**Experiment No. 11**

# Title: BURP Intruder Tab

**Roll No.: 16010420075 Experiments No.: 11**

# Aim: To demonstrate BURP Intruder

\

**Resources:** virtual box

**Theory**

Burp Intruder is a program that automates customized web application attacks. It's highly powerful and adaptable, and it can be used to do everything from brute-force guessing web directories to active exploitation of complicated blind SQL injection vulnerabilities.

Burp Intruder works by taking an HTTP request (referred to as the "base request"), altering it in a methodical manner, issuing each modified version of the request, and evaluating the application's answers for interesting features.

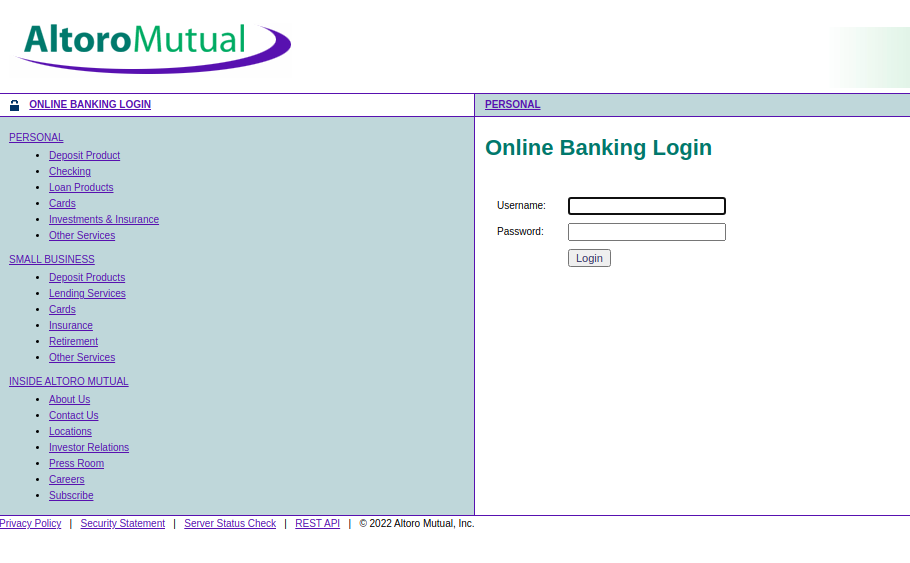
You must indicate one or more sets of payloads for each assault, as well as the spots in the basic request where the payloads should be placed. There are numerous methods for creating payloads (including simple lists of strings, numbers, dates, brute force, bit flipping, and many others). Different algorithms can be used to arrange payloads into payload slots. Several tools are provided to assist in the analysis of the data and the identification of intriguing topics for further inquiry.

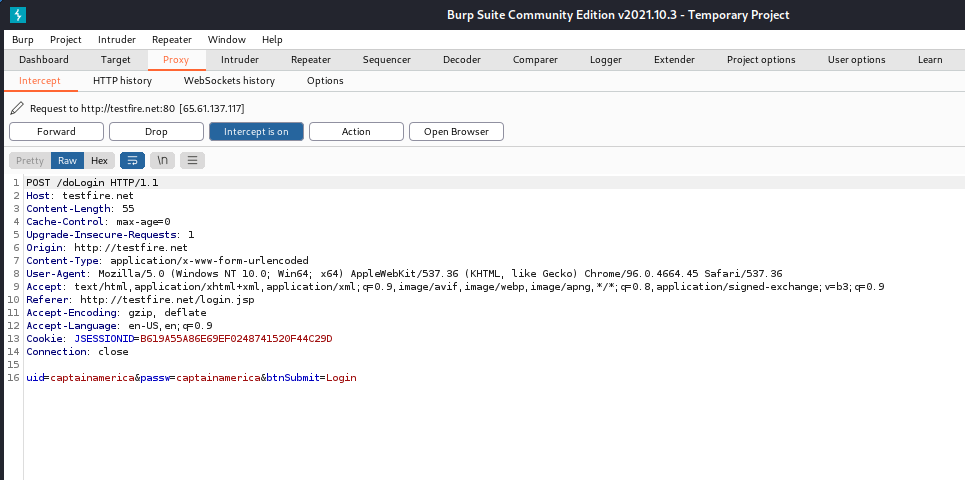
Many input-based vulnerabilities, including as SQL injection, cross-site scripting, and file path traversal, can be discovered by sending various test strings as request parameters and looking for error messages and other oddities in the application's responses. Manual testing is a time-consuming and arduous task given the size and complexity of today's apps.

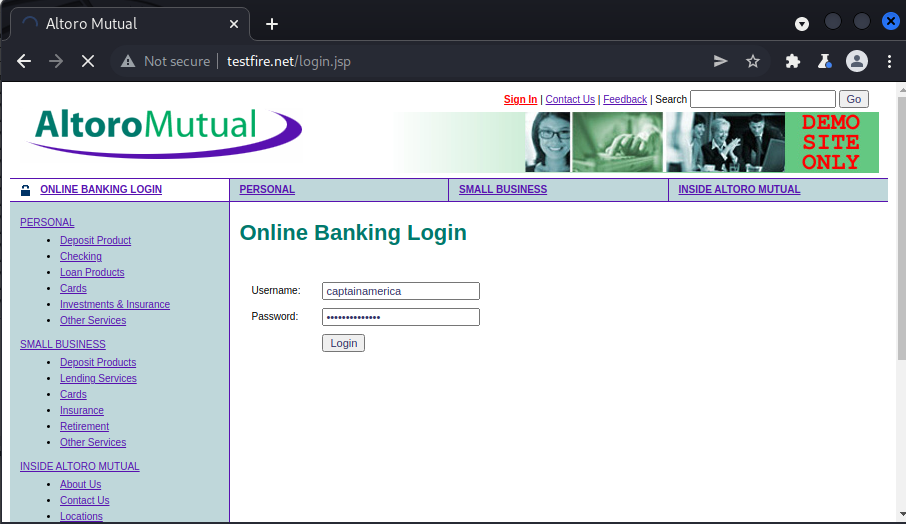
**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**IMPLEMENTATION AND RESULTS:**

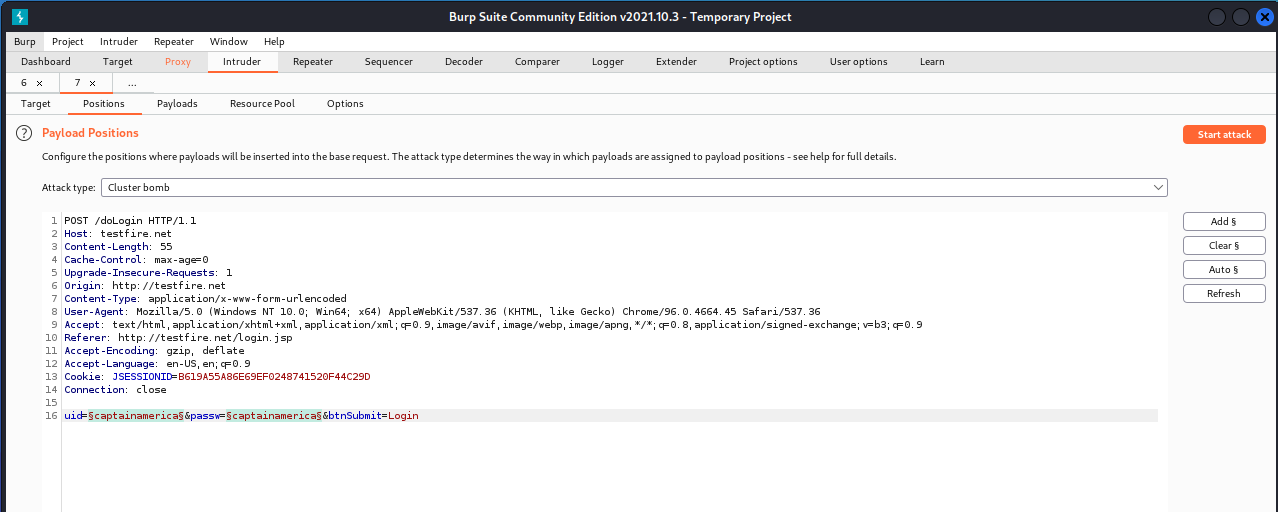
1. Go to [www.testfire.net](http://www.testfire.net) using BURP Site Intruder
2. For demo purposes, we will use captainamerica and username and captianamerica as password.We will be intercepting the request on the burp suite to change the username and password.



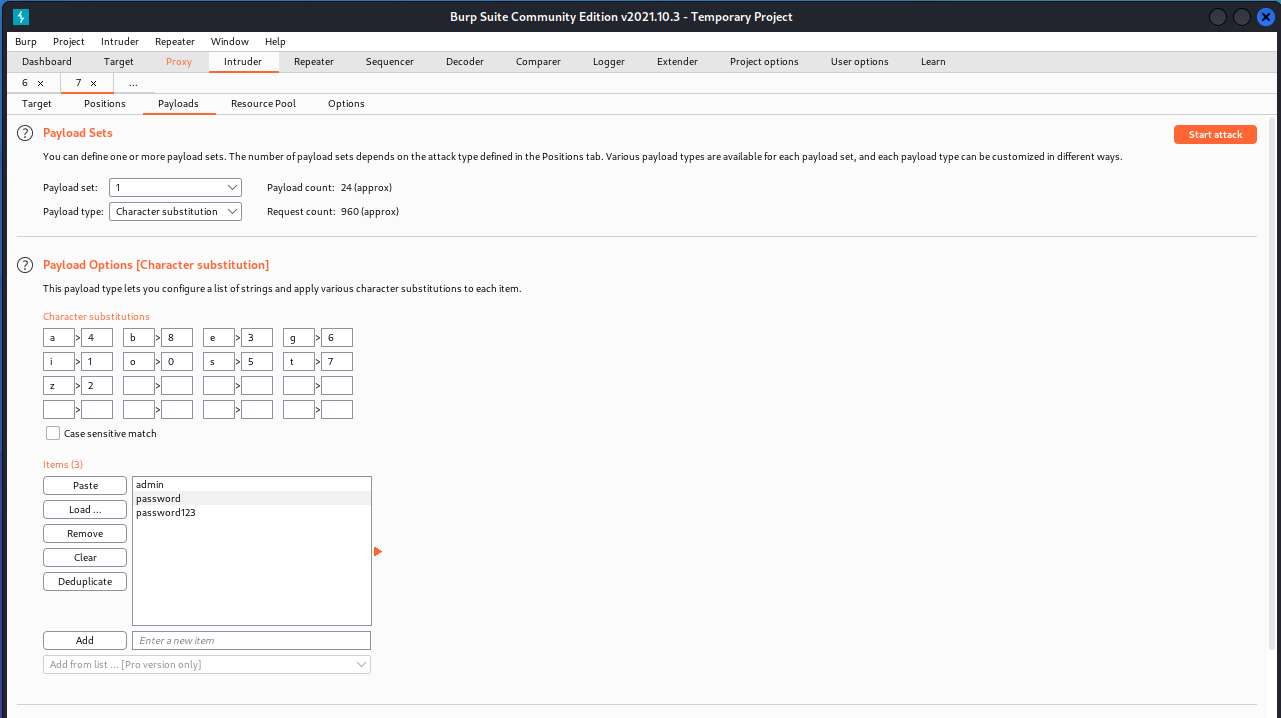


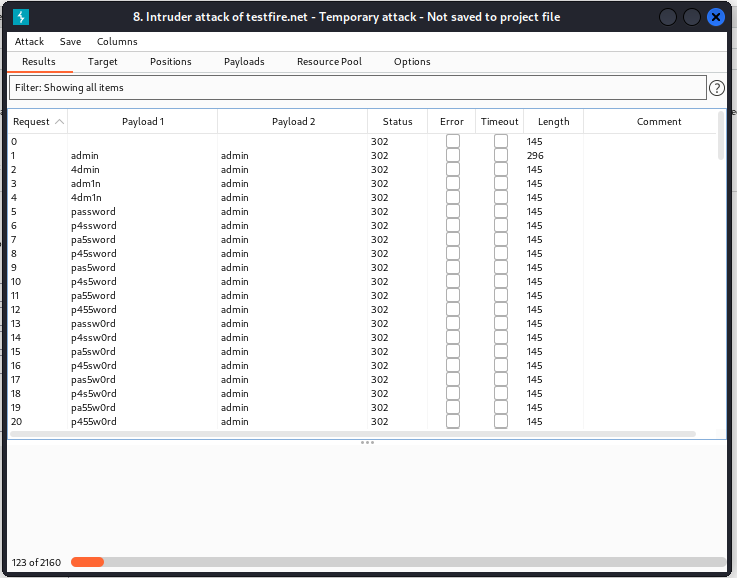


1. The request will be sent to Burp Suite Intruder, which will brute force the password. We'll clear the selections for brute force in the Position tab of Burp Suite Intruder, and then specifically choose our erroneously entered username and password on the page. This enables Burp Suite to highlight the fields that needs to be brute-forced.

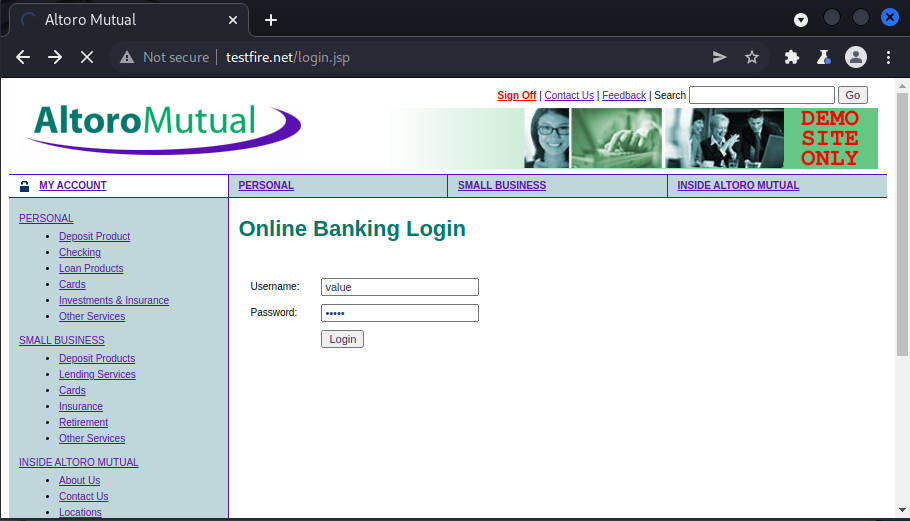


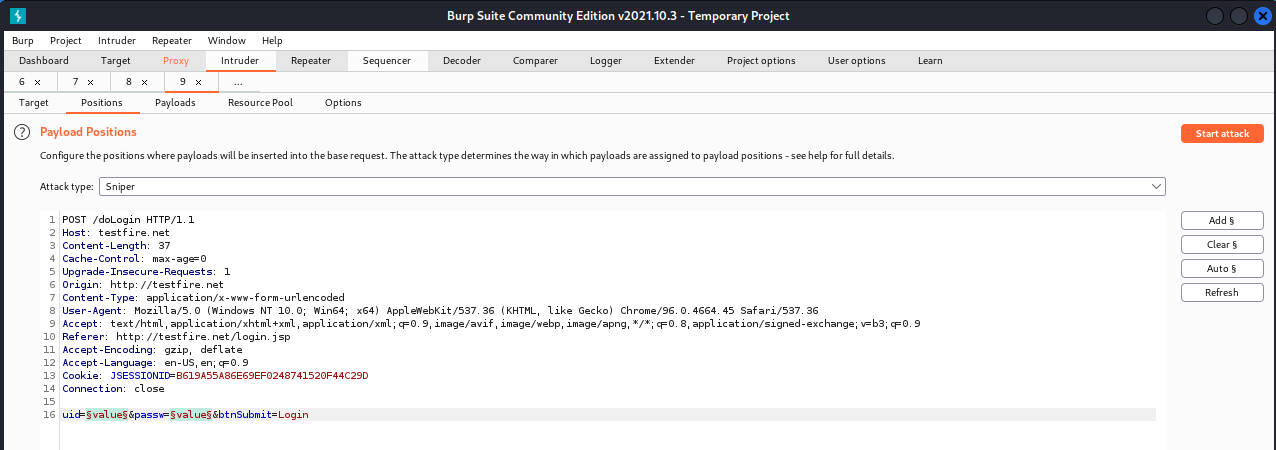
1. In this suite, we'll use the Cluster Bomb Attack Type. This is because both the username and password sections will be brute-forced. The attack iterates through each payload set one by one, testing all possible payload combinations. If there are two payload positions, the attack will place the first payload from payload set 2 in position 2, then iterate through all the payloads in payload set 1 in position 1; finally, it will place the second payload from payload set 2 in position 2, then iterate through all the payloads in payload set 1 in position 1. This attack type is appropriate when an attack necessitates the insertion of unrelated or unknown input in many locations across the request (e.g., when guessing credentials, a username in one parameter, and a password in another parameter like this case).

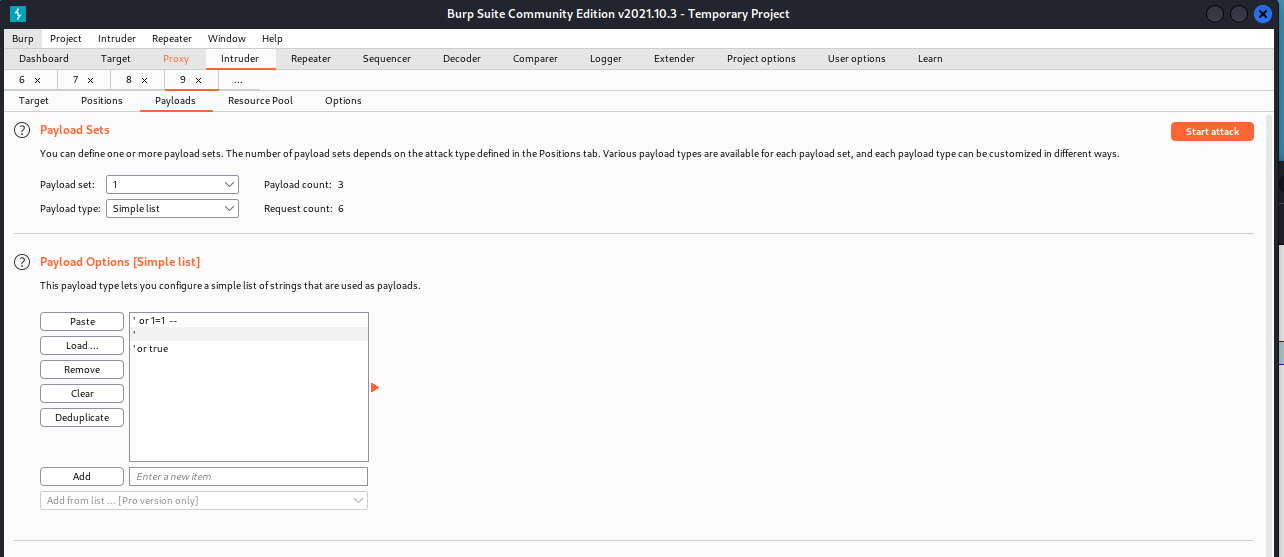


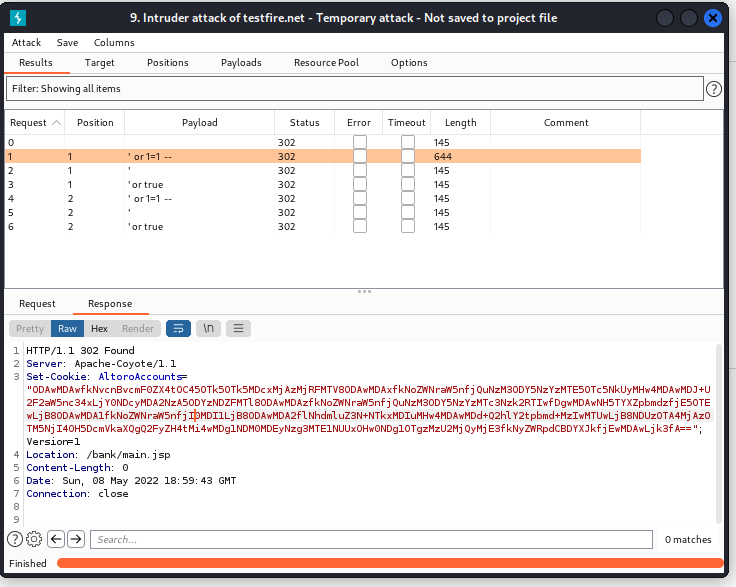


1. Admin and admin have triggered a different duration than other brute forces, as we can see in the first choice of the payloads. The proper pattern is indicated by a change in status code or length in comparison to other possibilities. Using the brute force method, we were able to crack the password and username accurately.

Now, for the SQL injection attack on the website, we'll use value in the username and password input fields, and we won't be able to use any input like ‘ because the website will sanitize the input field, which is a popular technique of SQL injection prevention.



1. In the payload section, we'll list the many SQL injection techniques that can be used to get access to various users. Because a SQL injection assault can take a long time, I've put the solution to SQL injection at the top of the list, along with only a few payload options.



1. We have been granted admin access to the website, as evidenced by the cookie and location. As a result, our SQL injection has been successful.

**Outcomes:**

**CO-3:** Comprehend purpose of Anonymity and Foot printing.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Conclusion: (Conclusion to be based on the objectives and outcomes achieved)**

Usage of BURP Intruder Suite was successfully understood and its tasks were accomplished.

**Grade: AA / AB / BB / BC / CC / CD /DD**

**Signature of faculty in-charge with date**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**REFERENCES:**

* [www.kali.org](http://www.kali.org)