R V COLLEGE OF ENGINEERING

Name: ANKIT **USN:** 1RV18IS007 **Dept/Lab:** ISE/CSDF **Expt No.:** 03 a
Date: 26/11/2021 **Title:** INFORMATION GATHERING TOOLS

---

b. Burp Suite

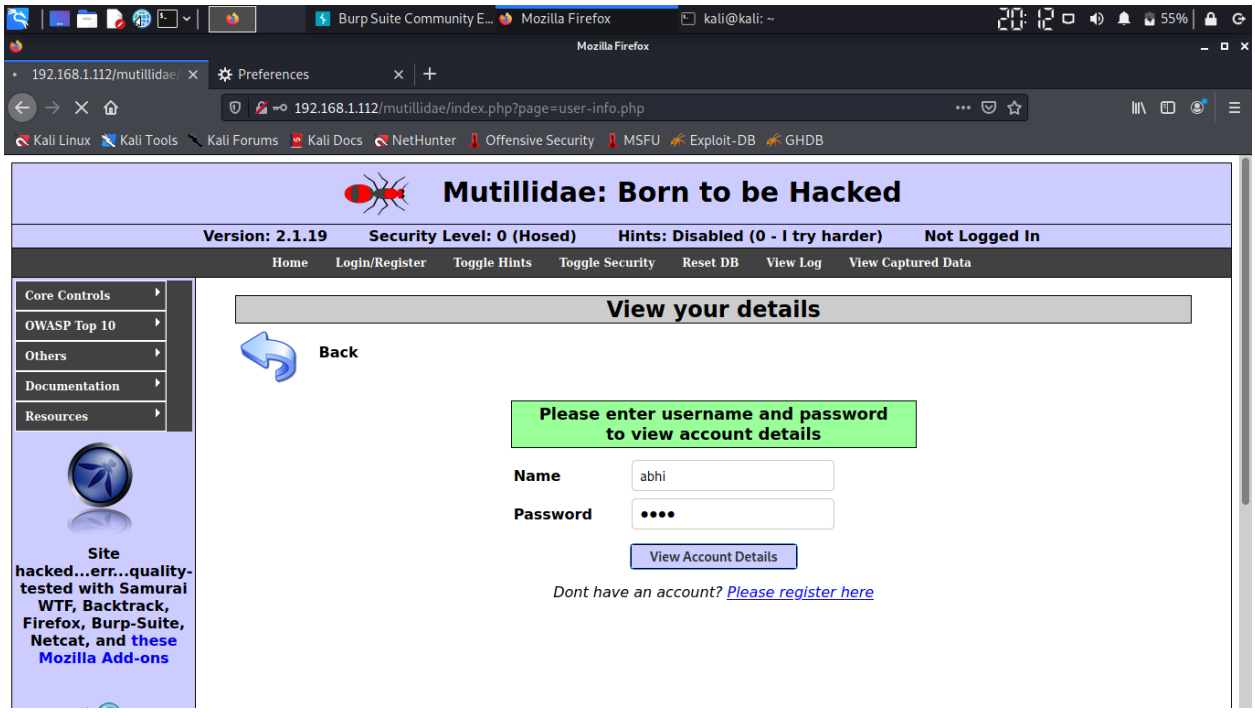
INTRODUCTION

Burp Suite is an integrated platform for performing security testing of web applications. 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.Our target will be Mutillidae, an intentionally vulnerable web app included as part of Metasploitable 2, an intentionally vulnerable Linux virtual machine (VM) designed for testing and practicing purposes.

EXECUTION STEPS

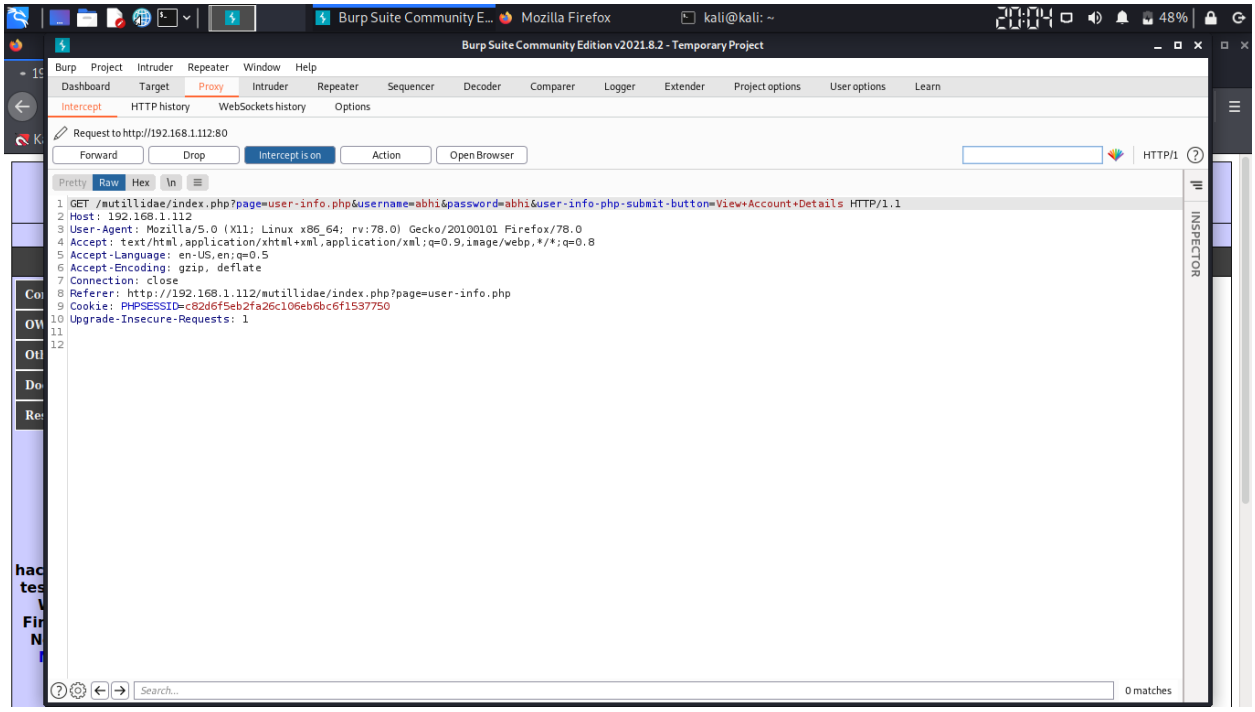
1. **Install a Metasploitable 2 Virtual Machine**
   We need the ip address of the metasploitable VM which can be found using the ifconfig command.

2. **Configure Mutillidae in Your Attack Browse**
   Navigate to a web browser and go to that IP address.Click on "Mutillidae" to enter the web app, then navigate to "OWASP Top 10." Now, select "Injection (SQL)," followed by "Extract Data," then "User Info.".A login screen will appear.



3. **Configure Your Attack Browser for Burp Suite**
   Open up the browser's "Preferences," click on "Advanced," then the "Network" tab. Select "Settings" next to the Connection spot, then make sure it's set to "Manual proxy configuration" and enter 127.0.0.1 as the HTTP Proxy and 8080 as the Port. Next, check "Use this proxy server for all protocols," make sure there is nothing listed under No Proxy for, then click "OK." We're now ready to fire up Burp Suite.

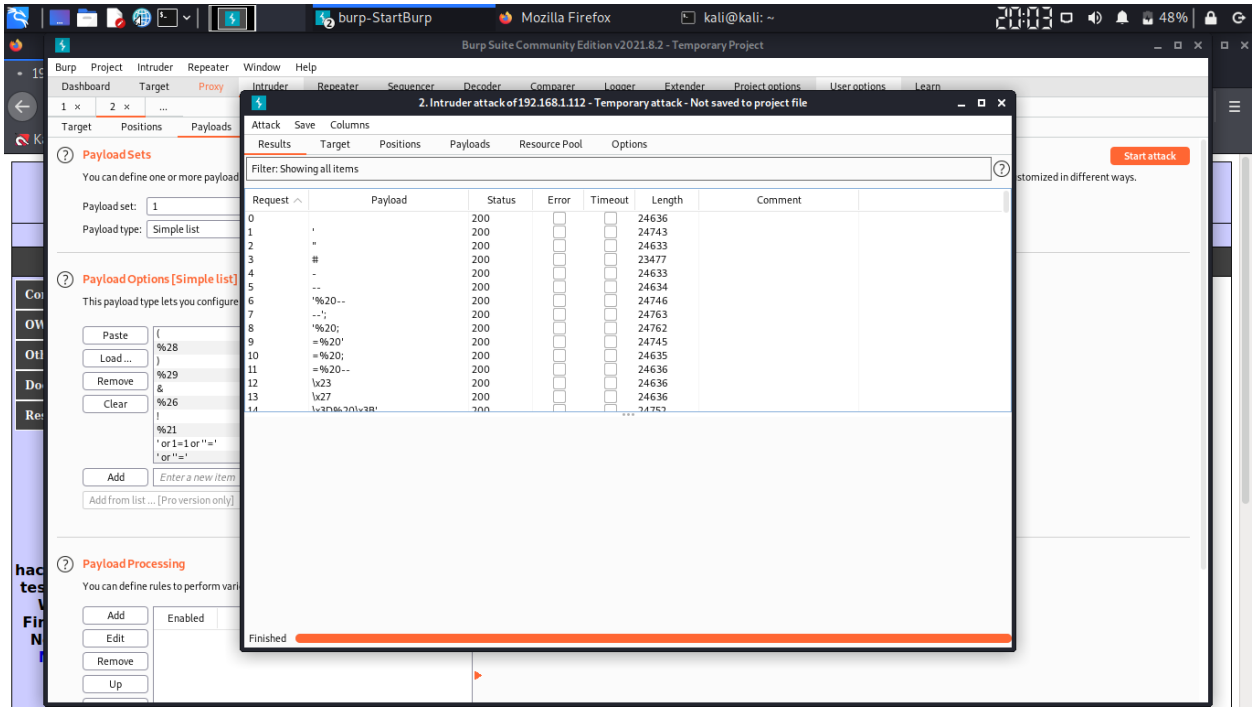
4. **Intercept the Request with Burp Suite**
   Open up the Burp Suite app in Kali, start a new project, then go to the "Proxy" tab and ensure that "Intercept is on" is pressed. This will allow us to modify the request from the webpage and insert different values to test for SQL injection



5. **Configure Positions & Payloads in Burp Suite**

Next, go to the "Intruder" tab, and click on "Positions." Burp Suite automatically configures the positions where payloads are inserted when a request is sent to intruder, but since we are only interested in the username field, we can clear all positions by pressing "Clear" on the right. Highlight the value entered for username, and click the "Add" button. We will use the "Sniper" attack type which will run through a list of values in the payload and try them one at a time.

6. **Configure Positions & Payloads in Burp Suite**
   Click the "Start attack" button, and a new window will pop up showing the intruder attack.



CONCLUSION

1. Although SQL injection has been known as a severe vulnerability for quite some time, it continues to be one of the most common methods of exploitation today
2. This type of attack allows one to retrieve sensitive information, modify existing data, or even destroy entire databases. The most common attack vector for SQL injection is through input fields — login forms, search forms, text boxes, and file upload functions are all excellent candidates for exploitation.

REFERENCES

1. https://null-byte.wonderhowto.com/how-to/attack-web-applications-with-burp-suite-sql-injection-0184090/
2. https://www.kali.org/tools/burpsuite/#:~:text=Burp%20Suite%20is%20an%20integrated,finding%20and%20exploiting%20security%20vulnerabilities.