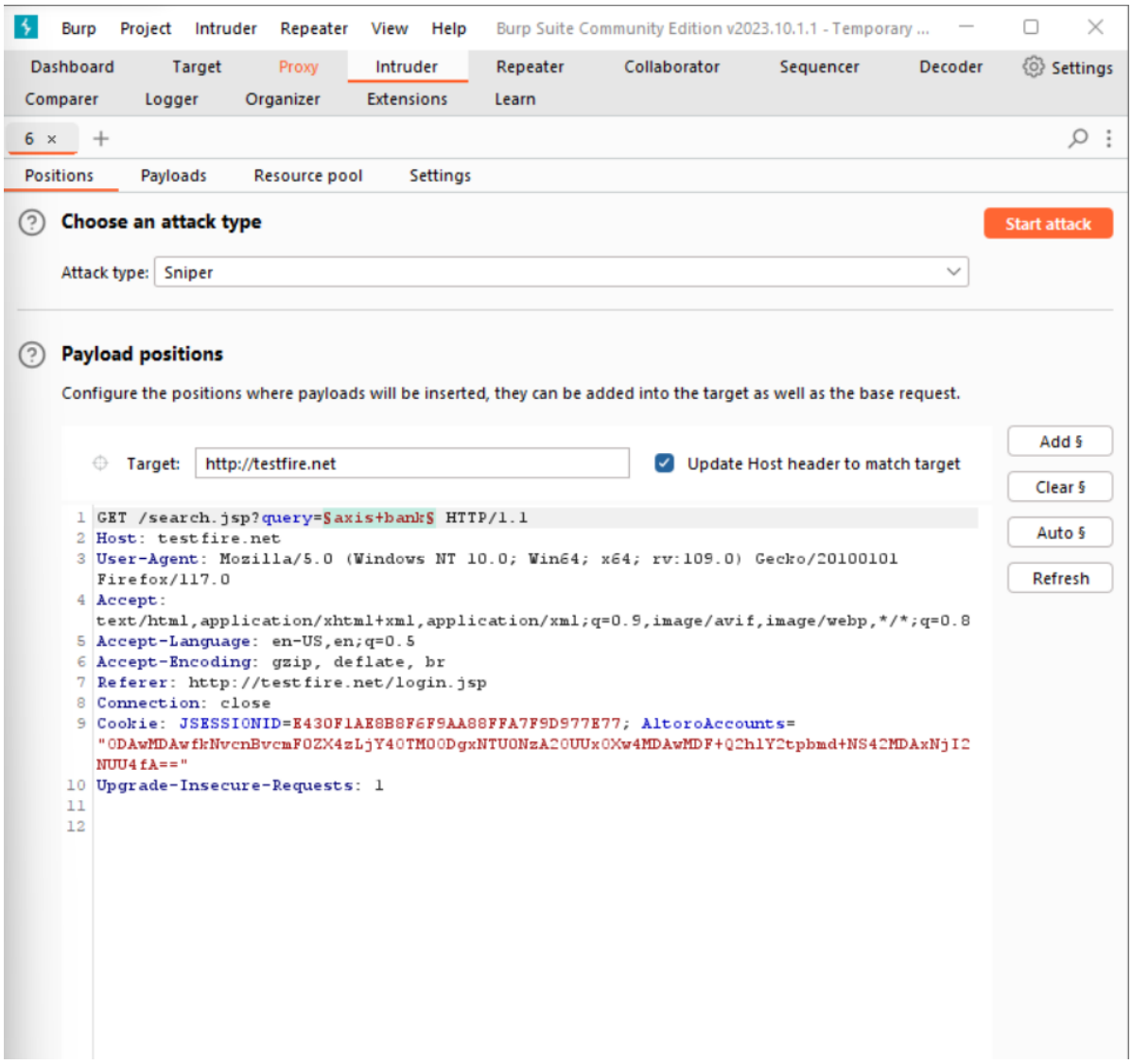
Testing the vulnerabilities on testfire.net

1. **SQL injection:**

   → First I turned the intercept on and went to the browser and search something which in this example is “axis bank”, here i saw that i can exploit this vulnerability and inject loads of SQL codes to the search bar and send lots of requests:



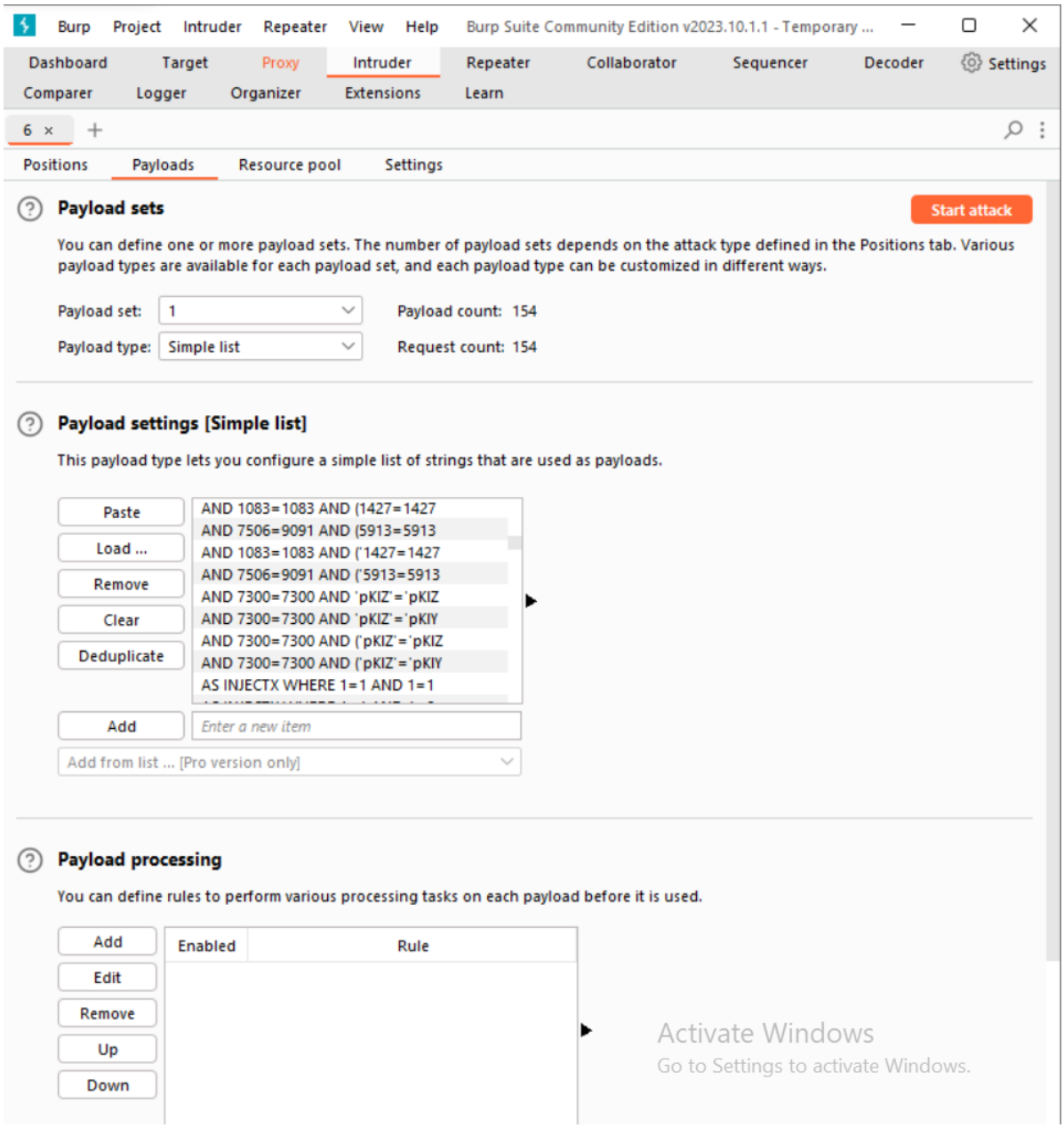
→ Then I send this from proxy to the intruder, where now i will perform the sql injection. I picked :



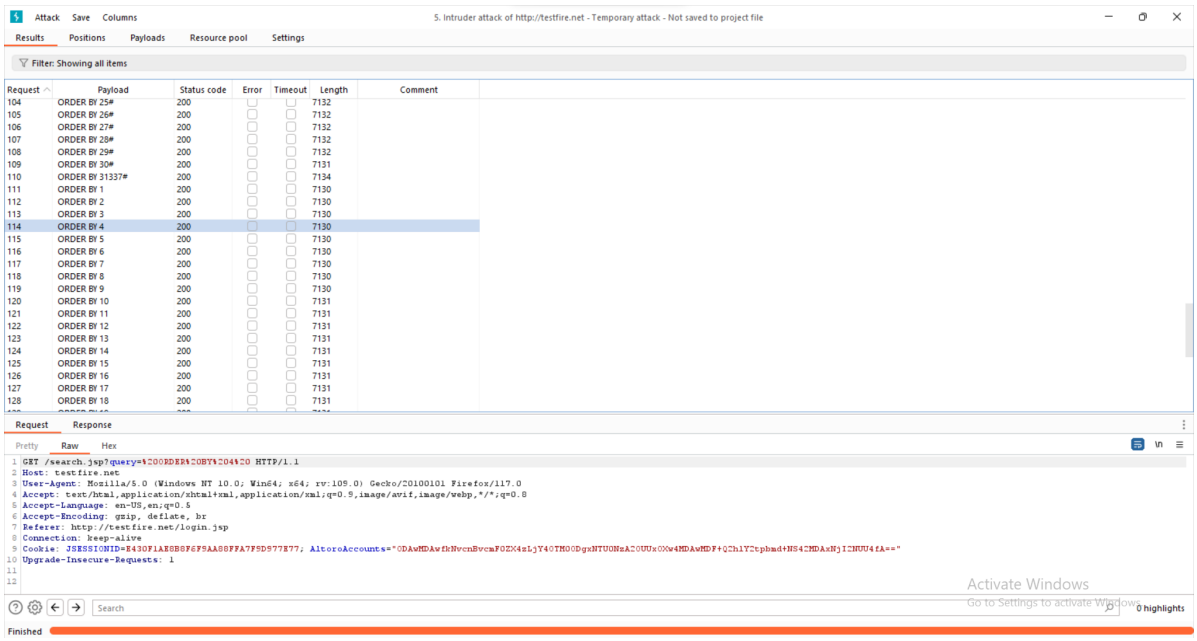
Here we chose a sniper attack because we only had 1 payload.

I picked the search option in the url as the payload position, now using the sql payloads, loads of requests will be sent to the server.

→ Then i picked up a payload from github and started the sql attack:

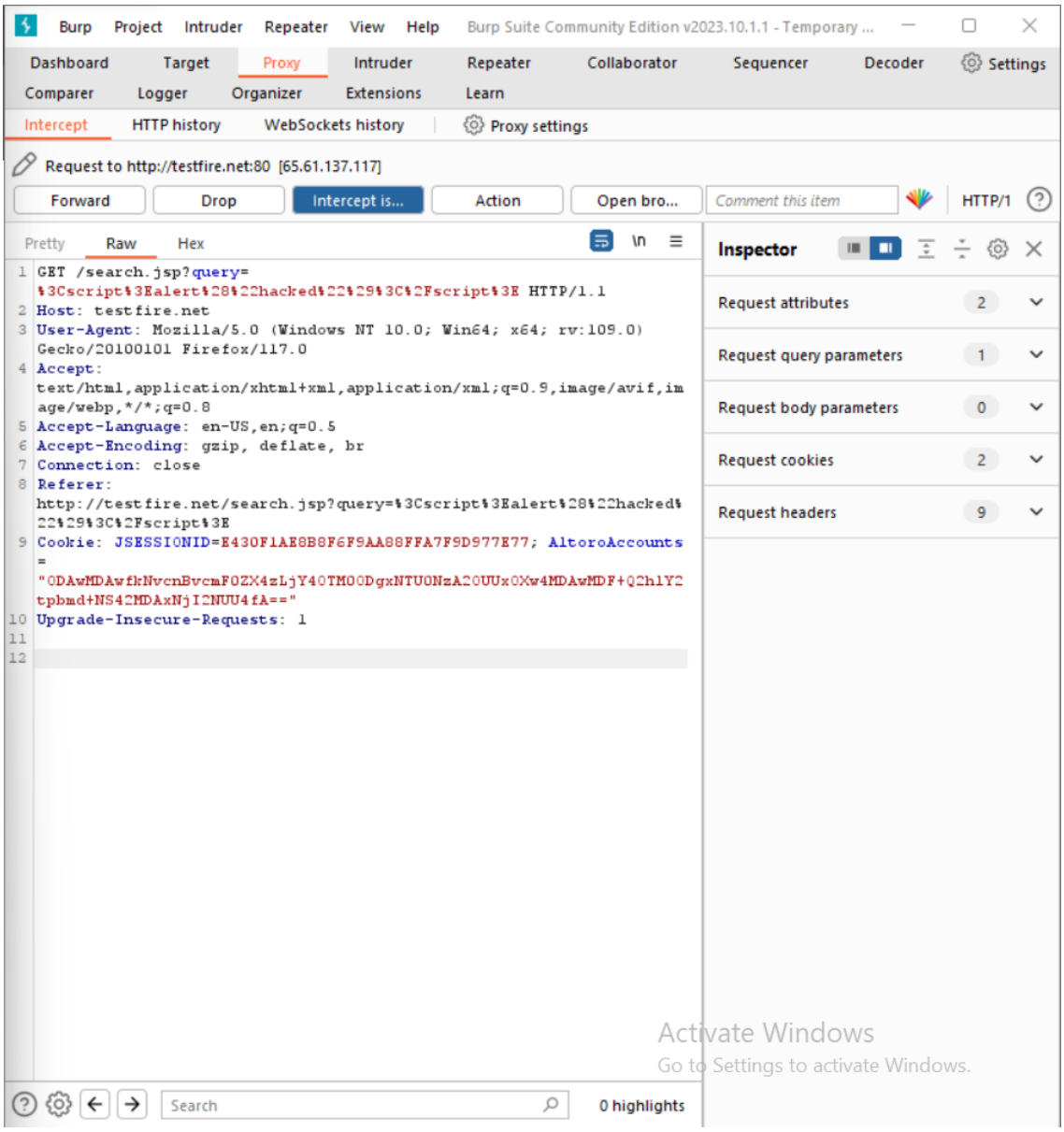


→ We got 200 response codes from all the requests meaning that all requests were successful, here is detailed information about one of the requests:

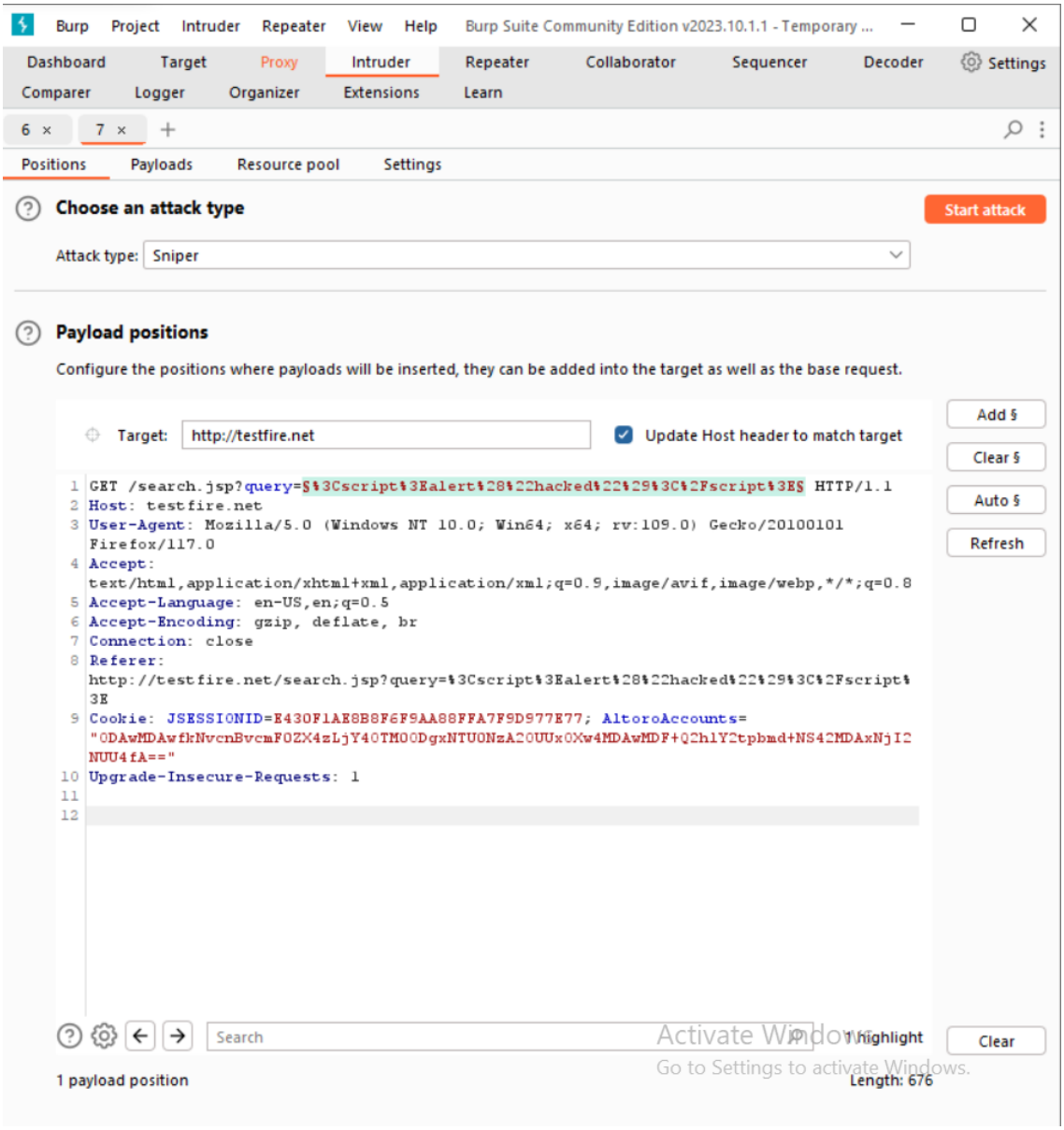


2. **Cross-Site Scripting (XSS)**

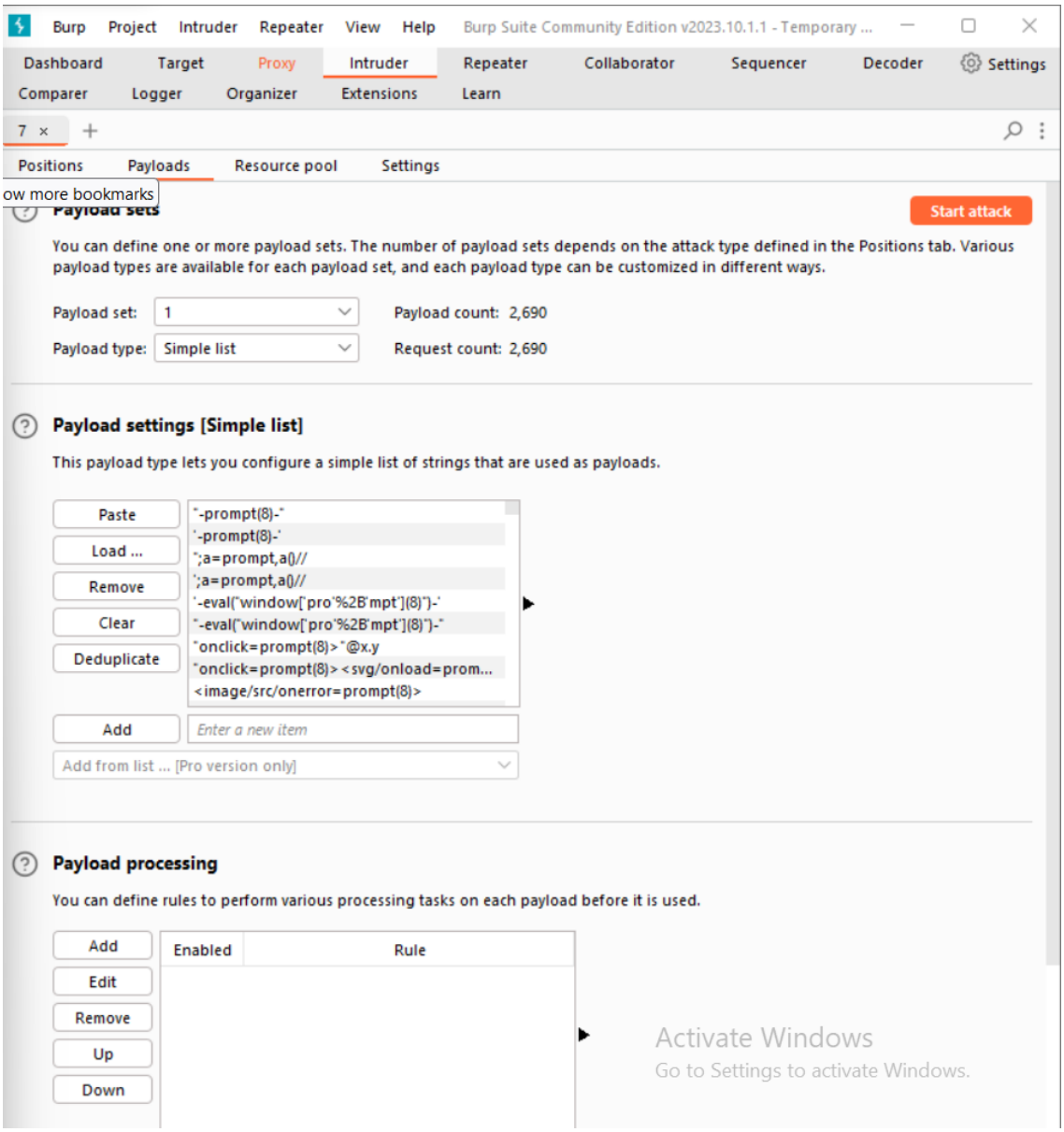
   → First we will get the code in the burp suite after turning the intercept on and passing on the request:



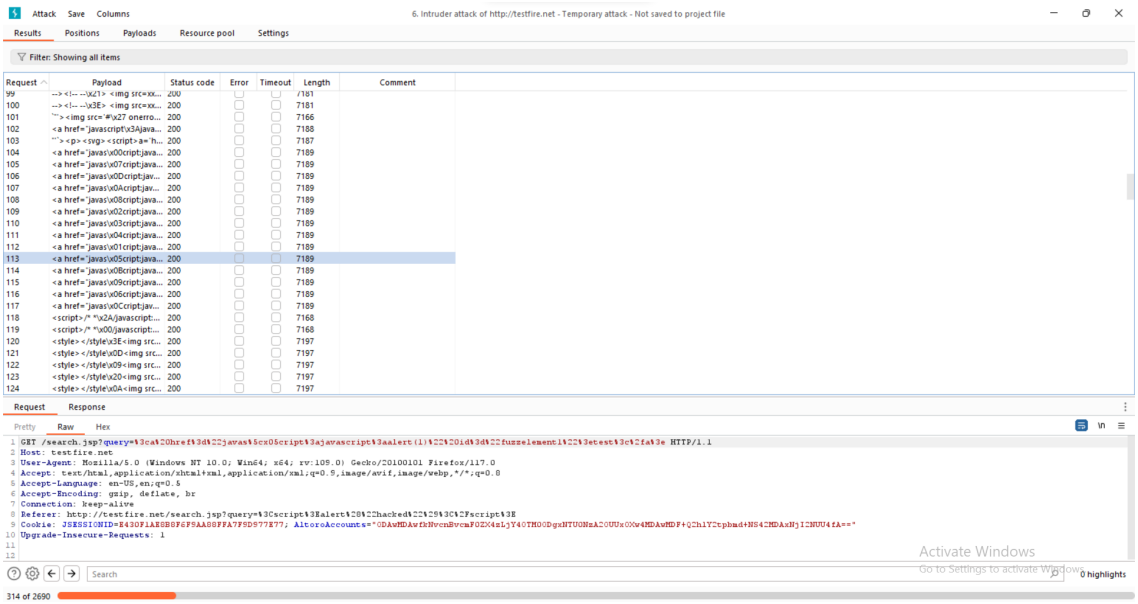
→ We will now pass this to the intruder from proxy and set the attack to sniper and add the target which is obviously the searching script:



→ Now i picked up a XSS payload list from github and started the attack:

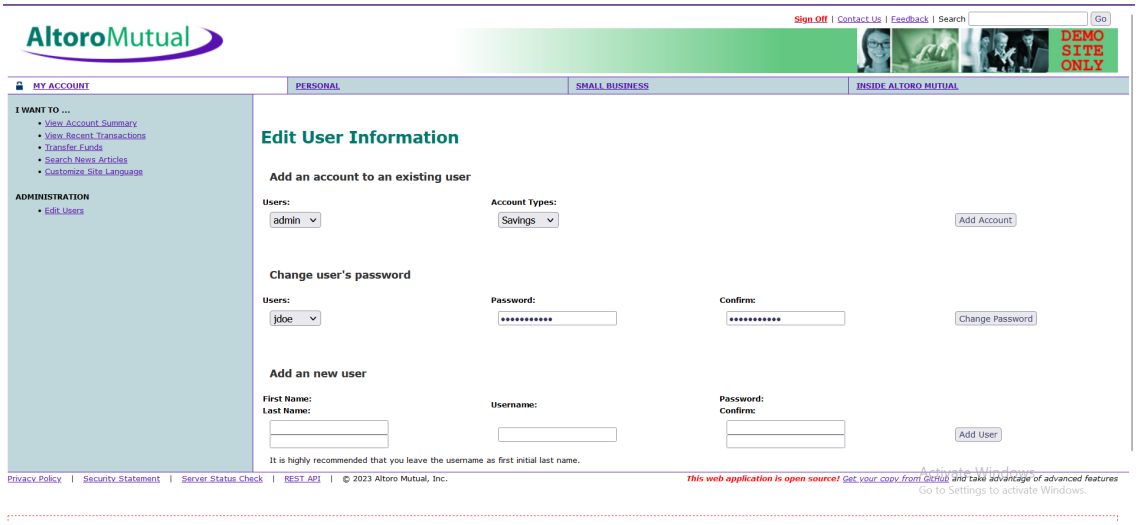


→ Here we can see that our requests responds with 200 status code. Which means they are successful, here we can also see more information of one successful request:

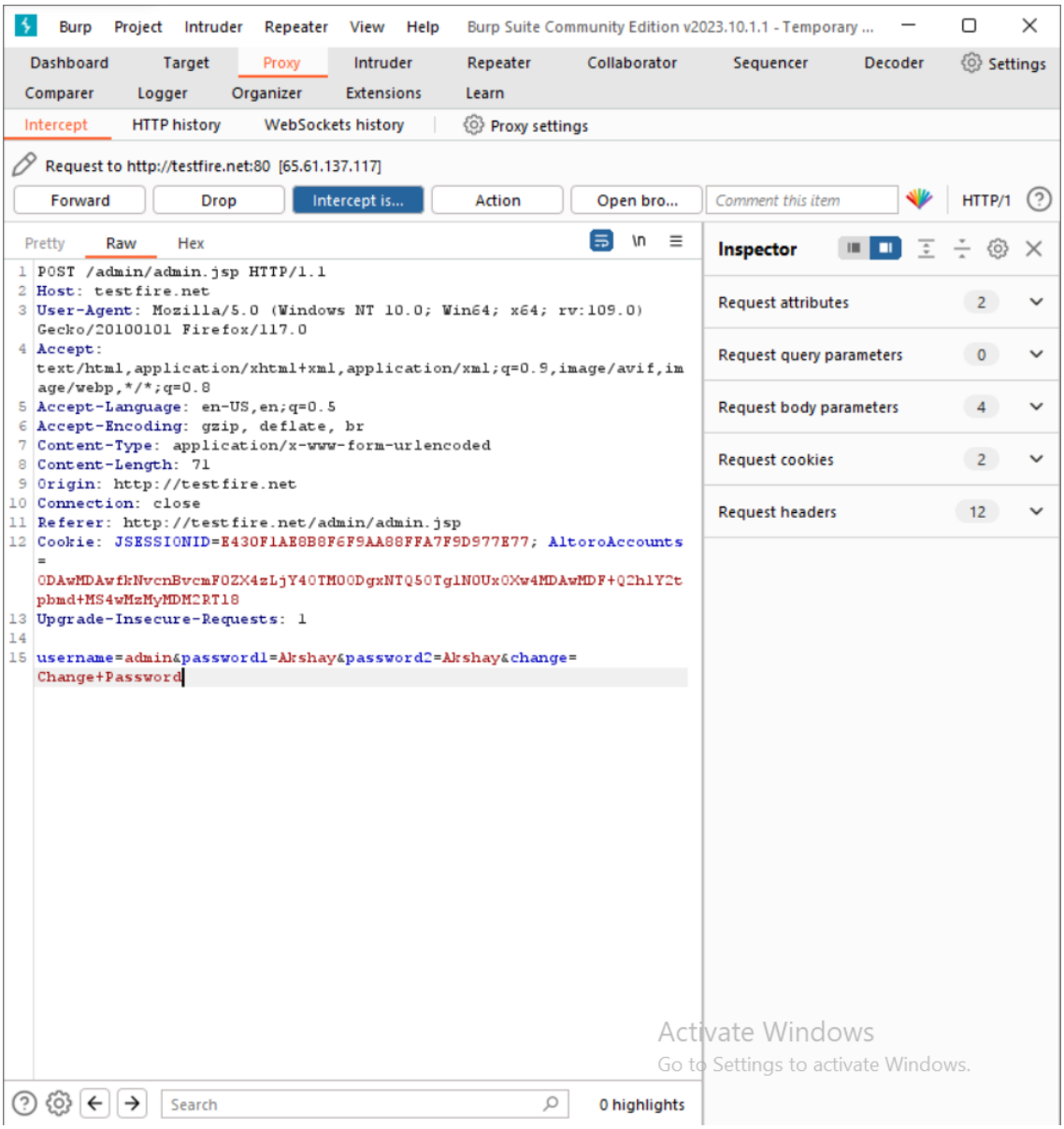


3. **Cross-site Request Forgery (CSRF)**

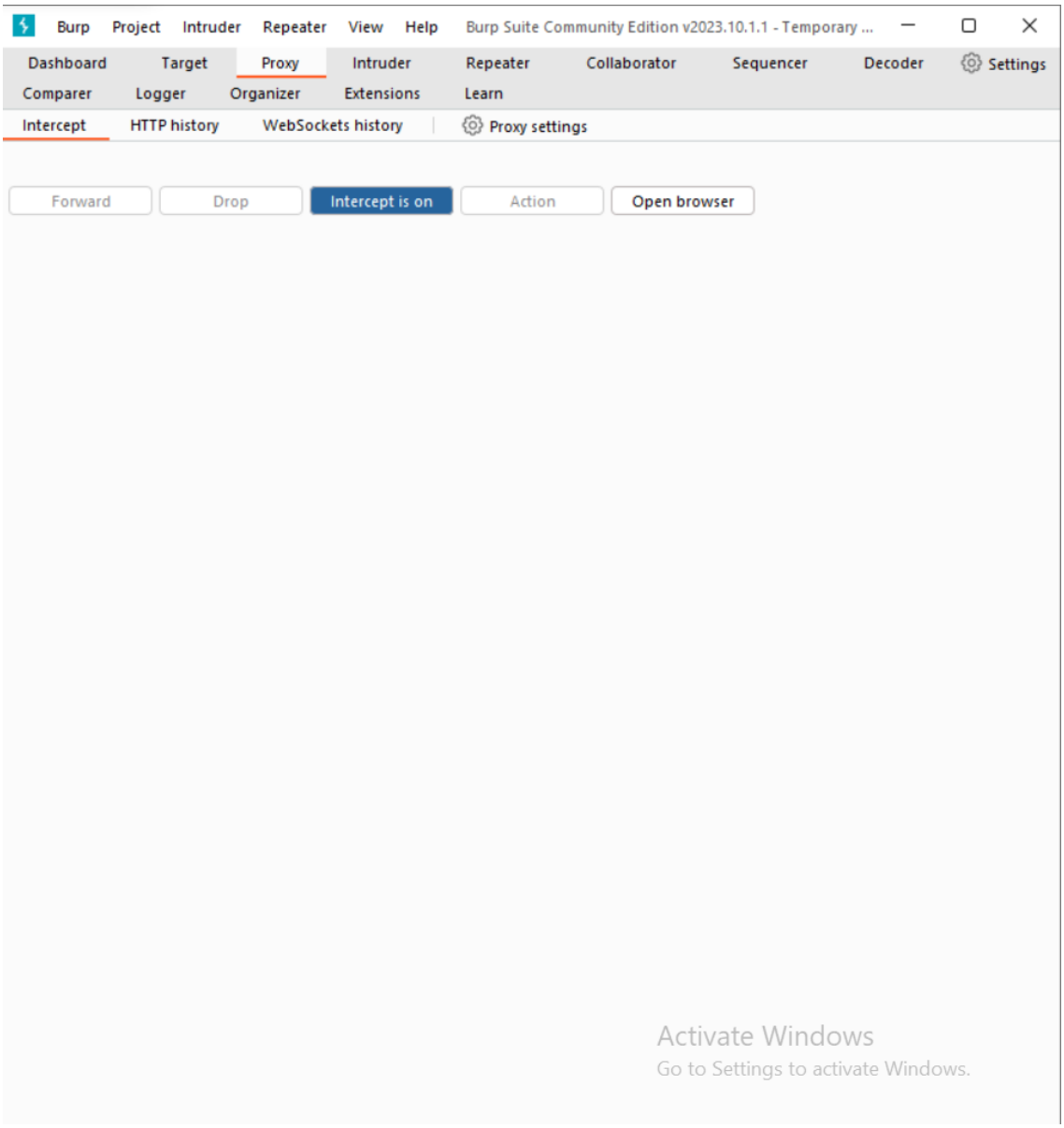
→ Suppose a user is changing his/her password:

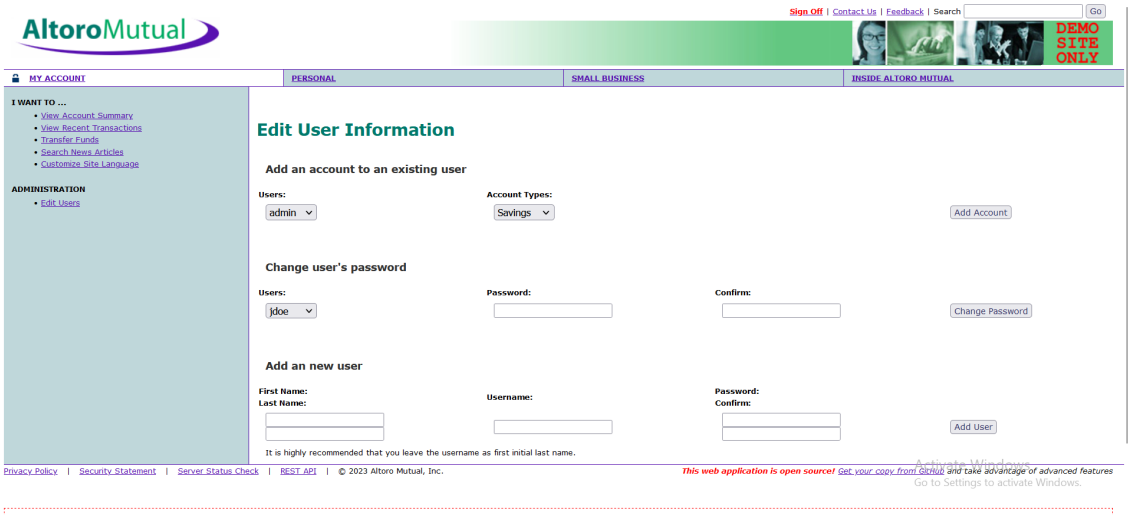


→ Since we have turned on the intercept, the information will be gathered in between and we will get the new password:

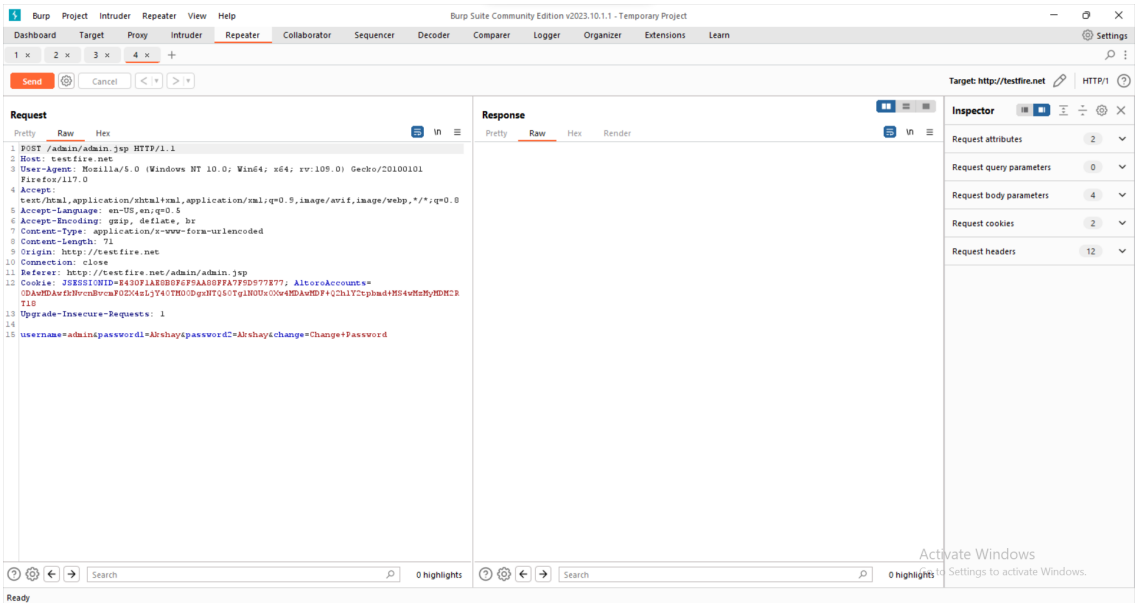


→ Now what we will do is that we will pass this to repeater and forward the request from the proxy. This will show that the password has been changed at the user's interface and hence will show no error:

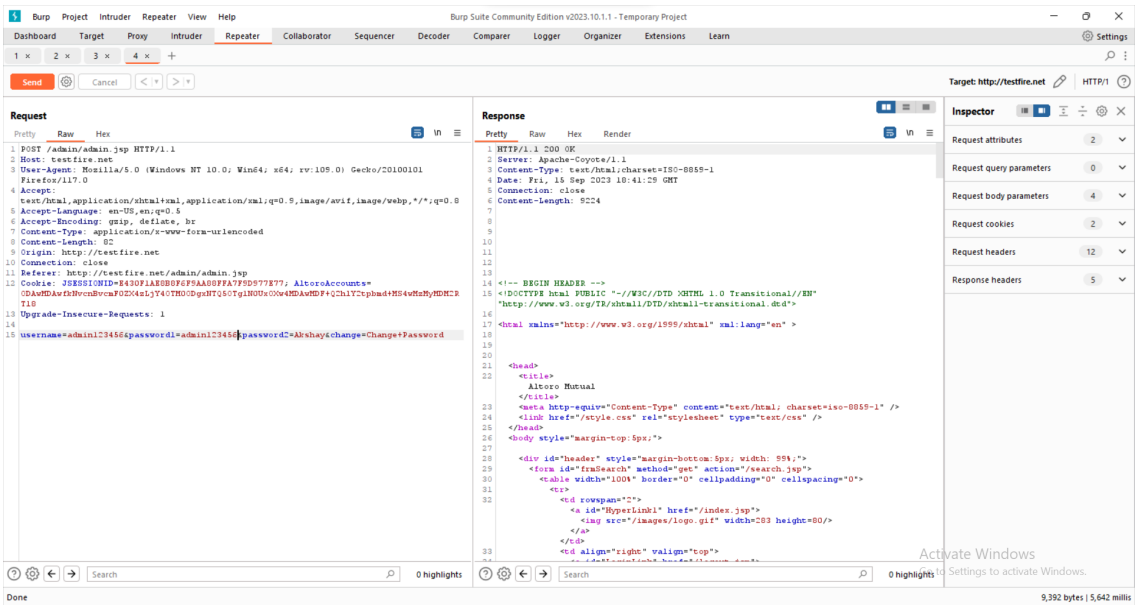

Burp
Project
Intruder
Repeater
View
Help
Burp Suite Community Edition v2023.10.1.1 - Temporary ...
Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Settings
Comparer
Logger
Organizer
Extensions
Learn
Intercept
HTTP history
WebSockets history
Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
Activate Windows
Go to Settings to activate Windows.



→ Now that the user is unaware of the situation as he has been given no error and that the password has been changed, we will switch over to the repeater:



→ Now we will change the password here to “Admin123456” (as different length to previous password). In the below screenshot we can see that the password has been changed as we got 200 status code:


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.10.1.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send Cancel
Target: http://testfire.net
HTTP/1
Request
Pretty Raw Hex
POST /admin/admin.jsp HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 82
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/admin/admin.jsp
Cookie: JSESSIONID=E430F1AE8B6F6F9AA86FFA7F5D577E77; AltoroAccounts=ODAwMDAwfkNvcnBvcmF0ZX4zLjY4OTM0ODgxNTQ5OTgiNGUxO0w4MDAwMDF+QCh1Y2tpbmd+MS4wMzMyMDM2RT10
Upgrade-Insecure-Requests: 1
username=admin123456&password1=admin123456&password2=Akshay&change=Change+Password
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Fri, 15 Sep 2023 18:41:29 GMT
Connection: close
Content-Length: 9224
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
<head>
<title>
Altoro Mutual
</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2">

</td>
<td align="right" valign="top">
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 4
Request cookies 2
Request headers 12
Response headers 5
Search
0 highlights
Search
0 highlights
Activate Windows
Go to Settings to activate Windows.
Done
9,392 bytes | 5,642 millis