**Performing Web Application Security Testing Using Burp Suite**

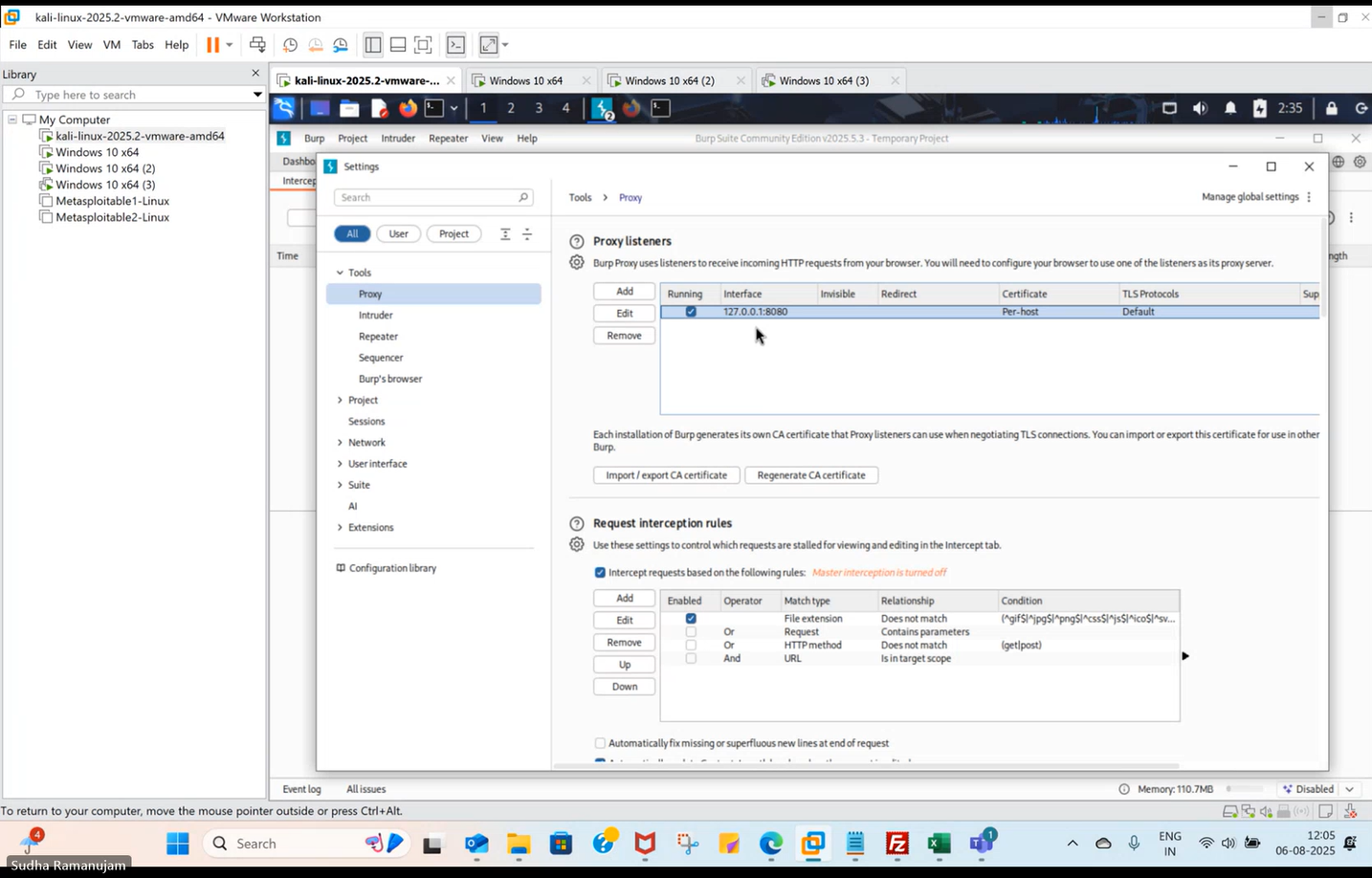
**Burp Suite developed by portswigger is an integrated web security testing tool that works as an intercepting proxy between the browser and the target web server , allowing testers to capture, analyse, and manipulate HTTP(S) traffic, to detect and exploit vulnerabilities in web applications.**

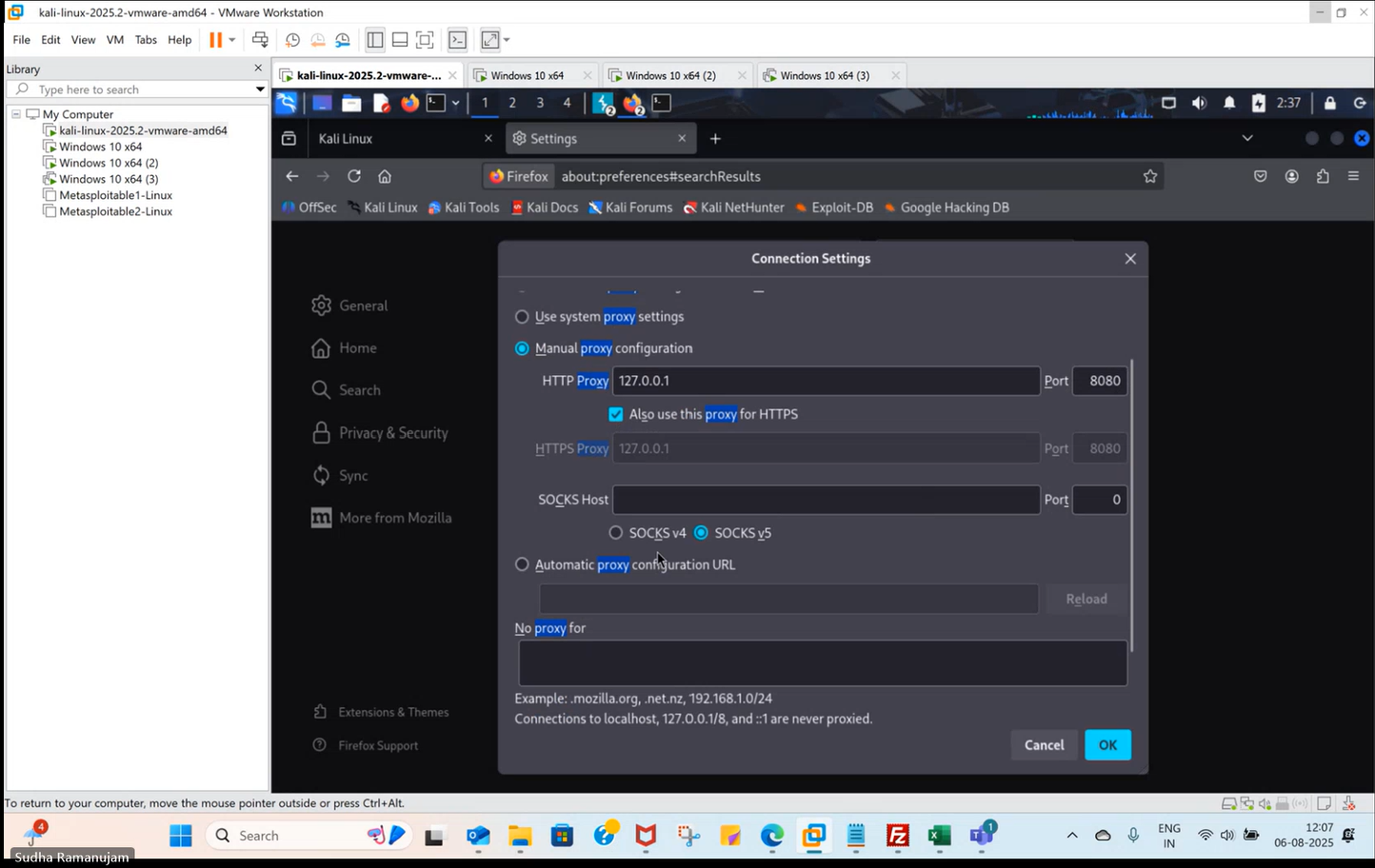
**Burp Suite is used for:**

* **Intercepting and modifying web traffic**
* **Scanning for vulnerabilities**
* **Performing manual security testing**
* **Automating attacks using payloads**
* **Mapping application structure**
* **Generating security reports**

**Different types of testing that can be performed for example not limited to:**

* **Authentication**
* **Access**
* **Privileges**
* **Session Hijacking**
* **XSS – cross site scripting**
* **Cookies Hijacking**
* **Brute force**

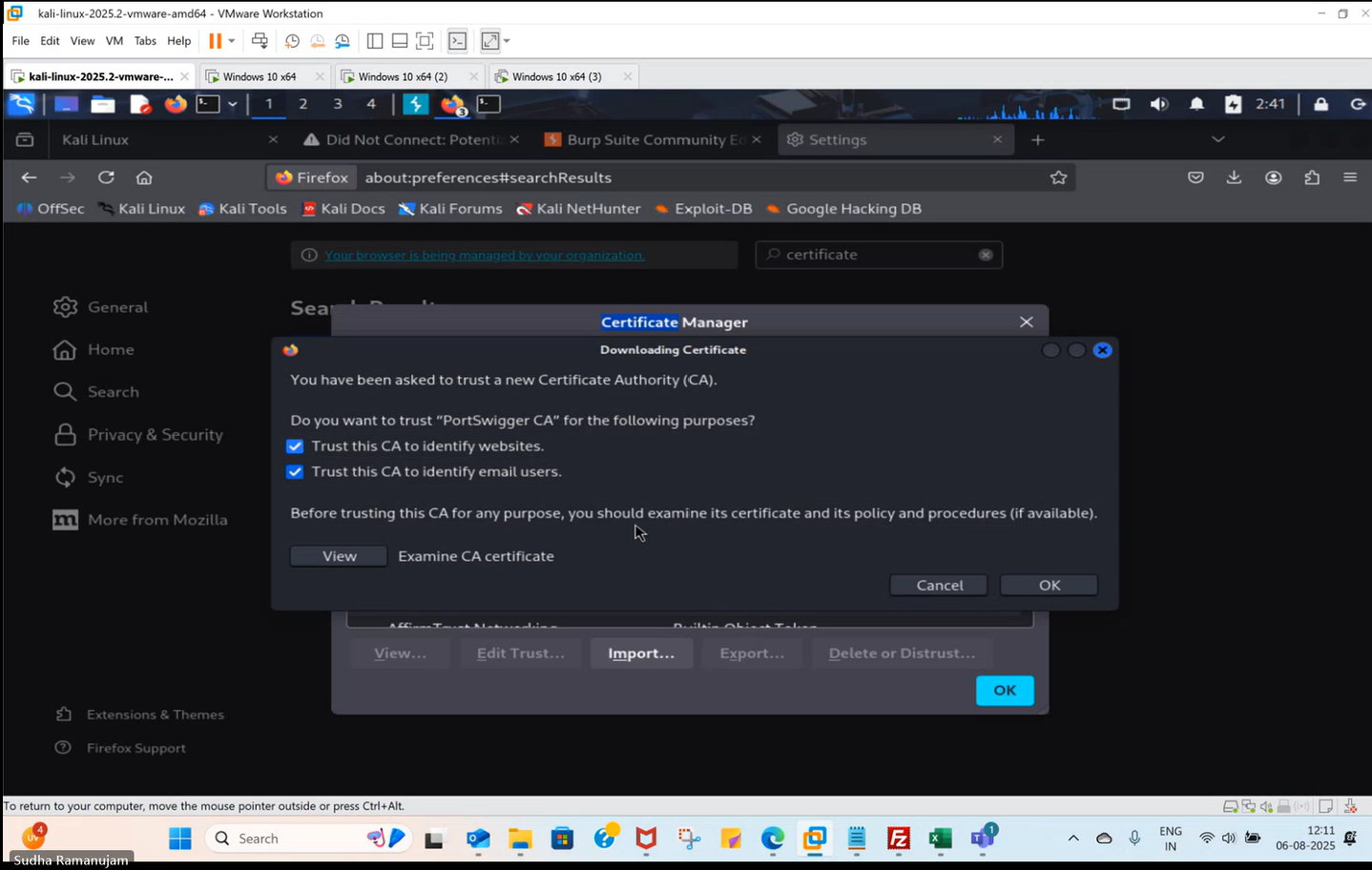
****

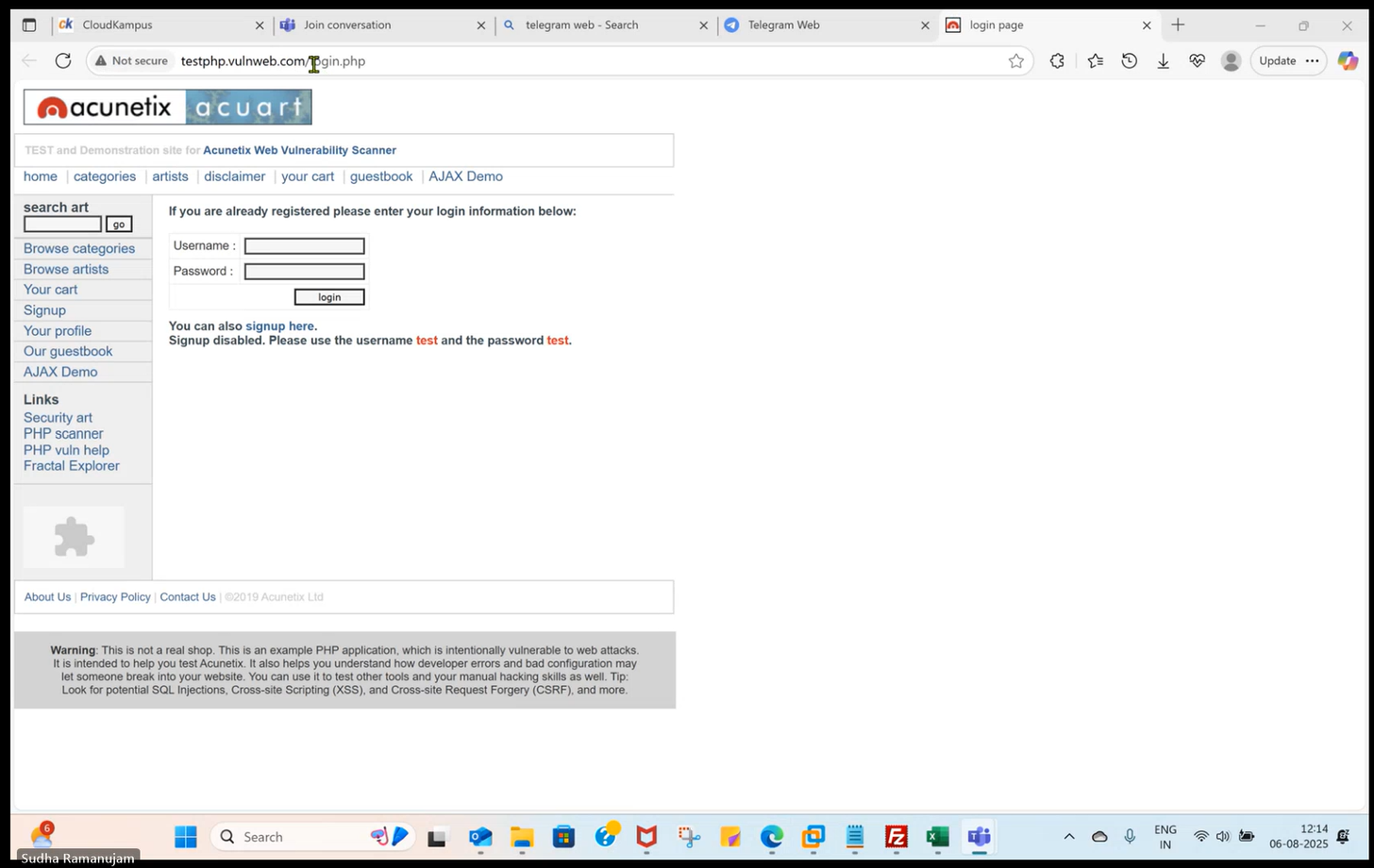
****

**Download certificate from Burp/**

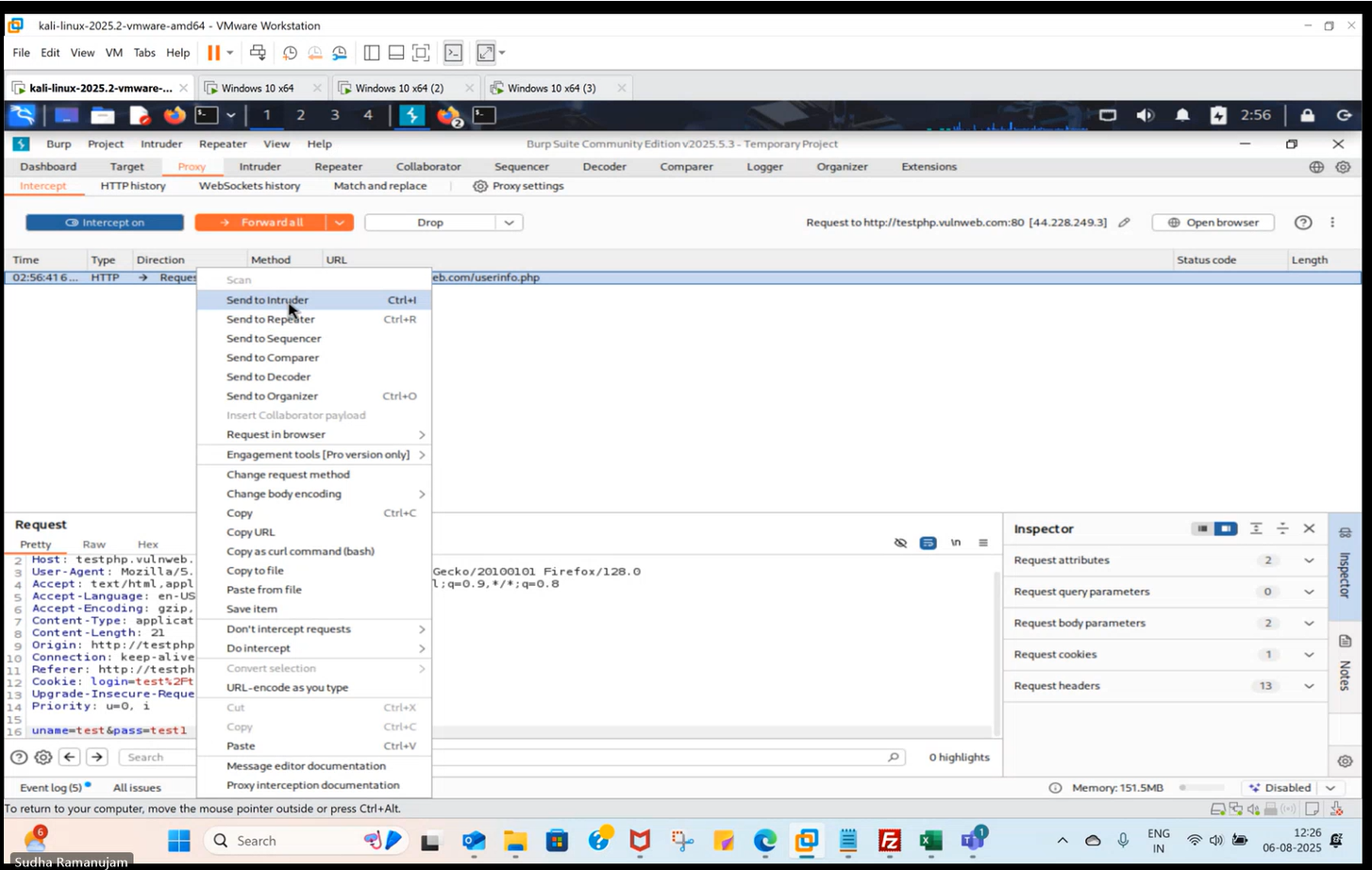
****

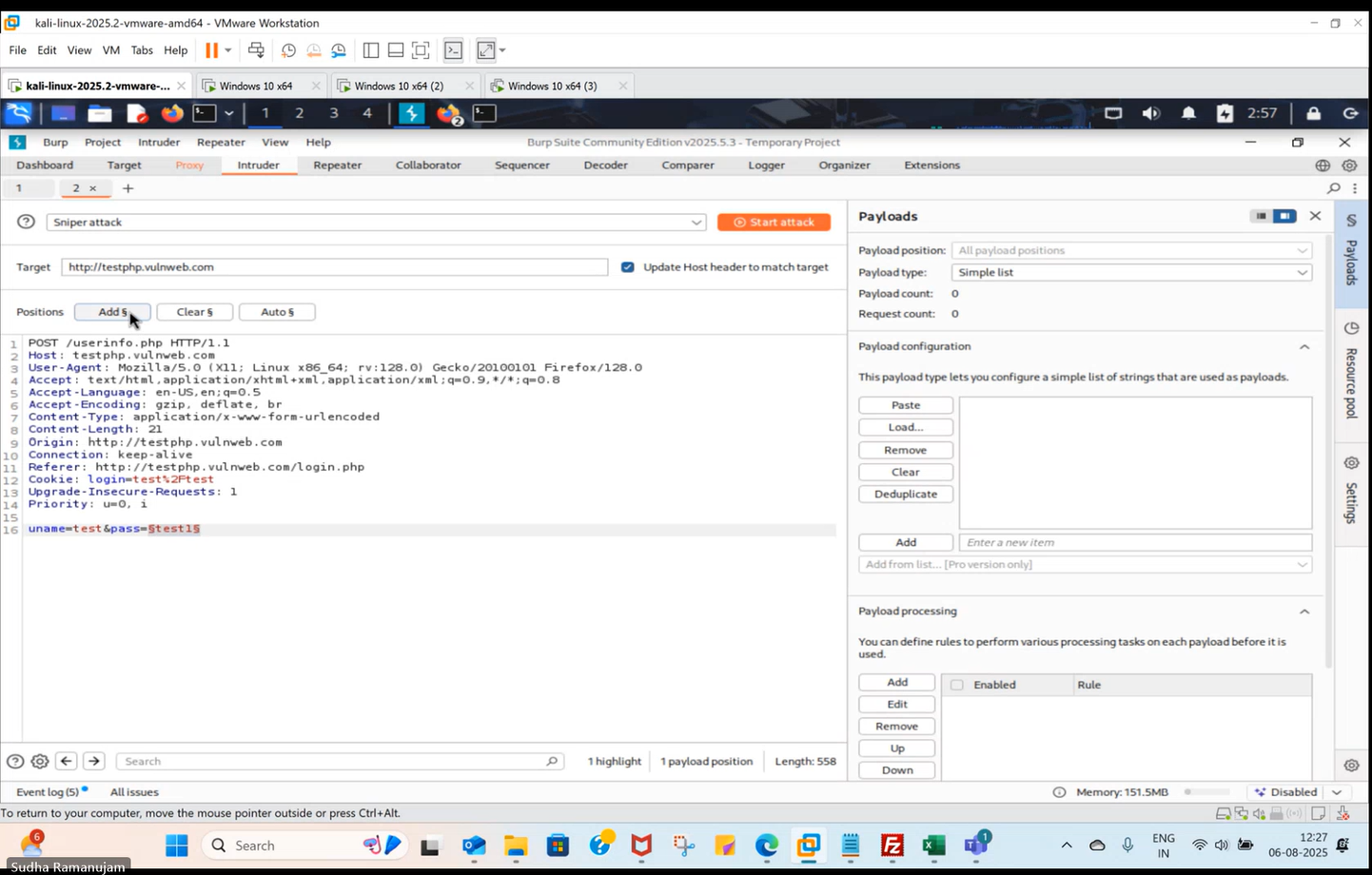
**Import certificate into firefox settings**

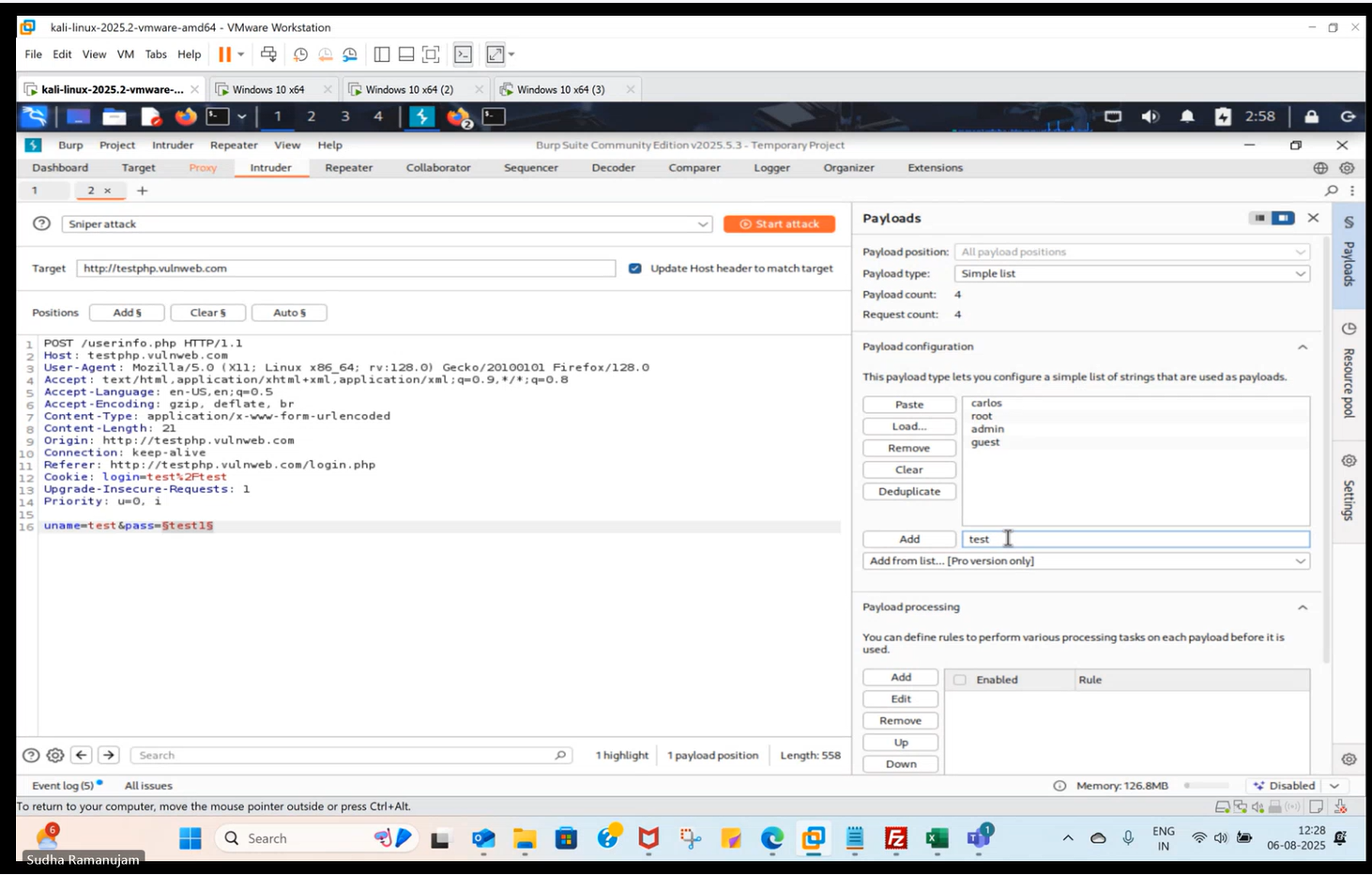
****

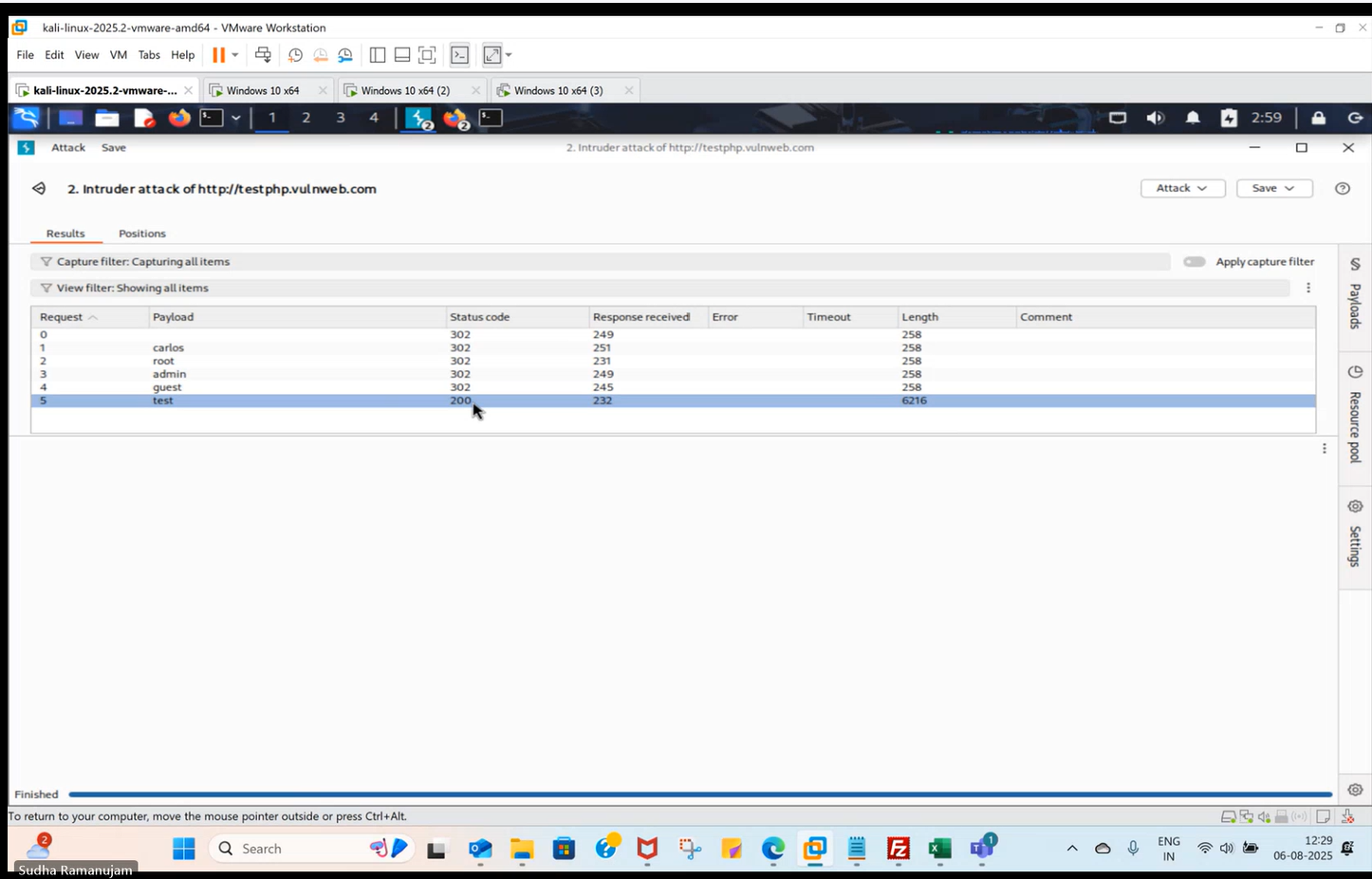
****

****

****

****

****

****

**1. Introduction**

This manual provides a step-by-step guide for using **Burp Suite** to perform web application penetration testing.  
You will learn how to:

* Configure Burp Suite
* Route browser traffic through Burp proxy
* Map the application
* Scan for vulnerabilities
* Analyze findings & generate reports

This guide is ideal for QA engineers, automation testers transitioning to security, and entry-level penetration testers.

**2. System Requirements**

**Software Needed**

* **Burp Suite Community** or **Professional**
* Java (if using older editions)
* Modern browser (Chrome/Firefox)

**Optional**

Vulnerable test sites:

* **OWASP Juice Shop**
* **TestFire (demo.testfire.net)**
* **DVWA (Damn Vulnerable Web App)**
* **Testphp.vulnweb.com/login.php**

**3. Launching Burp Suite**

1. Open **Burp Suite**.
2. Select:
   * **Temporary Project** → recommended for practice
   * **Use Burp Defaults**
3. Burp opens with tabs such as:
   * Proxy
   * Target
   * Intruder
   * Repeater
   * Scanner (Pro)
   * Decoder
   * Extender

**4. Setting Up Browser Proxy**

Burp operates by intercepting browser traffic through a proxy.

**Configuration**

* Proxy IP: **127.0.0.1**
* Port: **8080**

**Method A — Burp’s Built-in Browser (Recommended)**

1. Go to **Proxy → Intercept**
2. Click **Open Browser**
3. A Chromium-based browser opens with proxy pre-configured

**Method B — External Browser (Optional)**

1. Open Firefox/Chrome
2. Set manual proxy to:
   * HTTP: **127.0.0.1**
   * Port: **8080**
3. Install Burp CA certificate:
   * Visit http://burp
   * Download & install certificate to trusted root authorities

**5. Adding Target to Scope**

To avoid accidental attacks on unintended sites:

1. Go to **Target → Site Map**
2. Right-click your test domain
3. Select **Add to Scope**
4. Accept the warning
5. Burp will now focus analysis on in-scope URLs only

**6. Browsing the Application (Traffic Interception)**

1. Ensure **Proxy → Intercept** is ON if you want to inspect every request
2. Browse the target application
3. All traffic appears in:
   * Proxy → HTTP history
   * Target → Site Map

You can turn **Intercept → OFF** to browse normally while still logging all traffic.

**7. Scanning the Application (Burp Pro Only)**

If using **Burp Suite Community**, scanning is manual.  
If using **Burp Suite Professional**, you get full automated scanning.

**7A. Manual Scanning (Community Edition)**

Perform manual vulnerability checks using:

**Repeater**

* Send requests to Repeater
* Modify parameters
* Reissue requests
* Verify responses and exploitability

**Intruder**

* Launch brute-force payloads
* Useful for:
  + Fuzzing
  + Testing authentication
  + Parameter manipulation

**Decoder**

* Decode:
  + Base64
  + URL encoded
  + Hashes

**Comparer**

* Compare responses to detect behaviour differences

**7B. Automated Scanning (Burp Suite Professional)**

1. Right-click the target domain or URL
2. Select **Scan → Active Scan**
3. Configure:
   * Scan speed
   * In-scope configuration
4. Start scan

**Burp Scanner Tests for:**

* SQL Injection
* XSS (Reflected/Stored)
* Authentication Bypass
* Server Misconfigurations
* CSRF
* Path Traversal
* Insecure Direct Object Reference
* Session Issues

**Scan Progress**

Displayed under:

* **Dashboard → Issues**
* **Dashboard → Tasks**

**8. Reviewing Vulnerabilities**

Findings are available under **Dashboard → Issue Activity**.

**For each issue:**

1. Click the vulnerability description
2. View:
   * Severity (High/Medium/Low/Info)
   * CWE & OWASP references
   * Affected URL
   * Request/Response evidence
   * Remediation steps

**Recommended Review Tabs**

* **Request** – payload sent
* **Response** – server behaviour
* **Issue Detail** – technical explanation
* **Advisory** – fix guidance

**9. Using Key Burp Tools**

**Repeater**

Used for manual exploitation.  
Steps:

1. Right-click request → “Send to Repeater”
2. Modify parameters
3. Inspect server responses

**Intruder**

Used for automation-based attacks.  
Steps:

1. Send request to **Intruder**
2. Set:
   * Attack type (Sniper, Battering Ram, Pitchfork, Cluster Bomb)
   * Positions (parameters to test)
   * Payloads
3. Start attack
4. Analyze response patterns

**Logger++ (Optional Add-on)**

Gives full traffic logging.  
Install via: **Extender → BApp Store**

**10. Generating Security Reports**

**Burp Suite Professional** supports detailed reporting.

**Steps**

1. Go to **Dashboard → Issues**
2. Select vulnerabilities
3. Click **Report**
4. Choose:
   * HTML or XML
   * Include request/response pairs
   * Include remediation advice
5. Export the report

You get a professional pentest-style output.

**11. Best Practices**

✔ Keep Intercept OFF when normal browsing  
✔ Use Scope to avoid scanning non-target websites  
✔ Validate vulnerabilities manually using Repeater  
✔ Do not Active Scan without permission  
✔ Save project files regularly  
✔ Use Intruder throttling to avoid overloading servers

**12. Conclusion**

You now know how to perform full web application security testing using **Burp Suite**:

* Browser proxy setup
* Traffic interception
* Application mapping
* Manual/automated scanning
* Manual exploitation techniques
* Reporting