A project report on

Install VMWare and Kali Linux, and demonstrate the usage and all relevant commands of the BurpSuite tool.

18CSE478T – Operation System Security

Submitted by

Lynn Fernandes (RA2111030010033)
Balwant Patra (RA2111030010045)

Under the guidance of

Dr. M Mahalakshmi
Assistant Professor, NWC

in partial fulfillment of the requirements for the degree of

BACHELOR OF TECHNOLOGY
in
COMPUTER SCIENCE ENGINEERING
with specialization in Cyber Security

DEPARTMENT OF NETWORKING AND COMMUNICATIONS
COLLEGE OF ENGINEERING AND TECHNOLOGY SRM
INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR- 603 203

JULY 2024

BONAFIDE CERTIFICATE

This is to certify that 18CSE478T – Operation System Security, Mini Project titled "**Install VMWare and Kali Linux, and demonstrate the usage and all relevant commands of the BurpSuite tool.**" is the bonafide work of **Lynn Fernandes (RA2111030010033)** and **Balwant Patra (RA2111030010045)** who carried out the project work under my supervision. Certified further, that to the best of my knowledge the work reported here in does not form part of any other thesis or dissertation on the basis of which a degree or award was conferred on an earlier occasion for this or any other candidate

SIGNATURE

Dr. M Mahalakshmi
Assistant Professor
Department of Networking and Communications
SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

SIGNATURE

Lynn Fernandes
Balwant Patra

TABLE OF CONTENTS

ABSTRACT

In cybersecurity and penetration testing, virtualization tools like VMware are essential for creating secure, isolated environments conducive to experimentation. This abstract focuses on the installation of VMware Workstation or VMware Player to host virtual machines (VMs) and setting up Kali Linux—a specialized distribution renowned for its extensive penetration testing tools. Begin by downloading and installing VMware on the host system, enabling the creation of VMs configured to support Kali Linux effectively. Once VMware is installed, proceed to download the latest Kali Linux ISO from the official website and use it to set up a VM within VMware, ensuring adequate allocation of resources such as CPU cores, RAM, and disk space. Post-installation, update Kali Linux using standard package management tools (`apt-get update` and `apt-get upgrade`) to ensure all security patches and essential tools are up to date.

For demonstrating web application security testing, this abstract introduces Burp Suite, a powerful toolkit widely used for assessing web application vulnerabilities. Burp Suite's capabilities include intercepting and modifying HTTP/S requests, scanning for vulnerabilities, performing automated attacks, and manually testing application responses. Participants will gain hands-on experience with Burp Suite's Proxy feature to intercept and modify web traffic, its Scanner module for automated vulnerability detection, the Intruder module for customizable attacks, and the Repeater module for detailed request manipulation and testing. By showcasing these tools within a controlled environment, this abstract aims to equip participants with practical skills essential for identifying and mitigating web application security risks effectively.

INTRODUCTION

In the realm of cybersecurity and ethical hacking, the ability to create secure and isolated testing environments is paramount. Virtualization technologies such as VMware provide the foundation for establishing these environments, allowing for the safe deployment and operation of various operating systems and tools. This abstract delves into the process of setting up VMware Workstation or VMware Player to host virtual machines (VMs), specifically configured for running Kali Linux—a specialized distribution favored for its robust suite of penetration testing tools. Alongside the installation of Kali Linux from the latest ISO, this exploration includes essential updates and configurations to prepare the environment for penetration testing exercises. Additionally, the abstract explores the practical application of Burp Suite, a leading web application security testing tool renowned for its comprehensive capabilities in analyzing, intercepting, and manipulating HTTP/S traffic. By demonstrating the setup and usage of these tools within a controlled environment, participants gain foundational knowledge essential for conducting effective security assessments and mitigating vulnerabilities in web applications.

REQUIREMENTS

Hardware Requirements

CPU:

- Minimum: Dual-core processor (Intel Core i3 or AMD equivalent)
- Recommended: Quad-core processor (Intel Core i5 or AMD equivalent)

RAM:

- Minimum: 4 GB RAM
- Recommended: 8 GB RAM or more

Storage:

- Minimum: 20 GB free disk space for VMware and virtual machines
- Recommended: 40 GB or more for comfortable operation, especially if running multiple VMs simultaneously

Graphics:

- Basic graphics support capable of running VMware's graphical interface smoothly

Network:

- Ethernet or WiFi adapter for internet connectivity within virtual machines

Operating System:

- Host OS: Compatible with VMware Workstation or VMware Player (Windows, macOS, or Linux)

Software Requirements

- **VMware Workstation** or **VMware Player**: Install the latest version compatible with your operating system (Windows, macOS, Linux). VMware provides the platform for creating and managing virtual machines (VMs).

- **Host Operating System**: Ensure your host OS is compatible with VMware Workstation or VMware Player. Commonly used OS include Windows (7/8/10), macOS (OS X 10.9 or later), and various Linux distributions.

●Download the latest Kali Linux ISO from the official website (https://www.kali.org/downloads/). This ISO will be used to install Kali Linux on a virtual machine within VMware.

●Burp Suite is available in different editions. The Community Edition is suitable for basic security testing tasks and can be downloaded from PortSwigger's website: Burp Suite Community Edition.

●Ensure network connectivity within VMware virtual machines. VMware offers various networking options (NAT, bridged, host-only) to suit different testing scenarios.

●Use a text editor within Kali Linux for script editing and configuration adjustments (e.g., Vim, Nano).

●Have a web browser installed within Kali Linux for testing and interacting with web applications during security assessments (e.g., Firefox, Chromium).

●Familiarize yourself with package management tools (`apt-get` or `apt` in Kali Linux) for installing, updating, and managing software packages and dependencies.

●Burp Suite requires Java to run. Ensure a compatible version of JRE is installed on your host system or within the virtual machine running Burp Suite.

IMPLEMENTATION

Step 1: Install VMware

1. **Download VMware:**
   - Visit the VMware website (https://www.vmware.com/) and download the appropriate version of VMware Workstation or VMware Player for your operating system.
2. **Install VMware:**
   - Follow the installation wizard prompts to install VMware on your host system.
   - Launch VMware after installation and ensure it's ready to create and manage virtual machines.

Step 2: Set Up a Virtual Machine for Kali Linux

1. **Download Kali Linux ISO:**
   - Go to the official Kali Linux website (https://www.kali.org/downloads/) and download the latest Kali Linux ISO image.
2. **Create a New Virtual Machine:**
   - Open VMware, click on "Create a New Virtual Machine" or "New Virtual Machine" depending on your version.
   - Choose "Installer disc image file (ISO)" and browse to the downloaded Kali Linux ISO file.
3. **Configure Virtual Machine Settings:**
   - Allocate resources (CPU cores, RAM, disk space) according to your hardware capabilities and the demands of Kali Linux.
   - Choose networking options (NAT, bridged, or host-only) based on your testing requirements.
4. **Install Kali Linux:**
   - Start the virtual machine and follow the on-screen instructions to install Kali Linux using the graphical installer.
   - Set up root and user credentials during the installation process.

Step 3: Install Burp Suite

1. **Download Burp Suite Community Edition:**
   - Go to PortSwigger's website (https://portswigger.net/burp/communitydownload) and download the Community Edition of Burp Suite.

2. **Install Burp Suite:**
   - Extract the downloaded archive and run the Burp Suite installer.
   - Follow the installation prompts and choose default settings or customize as needed.
3. **Launch Burp Suite:**
   - After installation, launch Burp Suite from your desktop environment or command line.

Step 4: Configure Burp Suite

1. **Configure Proxy Settings:**
   - In Burp Suite, navigate to the "Proxy" tab and configure your browser to use Burp Suite as a proxy (typically using localhost on port 8080).
2. **Explore Features:**
   - Familiarize yourself with Burp Suite's various modules such as Proxy, Scanner, Intruder, and Repeater for intercepting requests, scanning for vulnerabilities, performing attacks, and testing responses.

Step 5: Start Testing and Analysis

1. **Intercept Traffic:**
   - Use Burp Suite's Proxy to intercept HTTP/S requests between your browser and web applications. Analyze and modify requests/responses to identify vulnerabilities.
2. **Use Scanner Module:**
   - Utilize the Scanner module to automate vulnerability detection in web applications. Configure scanning options and review scan results for potential security issues.
3. **Perform Manual Testing:**
   - Employ the Intruder module for performing manual attacks like fuzzing or brute-force to identify weaknesses in input validation or session management.
4. **Validate and Document Findings:**
   - Use the Repeater module to repeat and manipulate requests to validate vulnerabilities and document findings for further analysis or reporting.

BURP SUITE USAGE

Intercepting Traffic

- **Set Up Proxy**: Configure Burp Suite as a proxy and intercept HTTP/S traffic between your browser and the server.
- **Browser Configuration**: Set your browser to use Burp Suite on localhost and port 8080.
- **Intercept Requests**: Analyze and manipulate requests and responses in real-time to identify vulnerabilities or modify parameters.

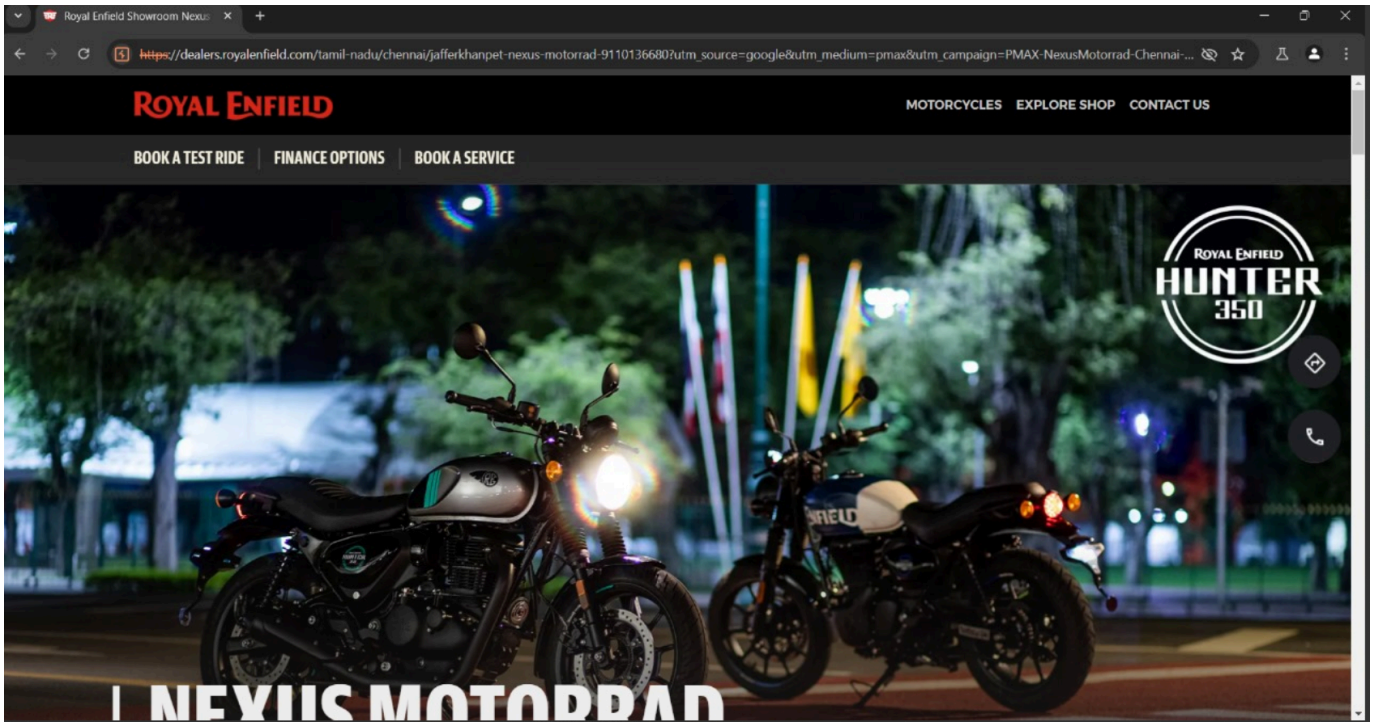
Cracking Passwords

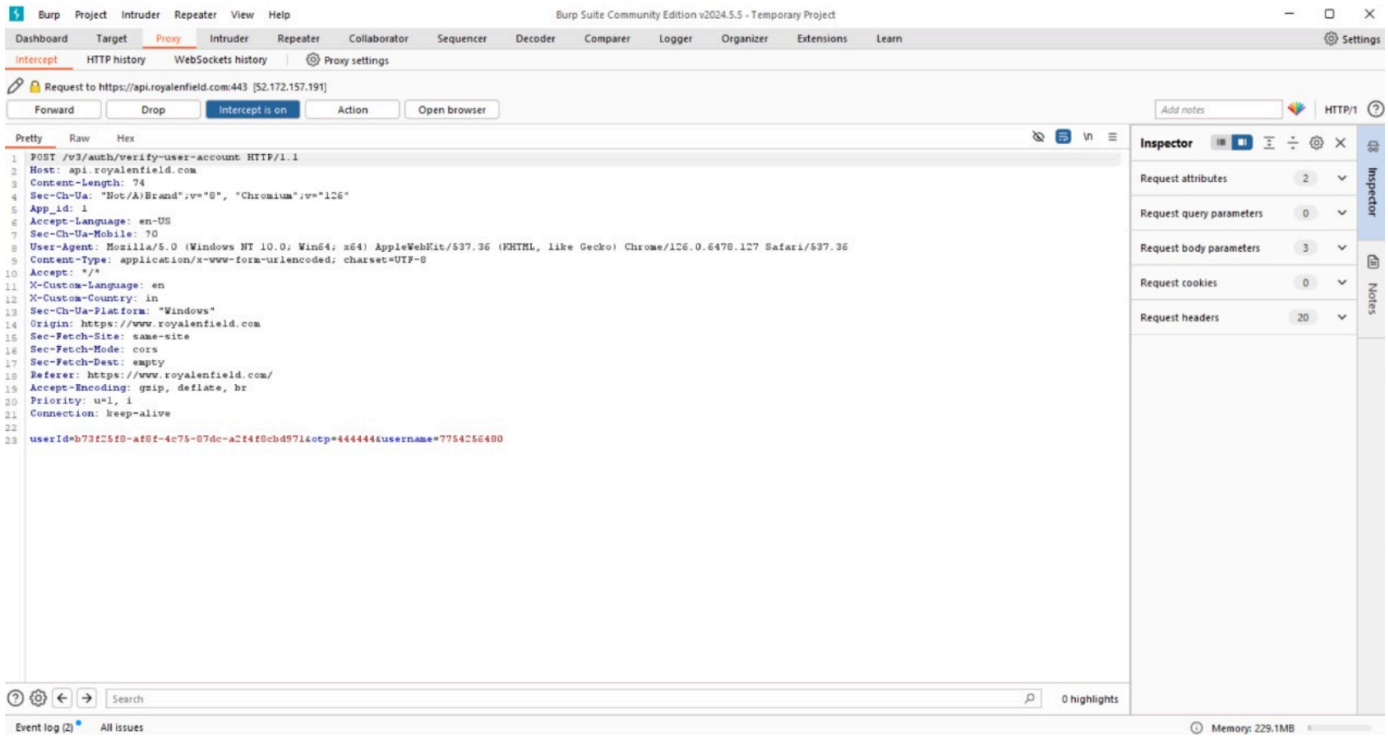
- **Using Intruder**: Load a list of passwords or configure custom payloads in the Intruder tab.
- **Configure Payloads**: Define positions and options for payload attacks, then start the attack to test each payload systematically.
- **Analyze Results**: Review server responses to identify successful login attempts and vulnerabilities in password security.

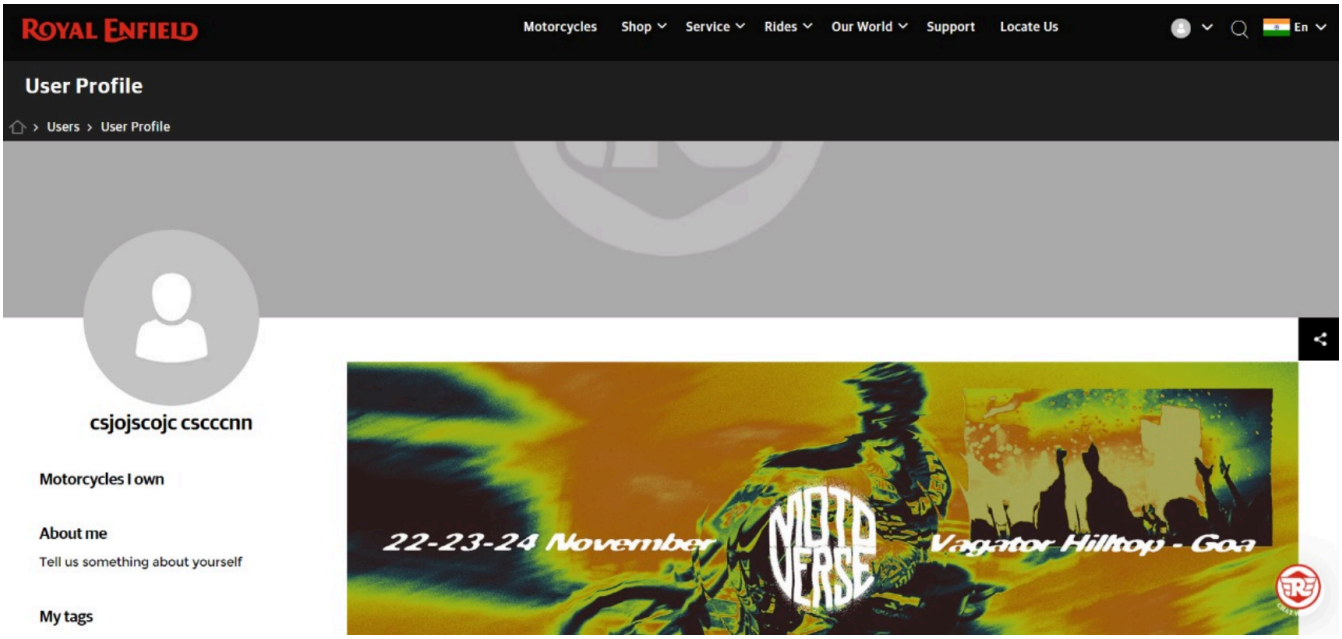
Falsifying Verification of Email and Phone Numbers

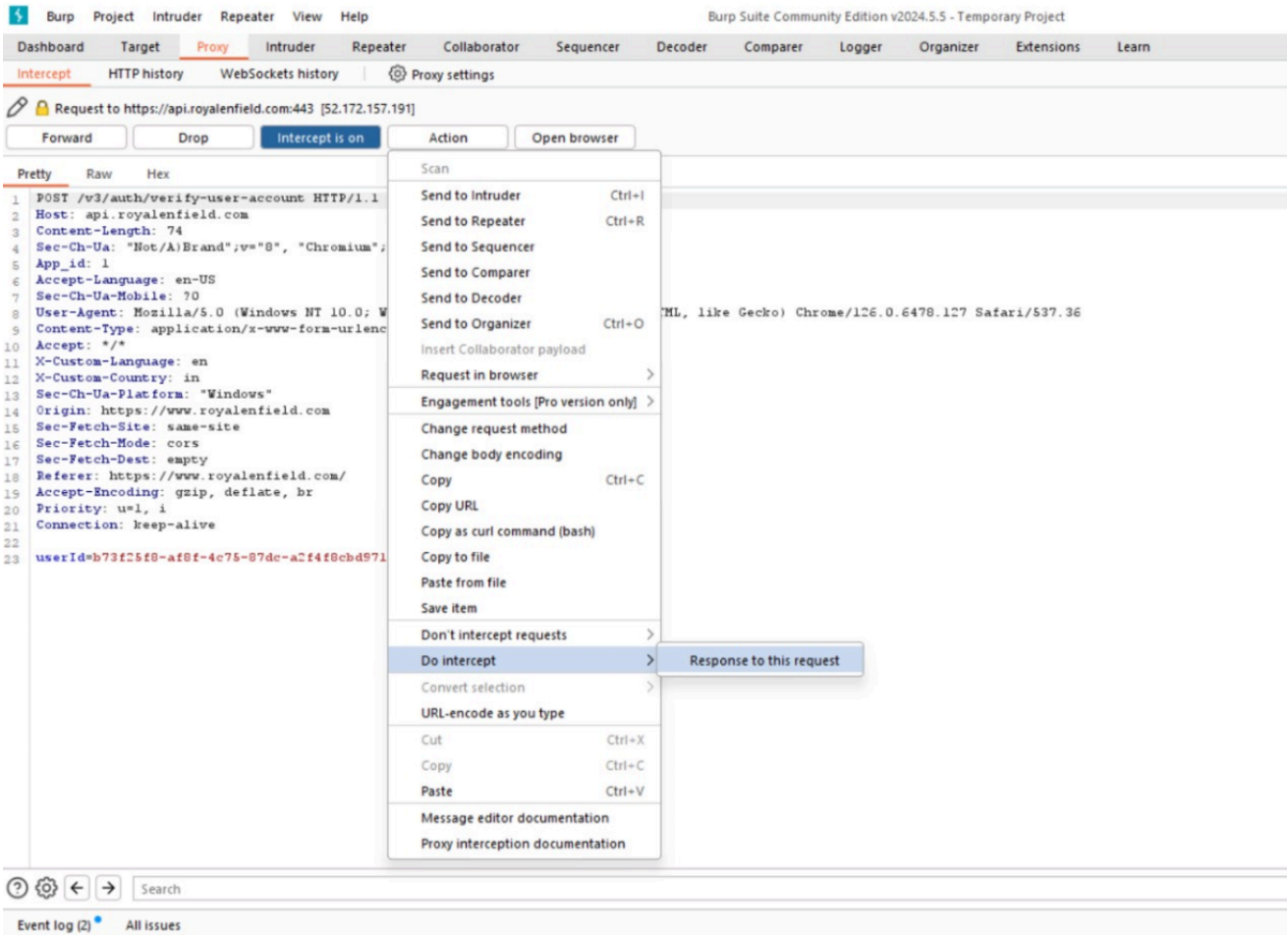
- **Using Repeater**: Capture and modify requests involving email or phone number verification.
- **Modify Parameters**: Change email or phone number parameters to falsified values and resend the request.
- **Observe Server Response**: Analyze how the server responds to verify if falsified information is accepted or if validation errors occur.

Implementation Screenshots

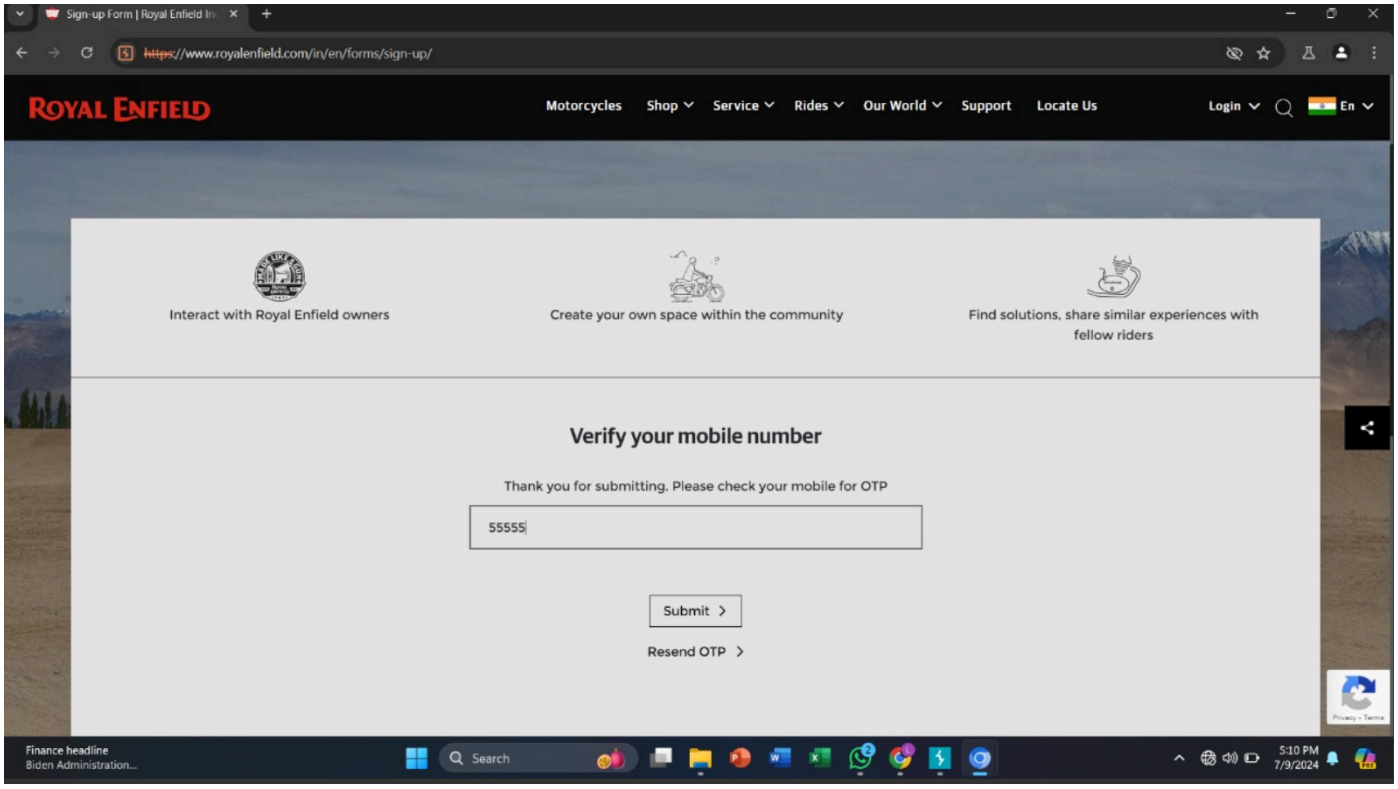


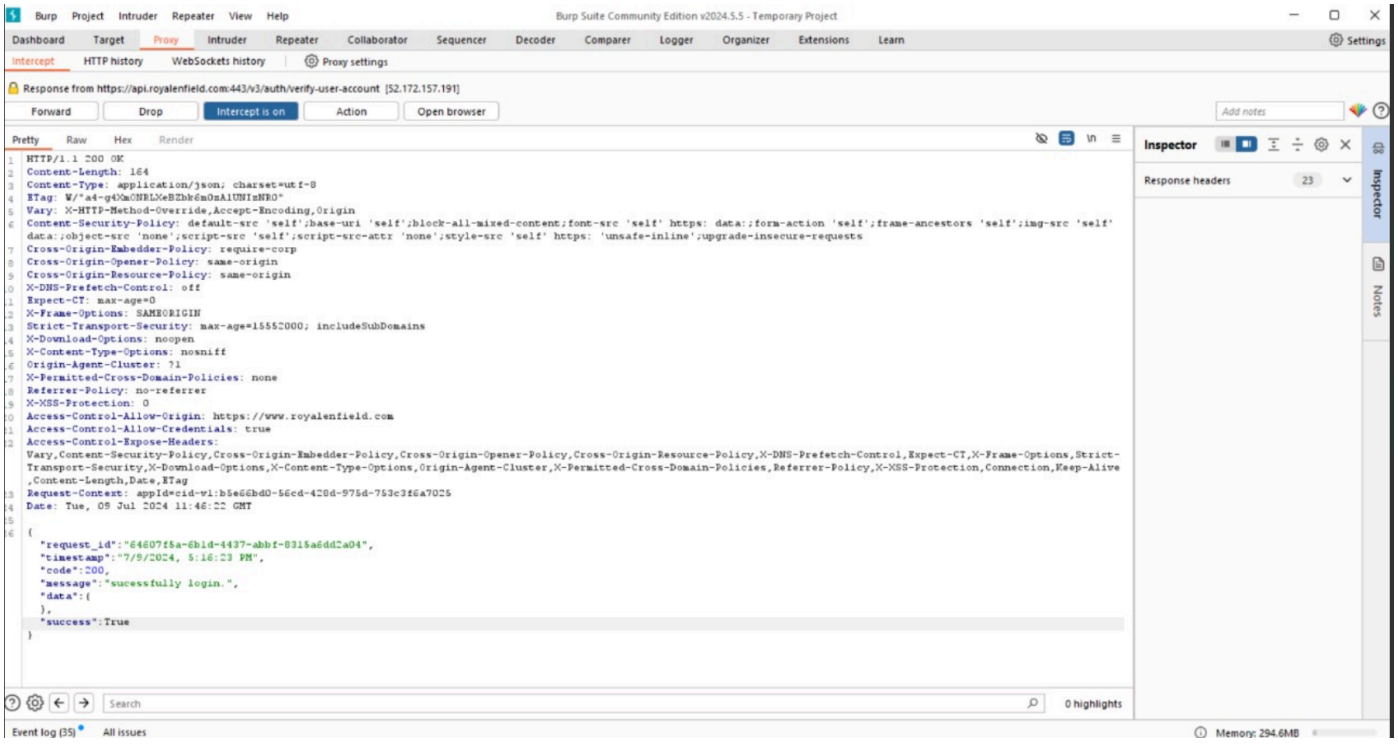


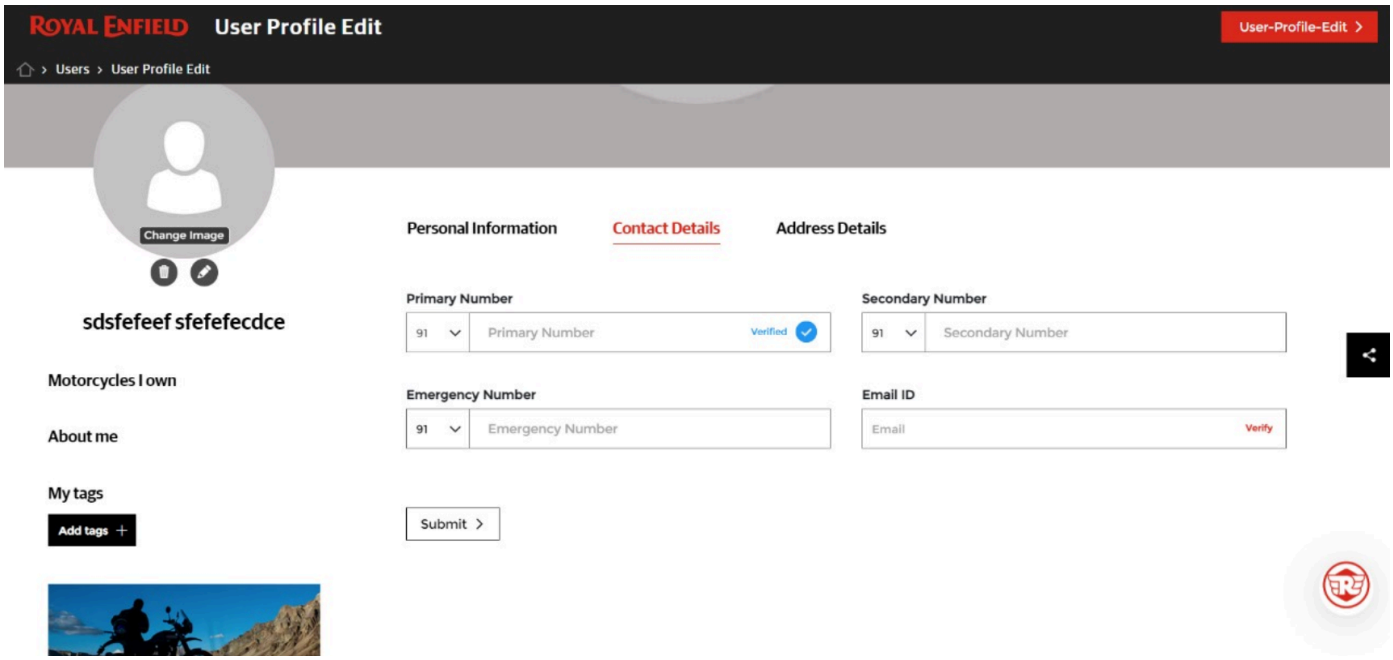

ROYAL ENFIELD
Motorcycles
Shop
Service
Rides
Our World
Support
Locate Us
En
User Profile
Users > User Profile
csjojscojc cscccnn
Motorcycles I own
About me
Tell us something about yourself
My tags
22-23-24 November
MOTOVERSE
Vagator Hilltop - Goa


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.5.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to https://api.royalenfield.com:443 [52.172.157.191]
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
POST /v3/auth/verify-user-account HTTP/1.1
Host: api.royalenfield.com
Content-Length: 74
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";
App_id: 1
Accept-Language: en-US
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; W
Content-Type: application/x-www-form-urlenc
Accept: */*
X-Custom-Language: en
X-Custom-Country: in
Sec-Ch-Ua-Platform: "Windows"
Origin: https://www.royalenfield.com
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.royalenfield.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
userId=b73f25f8-af8f-4c75-87dc-a2f4f8cbd971
ML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer Ctrl+O
Insert Collaborator payload
Request in browser
Engagement tools [Pro version only]
Change request method
Change body encoding
Copy Ctrl+C
Copy URL
Copy as curl command (bash)
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Response to this request
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Proxy interception documentation
Search
Event log (2)
All issues

OUTPUT SCREENSHOTS







CONCLUSION

In summary, Burp Suite emerges as an indispensable tool in the arsenal of cybersecurity professionals for conducting thorough and effective security assessments of web applications. Its capability to intercept and manipulate HTTP/S traffic through the Proxy module provides invaluable insights into how data flows between clients and servers, enabling analysts to identify vulnerabilities such as insecure transmission of sensitive information or inadequate input validation.

The Intruder module within Burp Suite facilitates systematic and targeted attacks on authentication mechanisms, including password cracking. By configuring custom payloads and systematically testing each variation, security testers can assess the strength of password policies and identify weak or easily guessable passwords that could pose security risks if exploited by malicious actors.

Furthermore, the Repeater module empowers testers to falsify verification processes for email addresses and phone numbers. This feature allows security teams to simulate attacks where malicious users attempt to bypass authentication or validation mechanisms by submitting falsified information. Analyzing server responses to these modified requests helps in understanding how resilient the application is against such deception and whether it adequately validates user inputs.

Ethical considerations are paramount throughout these testing activities. Responsible usage of Burp Suite requires obtaining proper authorization from relevant stakeholders and ensuring compliance with legal regulations such as data protection laws. Moreover, ethical hackers must prioritize user privacy and safety, refraining from actions that could cause harm or disrupt normal operations of the tested systems.

In conclusion, Burp Suite not only equips cybersecurity professionals with powerful tools to uncover vulnerabilities and strengthen defenses but also underscores the importance of ethical hacking practices in safeguarding digital assets and user trust. By employing Burp Suite in controlled and ethical testing environments, organizations can proactively identify and remediate security weaknesses, ultimately enhancing their overall cybersecurity posture and resilience against evolving cyber threats.

REFERENCES

1) https://medium.com/@marufrigan9/how-hackers-trick-you-understanding social-engineering-with-set-4a232aa52e43

This Medium article explores how hackers use the Social Engineer Toolkit (SET) to execute social engineering attacks, providing insights into common tactics and vulnerabilities.

2) https://www.vmware.com/products/workstation-player/workstation player-evaluation.html.html

VMware Workstation Player's evaluation page allows users to download and try out the software for free, providing a platform to create and manage virtual machines on a single physical machine.

3) https://www.kali.org/docs/virtualization/install-virtualbox-guest-vm/

This documentation from Kali Linux guides users through installing a VirtualBox guest virtual machine (VM) on their host system, which is useful for testing and running Kali Linux in a virtualized environment.

4) https://owasp.org/

OWASP (Open Web Application Security Project) provides valuable resources on web application security.

5)https://portswigger.net/burp/documentation/desktop/getting-started/intercepting-http-traffic

PortSwigger's intercept feature in Burp Suite allows users to capture and modify HTTP/S traffic between clients and servers, aiding in security testing and vulnerability identification with real-time analysis and manipulation capabilities.