VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

INFORMATION SECURITY MANAGEMENT LAB

EXPERIMENT-6

GROUP NO. :	**11**
Name :	**Namit Mehrotra**
REG. NO. :	**21BCE0763**
SUBJECT CODE :	**BCSE354E**
SUBJECT TITLE :	**Information Security Management**
LAB SLOT :	**L29+L30**
SEMESTER :	**Winter Semester 2023-2024**
GUIDED BY :	**NIHA K**

INFORMATION SECURITY MANAGEMENT LAB

NAME: NAMIT MEHROTRA
REG NO:.21BCE0763
SLOT: L29+L30

EXPERIMENT-1
STUDY OF ISM TOOLS

1. Nmap

Description:

Nmap, short for Network Mapper, is your free and open-source network exploration and security auditing tool. Think of it as a powerful flashlight illuminating the hidden devices, services, and vulnerabilities lurking within your network.

Download :

- Link: https://nmap.org/download

Feasibility:

- System Requirements: Runs on major operating systems like Windows, Linux, and macOS. Lightweight and requires minimal resources.
- Skill Level: Beginner-friendly with basic features, but advanced options require network security knowledge and penetration testing methodologies.
- Ethical Use: Authorized scanning on systems you have permission for is crucial. Misuse for illegal purposes can have serious consequences.
- Open source (available under the Nmap Public Source License)
- Platforms: Linux, Windows, Mac OS X, and other UNIX platforms

Applications:

- Network discovery: Identifying active devices on a network
- Port scanning: Discovering open ports and running services
- Service and operating system detection: Fingerprinting applications and identifying underlying OS
- Security auditing: Vulnerability scanning and network security assessment
- Network inventory and monitoring: Tracking changes in network devices and services

Experiments:

- Scan your own network to understand its composition and identify potential vulnerabilities.
- Perform basic port scans on external targets (with proper authorization).

- Use advanced techniques like OS detection and version scanning.
- Experiment with scripting and automation using the Nmap Scripting Engine (NSE).

Basic Skills Needed to Use the Tool:

- Basic understanding of networking concepts like IP addresses, ports, and protocols
- Familiarity with the command line interface (CLI)
- Willingness to learn and experiment
- Important Note: Always use Nmap responsibly and ethically. Do not scan networks without proper authorization.

Additional Resources:

- Nmap documentation: https://nmap.org/docs.html
- Nmap tutorial: https://nmap.org/book/
- Nmap Scripting Engine (NSE): https://nmap.org/book/man-nse.html

Nmap uses different techniques to perform scanning, including: TCP connect() scanning, TCP reverse ident scanning, FTP bounce scanning and so on.

2. Wireshark

Description:

- Wireshark is one of the tools which is used globally by many for analyzing network protocol. This tool will help you to capture using pcap, store and analyze each packet in a detailed fashion. Wireshark supports OS platforms like Windows, Linux, Solaris, macOS etc. Wireshark is also an open-source tool similar to the tcpdump with a user interface option. The main features of Wireshark are that real-time data can be analyzed from different types of protocols. Also colour coding feature is available in the platform to show the packets when it matches any specific rule. This tool will capture packets only from the pcap-supported networks.

DOWNLOAD:

LINK: https://www.wireshark.org/download.html

Feasibility:

- System Requirements: Windows, Linux, macOS, and other Unix-like platforms. Minimum specs are modest, but performance improves with more RAM and a faster CPU.
- Skill Level: Beginner-friendly interface and extensive resources, but understanding network protocols and packet analysis helps for advanced features.

- Ethical Use: Crucial to capture traffic only on authorized networks with proper permission.

Applications:

- Network Troubleshooting: Analyze network traffic to diagnose slowdowns, connection drops, and performance bottlenecks.
- Security Analysis: Monitor traffic for suspicious activity, detect vulnerabilities, and investigate potential threats.
- Software Development: Test and debug network protocols and applications, analyze data flow, and understand network behavior.
- Education and Training: Learn about network protocols, gain practical experience in network analysis, and prepare for network certifications.

Experiments:

- Analyze your internet traffic to understand data exchange and privacy implications.
- Examine website communication to see how data flows and websites operate.
- Study network protocols like TCP/IP, DNS, or HTTP to learn their inner workings.
- Simulate network attacks like ARP spoofing or DNS poisoning for educational purposes.

Open Source or Not:

Wireshark is completely open-source and free to use, making it accessible to everyone. Its open-source nature also fosters continuous development and improvement by the community.

Basic Skills Needed to Use That Tool:

To get started with Wireshark, you'll need basic computer literacy and a fundamental understanding of networking concepts. Familiarity with TCP/IP, network protocols, and basic packet analysis principles will be beneficial. As you delve deeper, knowledge of scripting languages like Lua can unlock advanced features.

Wireshark is a powerful tool that can unlock a fascinating world of network communication. Whether you're a seasoned network pro or a curious beginner, Wireshark offers valuable insights and endless learning opportunities.

3. Metasploit

DESCRIPTION:

- Metasploit is a powerful and famous open-source penetration testing tool used in cyber security industry. This tool will be used by cyber attackers and as well as cyber defenders. All that matters is that how they use the tool. Metasploit has many inbuilt modules which can be used for exploiting, payload executions, auxiliary functions, encoding, listening, executing shell codes, Nops. This tool can be used to perform security assessments that enhance the company's security posture.
- Metasploit is a powerful open-source penetration testing framework that helps security professionals identify and exploit vulnerabilities in computer systems. It provides a vast collection of exploits, payloads, auxiliary modules, and encoders that can be used to simulate real-world attacks and assess the security posture of networks and systems.

DOWNLOAD:

Link: https://www.metasploit.com/

Feasibility:

- System Requirements: Windows, Linux, macOS, and other Unix-like platforms. Minimum specs are modest, but performance improves with more RAM and a faster CPU.
- Skill Level: Beginner-friendly interface and extensive resources, but understanding network protocols and packet analysis helps for advanced features.
- Ethical Use: Crucial to capture traffic only on authorized networks with proper permission.

Applications:

- Penetration Testing: Simulate real-world attacks to identify and exploit vulnerabilities in networks and systems.
- Vulnerability Research: Develop and test new exploits for known vulnerabilities.
- Security Awareness Training: Demonstrate the potential consequences of security vulnerabilities to raise awareness among users and administrators.
- Malware Analysis: Analyze malware samples to understand their functionality and how they work.

Experiments:

- Exploiting web applications: Use web-based exploits to gain access to vulnerable web servers.

- Escalating privileges: Once you have gained initial access to a system, use privilege escalation exploits to gain higher levels of access.
- Lateral movement: Move laterally through a network once you have gained access to a single system.
- Developing custom exploits: Use Metasploit's scripting language to develop your own exploits for specific vulnerabilities.

Basic Skills Needed to Use That Tool:

- Strong understanding of network security concepts: This includes knowledge of operating systems, networking protocols,.
- Familiarity with scripting languages like Ruby can be helpful, but not required.
- Strong critical thinking and problem-solving skills.
- Knowledge of ethical hacking principles and responsible use of security tools.

4. Burpsuite:

DESCRIPTION:

Burp suite is a combined platform of several tools which are used in the penetration testing field. This is the favourite tool for all pen testers and bug bounty hunters. This tool was developed by the company “Port Swigger”. There are various tools like Spider, Proxy, Intruder, Repeater, Sequencer, Decoder, Extender, Scanner etc., which are used for different security testing processes. This tool can be used at project-level as well as at user-level.

Download

LINK: https://portswigger.net/burp/download: https://portswigger.net/burp/download

Feasibility (System Requirements and More):

- System Requirements:
- Operating System: Windows, Linux, macOS
- Java: Version 8 or later (required for all editions)
- Memory: 4 GB RAM minimum, 8 GB or more recommended for optimal performance
- CPU: 2 GHz or faster recommended
- Disk Space: 200 MB for installation, additional space for logs and project data
- Skill Level:
- Beginner: Intuitive interface and guided tutorials for learning web security fundamentals. Basic manual testing features are easy to grasp. Requires basic computer literacy and willingness to learn.

- Intermediate: Advanced features like automated scanning and vulnerability identification may require experience with web security concepts and tools. Understanding of HTTP and web technologies is beneficial.
- Security Professional: Comprehensive customization options and extension capabilities cater to specific needs and advanced penetration testing. Strong technical expertise and knowledge of web application security are essential.
- **Open Source or Not:**
- Community Edition: Free and open-source, offering core features like manual interception, proxy, and basic scanning.
- Professional Edition: Paid version with additional features like automated scanners, intruder for fuzzing, and advanced extensions.
- Enterprise Edition: Scaled version for large organizations with advanced collaboration features and centralized management.
- **Applications:**
- Manual Testing: Intercept and analyze HTTP requests and responses to identify vulnerabilities like SQL injection or XSS.
- Automated Scanning: Utilize built-in or custom scanners to detect common vulnerabilities in web applications.
- Fuzzing: Test applications with invalid data to uncover unexpected behavior and potential vulnerabilities.
- Penetration Testing: Simulate real-world attack scenarios to assess the overall security posture of web applications.
- Security Awareness Training: Demonstrate vulnerabilities and attack techniques to educate users and developers.
- **Experiments Available:**
- Analyze your own website traffic to understand data exchange and identify potential security concerns.
- Test a public vulnerability in a publicly available web application for educational purposes (with proper permission).
- Build your own custom extension to automate specific tasks or analyze data in new ways.
- **Basic Skills Needed:**
- Basic understanding of HTTP and web technologies: Familiarity with how web applications work and communicate will be helpful.
- Computer literacy and ability to learn new tools: Burp Suite offers extensive documentation and tutorials, but basic tech skills are necessary.

- Ethical mindset: Remember, responsible use is crucial. Always use Burp Suite on authorized systems and networks with proper permission.

5. Aircrack-NG:

DESCRIPTION:

Aircrack-ng is an open-source project, and its source code is available on various platforms, including GitHub. You can obtain the latest version of the software by visiting the official repository. The source code is typically distributed under the GNU General Public License (GPL), ensuring that it remains free and open for users to modify and distribute .

DOWNLOAD:

Link: https://www.aircrack-ng.org/

Feasibility:

System Requirements:

- OperatingSystem: Windows, Linux, macOS, FreeBSD, OpenBSD, NetBSD, Solaris, eComStation 2
- Hardware: Requires a wireless network interface controller (NIC) that supports raw monitoring mode.

Skill Level:

- Basic: Aircrack-NG has a simple interface that makes it easy to use for basic tasks like monitoring traffic and cracking WEP keys.
- Intermediate: Advanced features like WPA/WPA2 cracking and packet injection require more technical knowledge and experience.

Ethical Use:

- Only use Aircrack-NG on authorized networks with proper permission. Misuse for illegal or unauthorized purposes can have serious consequences.

Applications:

- Network Analysis: Monitor traffic to identify vulnerabilities and potential threats.
- Penetration Testing: Simulate real-world attacks to assess network security.
- Security Auditing: Identify and fix security vulnerabilities.
- Research: Develop new security tools and techniques.

Experiments:

- Analyze traffic from your own network to understand how it works and identify potential security concerns.
- Crack a WEP key from a public wireless network for educational purposes (with proper permission).

- Simulate a WPA/WPA2 attack on a vulnerable network.

Basic Skills Needed:

- Basic understanding of network protocols: Familiarity with how wireless networks work will be helpful.
- Computer literacy and ability to learn new tools: Aircrack-NG offers extensive documentation and tutorials, but basic tech skills are necessary.
- Ethical mindset: Remember, responsible use is crucial. Always use Aircrack-NG on authorized networks and with proper permission.

Basic Skills Required:

Basic understanding of networking concepts (TCP/IP, OSI Model, protocols (TCP, UDP, IP, Ethernet))

- Familiarity with wireless security concepts (WEP, WPA/WPA2-PSK)
- Ability to interpret packet capture data
- Strong critical thinking and problem-solving skills

• A security analyst can use Aircrack-ng to identify wireless networks that are using weak or default passwords.

• A penetration tester can use Aircrack-ng to crack the password of a wireless network as part of a security assessment.

• A forensic investigator can use Aircrack-ng to collect evidence of a wireless attack.

• Aircrack-ng is a valuable tool for anyone who needs to assess the security of wireless networks. It is a powerful tool, but it should be used responsibly

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

INFORMATION SECURITY MANAGEMENT LAB

EXPERIMENT-2

GROUP NO. :	**11**
TEAM MEMBER 1 :	**Namit Mehrotra**
REG. NO. :	**21BCE0763**
TEAM MEMBER 2 :	**Purva Sharma**
REG.NO :	**21BCE0169**
SUBJECT CODE :	**BCSE354E**
SUBJECT TITLE :	**Information Security Management**
LAB SLOT :	**L29+L30**
SEMESTER :	**Winter Semester 2023-2024**
GUIDED BY :	**NIHA K**

INSTALLATION Procedure

Burp Suite, a widely employed cybersecurity tool for web application security testing, can be installed on Windows by following these steps. Ensure your system meets the specified minimum requirements:

Minimum Requirements for Kali Linux Installation:

Operating System: Kali Linux (version compatible with Burp Suite).

Memory (RAM): At least 2 GB RAM.

Disk Space: Ensure a minimum of 500 MB free disk space.

For Kali Linux, additional considerations include compatibility with the specific version of the operating system.

Now, let's consider the installation procedure for windows

Minimum Requirements for Windows Installation:

Operating System: Windows 7 or later.

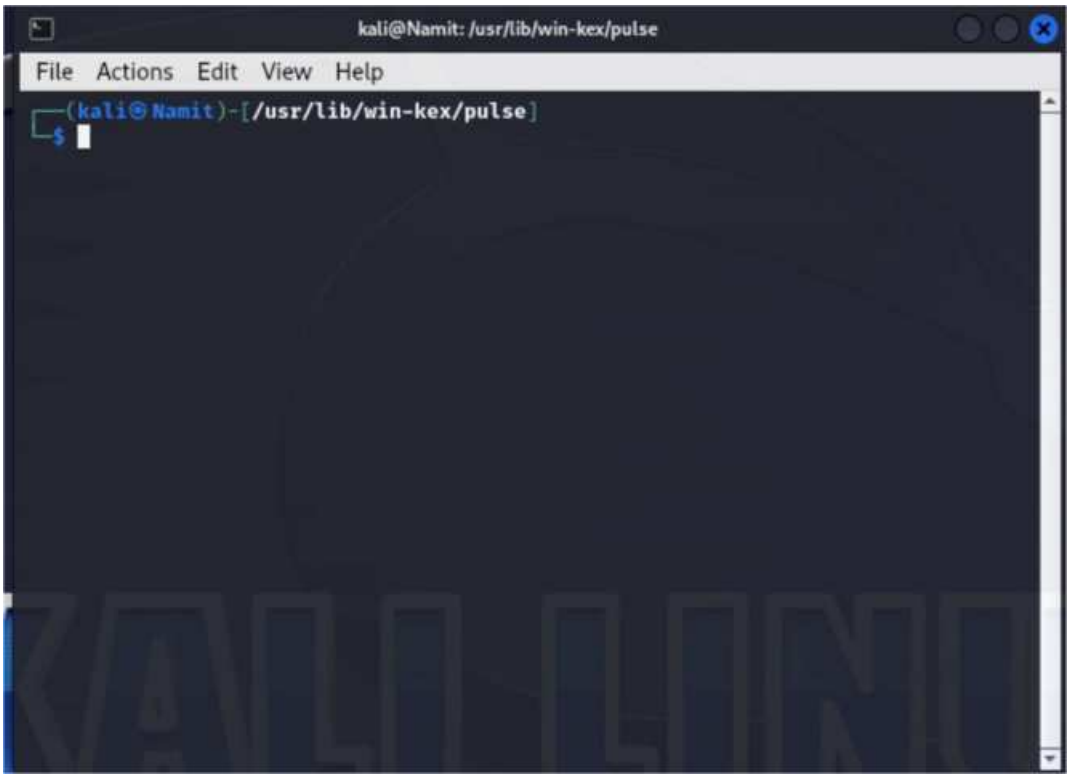
Memory (RAM): At least 2 GB RAM.

Disk Space: A minimum of 500 MB free disk space.

Installation Procedure in Kali Linux:

1. Using sudo apt install:

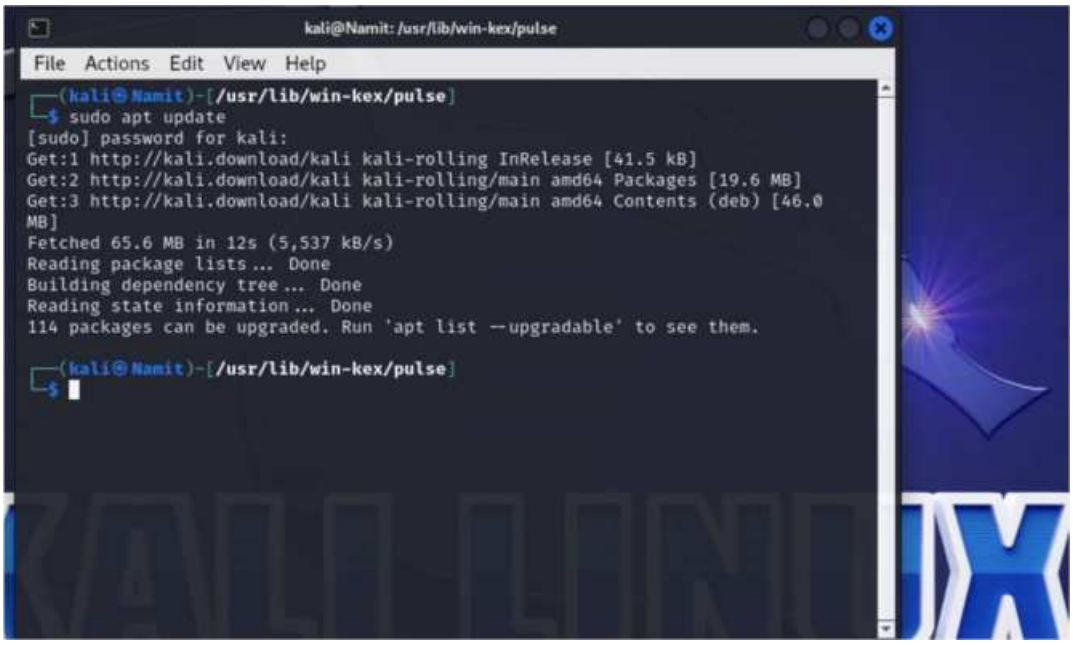
1. **Open a Terminal:**
    - Open a terminal on your Kali Linux system.



2. **Update Package List:**

   - Update the package list to make sure you have the latest information about available packages.

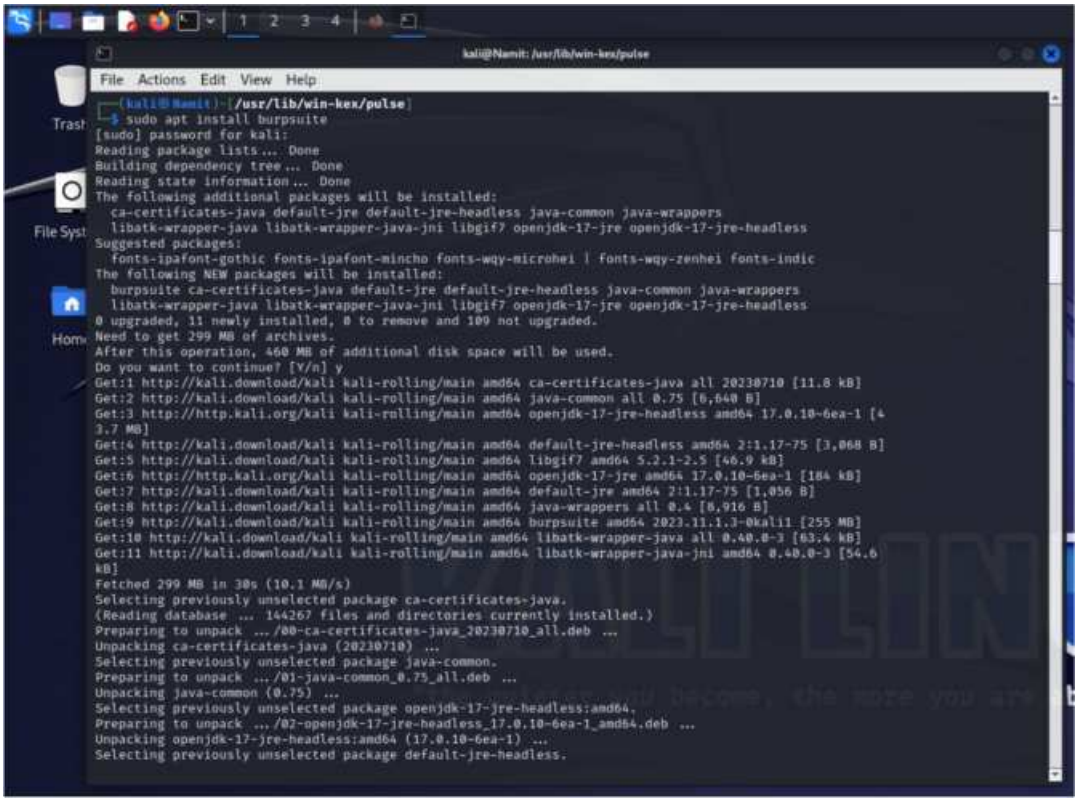
     sudo apt update



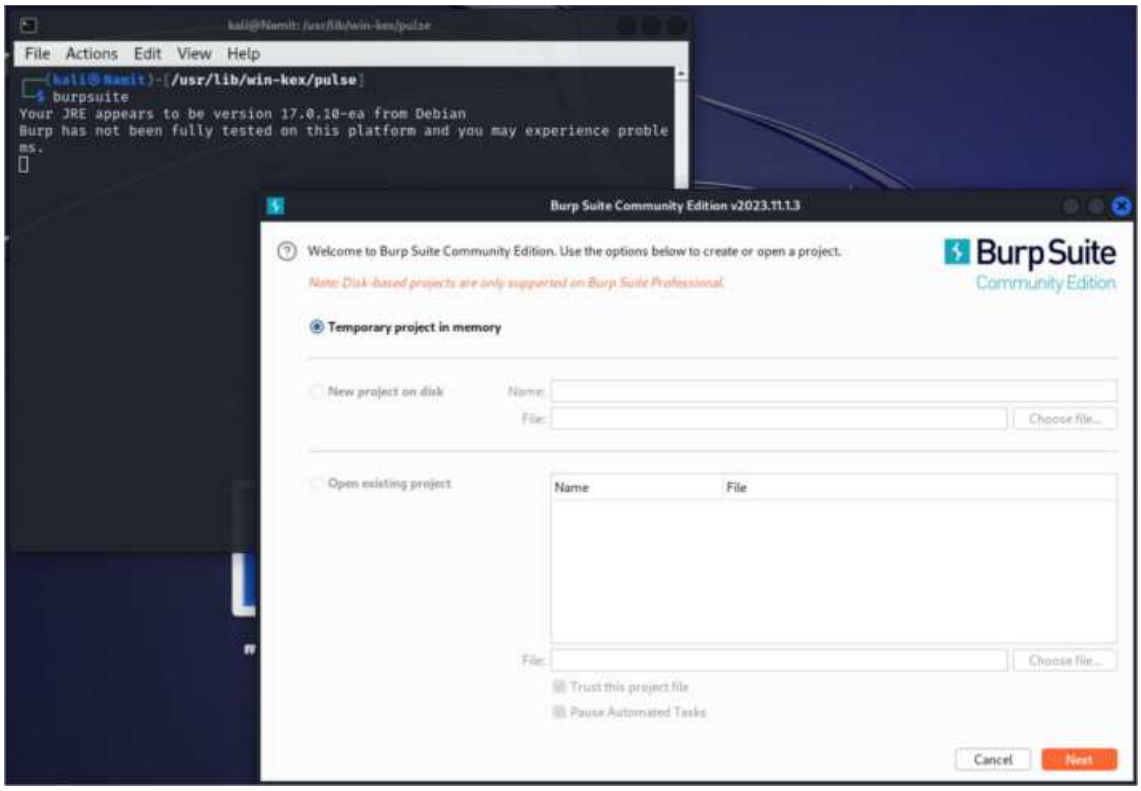
3. **Install Burp Suite:**

   - Use the **sudo apt install** command to install Burp Suite.

     sudo apt install burpsuite

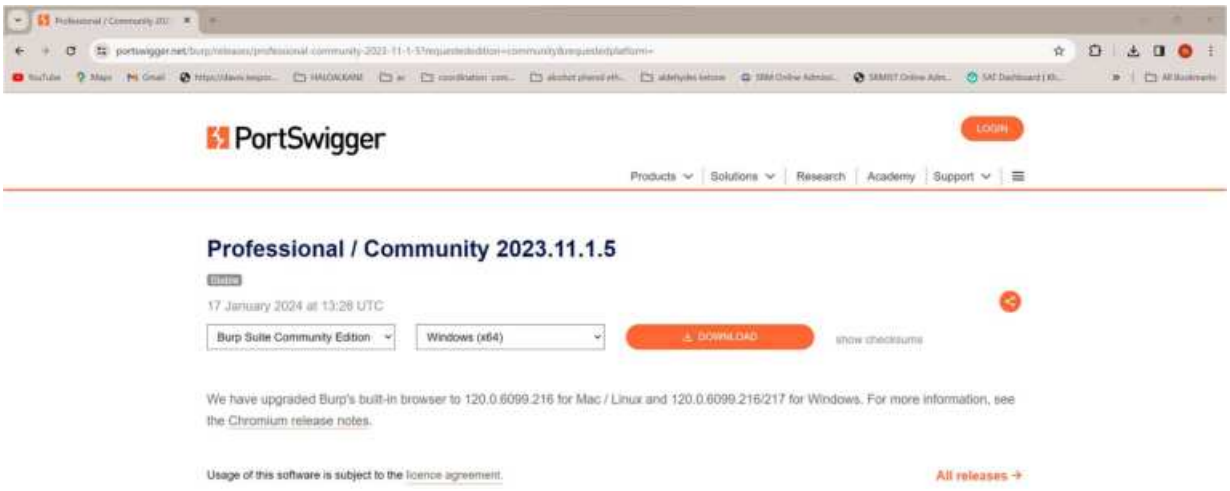


4. **Launch Burp Suite:**
    - Once the installation is complete, you can launch Burp Suite from the applications menu or by typing **burpsuite** in the terminal.



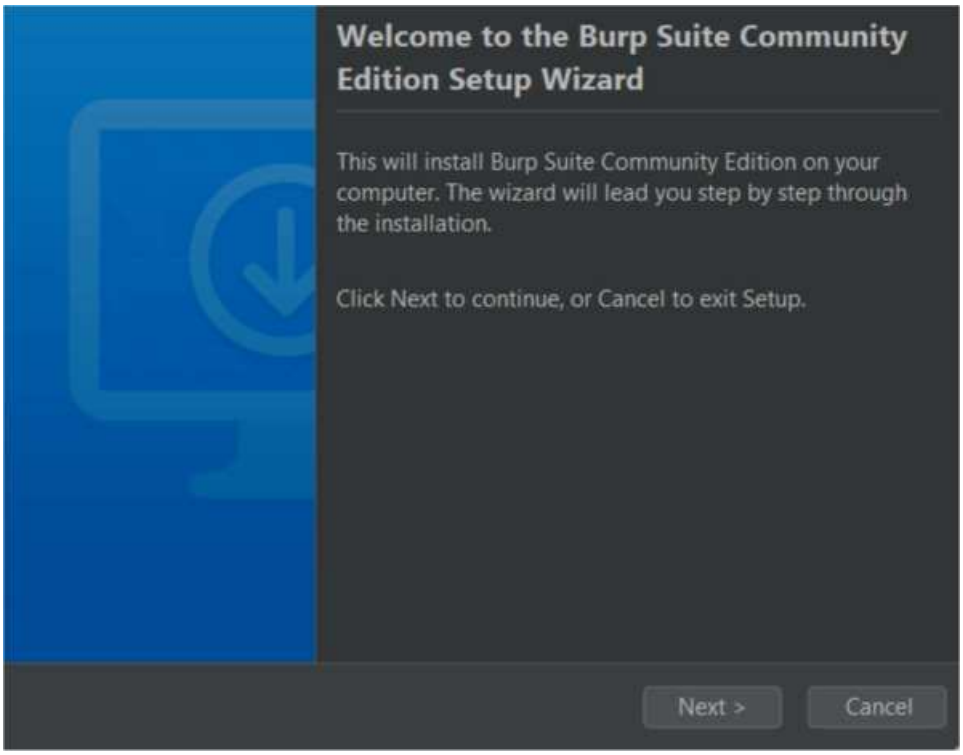
2. Download from the Official Website for windows:

1. **Visit the Burp Suite Website:** Go to the official Burp Suite website at https://portswigger.net/burp.
2. **Download Burp Suite:**
    - Navigate to the "Download" section.
    - Choose the appropriate edition (Community or Professional) and click on the download link.
    - Save the installer file to your computer.



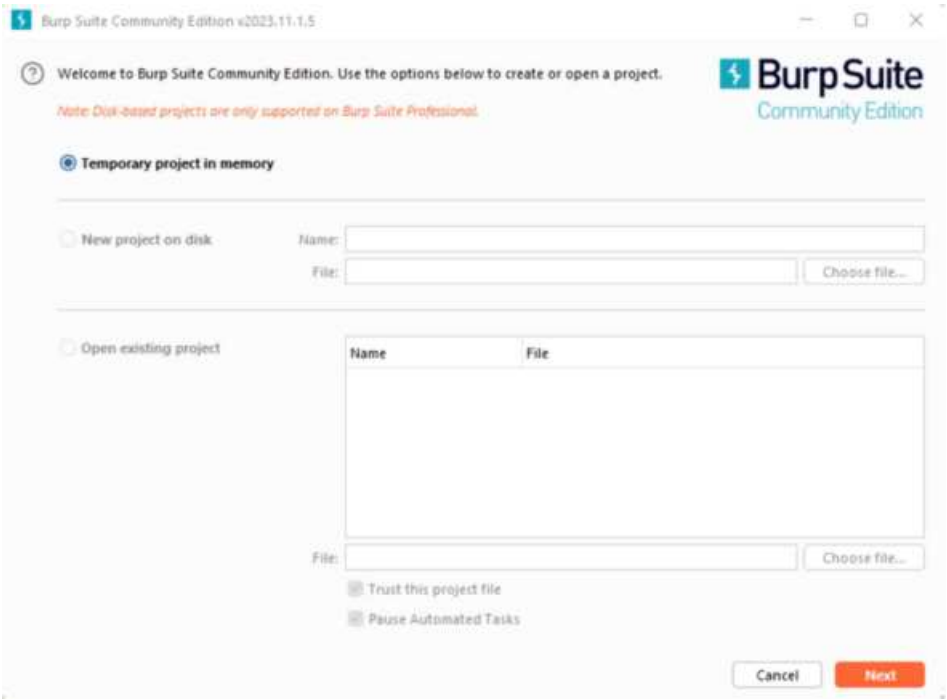
3. **Run installer file**

- Once the download is complete, run the
- Follow the instructions to complete the installation



4. **Run Burpsuite**

After installation, you can launch Burp Suite



5. **Verify Burp Suite's Operational Status:**

   1. Navigate to the "Proxy" tab within Burp Suite.
   2. Confirm that the Intercept feature is disabled by default, and ensure the Proxy listener is actively running on 127.0.0.1:8080.
   3. By default, Burp Suite initiates a proxy listener on localhost:8080. This represents the host and port through which our browser connects to proxy traffic via Burp Suite. We will maintain these default settings. The Intercept tool is initially activated in Burp Suite's default configuration. To verify this setting, go to User Options > Miscellaneous > Proxy Interception. While Intercept may be enabled at startup, some users prefer to deactivate it, which can be achieved by selecting "Always disable." Regardless, users can manually toggle Intercept on and off through Proxy > Intercept > Toggle Intercept.

2. Perform a study on Information Security Management (ISM) Tool which you have choose and explain

Burp Suite, developed by PortSwigger, is widely employed in ethical hacking and penetration testing. It offers a suite of tools that empower users to manually modify requests, features an automated scanner to detect vulnerabilities, and provides an intercepting proxy for in-depth traffic analysis. Security professionals leverage its robust capabilities, including Burp Spider for comprehensive application crawling and mapping, as well as Burp Intruder for automating customized attacks. With its user-friendly interface, regular updates, and seamless integration options, Burp Suite stands out as the preferred tool in the dynamic field of cybersecurity, enabling experts to identify and address issues effectively.

Q. Which OSI Network layer it is used?

OSI Network Layer:

- Burp Suite primarily operates at Layer 7, the Application Layer, in the OSI model. Tailored specifically for the evaluation and security of online applications, Burp Suite proves indispensable in the realm of web application security testing.

Q. List the protocol it handles and explain each.

Protocols Supported:

A. HTTPS (Hypertext Transfer Protocol Secure):

Burp Suite can intercept and decode HTTPS traffic for encrypted communication, offering a crucial means to assess the security of applications utilizing secure connections.

B. HTTP (Hypertext Transfer Protocol):

Burp Suite intercepts and scrutinizes HTTP requests and responses, allowing security experts to inspect and modify the exchanged content between clients and servers.

C. FTP (File Transfer Protocol):

For fundamental FTP exchanges, Burp Suite enables security specialists to examine and control file transfers.

D. WebSocket:

Burp Suite's ability to intercept and analyze WebSocket traffic is crucial for testing contemporary web applications relying on real-time data transmission.

E. DNS (Domain Name System):

While not its primary focus, Burp Suite can assist in security evaluations related to DNS.

Q. Which kind of attack it handles and explain the diagnosing method or technique.

Types of Attacks and Diagnosing Methods:

Burp Suite, a versatile tool, is adept at identifying and addressing various security vulnerabilities. It handles common attacks such as:

A. Cross-Site Scripting (XSS): Intercepting and analyzing client-server traffic to locate and exploit XSS vulnerabilities.

B. Cross-Site Request Forgery (CSRF): Identifying and mitigating CSRF problems by examining requests and associated tokens.

C. SQL Injection: Testing for SQL injection vulnerabilities by modifying HTTP requests to detect and prevent unauthorized database access.

D. Session Hijacking: Assisting in identifying session management flaws and the associated risks of session hijacking.

E. Security Misconfigurations: Utilizing scanning features to discover web application misconfigurations, including exposed sensitive data or default credentials.

Q. Identify in which stage of Information Security Management System Lifecycle the tool will be used.

Information Security Management System Lifecycle Stage:

Burp Suite is most commonly utilized during the Testing and Evaluation stage of the Information Security Management System (ISMS) lifecycle. Security experts use it to examine online applications for vulnerabilities, conduct security audits, and perform penetration tests. This contributes to the detection and remediation of vulnerabilities before application deployment, ensuring a more secure environment for users.

In summary, Burp Suite, operating at the OSI model's Application Layer, is a valuable tool for web application security, supporting multiple protocols, addressing various types of attacks, and playing a prominent role in the testing and assessment stage of the Information Security Management System lifecycle.

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

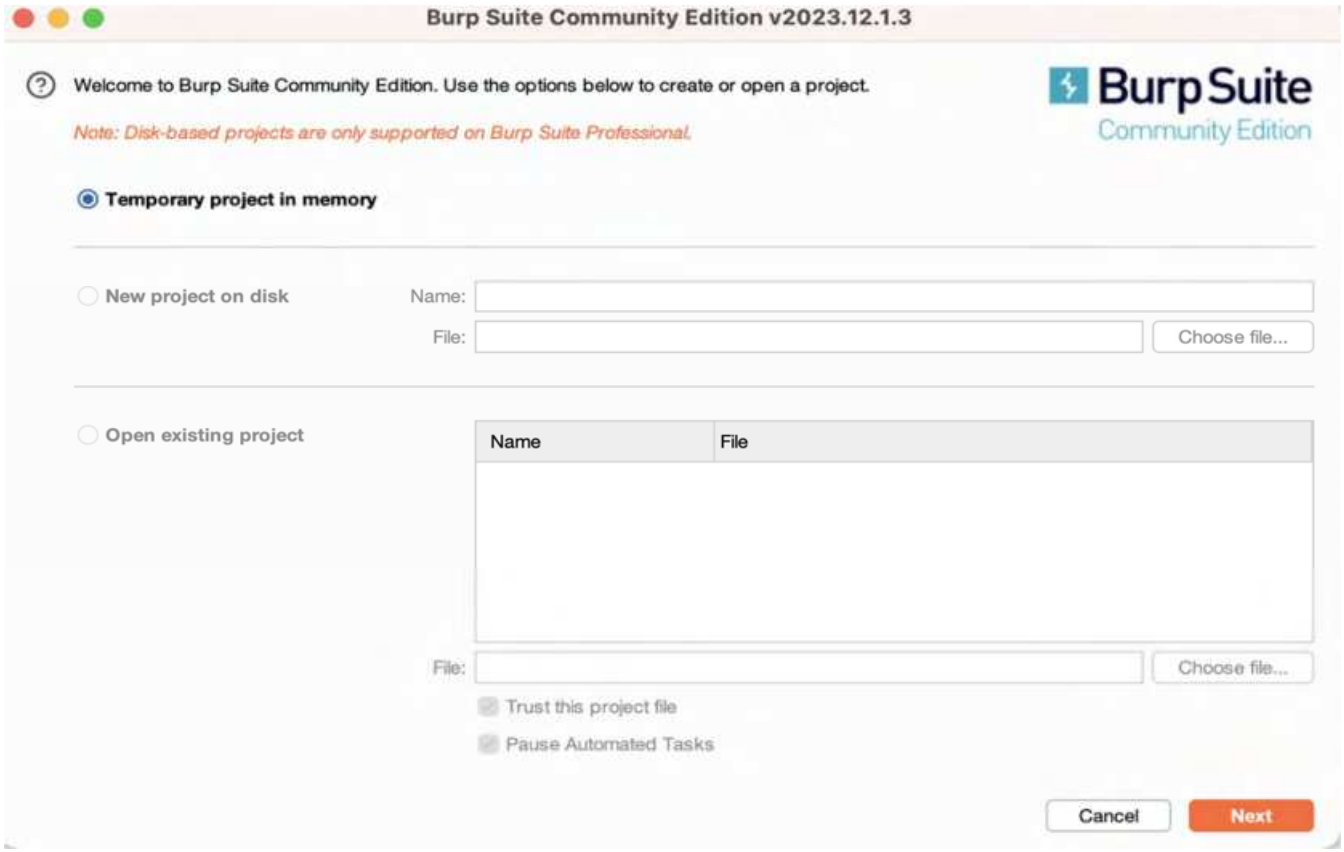
INFORMATION SECURITY MANAGEMENT LAB

EXPERIMENT-3

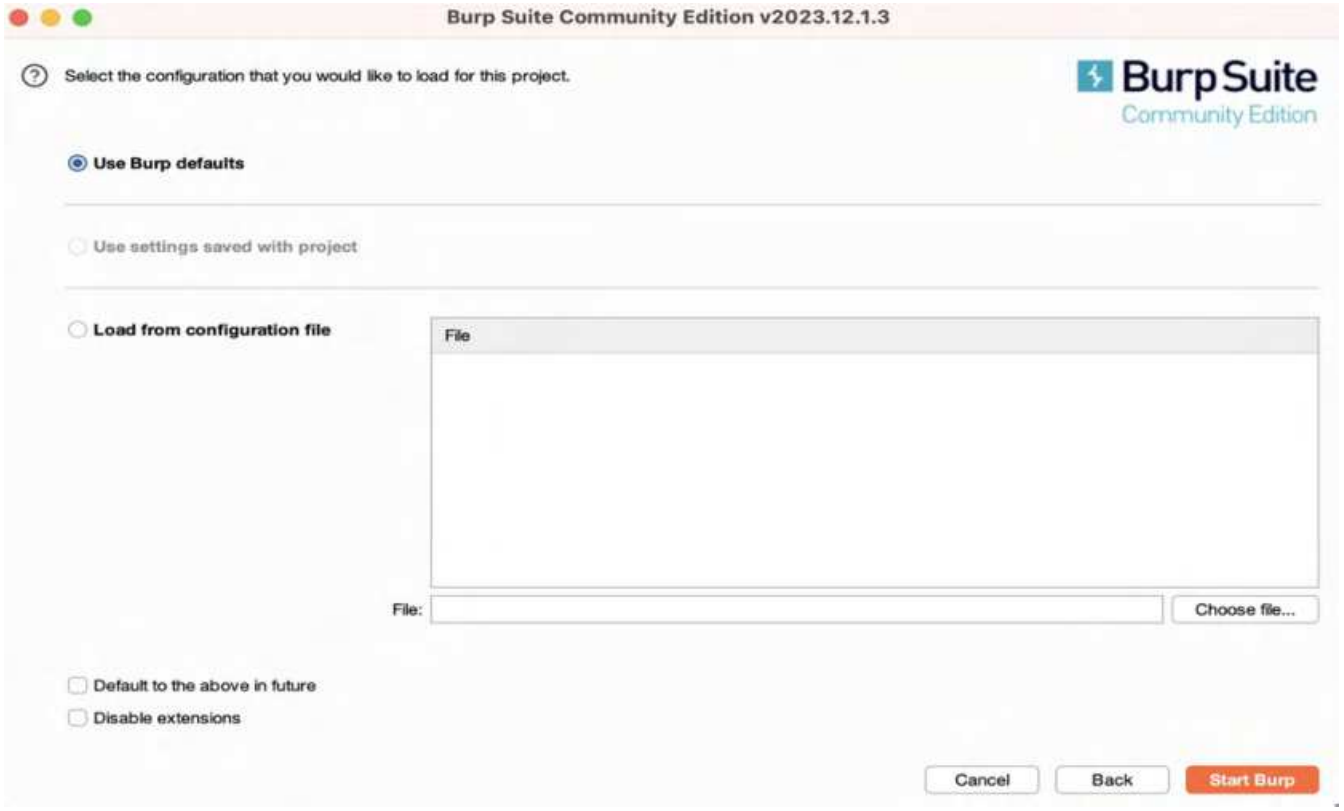
Features and Functionalities of Burp Suite

GROUP NO. :	**11**
TEAM MEMBER 1 :	**Namit Mehrotra**
REG. NO. :	**21BCE0763**
TEAM MEMBER 2 :	**Purva Sharma**
REG.NO :	**21BCE0169**
SUBJECT CODE :	**BCSE354E**
SUBJECT TITLE :	**Information Security Management**
LAB SLOT :	**L29+L30**
SEMESTER :	**Winter Semester 2023-2024**
GUIDED BY :	**NIHA K**

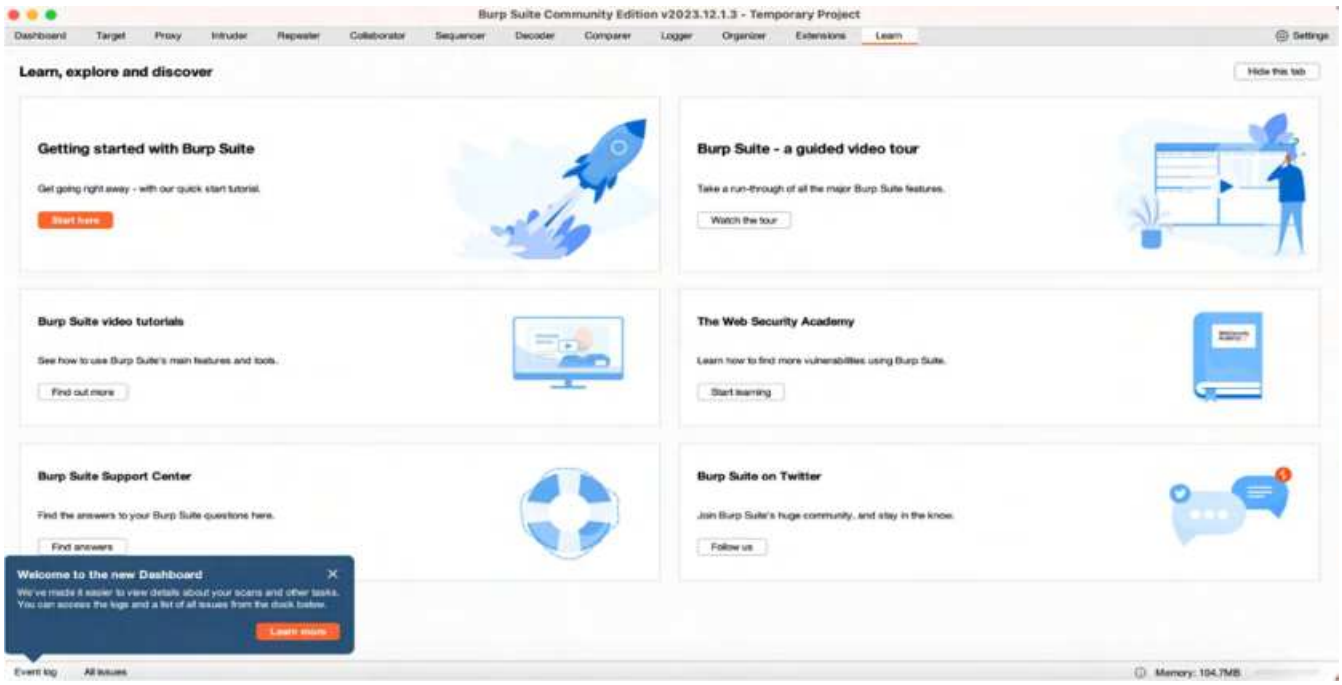
Features and Functionalities of Burp Suite:



-> Next



-> Start Burp



Manual penetration testing features:

- **Intercept everything your browser sees:** Burp Suite's built-in browser works right out of the box - enabling you to modify every HTTP message that passes through it.
- **Quickly assess your target:** Determine the size of your target application. Auto-enumeration of static and dynamic URLs, and URL parameters.
- **Speed up granular workflows:** Modify and reissue individual HTTP and WebSocket messages, and analyze the response - within a single window.
- **Manage recon data:** All target data is aggregated and stored in a target site map - with filtering and annotation functions.
- **Expose hidden attack surface:** Find hidden target functionality with an advanced automatic discovery function for "invisible" content.
- **Break HTTPS effectively:** Proxy even secure HTTPS traffic, using Burp Suite's built-in instrumented browser.
- **Work with HTTP/2:** Burp Suite offers unrivalled support for HTTP/2-based testing - enabling you to work with HTTP/2 requests in ways that other tools cannot.
- **Work with WebSockets:** WebSockets messages get their own specific history - allowing you to view and modify them.
- **Manually test for out-of-band vulnerabilities:** Make use of a dedicated client to incorporate Burp Suite's out-of-band (OAST) capabilities during manual testing.
- **DOM Invader:** Use Burp Suite's built-in browser to test for DOM XSS vulnerabilities more easily - with DOM Invader.
- **Assess token strength:** Easily test the quality of randomness in data items intended to be unpredictable (e.g. tokens).

Advanced / custom automated attacks:

- **Faster brute-forcing and fuzzing:** Deploy custom sequences of HTTP requests containing multiple payload sets. Radically reduce time spent on many tasks.
- **Query automated attack results:** Capture automated results in customized tables, then filter and annotate to find interesting entries / improve subsequent attacks.
- **Construct CSRF exploits:** Easily generate CSRF proof-of-concept attacks. Select any suitable request to generate exploit HTML.
- **Facilitate deeper manual testing:** See reflected/stored inputs even when a bug is not confirmed. Facilitates testing for issues like XSS.
- **Scan as you browse:** The option to passively scan every request you make, or to perform active scans on specific URLs.
- **Automatically modify HTTP messages:** Settings to automatically modify responses. Match and replace rules for both responses and requests.

Automated scanning for vulnerabilities:

- **Browser-powered scanning:** Burp Scanner uses its embedded browser to render its target - enabling it to navigate even complex single-page applications (SPAs).
- **Harness pioneering OAST technology:** High signal: low noise. Scan with pioneering, friction-free, out-of-band-application security testing (OAST).
- **Remediate bugs effectively:** Custom descriptions and step-by-step remediation advice for every bug, from PortSwigger Research and the Web Security Academy.
- **Fuel vulnerability coverage with research:** Cutting-edge scan logic from PortSwigger Research combines with coverage of over 100 generic bugs.
- **BChecks:** Create custom scan checks for Burp Scanner, written in a simple text-based language.
- **API scanning:** Discover more potential attack surfaces. Burp Scanner parses JSON or YAML API definitions - scanning any API endpoints it finds.
- **Authenticated scanning:** Scan privileged areas of target applications, even if they use complex login mechanisms like single sign-on (SSO).
- **Conquer client-side attack surfaces:** A built-in JavaScript analysis engine helps to find holes in client-side attack surfaces.
- **Configure scan behavior:** Customize what you audit, and how. Skip specific checks, fine-tune insertion points, and much more. Or use preset scan modes to get an overview.

Productivity tools:

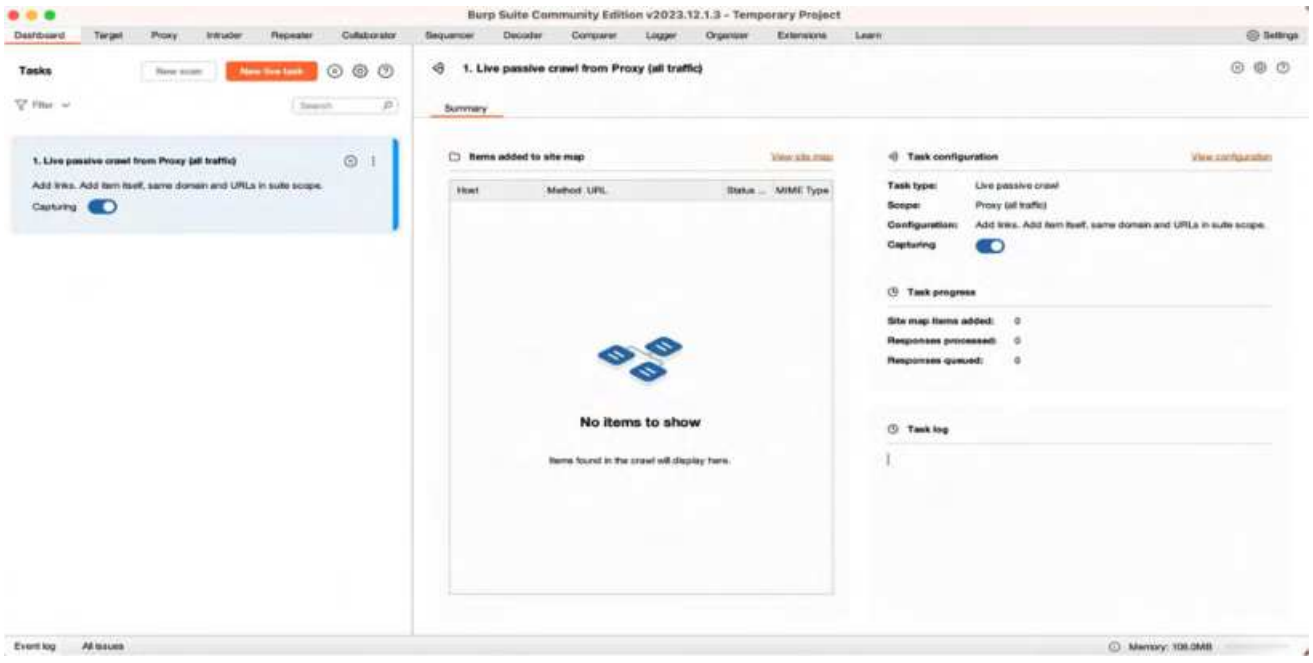
- **Deep-dive message analysis:** Show follow-up, analysis, reference, discovery, and remediation in a feature-rich HTTP editor.
- **Utilize both built-in and custom configurations:** Access predefined configurations for common tasks, or save and reuse custom configurations.
- **Project files:** Auto-save everything you do while on an engagement, as well as the configuration settings you use.
- **Burp Logger:** See every HTTP message that passes through Burp Suite's tools - all in one place - with Burp Logger.
- **Speed up data transformation:** Decode or encode data, with multiple built-in operations (e.g. Hex, Octal, Base64).
- **Burp Organizer:** Store and annotate interesting messages you find while testing, so you can come back to them later.

- **Make code more readable:** Automatically pretty-print code formats including JSON, JavaScript, CSS, HTML, and XML.
- **Easily remediate scan results:** See source, discovery, contents, and remediation, for every bug, with aggregated application data.
- **Search function:** Search everywhere in Burp Suite Professional at once, with its powerful search function.
- **Simplify scan reporting:** Customize with HTML / XML formats. Report all evidence identified, including issue details.

BApp extensions:

- **Create custom extensions:** The Montoya API ensures universal adaptability. Code custom extensions to make Burp work for you.
- **Hackvertor:** Convert between various encodings with Hackvertor. Use multiple nested tags to perform layered encoding. Even execute your own code with custom tags - and more.
- **Autorize:** When testing for authorization vulnerabilities, save time and perform repeat requests with Autorize.
- **Turbo Intruder:** Configured in Python, with a custom HTTP stack, Turbo Intruder can unleash thousands of requests per second.
- **J2EE Scan:** Expand your Java-specific vulnerability catalogue and hunt the most niche bugs, with J2EEScan.
- **Access the extension library:** The BApp Store customizes and extends capabilities. Over 250 extensions, written and tested by Burp users.
- **Upload Scanner:** Adapt Burp Scanner's attacks by uploading and testing multiple file-type payloads, with Upload Scanner.
- **HTTP Request Smuggler:** Scan for request smuggling vulnerabilities - and exploit them more easily by having HTTP Request Smuggler tweak offsets automatically for you.
- **Param Miner:** Quickly find unkeyed inputs with Param Miner - can guess up to 65,000 parameter names per second.
- **Backslash Powered Scanner:** Find research-grade bugs, and bridge human intuition and automation, with Backslash Powered Scanner.

Dashboard:



The Burp Suite dashboard is a central hub for managing and controlling various aspects of the tool. It consists of several tabs, each serving a specific purpose. Let's dive into each section in detail:

1. Target Tab: The "Target" tab in Burp Suite is a crucial component that allows users to manage and control the scope of their testing.

Functionality:

- Identifies and manages the target scope for testing.
- Allows you to add, remove, or modify target scope.

How to Use:

- Add a target by entering the URL and clicking "Add to Scope."
- Modify scope options like including or excluding specific URLs or entire domains.

2. Proxy Tab: The Proxy tab in Burp Suite is a powerful tool that allows you to intercept and manipulate HTTP/S traffic between your browser and the target web application.

Functionality:

- Manages proxy settings for intercepting and modifying HTTP/S traffic.
- Shows intercepted requests for analysis.

How to Use:

- Configure browser proxy settings to use Burp.
- Intercept requests, modify them, and forward them to the server.

3. Spider Tab: Automatically crawls the target web application in Burp Suite, mapping its structure to identify accessible content and functionality. Set the scope in the Target tab, initiate the Spider, and analyze results in the "Spider" sub-tab for discovered URLs.

Functionality:

- Crawls the target application, discovering and mapping its structure.
- Helps identify all accessible content and functionality.

How to Use:

- Set the scope in the Target tab and click "Spider."
- Analyze results in the "Spider" sub-tab for discovered URLs.

4. Scanner Tab: Automates security testing by scanning the target for vulnerabilities. Configure settings, launch the scanner to identify and report potential security issues in the web application.

Functionality:

- Automates the identification of security vulnerabilities.
- Integrates various scanning tools.

How to Use:

- Select the target, configure scan settings, and click "Start scan."
- Review the scan results in the "Scanner" sub-tab.

5. Intruder Tab: Burp Intruder is a powerful tool for performing highly customizable, automated attacks against websites. It enables you to configure attacks that send the same request over and over again, inserting different payloads into predefined positions each time. Among other things, you can use Intruder to:

- Fuzz for input-based vulnerabilities.
- Perform brute-force attacks.
- Enumerate valid identifiers and other inputs.
- Harvest useful data.

Functionality:

- Automates customized attacks on web applications.
- Aids in identifying vulnerabilities through parameter manipulation.

How to Use:

- Define attack positions, payloads, and other settings.
- Launch the attack and analyze the responses in the "Intruder" sub-tab.

6. Repeater Tab: Burp Repeater is a tool that enables you to modify and send an interesting HTTP or WebSocket message over and over.

You can use Repeater for all kinds of purposes, for example to:

- Send a request with varying parameter values to test for input-based vulnerabilities.
- Send a series of HTTP requests in a specific sequence to test for vulnerabilities in multi-step processes, or vulnerabilities that rely on manipulating the connection state.
- Manually verify issues reported by Burp Scanner.

Functionality:

- Allows manual testing and analysis of individual HTTP requests.
- Useful for fine-tuning or retesting specific requests.

How to Use:

- Select a request in the Proxy history and send it to the Repeater.
- Modify and resend the request, and observe responses.

7. Decoder Tab: Burp Decoder enables you to transform data using common encoding and decoding formats. You can use Decoder to:

- Manually decode data.
- Automatically identify and decode recognizable encoding formats, such as URL-encoding.
- Transform raw data into various encoded and hashed formats.

  Decoder enables you to apply layers of transformations to the same data. This enables you to unpack or apply complex encoding schemes. For example, to generate modified data in the correct format for an attack, you could:

1. Apply URL-decoding, then HTML-decoding.
2. Edit the decoded data.
3. Reapply the HTML-encoding, then the URL-encoding.

Functionality:

- Decodes and encodes data to facilitate analysis.
- Supports various encoding schemes (Base64, URL, etc.).

How to Use:

- Paste encoded data, select the encoding type, and decode.

8. **Comparer Tab:** Burp Comparer enables you to compare any two items of data. You can use Comparer to quickly and easily identify subtle differences between requests or responses. For example:

- To compare responses to failed logins that use valid and invalid usernames, for username enumeration.
- To compare large responses with different lengths that you have identified in an Intruder attack.
- To compare similar requests that give rise to different application behavior.
- To compare responses when testing for blind SQL injection bugs using Boolean condition injection, to see whether injecting different conditions results in a relevant difference in responses.

Functionality:

- Compares two pieces of data or requests for differences.
- Useful for identifying variations in responses.

How to Use:

- Paste or load two pieces of data, click "Compare," and analyze the differences.

9. **Extender Tab:** Enables customizing and extending Burp Suite's functionality. Use the Extender tab to load and manage extensions, scripts, or plugins for tailored testing and automation.

Functionality:

- Allows the integration of third-party extensions.
- Extends Burp's functionality with custom tools and scripts.

How to Use:

- Manage and load extensions from the BApp Store.
- Create your own extensions to enhance capabilities.

10. Options Tab: Configures global settings in Burp Suite, allowing users to customize preferences, proxy listeners, and other application-wide parameters. Adjust settings for optimal testing and workflow efficiency.

Functionality:

- Configures global settings for Burp Suite.
- Customizes various aspects like display, proxy, and security settings.

How to Use:

- Adjust settings according to your testing requirements.

11. Project Tab: Organizes testing activities within Burp Suite, facilitating the management of multiple projects. Create, save, and load project files, enabling efficient collaboration and organization of scan data and configurations.

Functionality:

- Manages multiple projects for organized testing.
- Saves and loads project configurations.

How to Use:

- Create, save, and load projects for different applications

12. Alerts Tab: Displays and tracks security alerts generated during testing in Burp Suite. View detailed information on identified vulnerabilities, prioritize remediation efforts, and manage the security findings efficiently.

Functionality:

- Lists and categorizes discovered vulnerabilities.
- Provides detailed information on each issue.

How to Use:

- Review alerts after scans to prioritize and address vulnerabilities.

The Burp Suite dashboard is a comprehensive interface that empowers users to perform a wide range of security testing activities, from initial mapping and analysis to automated scanning and manual exploitation. Each tab serves a specific purpose, contributing to the overall effectiveness of the tool in identifying and mitigating security risks in web applications.

➢ Proxy Tab:

The Proxy tab in Burp Suite is a powerful tool that allows you to intercept and manipulate HTTP/S traffic between your browser and the target web application. Here's a detailed overview of the Proxy tab:

Proxy Tab Overview:

Interception:

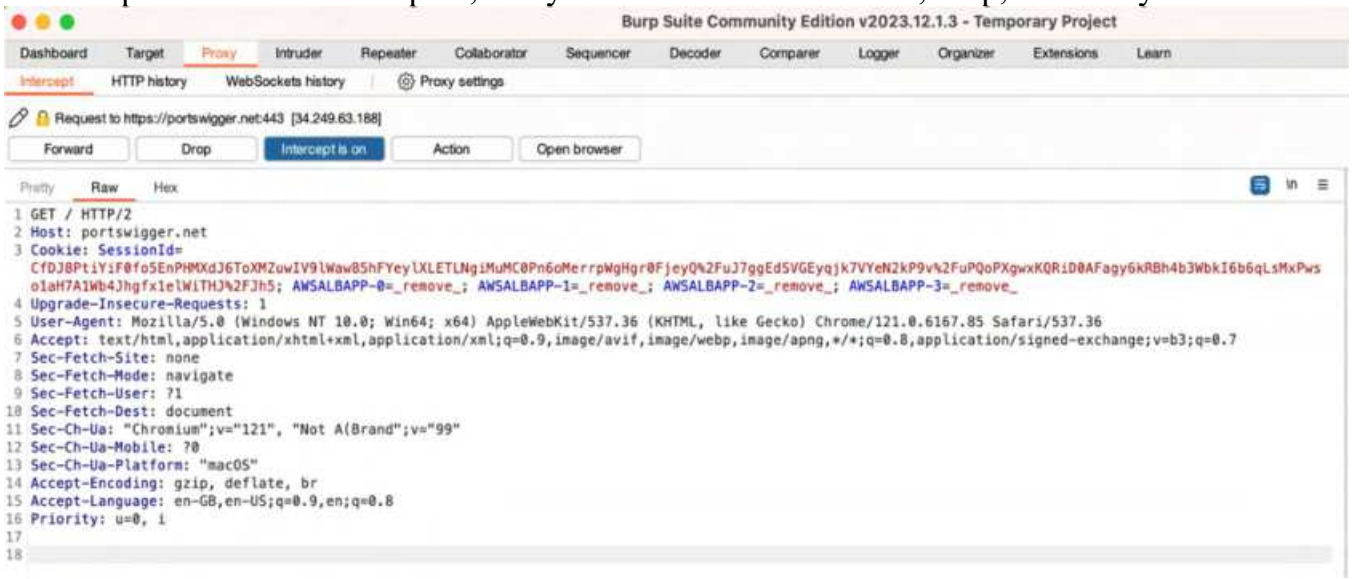
Functionality:

- Intercepts and allows modification of HTTP/S requests and responses.
- Essential for manual testing and analysis of web application traffic.

How to Use:

- Enable the interception by clicking "Intercept is on" in the Proxy tab.

- Requests will be intercepted, and you can choose to forward, drop, or modify them.



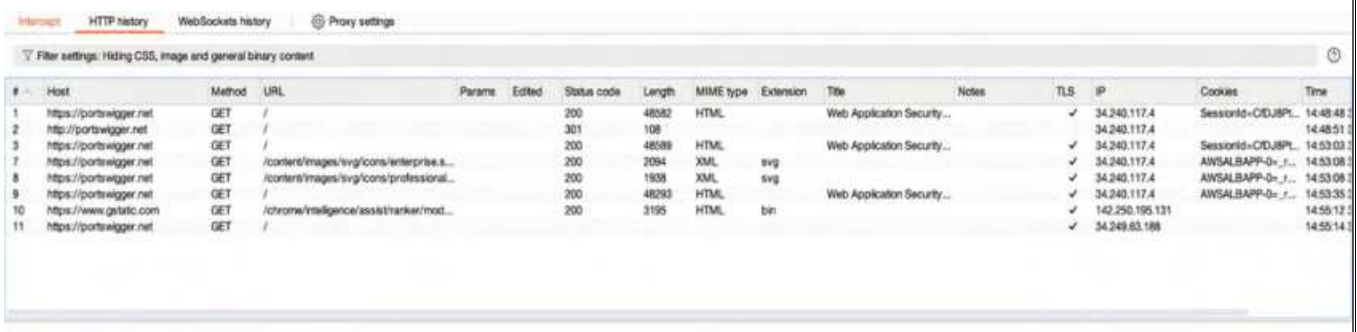
HTTP History:

Functionality:

- Logs all HTTP/S requests and responses passing through the proxy.
- Allows for easy review and analysis of the traffic.

How to Use:

- View and filter the HTTP history to inspect requests and responses.



Scope:

Functionality:

- Defines the target scope for testing.
- Allows you to include or exclude specific URLs or entire domains.

How to Use:

- Configure scope settings in the Target tab to focus testing on specific areas.

Options:

Functionality:

- Configures various proxy options and settings.
- Includes options for interception, request handling, and display.

How to Use:

- Adjust proxy options according to your testing requirements.

WebSockets:

Functionality:

- Handles WebSocket traffic for applications using this communication protocol.
- Enables interception and analysis of WebSocket messages.

How to Use:

- Enable WebSocket support in the Proxy options and monitor WebSocket messages.

HTTP/2:

Functionality:

- Supports the interception and analysis of HTTP/2 traffic.
- Allows for testing and manipulation of applications using HTTP/2.

How to Use:

- Enable HTTP/2 support in the Proxy options and monitor HTTP/2 traffic.

Options Sub-Tab:

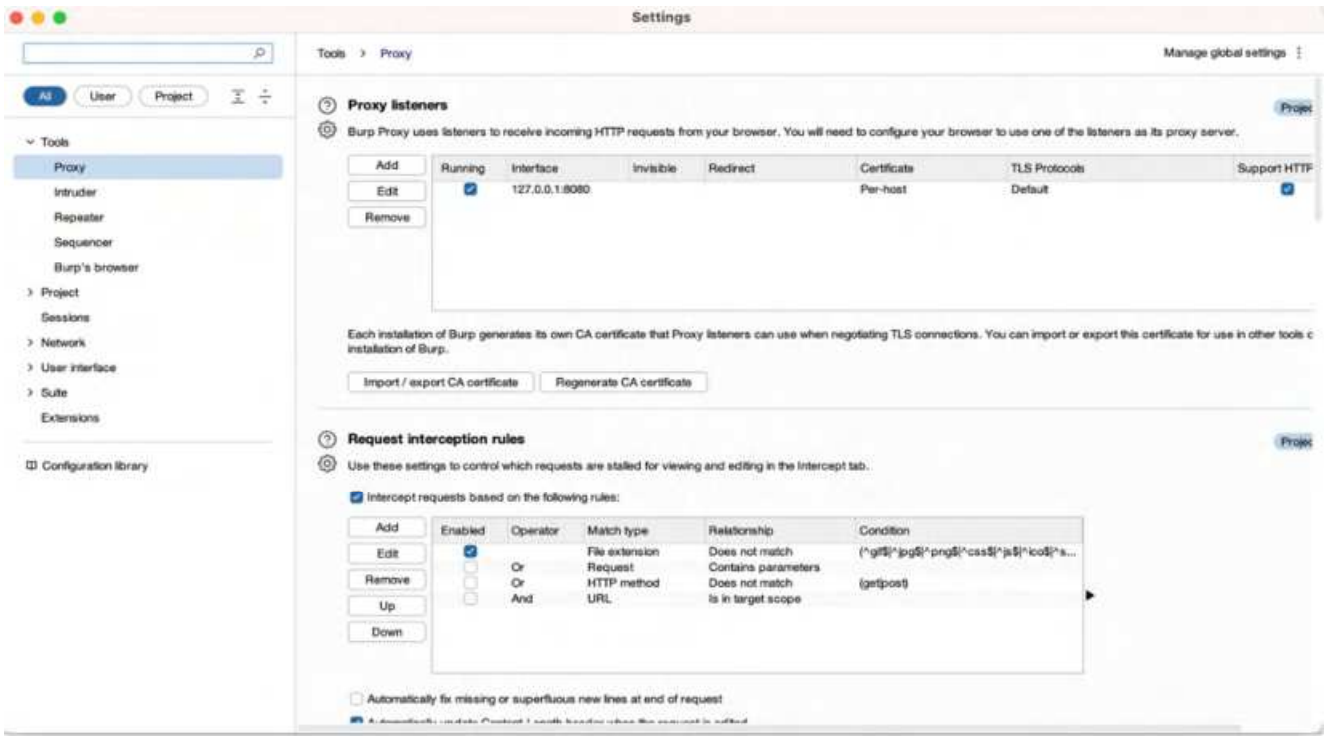
Functionality:

- Provides detailed configuration options for the proxy.
- Allows customization of proxy listeners, interception rules, and more.

How to Use:

- Access the Options sub-tab to fine-tune proxy settings based on your requirements.

Proxy Settings:



How to Set up Burp Suite Proxy:

In Burp Suite, the Certificate Authority (CA) certificate is a crucial component when using the Proxy tool. The Proxy tool allows you to intercept and manipulate HTTP/S traffic between your browser and the target web application. When you enable interception in Burp Suite, it acts as a proxy between your browser and the target server, allowing you to view and modify the requests and responses.

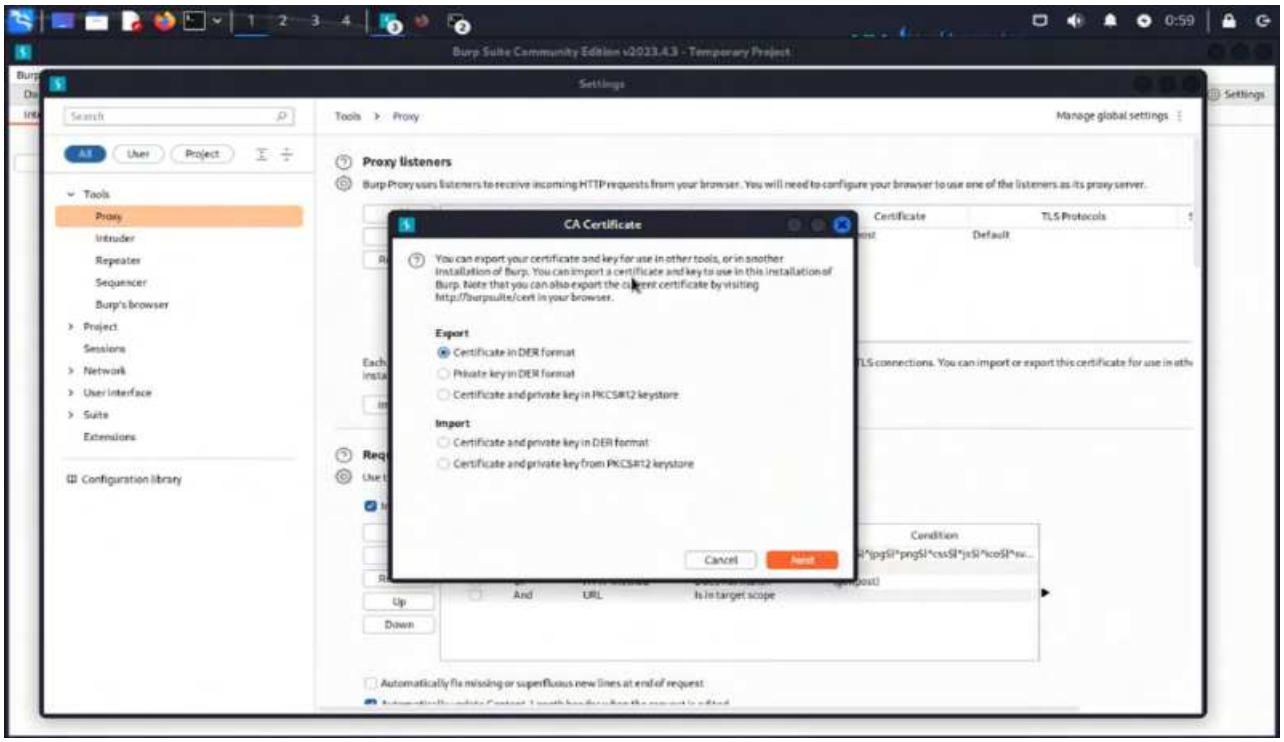
Here's how the CA certificate works in the Proxy tab:

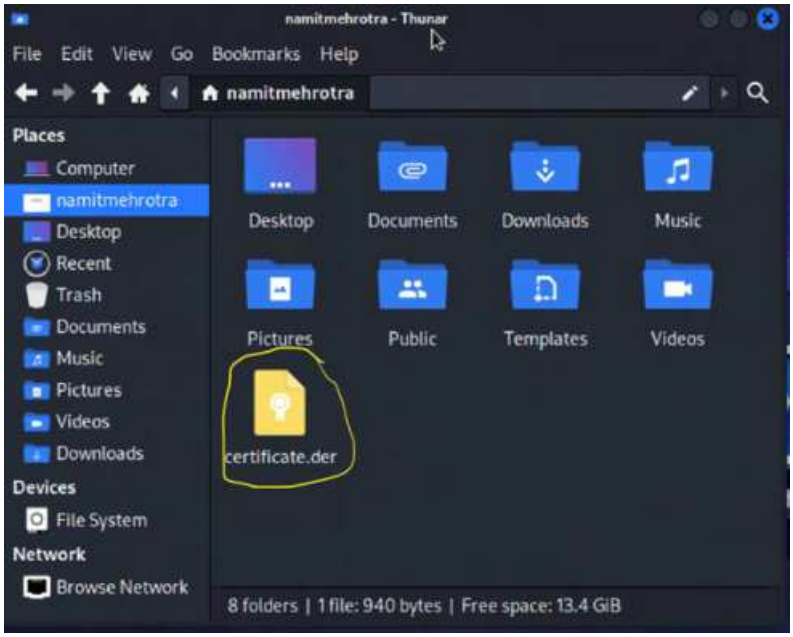
1. **Generate CA Certificate:** Burp Suite generates its own CA certificate, which is used to sign SSL certificates for the sites you visit. This CA certificate is unique to your Burp Suite instance.
2. **Install CA Certificate:** To intercept and modify HTTPS traffic, your browser must trust the Burp Suite CA certificate. You need to install this CA certificate in your browser's certificate store. The CA certificate is usually found in the "User Options" section under the "Proxy" tab in Burp Suite.
3. **Intercept HTTPS Traffic:** Once the CA certificate is installed and the interception is enabled in the Proxy tab, Burp Suite can decrypt and inspect HTTPS traffic between your browser and the target server. This allows you to see and modify the content of encrypted connections.
4. **Configure Browser:** After installing the CA certificate, you need to configure your browser to use Burp Suite as a proxy. Set the browser's proxy settings to use Burp Suite as the proxy server on a specific port (default is 127.0.0.1:8080).
5. **SSL Handshake:** When you visit an HTTPS site, the SSL handshake occurs. Burp Suite generates a new SSL certificate for the target site signed by its CA certificate. Since your

browser trusts the Burp Suite CA, it accepts the certificate, allowing Burp Suite to intercept and modify the encrypted traffic.

6. **Modify Requests and Responses:** With the CA certificate in place, you can now intercept and modify both HTTP and HTTPS traffic using Burp Suite. This is useful for security testing, debugging, and analyzing how applications handle different types of requests and responses.

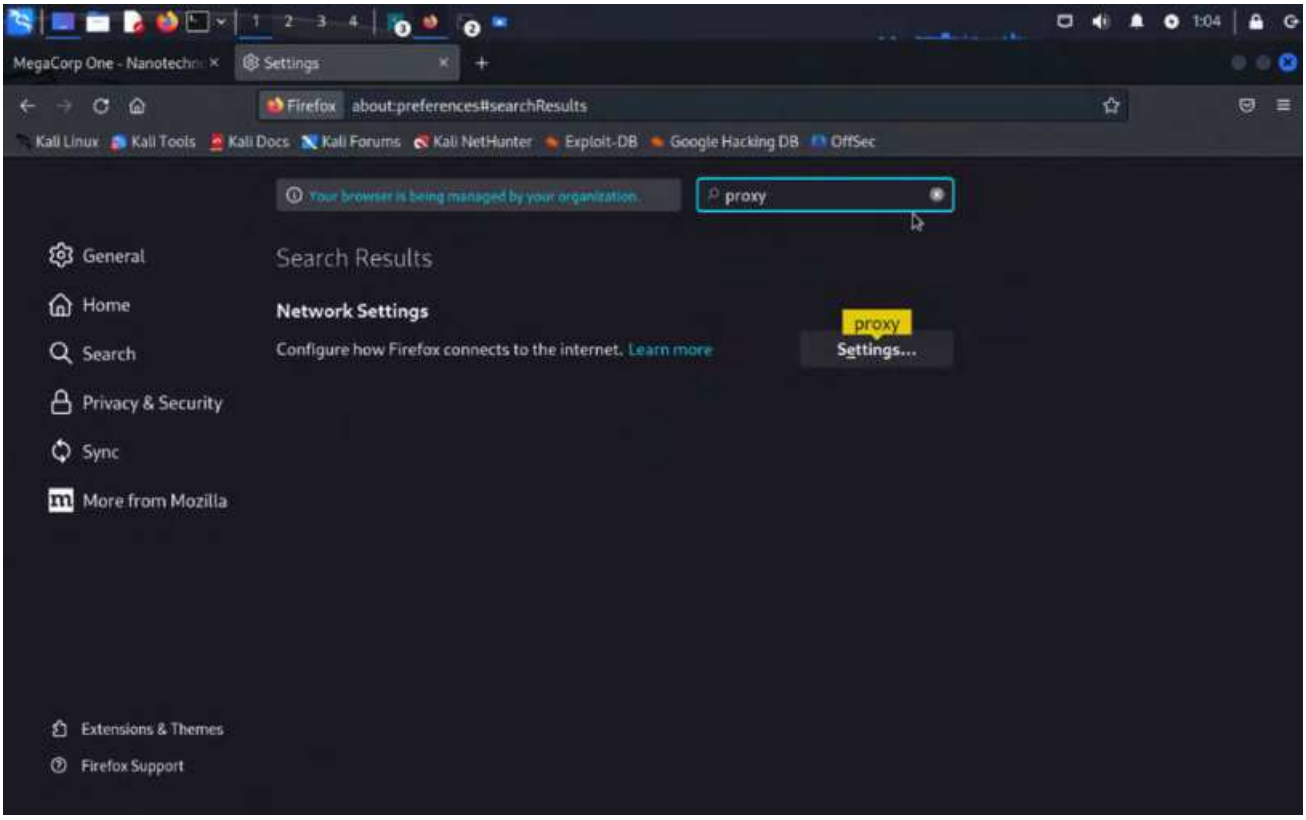
Remember that using a proxy to intercept HTTPS traffic requires careful handling and compliance with ethical and legal standards. It's typically used for security testing and debugging in controlled environments. Always ensure that you have the necessary permissions and adhere to relevant laws and regulations when intercepting and manipulating network traffic.



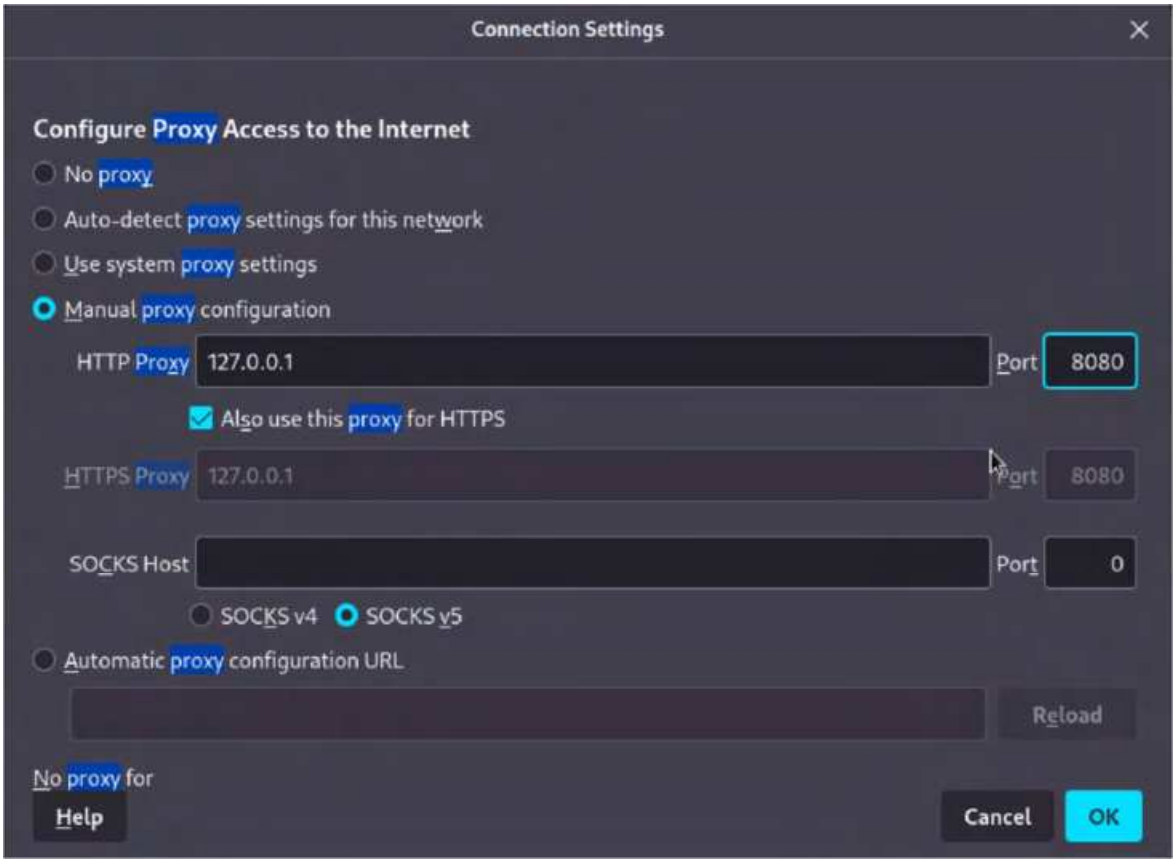


How to Use Burp Suite Proxy:

Configure Browser:

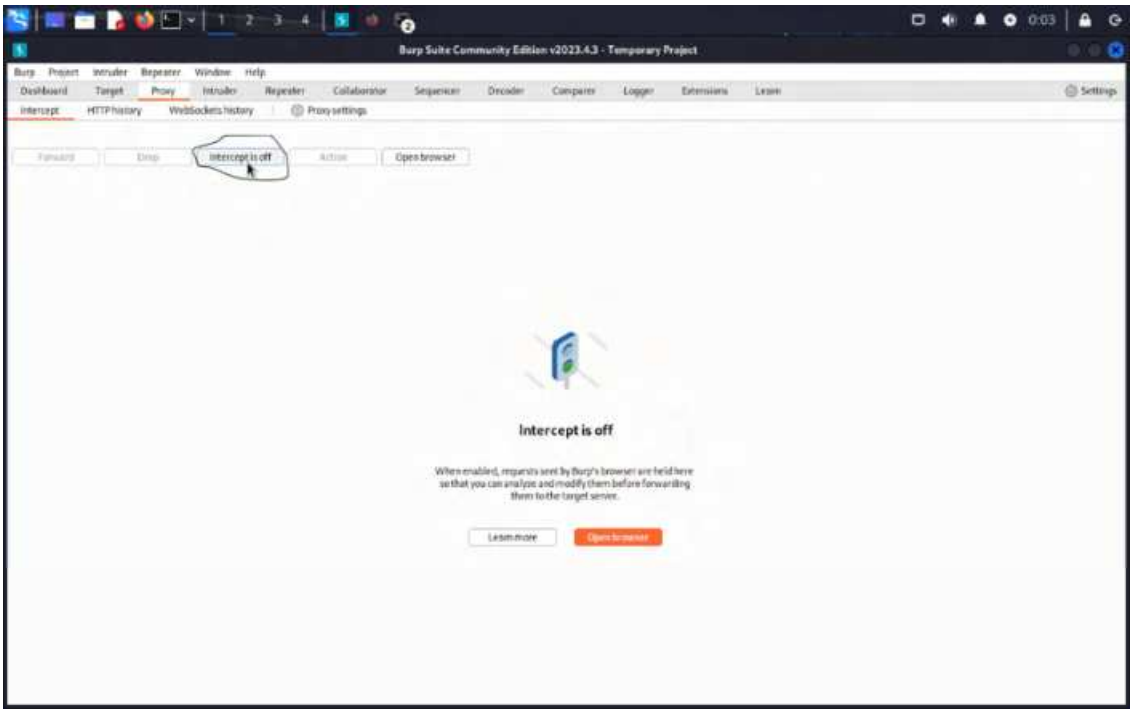


- Set your browser to use Burp as a proxy. Configure the proxy settings to point to Burp's proxy listener (default is 127.0.0.1:8080).



Enable Interception:

- In the Proxy tab, click on the "Intercept is off" button to toggle interception on.
- Intercepted requests will be displayed, and you can choose to forward, drop, or modify them.



Review Traffic:

- Use the HTTP History tab to review all intercepted requests and responses.
- Filter the history to focus on specific URLs or methods.

Modify Requests:

- In the Intercept tab, modify requests before forwarding them to the server.
- Make changes such as parameter manipulation or header modifications.

Configure Scope:

- Set the testing scope in the Scope tab to include or exclude specific URLs or domains.
- This helps focus testing on relevant areas of the application.

WebSocket and HTTP/2:

- Enable WebSocket and HTTP/2 support in the Proxy options if your application uses these protocols.
- Monitor and intercept WebSocket messages or HTTP/2 traffic.

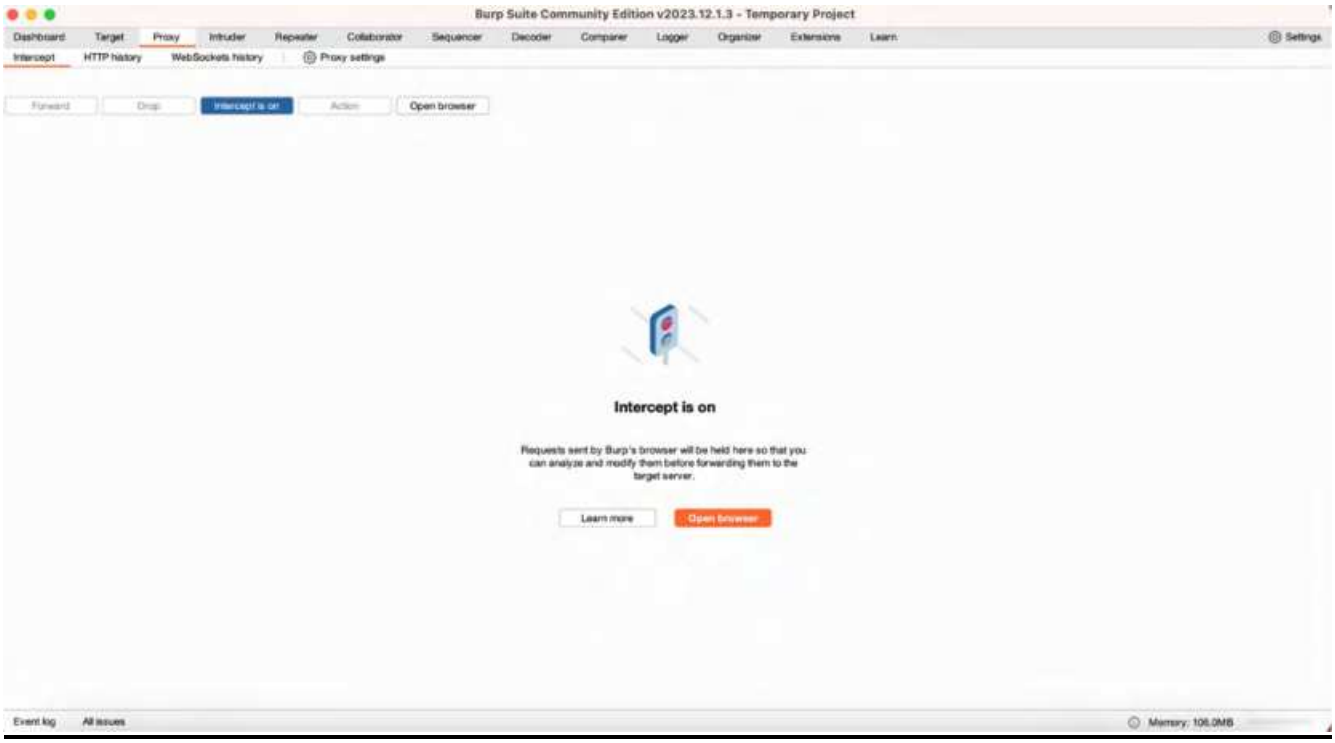
Options Configuration:

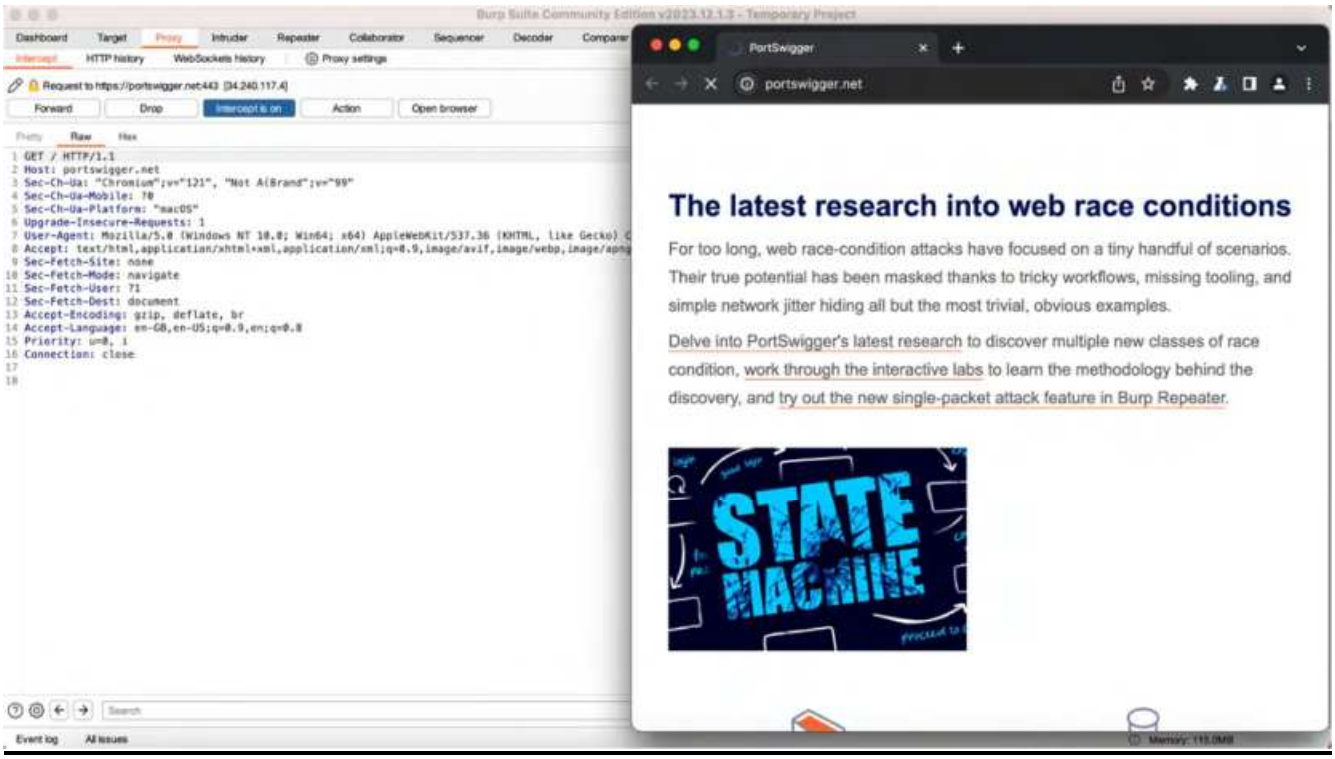
- Access the Options sub-tab to configure advanced settings for the proxy.
- Customize listeners, interception rules, and other options based on your testing needs.

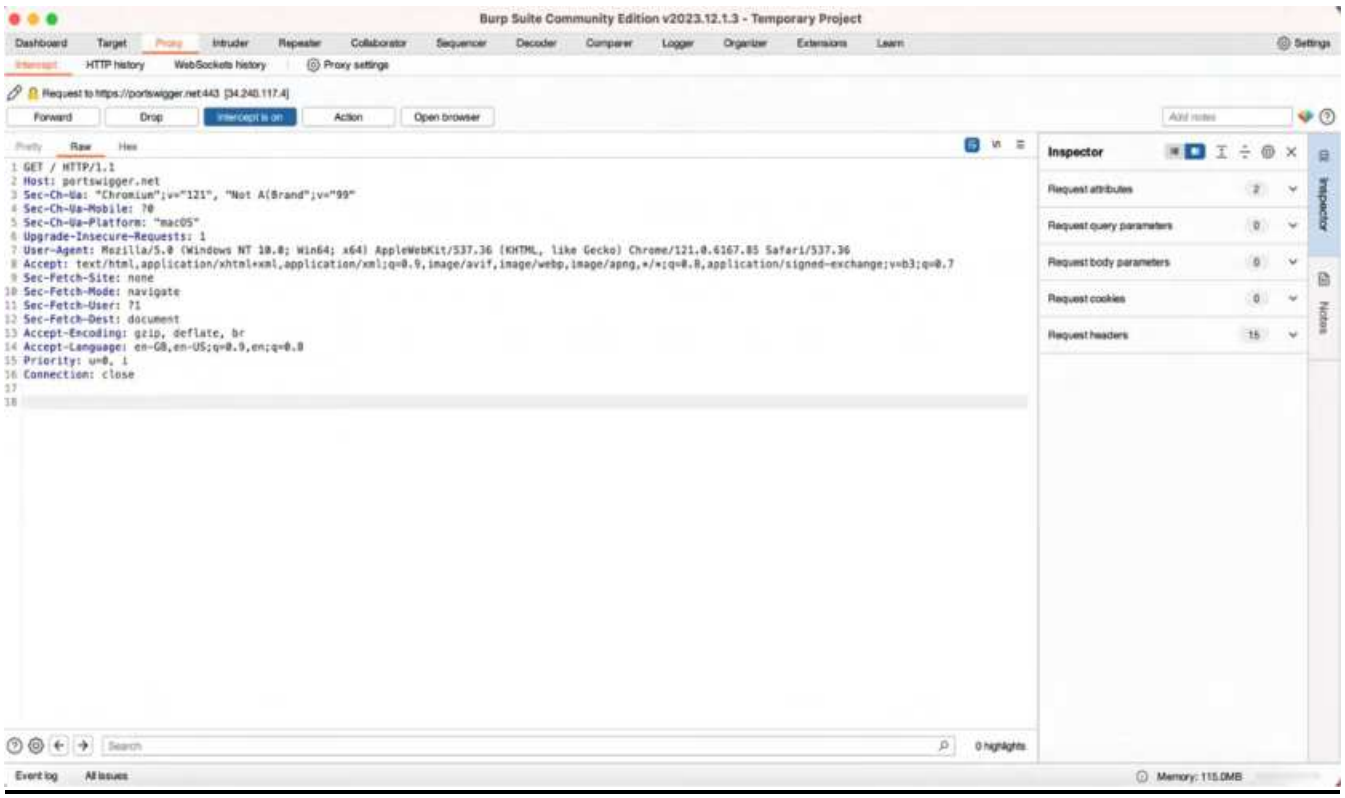
Using Burp Suite's Proxy effectively is crucial for identifying security vulnerabilities in web applications. It provides a centralized point for inspecting and manipulating traffic, ensuring a thorough analysis of communication between the browser and the target application.

Intercept HTTP traffic with Burp Proxy:

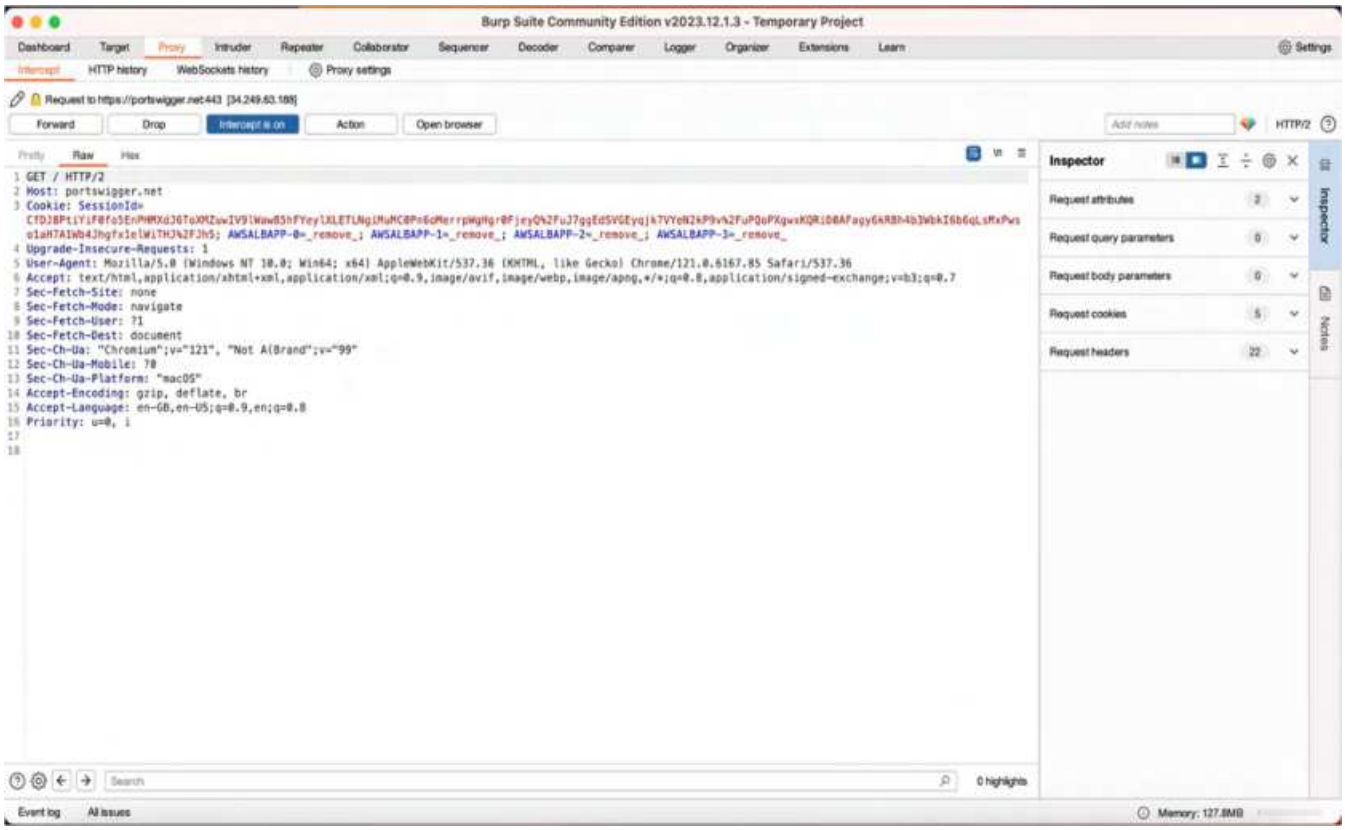
-> proxy -> Intercept on -> Open browser ->






Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Request to https://portswigger.net:443 [34.240.117.4]
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: portswigger.net
3 Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: "macOS"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
15 Priority: u=0, i
16 Connection: close
17
18
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 0
Request headers 15
Search 0 highlights
Event log All issues
Memory: 115.0MB

-> forward


Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Request to https://portswigger.net:443 [34.249.63.188]
Forward Drop Intercept is on Action Open browser
HTTP/2
Pretty Raw Hex
1 GET / HTTP/2
2 Host: portswigger.net
3 Cookie: SessionId=
CfDJBPtiYifBfo5EnPHMXdJ6ToXMZwwIV9lWaw85hfYeylXLETLNgiHuNC8Pn6dMerrpWgHgr0FjeyQ%2FuJ7gqEdSVGEyqjk7VYeN2kP9v%2FuPQoPXgwxKQRiD8AFagy6kR8h4bJWbkI6b6qLsMxPwso1aH7AIWb4JhgfxlelWiTHJ%2FJh5; AWSALBAPP-0=_remove_; AWSALBAPP-1=_remove_; AWSALBAPP-2=_remove_; AWSALBAPP-3=_remove_
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Sec-Fetch-Site: none
8 Sec-Fetch-Mode: navigate
9 Sec-Fetch-User: ?1
10 Sec-Fetch-Dest: document
11 Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
12 Sec-Ch-Ua-Mobile: ?0
13 Sec-Ch-Ua-Platform: "macOS"
14 Accept-Encoding: gzip, deflate, br
15 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
16 Priority: u=0, i
17
18
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 5
Request headers 22
Search 0 highlights
Event log All issues
Memory: 127.8MB

➢ Intruder Tab:

Burp Intruder is a powerful tool for performing highly customizable, automated attacks against websites.

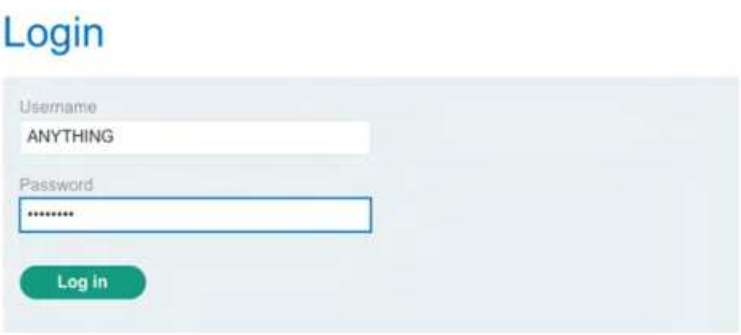
- Open Burp's browser, and use it to access the following URL:

https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-different-responses

Click **Access the lab** and log in to your PortSwigger account if prompted. This opens your own instance of a deliberately vulnerable blog website.

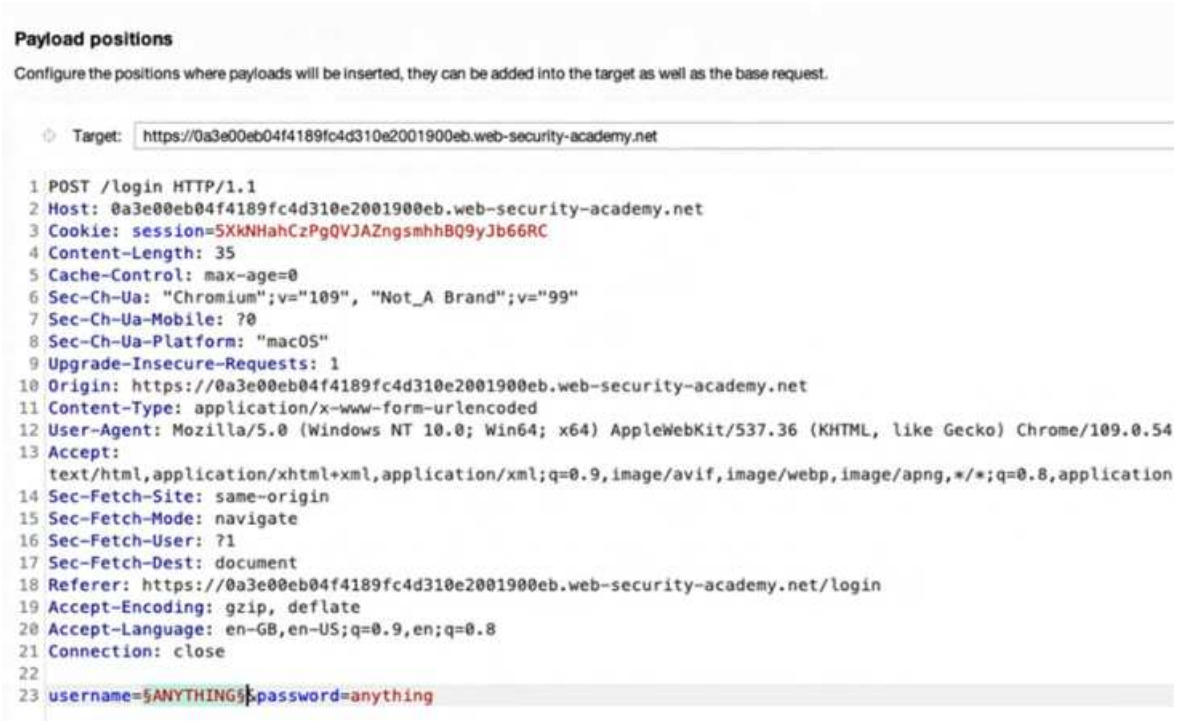
- **Try to log in**

Click **My account**, then try to log in using an invalid username and password.



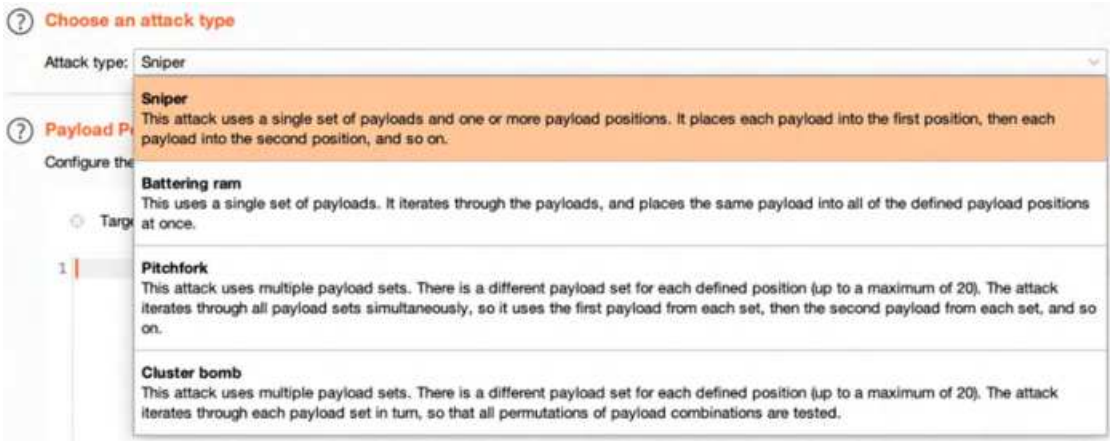
- Go to the Intruder tab. Observe that there is now a tab displaying the POST /login request. We'll use this as the base request for our attack.

Notice that the value of the username parameter that you previously highlighted is now marked as a payload position. This is indicated by the § characters at the beginning and end of the value. Burp Intruder will insert payloads at this position during the attack.



- **Select an attack type**

At the top of the screen, you can select different attack types. For now, just make sure this is set to **Sniper**.



- **Add the payloads**

You now just need to configure the list of payloads that you want to use. For this demonstration, we'll try sending the request with different usernames to test how the login mechanism behaves.

Copy the following list of candidate usernames:

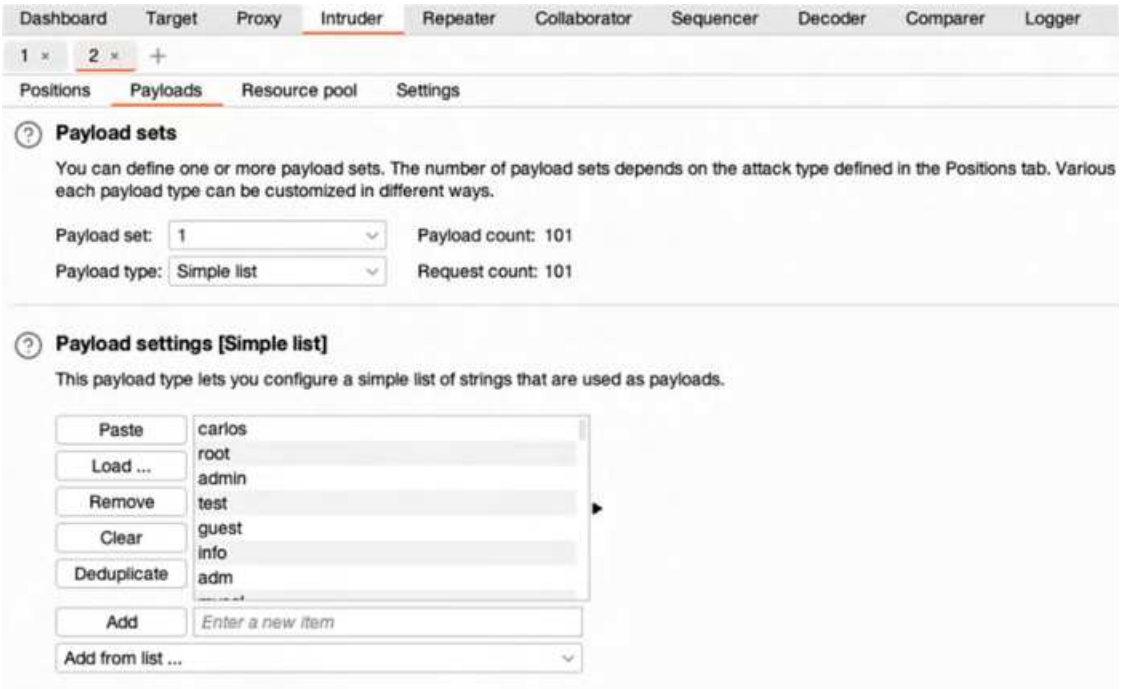
- Candidate usernames

Go to the **Payloads** tab.

Leave the **Payload type** set to **Simple list**.

In the **Payload settings** field, click **Paste** to add the copied usernames to the list.

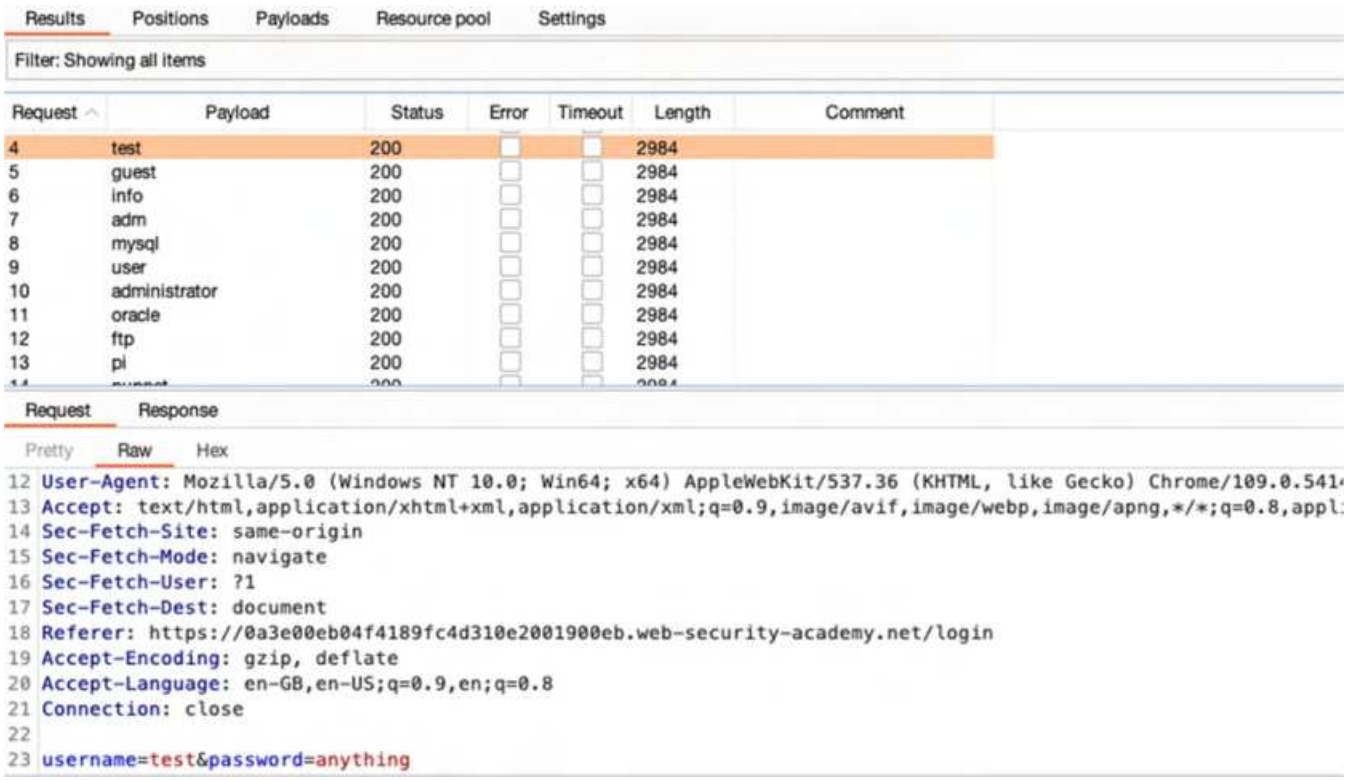
In the **Payload sets** section, you can see how many payloads you have added, and how many requests this attack will send. For this attack, you should see: Payload count: 101 / Request count: 101.



- **Start the attack**

In the upper-right corner, click **Start attack**. This opens a new attack window in which you can see each of the requests that Burp Intruder is making.

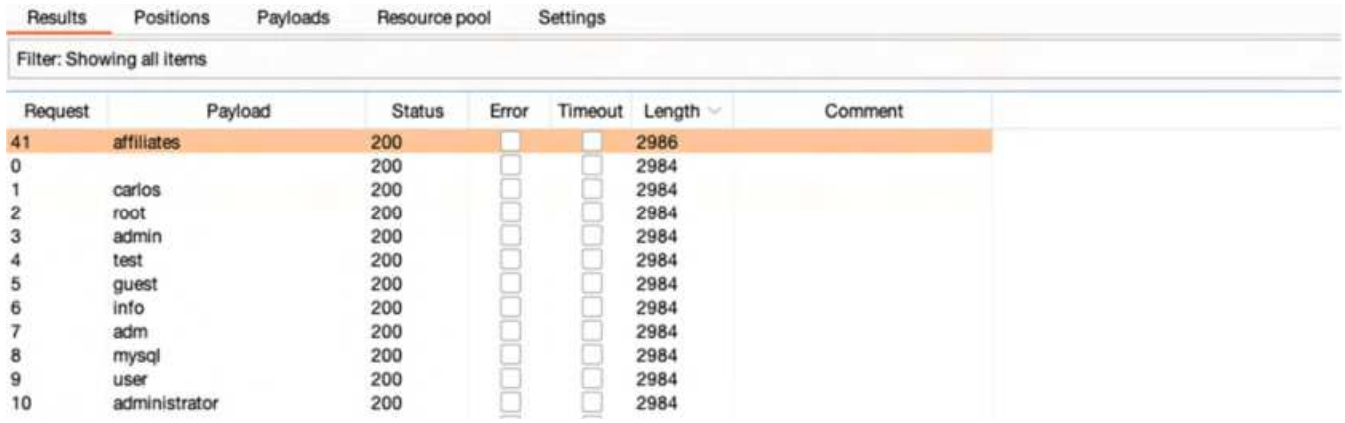
If you select one of the entries in the table, you can view the request and response in the message editor. Notice that the username parameter contains a different value from our payload list in each request.



- **Look for any irregular responses**

The attack window contains several columns displaying key information about each response.

Wait for the attack to finish, then click the heading of the **Length** column to sort the results. As you can see, one of the responses is a different length.

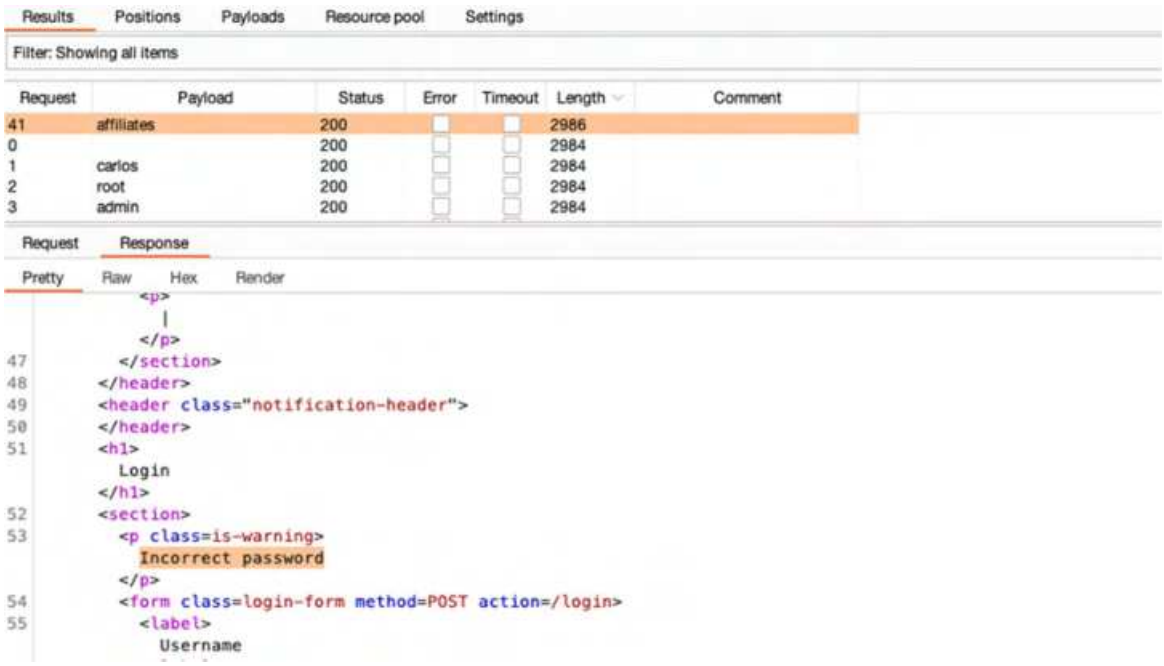


➢ Study the response

Select any request from the list to display it in the message editor.

Studying the responses, notice that most contain an Invalid username error message, but the one with the different length response has an Incorrect password error message.

This different response strongly suggests that this username might be valid in this case.



Now that you have a potentially correct username, the next logical step is to try to brute-force the password. Try repeating this attack, using the username you have identified and this list of candidate passwords.

➢ Target Tab:

The "Target" tab in Burp Suite is a crucial component that allows users to manage and control the scope of their testing. The Target tool enables you to define which targets are in scope for your current work. It also contains the site map and **Crawl paths** tab, which show you detailed information about your target applications. Here's a detailed overview of the Target tab:

Target Tab Overview:

Scope:

Functionality:

- Defines the scope of the testing by specifying the URLs and domains to include or exclude.
- Ensures that testing efforts are focused on specific areas of the application.

How to Use:

- Add target URLs to the scope by entering them in the "Include in scope" field.
- Use the "Exclude from scope" field to exclude specific URLs or domains.

Site Map:

Functionality:

- Displays a hierarchical representation of the target application's structure.
- Provides an overview of discovered pages and their relationships.

How to Use:

- Automatically populates as you navigate through the application or perform scans.
- Right-click on items to perform actions such as adding to scope or launching scans.

Issues:

Functionality:

- Lists and categorizes security issues discovered during testing.
- Provides detailed information about each identified vulnerability.

How to Use:

- View and filter discovered issues to prioritize and address security vulnerabilities.

Scope Control:

Functionality:

- Allows quick access to control the scope settings.
- Provides options to include or exclude specific URLs or domains on the fly.

How to Use:

- Adjust scope settings dynamically by clicking on the "Scope" button and making changes.

Export:

Functionality:

- Enables the export of the site map and discovered issues.
-

- Supports various formats, including XML and CSV.

How to Use:

- Export site maps or issues data for reporting or external analysis.

Engagement Tools:

Functionality:

- Facilitates engagement with the target application.
- Includes tools like the Spider, Scanner, and Repeater.

How to Use:

- Use engagement tools to map the application, identify vulnerabilities, and test individual requests.

How to Use Burp Suite Target Tab:

Add Targets to Scope:

- Enter target URLs in the "Include in scope" field to add them for testing.
- Use the "Exclude from scope" field to exclude specific URLs or domains.

Site Map Navigation:

- Navigate through the site map to understand the structure of the application.
- Right-click on items to perform actions like adding to scope or launching scans.

Scan Configuration:

- Before launching scans, ensure that the scope is appropriately configured.
- Adjust scope settings to focus on specific areas of the application.

Issue Review:

- Monitor the "Issues" tab for a categorized list of identified vulnerabilities.
- Prioritize and address vulnerabilities based on severity and impact.

Dynamic Scope Adjustment:

- Use the "Scope" button for dynamic adjustment of the testing scope.
- Modify scope settings on the fly to adapt to testing needs.

Export Data:

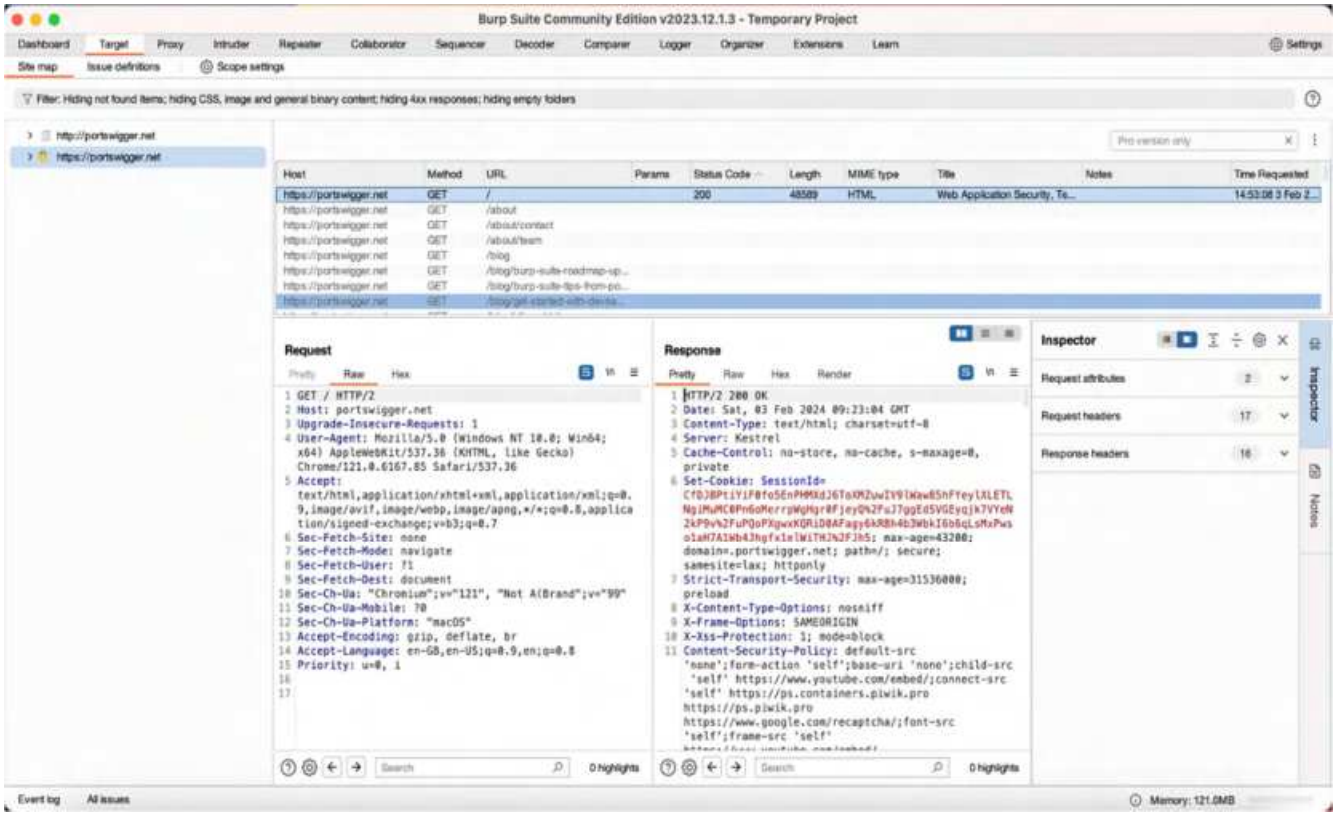
- Export the site map or issue data using the "Export" feature.
- Choose the desired format for reporting or external analysis.

Engagement Tools Integration:

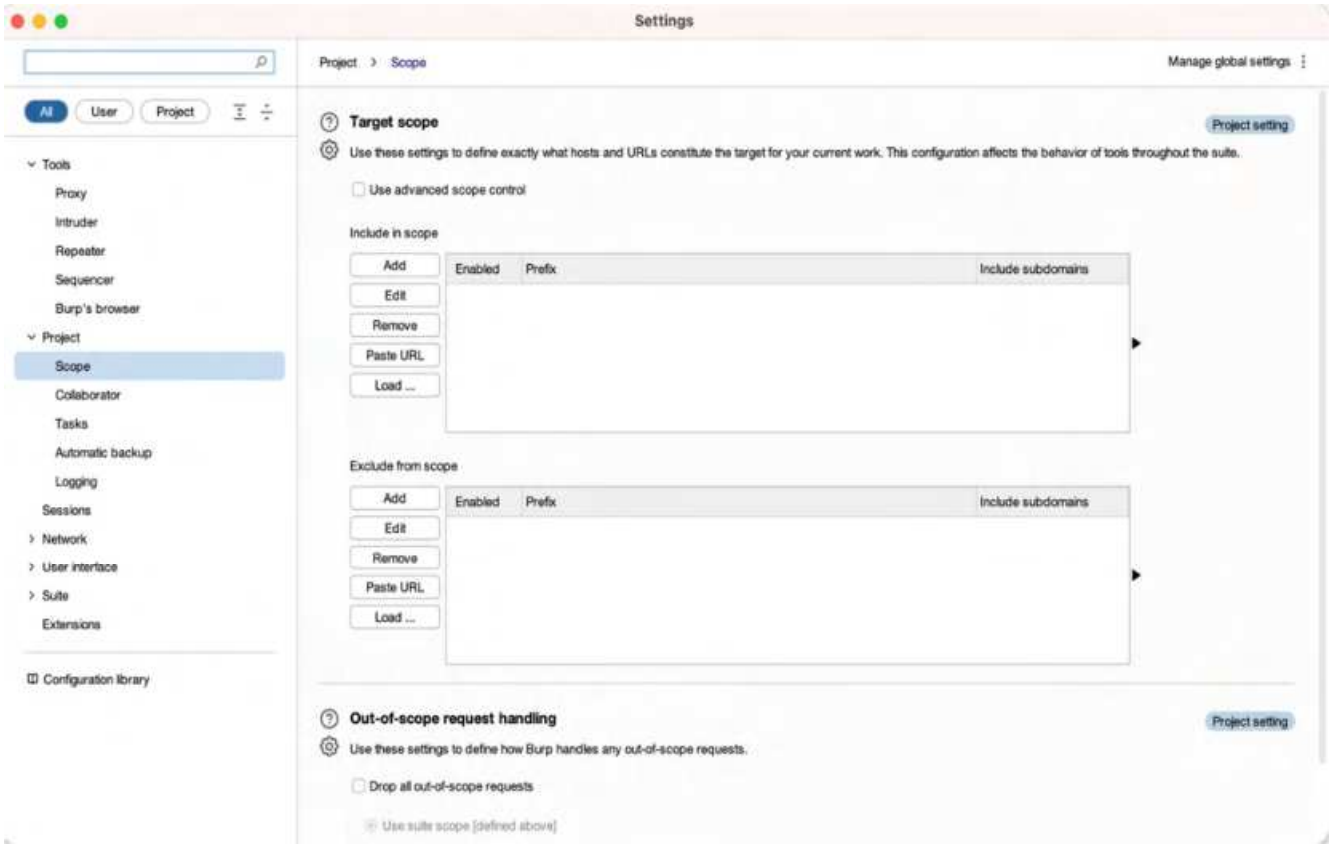
- Utilize engagement tools like Spider and Scanner directly from the Target tab.
- Perform comprehensive testing using tools available in the Burp Suite ecosystem.

The "Target" tab in Burp Suite serves as the control centre for managing the scope of your security testing efforts. By effectively using the features within this tab, you can ensure a

focused and thorough examination of the target application, identifying and addressing potential security issues.



Target scope settings:

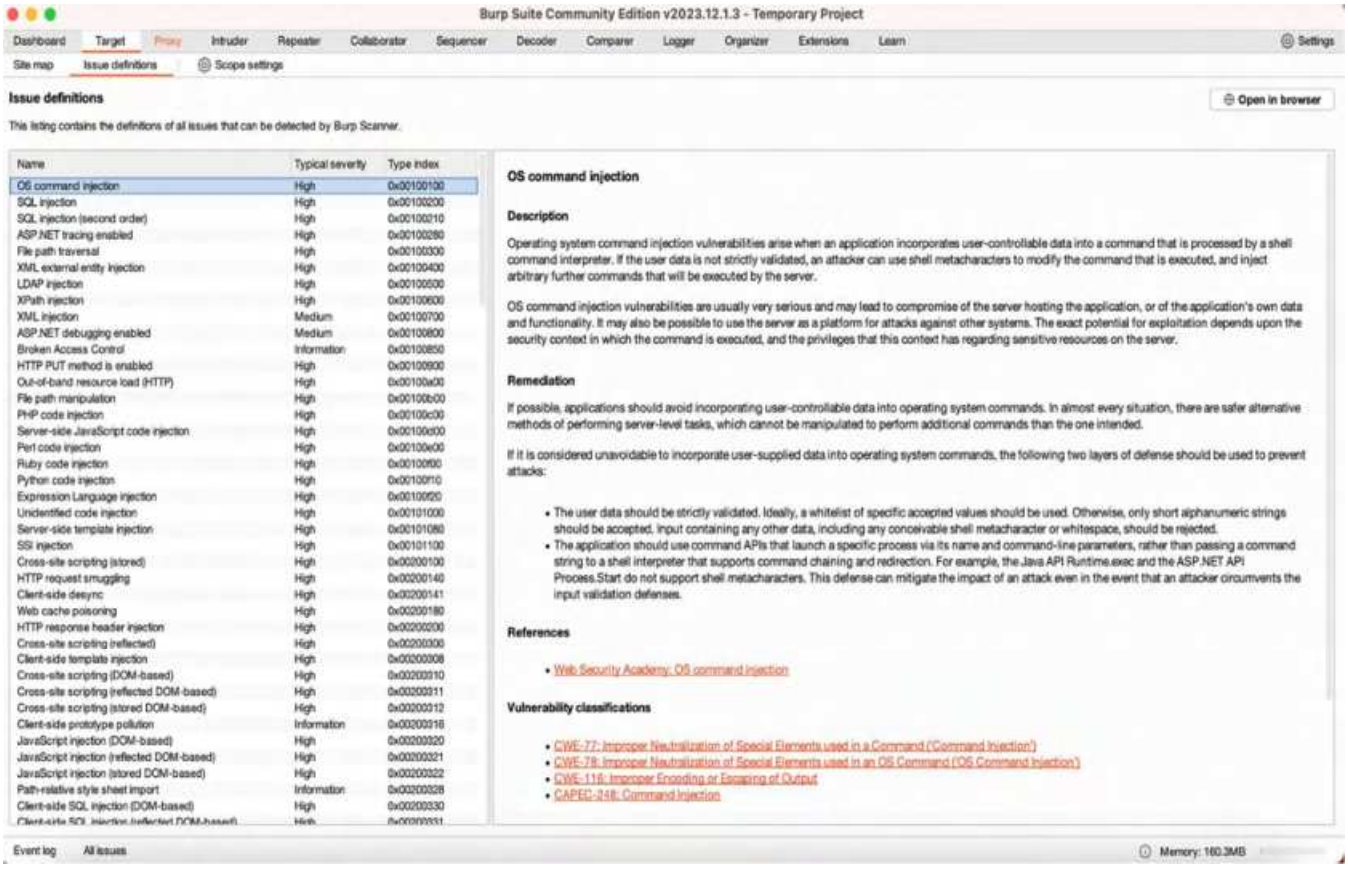


Site map:

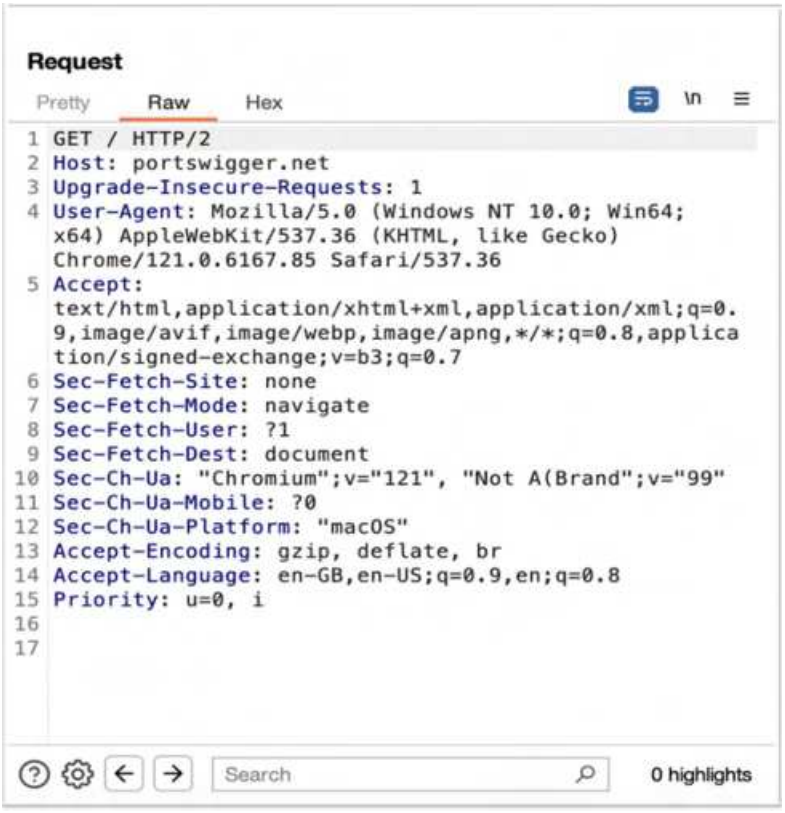
Items added to site map View site map

Host	Meth...	URL	Status ...	MIME Ty...
portswigger.net	GET	/	301	
portswigger.net	GET	/	200	HTML
portswigger.net		/content/images/logos/port...		
portswigger.net		/web-security		
portswigger.net		/research		
portswigger.net		/web-security/certification		
portswigger.net		/blog		
portswigger.net		/blog/burp-suite-tips-from-...		
portswigger.net		/blog/get-started-with-devs...		
portswigger.net		/blog/i-thought-it-was-a-co...		
portswigger.net		/blog/train-the-basics-bug-...		
portswigger.net		/about/team		
portswigger.net		/research/top-10-web-hac...		
portswigger.net		/web-security/getting-started		
portswigger.net		/blog/burp-suite-roadmap-...		
portswigger.net		/content/images/logos/favi...		
portswigger.net		/content/images/logos/appl...		
portswigger.net	GET	/content/pslandingpages.css	200	CSS
portswigger.net	GET	/content/fonts/ps-icons-sm...	200	woff
portswigger.net	GET	/content/fonts/ps-main/ps-i...	200	woff
portswigger.net		/users		
portswigger.net		/customers		
portswigger.net		/about		
portswigger.net		/careers		
portswigger.net		/legal		
portswigger.net		/contact		
portswigger.net		/support/reseller-faqs		
portswigger.net		/users/youraccount		
portswigger.net		/burp/enterprise		
portswigger.net	GET	/content/images/svg/icons/...	200	XML
portswigger.net		/burp/pro		
portswigger.net	GET	/content/images/svg/icons/...	200	XML

Issue Definitions:



Request:



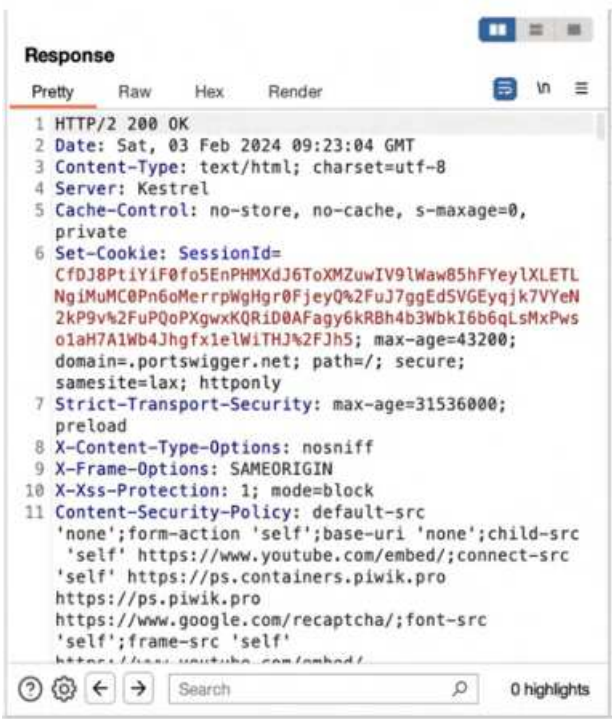
Request

Pretty Raw Hex \n

```
1 GET / HTTP/2
2 Host: portswigger.net
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
  x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/121.0.6167.85 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.
  9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
  tion/signed-exchange;v=b3;q=0.7
6 Sec-Fetch-Site: none
7 Sec-Fetch-Mode: navigate
8 Sec-Fetch-User: ?1
9 Sec-Fetch-Dest: document
10 Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
11 Sec-Ch-Ua-Mobile: ?0
12 Sec-Ch-Ua-Platform: "macOS"
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
15 Priority: u=0, i
16
17
```

Search 0 highlights

Response:

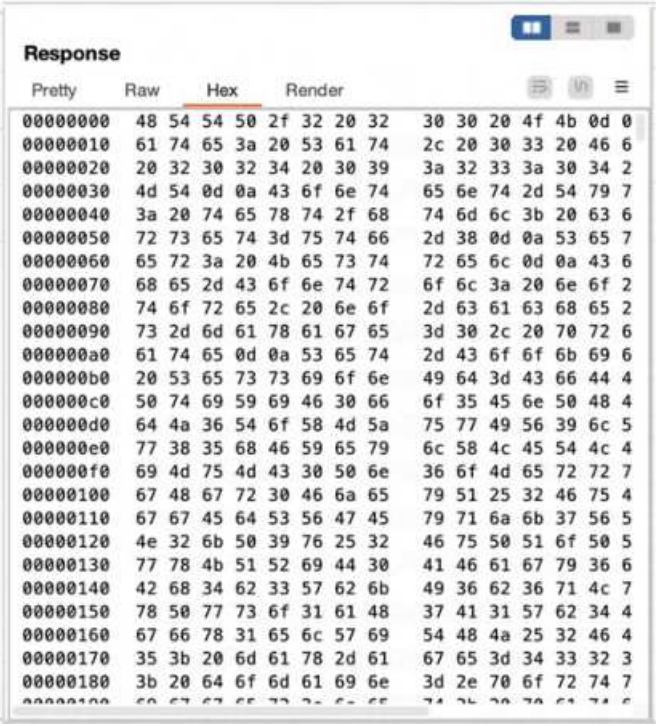


Response

Pretty Raw Hex Render \n

```
1 HTTP/2 200 OK
2 Date: Sat, 03 Feb 2024 09:23:04 GMT
3 Content-Type: text/html; charset=utf-8
4 Server: Kestrel
5 Cache-Control: no-store, no-cache, s-maxage=0,
  private
6 Set-Cookie: SessionId=
  CfDJ8PtiYiF0fo5EnPHMXdJ6ToXMZuwIV9lWaw85hFYeylXLETL
  NgiMuMC0Pn6oMerrpWgHgr0FjeyQ%2FuJ7ggEdSVGEyqjk7VYeN
  2kP9v%2FuPQoPXgwxKQRiD0AFagy6kRBh4b3WbkI6b6qLsMxPws
  o1aH7A1Wb4Jhgfx1elWiTHJ%2FJh5; max-age=43200;
  domain=.portswigger.net; path=/; secure;
  samesite=lax; httponly
7 Strict-Transport-Security: max-age=31536000;
  preload
8 X-Content-Type-Options: nosniff
9 X-Frame-Options: SAMEORIGIN
10 X-Xss-Protection: 1; mode=block
11 Content-Security-Policy: default-src
  'none';form-action 'self';base-uri 'none';child-src
   'self' https://www.youtube.com/embed/;connect-src
  'self' https://ps.containers.piwik.pro
  https://ps.piwik.pro
  https://www.google.com/recaptcha/;font-src
  'self';frame-src 'self'
```

Search 0 highlights



Response

Pretty Raw Hex Render

```
00000000  48 54 54 50 2f 32 20 32   30 30 20 4f 4b 0d 0
00000010  61 74 65 3a 20 53 61 74   2c 20 30 33 20 46 6
00000020  20 32 30 32 34 20 30 39   3a 32 33 3a 30 34 2
00000030  4d 54 0d 0a 43 6f 6e 74   65 6e 74 2d 54 79 7
00000040  3a 20 74 65 78 74 2f 68   74 6d 6c 3b 20 63 6
00000050  72 73 65 74 3d 75 74 66   2d 38 0d 0a 53 65 7
00000060  65 72 3a 20 4b 65 73 74   72 65 6c 0d 0a 43 6
00000070  68 65 2d 43 6f 6e 74 72   6f 6c 3a 20 6e 6f 2
00000080  74 6f 72 65 2c 20 6e 6f   2d 63 61 63 68 65 2
00000090  73 2d 6d 61 78 61 67 65   3d 30 2c 20 70 72 6
000000a0  61 74 65 0d 0a 53 65 74   2d 43 6f 6f 6b 69 6
000000b0  20 53 65 73 73 69 6f 6e   49 64 3d 43 66 44 4
000000c0  50 74 69 59 69 46 30 66   6f 35 45 6e 50 48 4
000000d0  64 4a 36 54 6f 58 4d 5a   75 77 49 56 39 6c 5
000000e0  77 38 35 68 46 59 65 79   6c 58 4c 45 54 4c 4
000000f0  69 4d 75 4d 43 30 50 6e   36 6f 4d 65 72 72 7
00000100  67 48 67 72 30 46 6a 65   79 51 25 32 46 75 4
00000110  67 67 45 64 53 56 47 45   79 71 6a 6b 37 56 5
00000120  4e 32 6b 50 39 76 25 32   46 75 50 51 6f 50 5
00000130  77 78 4b 51 52 69 44 30   41 46 61 67 79 36 6
00000140  42 68 34 62 33 57 62 6b   49 36 62 36 71 4c 7
00000150  78 50 77 73 6f 31 61 48   37 41 31 57 62 34 4
00000160  67 66 78 31 65 6c 57 69   54 48 4a 25 32 46 4
00000170  35 3b 20 6d 61 78 2d 61   67 65 3d 34 33 32 3
00000180  3b 20 64 6f 6d 61 69 6e   3d 2e 70 6f 72 74 7
```

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

INFORMATION SECURITY MANAGEMENT LAB

EXPERIMENT-4

Functionalities of Burp Suite

GROUP NO. :	**11**
TEAM MEMBER 1 :	**Namit Mehrotra**
REG. NO. :	**21BCE0763**
TEAM MEMBER 2 :	**Purva Sharma**
REG.NO :	**21BCE0169**
SUBJECT CODE :	**BCSE354E**
SUBJECT TITLE :	**Information Security Management**
LAB SLOT :	**L29+L30**
SEMESTER :	**Winter Semester 2023-2024**
GUIDED BY :	**NIHA K**

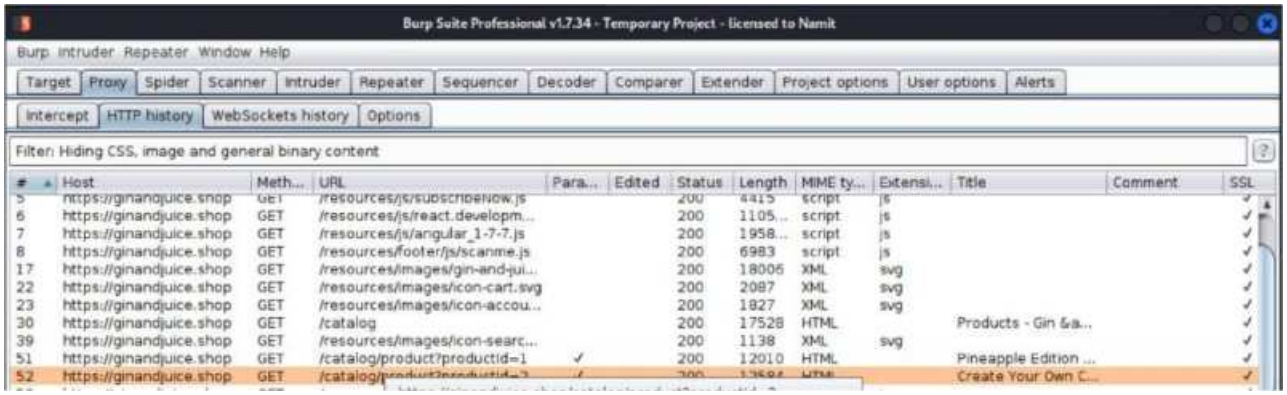
After documenting each feature of the tool and explaining its functionality in detail under experiment 3, provide a minimum of 6 to 10 scenarios (use case) where those functionality's will be used to solve the problems in Information Security Management along with detailed steps for each scenario.

1. **Identifying Cross-Site Scripting (XSS) Vulnerabilities**:

- **Scenario Question:** How would you utilize Burp Suite to identify and mitigate potential XSS vulnerabilities in the web application https://ginandjuice.shop/?
- **Scenario:** We suspect the web application https://ginandjuice.shop/ might be vulnerable to XSS attacks.
- **Steps**:

  1. **Proxy Setup**: Launch Burp Suite and configure your browser to use it as a proxy.
  2. **Interception**: Navigate to the target website and interact with different input fields.

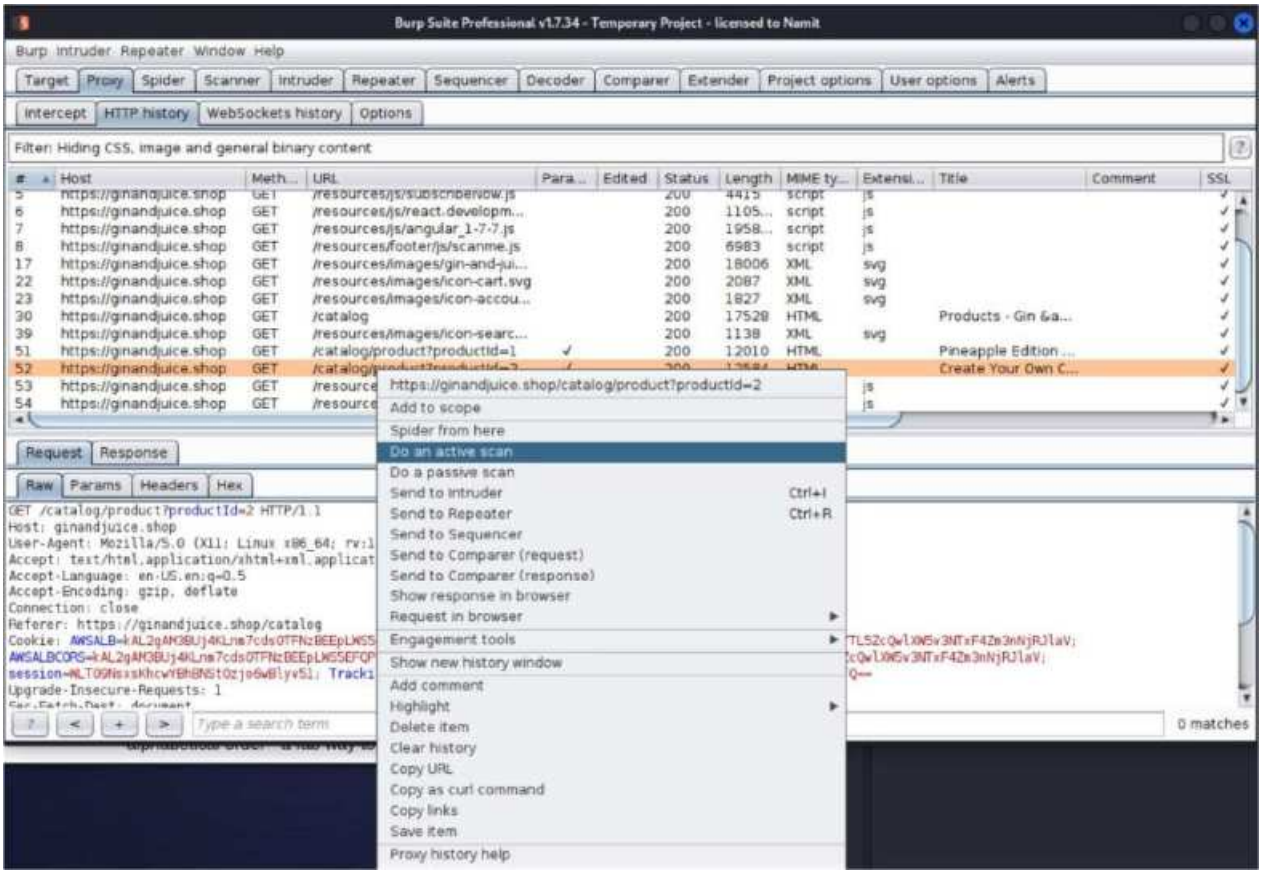
3. **Proxy Tab**: In Burp Suite, navigate to the Proxy tab and observe the requests/responses.

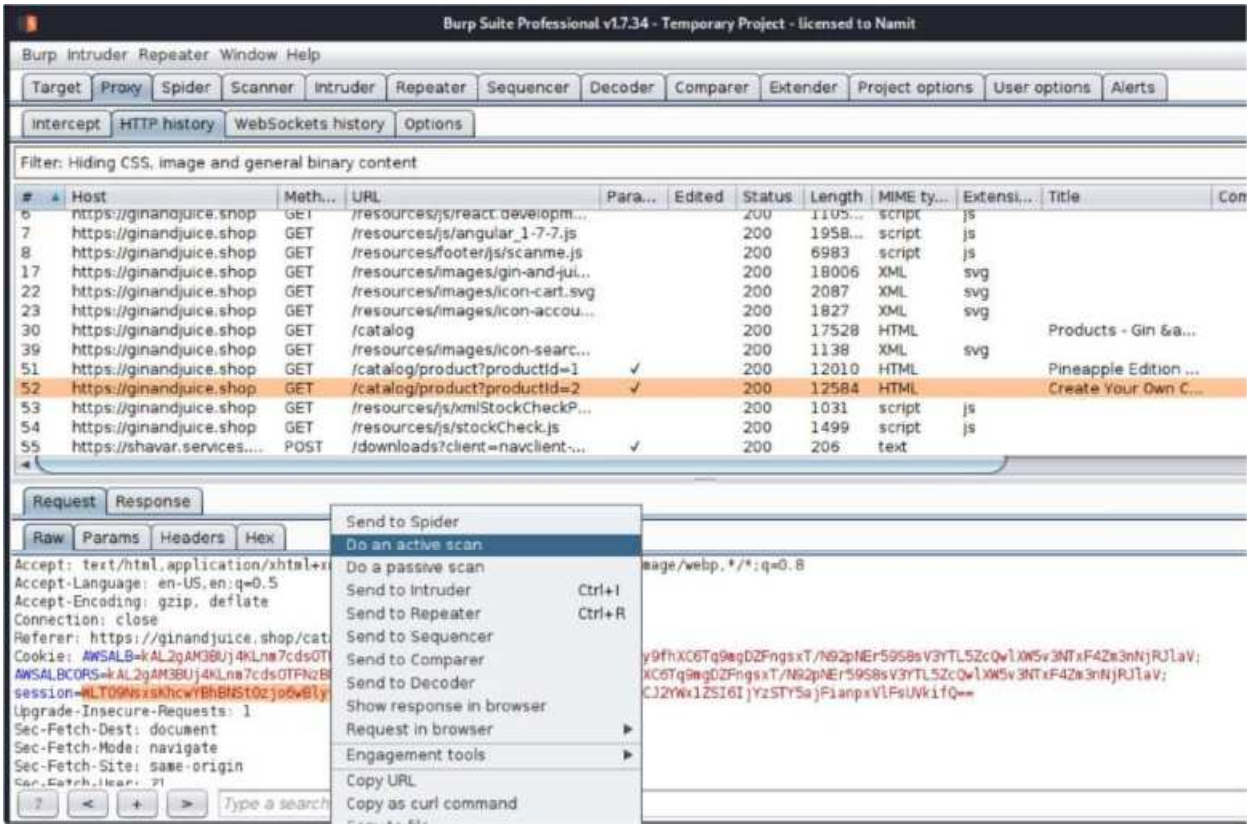


4. **Detection**: Look for suspicious input validation or encoding practices in the responses.

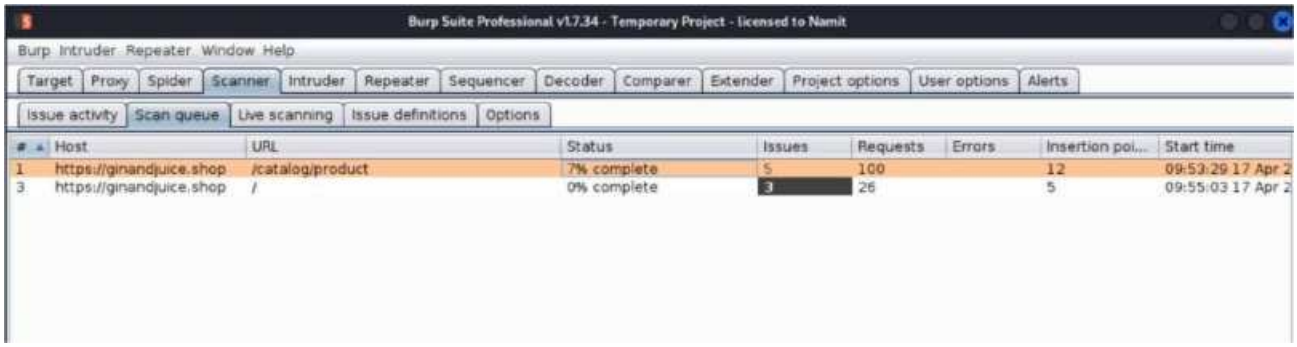
5. **Scanner**: Use Burp's Scanner to automatically scan for XSS vulnerabilities.

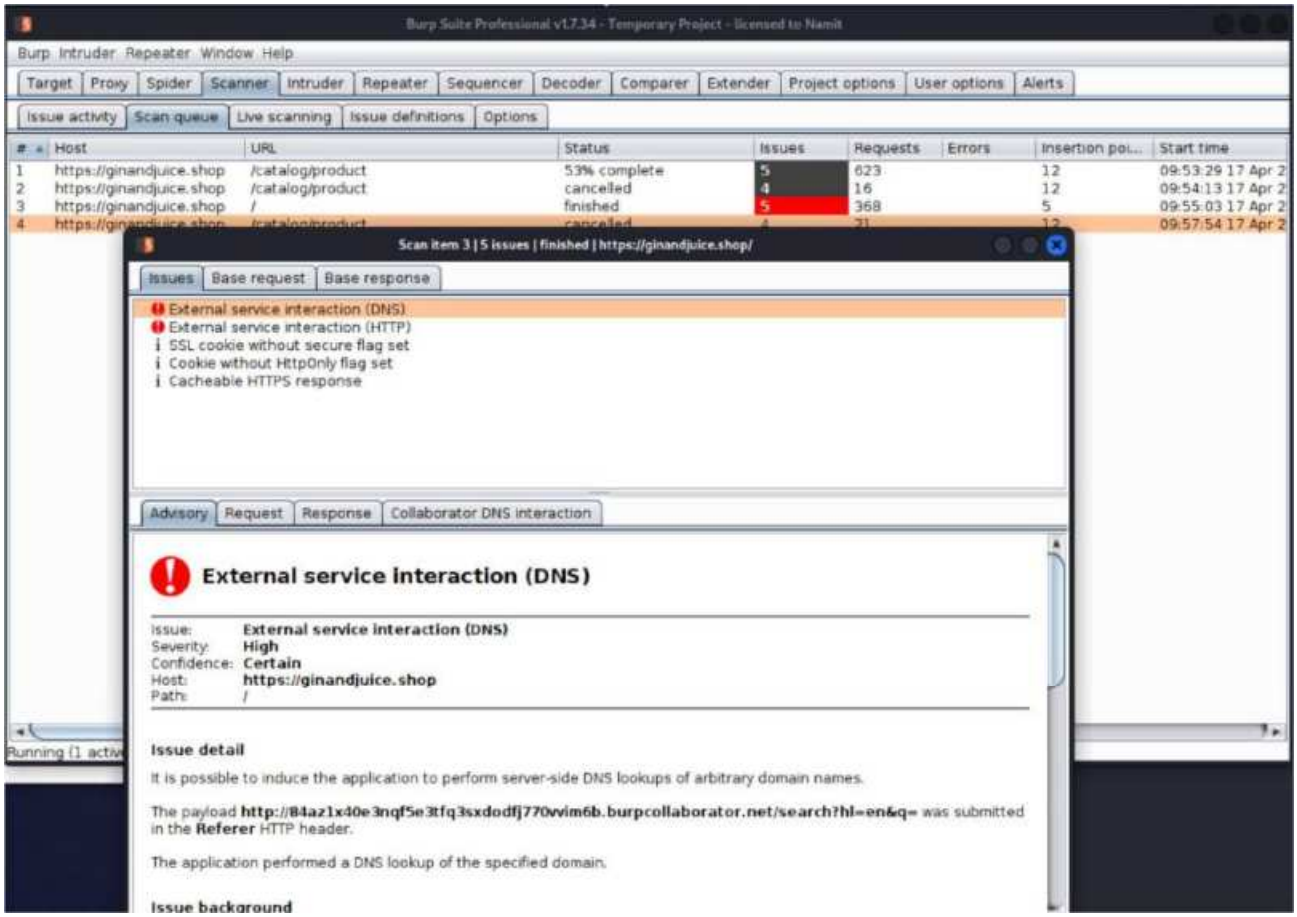
    - Configure the scanner to target input fields and parameters where XSS vulnerabilities are suspected.





6. **Analysis & Reporting**: Analyze the findings reported by Burp's Scanner in the Scanner tab.
    - Review any discovered XSS vulnerabilities and their severity.
    - Generate a detailed report highlighting the identified vulnerabilities and recommended mitigation measures.
    - Report any discovered vulnerabilities to the development team for remediation.





2. Authentication and Session Management Testing (Maintaining an authenticated session using Burp Suite)

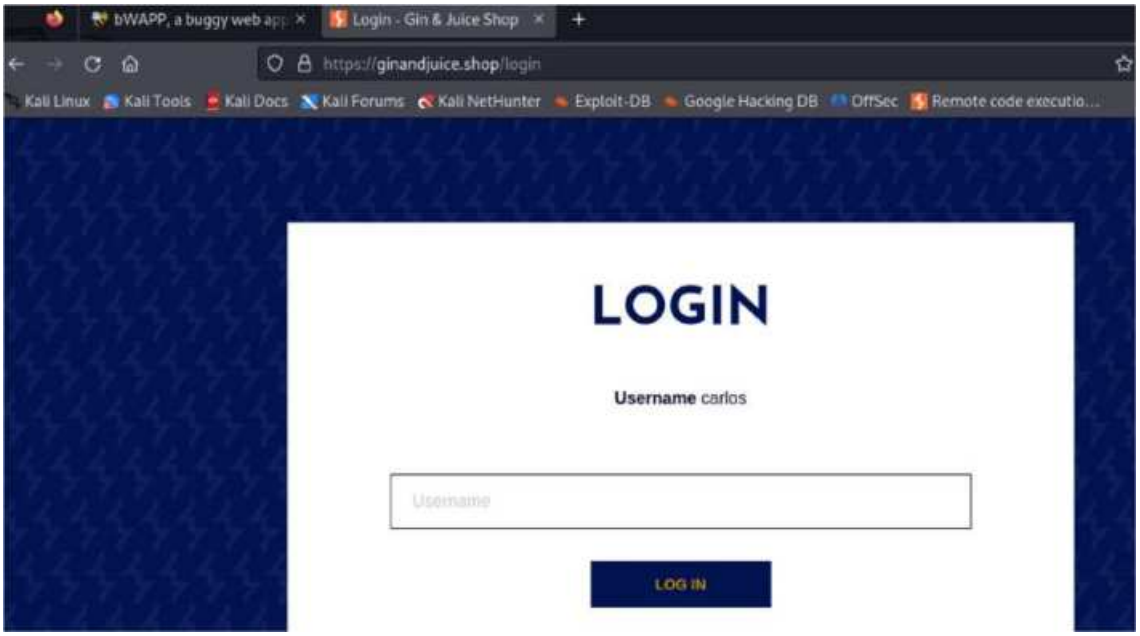
Scenario question: You need to evaluate the effectiveness of authentication and session management mechanisms on the website https://ginandjuice.shop/ to protect user accounts and sensitive data.

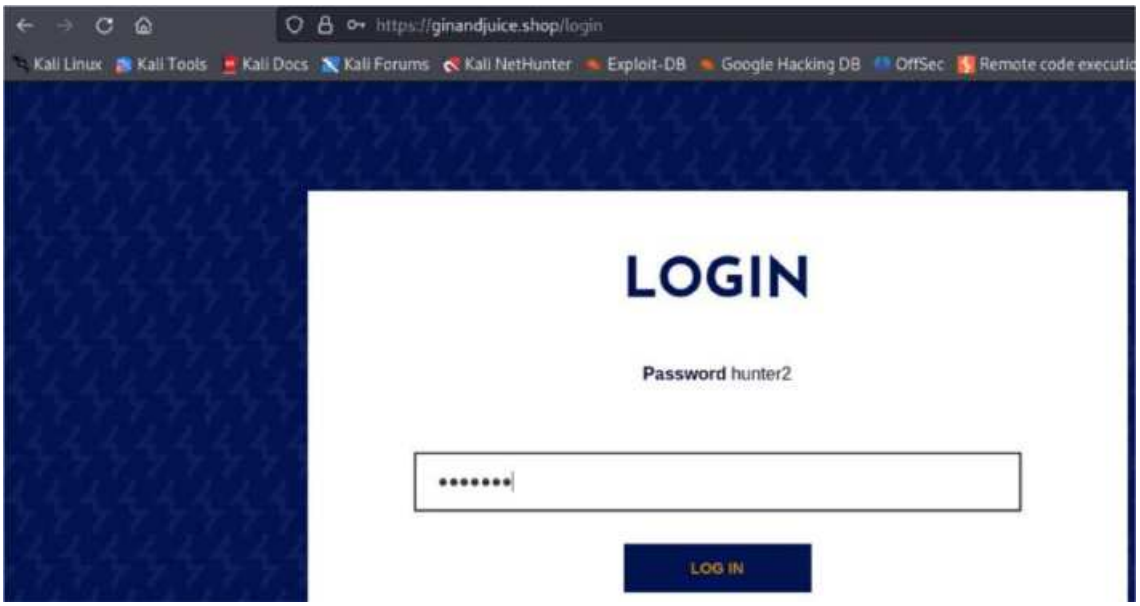
Scenario: We evaluate the effectiveness of authentication and session management mechanisms on the website https://ginandjuice.shop/ to protect user accounts and sensitive data.

Functionality: Burp Suite's "Repeater" and "Session Handling" tools enable manual testing of authentication and session management functionalities.

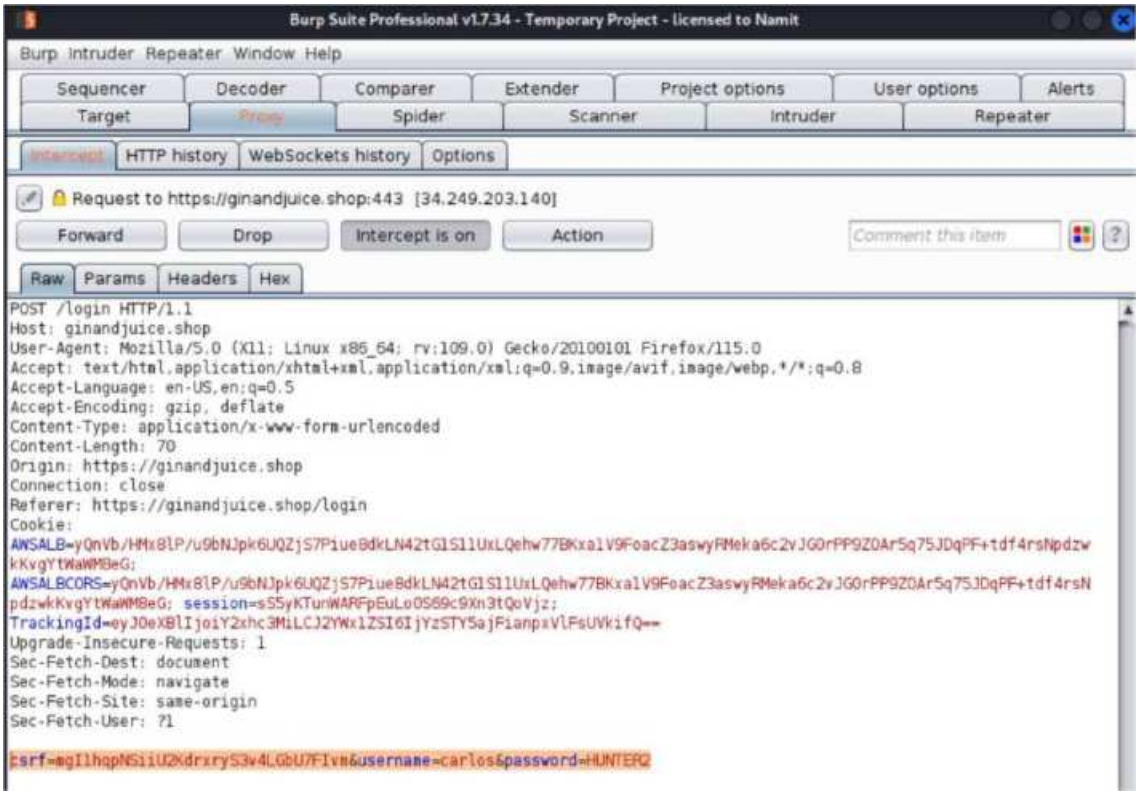
Steps:

1. **Capture Login Requests:**
    - Launch Burp Suite and configure it as a proxy.
    - Navigate to https://ginandjuice.shop/ and initiate the login process.

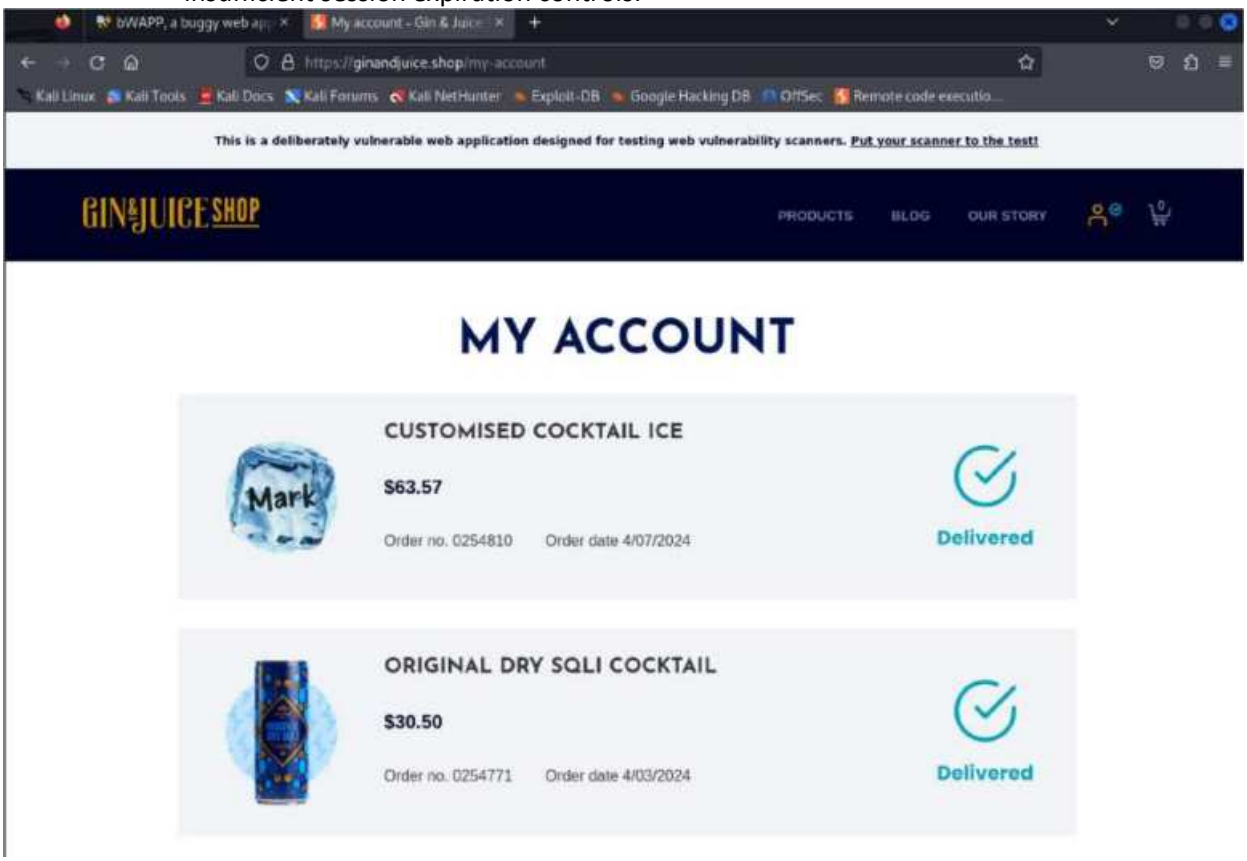




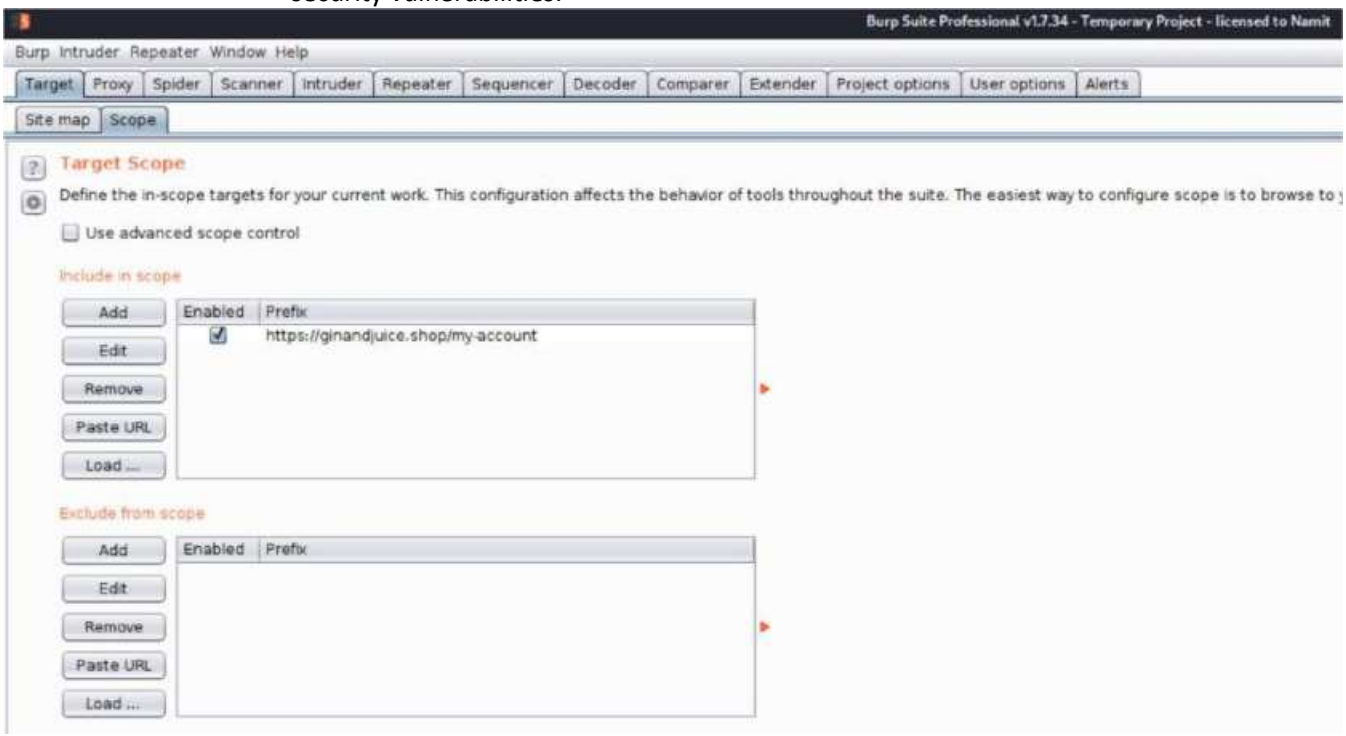
- Use Burp Suite's "Proxy" tool to capture the login requests and subsequent authenticated sessions.

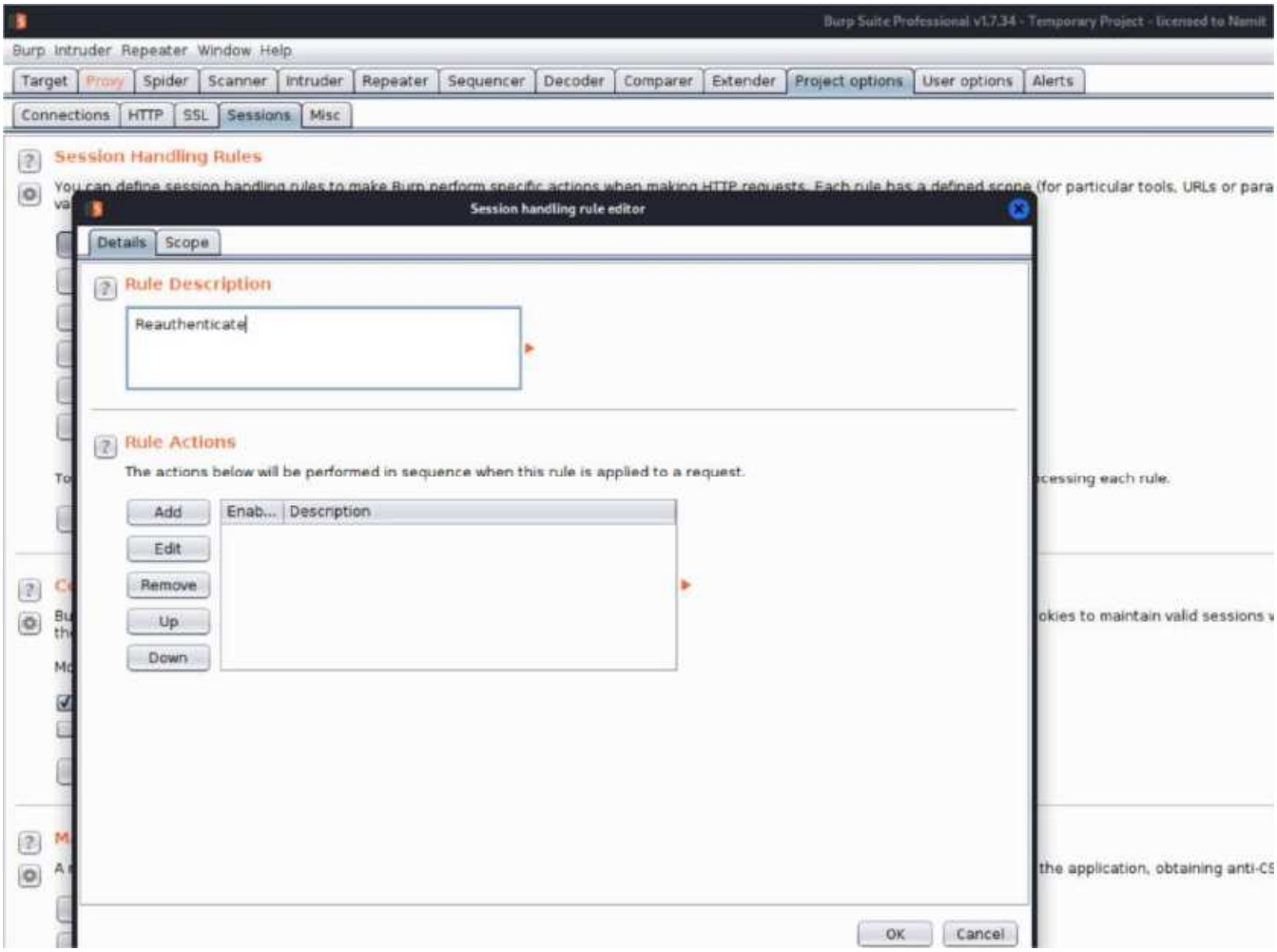


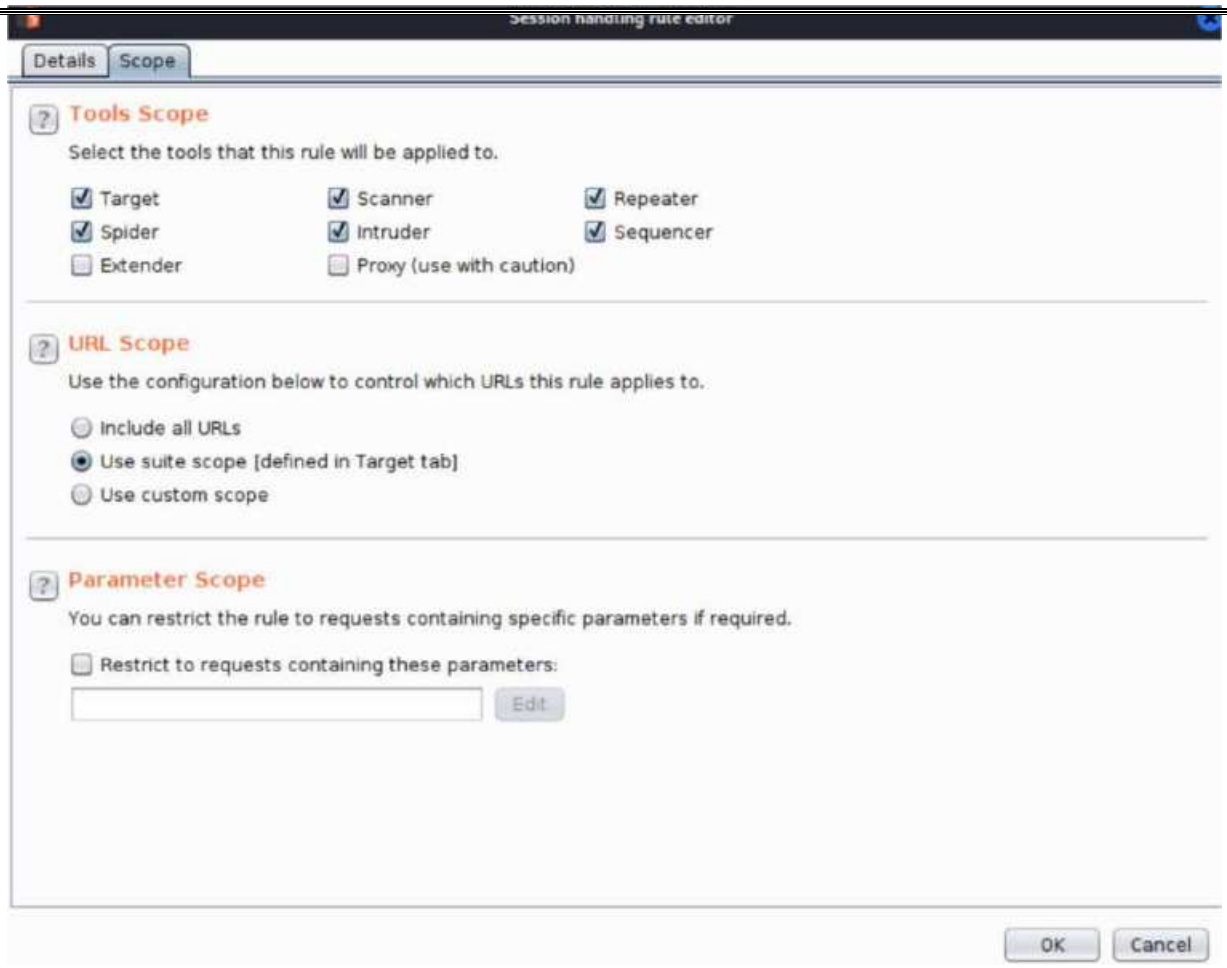
2. **Analyze Authentication Process:**
    - Examine the authentication process to identify potential weaknesses.
    - Look for indications of weak password policies, predictable session tokens, or insufficient session expiration controls.

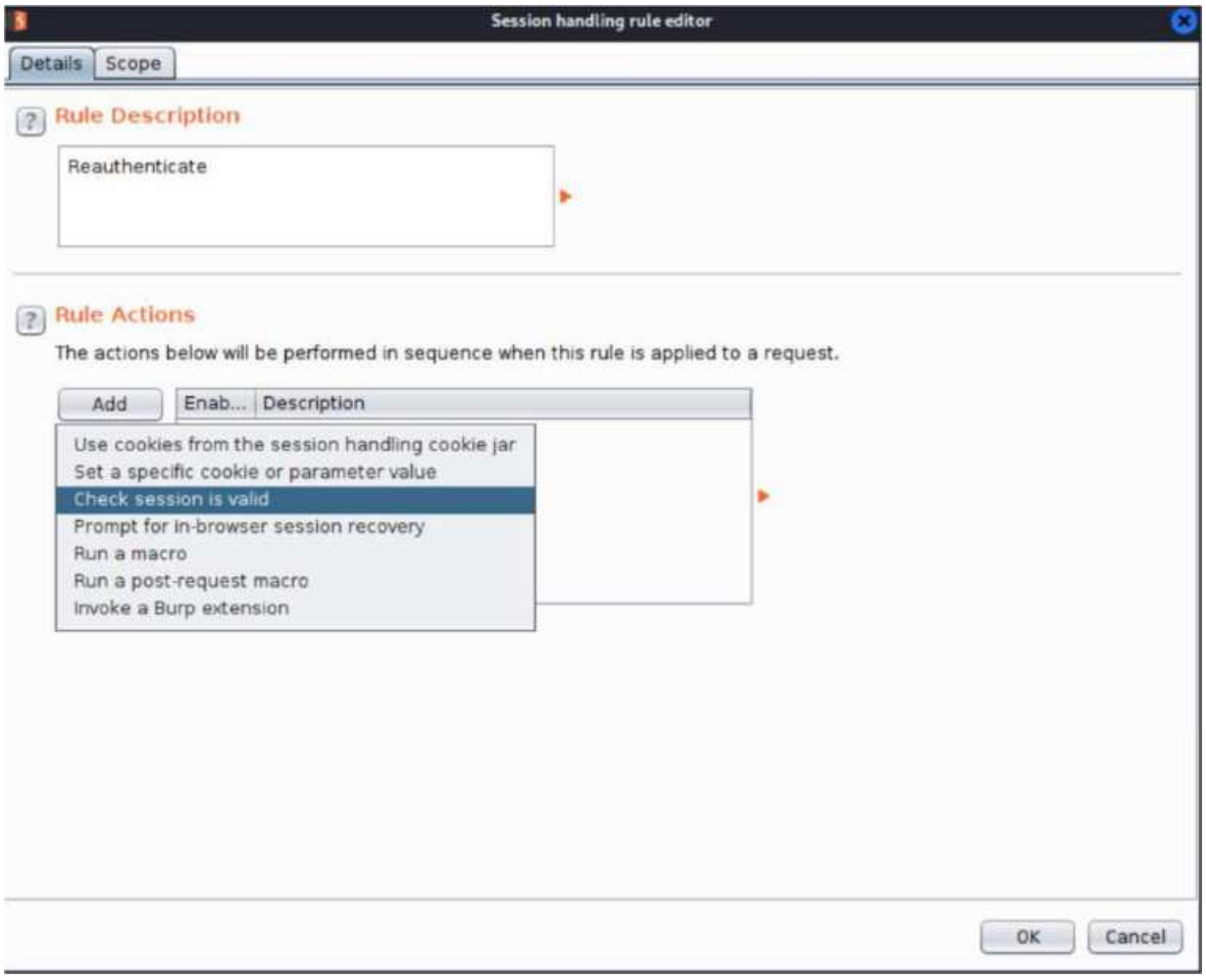


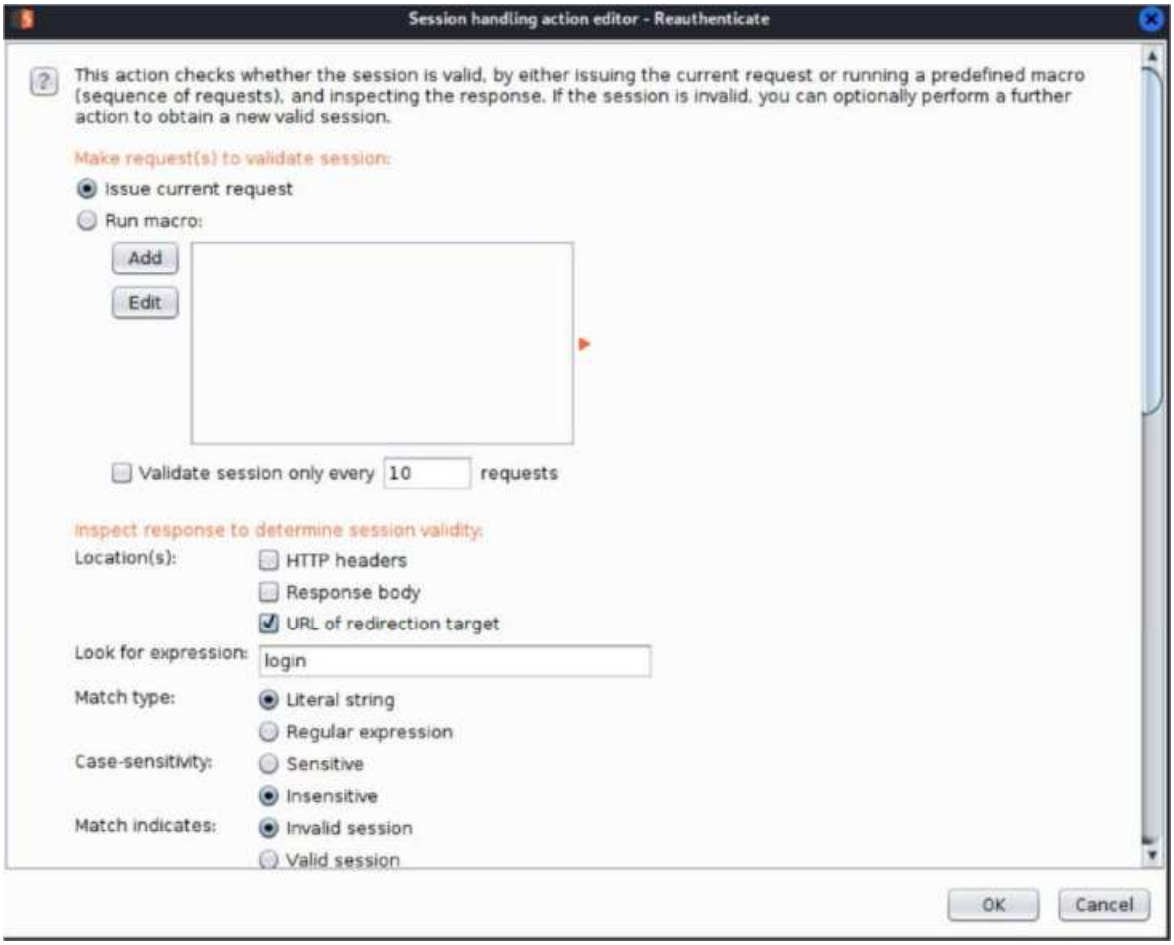
3. **Monitor Session Cookies and Headers:**
    - Monitor session-related cookies and headers for consistency and adherence to security best practices.
    - Look for inconsistencies or deviations from expected behavior that may indicate security vulnerabilities.

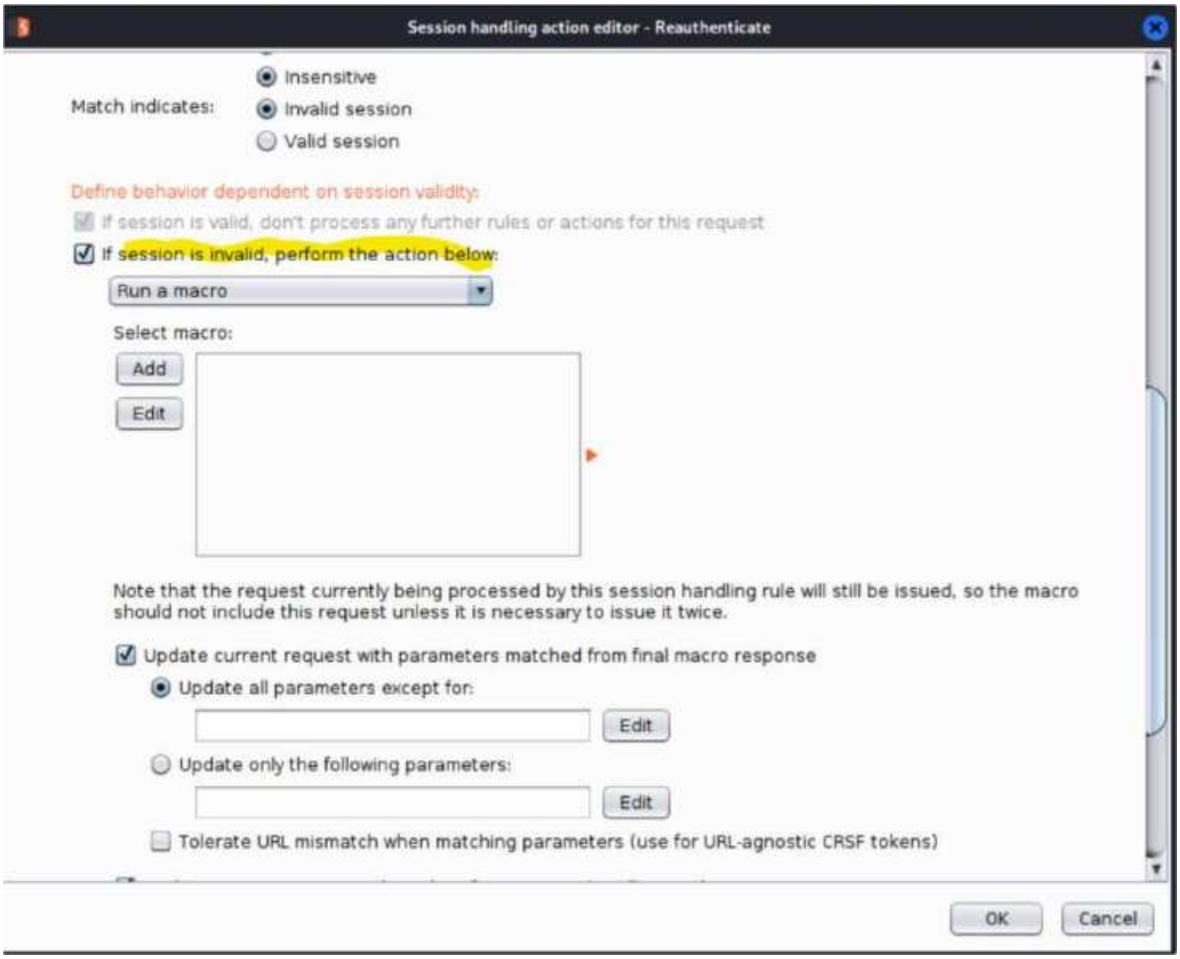


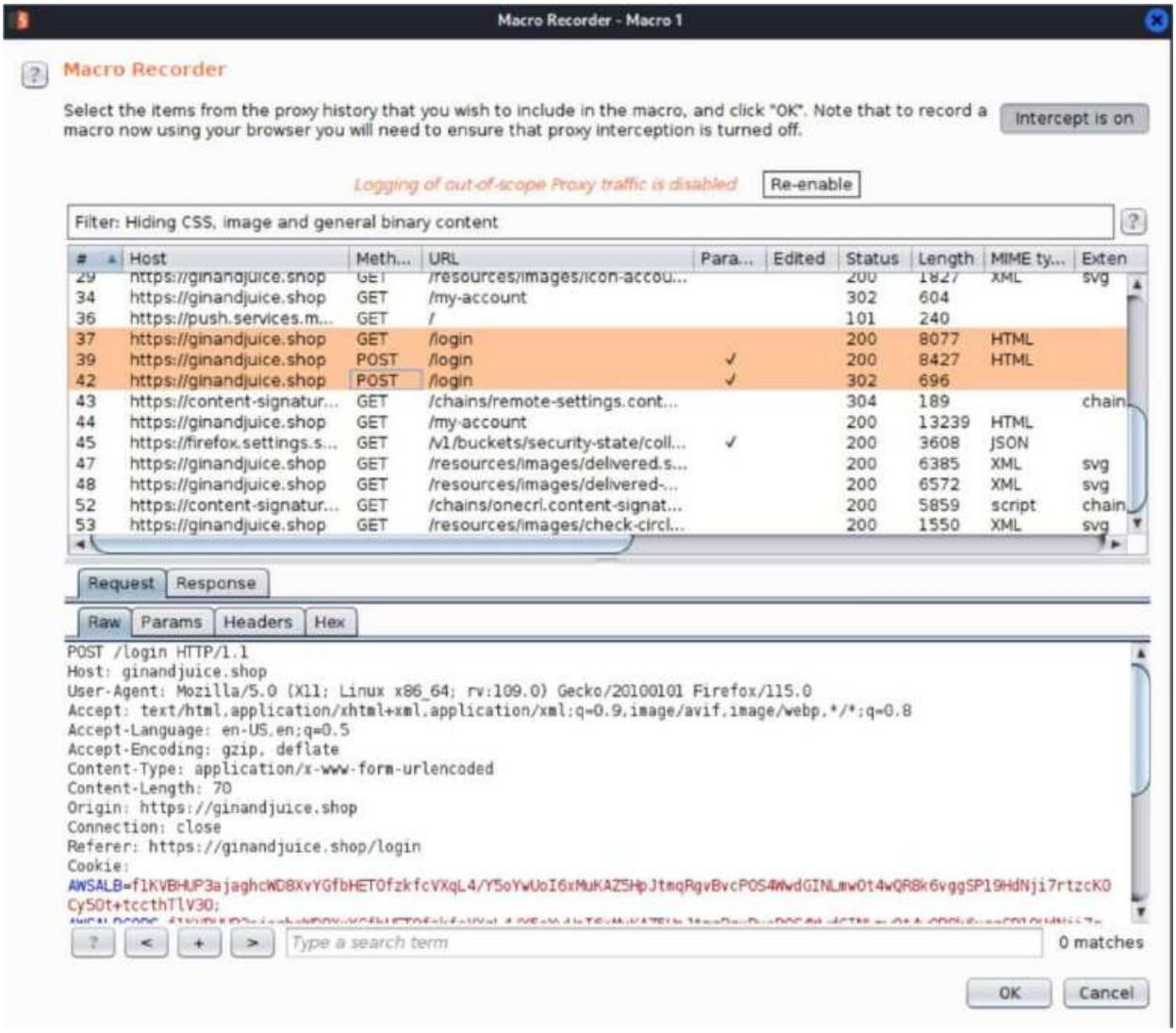


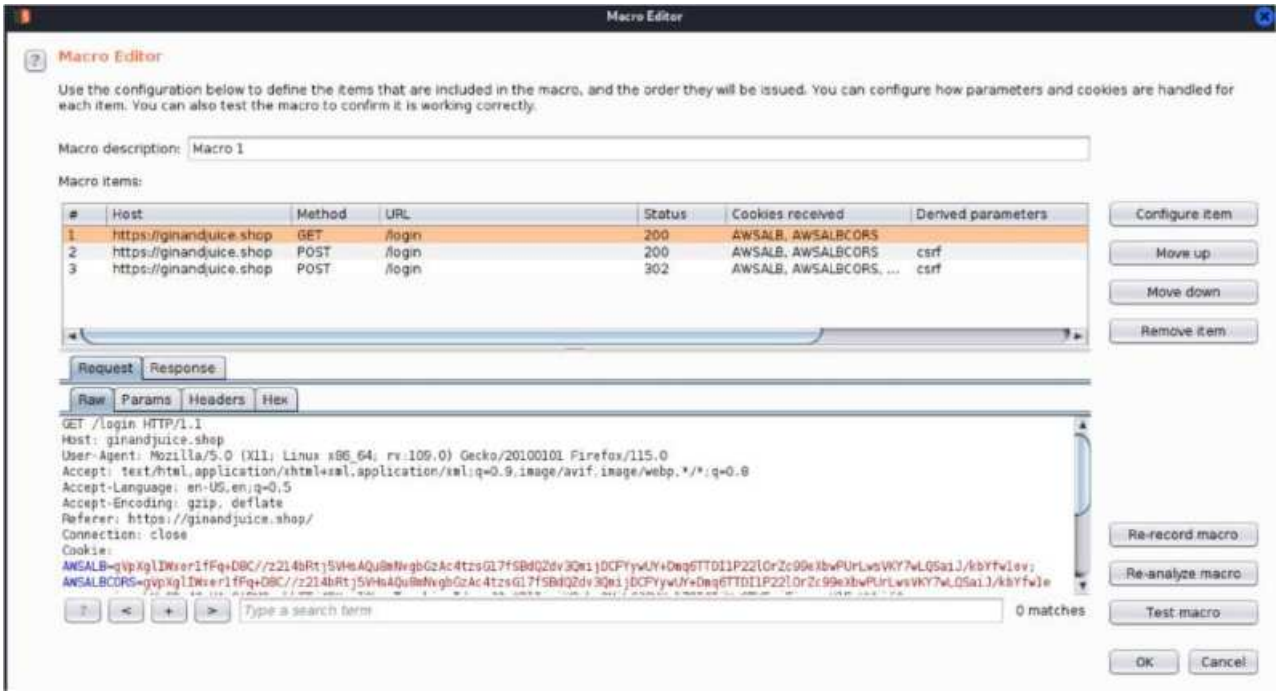

Session handling rule editor
Details
Scope
Tools Scope
Select the tools that this rule will be applied to.
Target
Scanner
Repeater
Spider
Intruder
Sequencer
Extender
Proxy (use with caution)
URL Scope
Use the configuration below to control which URLs this rule applies to.
Include all URLs
Use suite scope [defined in Target tab]
Use custom scope
Parameter Scope
You can restrict the rule to requests containing specific parameters if required.
Restrict to requests containing these parameters:
Edit
OK
Cancel

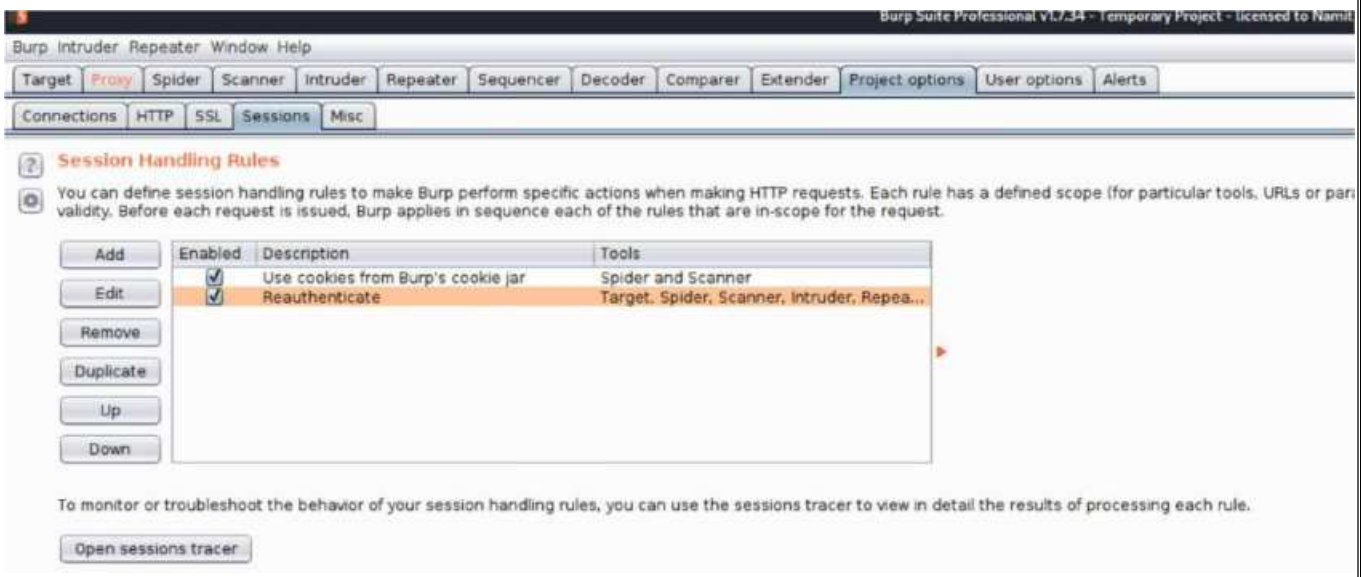

Session handling rule editor
Details
Scope
Rule Description
Reauthenticate
Rule Actions
The actions below will be performed in sequence when this rule is applied to a request.
Add
Enab...
Description
Use cookies from the session handling cookie jar
Set a specific cookie or parameter value
Check session is valid
Prompt for in-browser session recovery
Run a macro
Run a post-request macro
Invoke a Burp extension
OK
Cancel


Session handling action editor - Reauthenticate
This action checks whether the session is valid, by either issuing the current request or running a predefined macro (sequence of requests), and inspecting the response. If the session is invalid, you can optionally perform a further action to obtain a new valid session.
Make request(s) to validate session:
Issue current request
Run macro:
Add
Edit
Validate session only every 10 requests
Inspect response to determine session validity:
Location(s):
HTTP headers
Response body
URL of redirection target
Look for expression: login
Match type:
Literal string
Regular expression
Case-sensitivity:
Sensitive
Insensitive
Match indicates:
Invalid session
Valid session
OK
Cancel


Session handling action editor - Reauthenticate
Insensitive
Match indicates:
Invalid session
Valid session
Define behavior dependent on session validity:
If session is valid, don't process any further rules or actions for this request
If session is invalid, perform the action below:
Run a macro
Select macro:
Add
Edit
Note that the request currently being processed by this session handling rule will still be issued, so the macro should not include this request unless it is necessary to issue it twice.
Update current request with parameters matched from final macro response
Update all parameters except for:
Edit
Update only the following parameters:
Edit
Tolerate URL mismatch when matching parameters (use for URL-agnostic CRSF tokens)
OK
Cancel

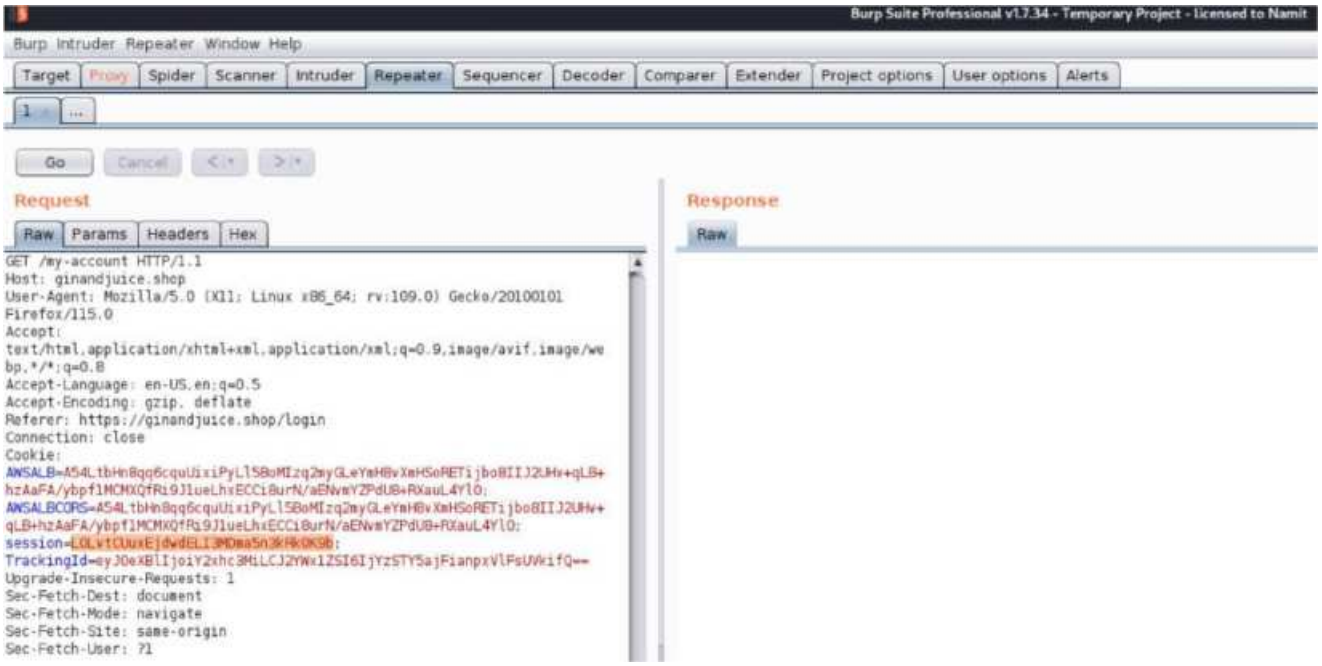

Macro Recorder - Macro 1
Macro Recorder
Select the items from the proxy history that you wish to include in the macro, and click "OK". Note that to record a macro now using your browser you will need to ensure that proxy interception is turned off.
Intercept is on
Logging of out-of-scope Proxy traffic is disabled
Re-enable
Filter: Hiding CSS, image and general binary content
Host Meth... URL Para... Edited Status Length MIME ty... Exten
34 https://ginandjuice.shop GET /my-account 302 604
36 https://push.services.m... GET / 101 240
37 https://ginandjuice.shop GET /login 200 8077 HTML
39 https://ginandjuice.shop POST /login ✓ 200 8427 HTML
42 https://ginandjuice.shop POST /login ✓ 302 696
43 https://content-signatur... GET /chains/remote-settings.cont... 304 189 chain
44 https://ginandjuice.shop GET /my-account 200 13239 HTML
45 https://firefox.settings.s... GET /v1/buckets/security-state/coll... ✓ 200 3608 JSON
47 https://ginandjuice.shop GET /resources/images/delivered.s... 200 6385 XML svg
48 https://ginandjuice.shop GET /resources/images/delivered-... 200 6572 XML svg
52 https://content-signatur... GET /chains/onecrl.content-signat... 200 5859 script chain
53 https://ginandjuice.shop GET /resources/images/check-circl... 200 1550 XML svg
Request Response
Raw Params Headers Hex
POST /login HTTP/1.1
Host: ginandjuice.shop
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 70
Origin: https://ginandjuice.shop
Connection: close
Referer: https://ginandjuice.shop/login
Cookie:
AWSALB=flKVBHUP3ajaghcWD8XvYGfbHETOfzkfcVXqL4/Y5oYwUoI6xMuKAZ5HpJtmqRgvBvcPOS4WwdGINLmwOt4wQR8k6vggSP19HdNji7rtzcKO
CySOt+tccthTlV3O;
Type a search term
0 matches
OK
Cancel


Macro Editor
Macro Editor
Use the configuration below to define the items that are included in the macro, and the order they will be issued. You can configure how parameters and cookies are handled for each item. You can also test the macro to confirm it is working correctly.
Macro description: Macro 1
Macro items:
Host Method URL Status Cookies received Derived parameters
1 https://ginandjuice.shop GET /login 200 AWSALB, AWSALBCORS
2 https://ginandjuice.shop POST /login 200 AWSALB, AWSALBCORS csrf
3 https://ginandjuice.shop POST /login 302 AWSALB, AWSALBCORS, ... csrf
Configure item
Move up
Move down
Remove item
Request Response
Raw Params Headers Hex
GET /login HTTP/1.1
Host: ginandjuice.shop
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://ginandjuice.shop/
Connection: close
Cookie:
AWSALB=gVpXglIWxerlfFq+D8C//z214bRtj5VHsAQu8mNvgbGzAc4tzsGl7fSBdQZdv3QmijDCFYywUY+Dmq6TTDI1P22lOrZc99eXbwPUrLwsVKY7wLQSa1J/kbYfwlev;
AWSALBCORS=gVpXglIWxerlfFq+D8C//z214bRtj5VHsAQu8mNvgbGzAc4tzsGl7fSBdQZdv3QmijDCFYywUY+Dmq6TTDI1P22lOrZc99eXbwPUrLwsVKY7wLQSa1J/kbYfwle
Type a search term
0 matches
Re-record macro
Re-analyze macro
Test macro
OK
Cancel

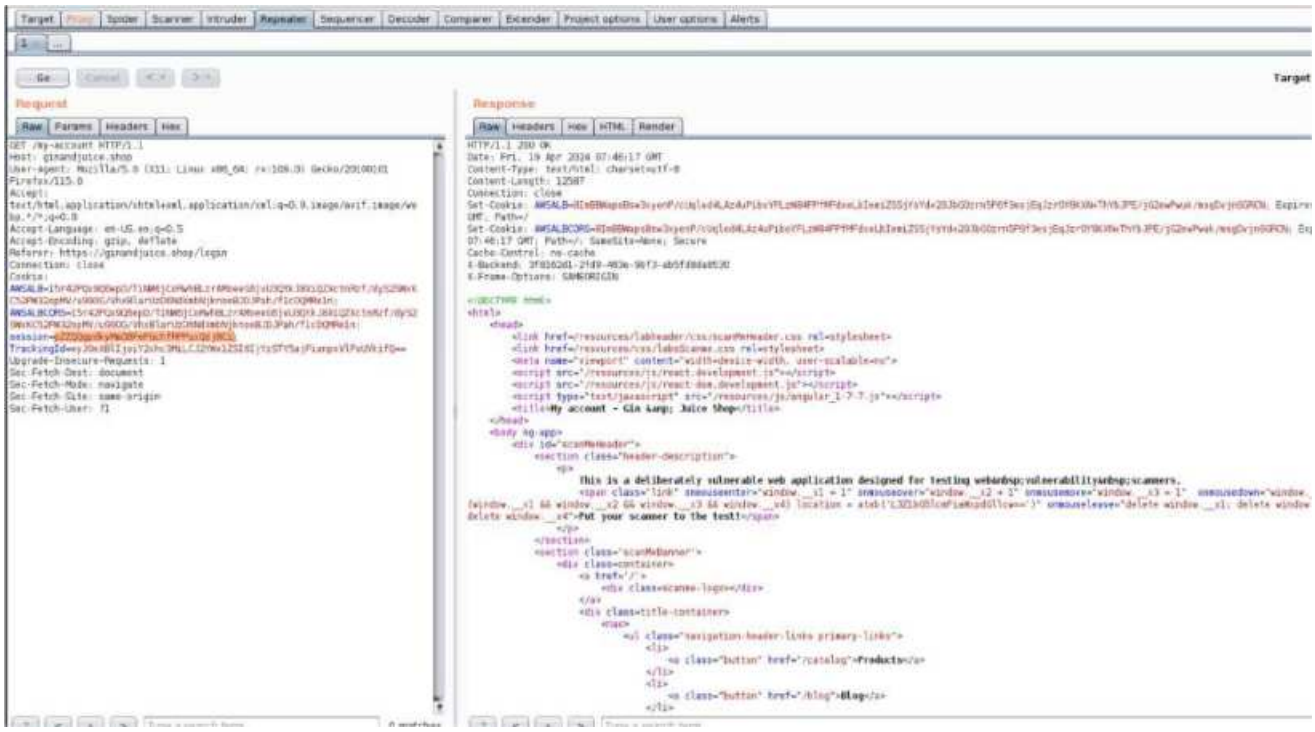


4. **Manipulate Parameters:**

- Utilize the "Repeater" tool in Burp Suite to manipulate session tokens or authentication parameters.

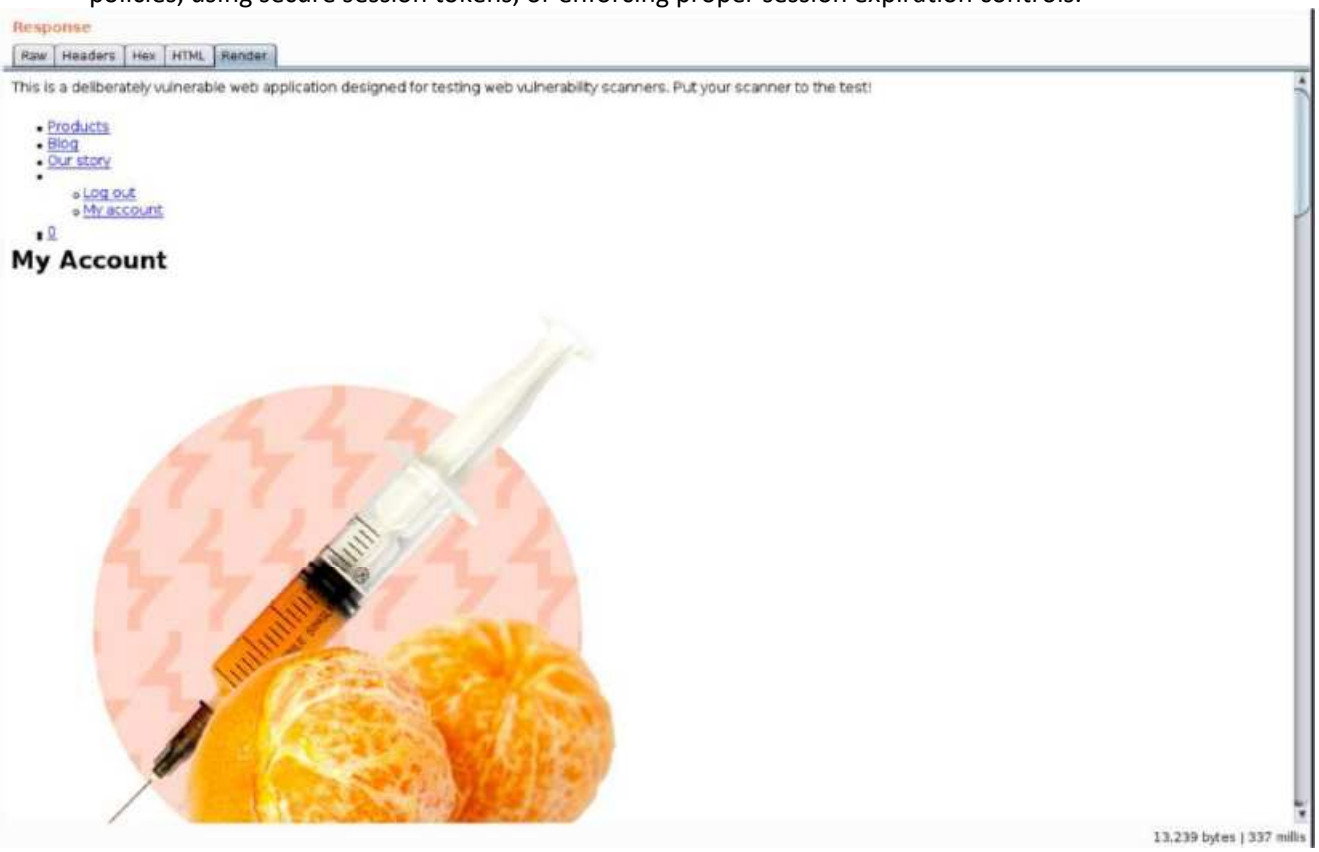


- Test for vulnerabilities such as session fixation or session hijacking by modifying session-related values.



5. **Generate Report:**

- Document any identified vulnerabilities or weaknesses in authentication and session management mechanisms.
- Provide detailed recommendations for improvement, such as implementing stronger password policies, using secure session tokens, or enforcing proper session expiration controls.



By following these steps, We can effectively assess the security of authentication and session management mechanisms on the website https://ginandjuice.shop/, helping to identify and mitigate potential risks to user accounts and sensitive data.

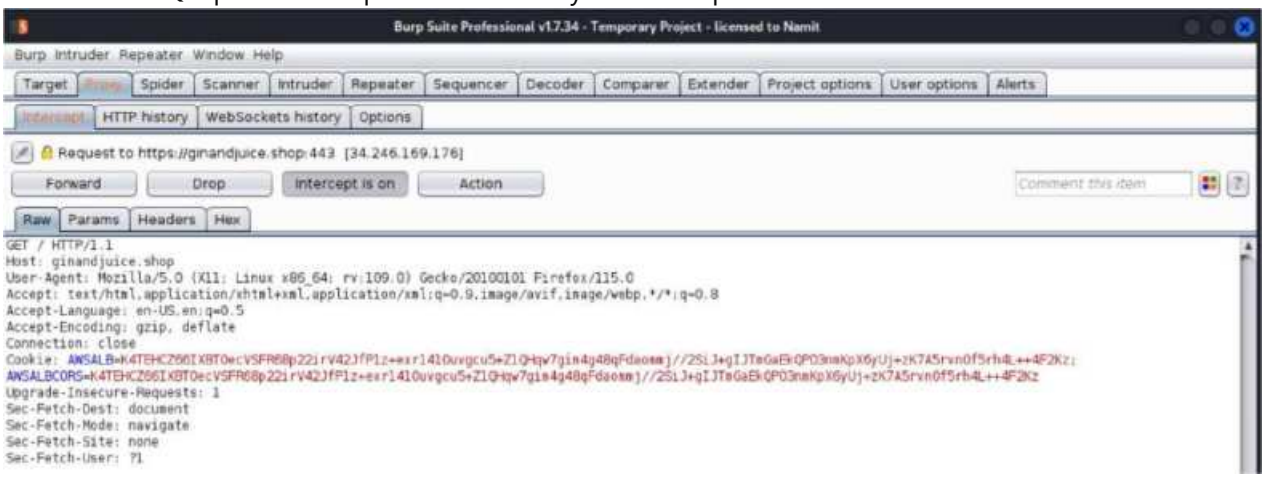
3. Testing for SQL Injection:

Scenario Question: Can you demonstrate how Burp Suite can be used to assess a web application's susceptibility to SQL injection attacks and verify the findings?

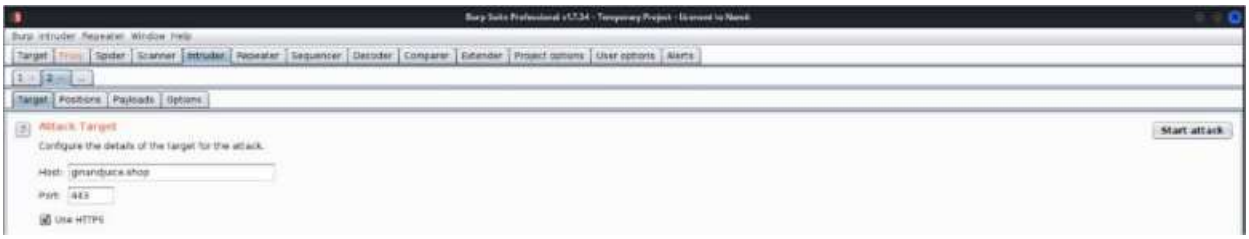
Scenario: We want to check if the website https://ginandjuice.shop/ is vulnerable to SQL injection attacks.

Steps:

1. **Proxy Setup:**
   - Configure Burp Suite as a proxy and ensure interception is enabled.
   - Navigate to https://ginandjuice.shop/ using your browser.
2. **Interception:**
   - Interact with input fields on the ginandjuice.shop website, such as search or login forms.
   - Observe SQL queries in requests in the Proxy tab of Burp Suite.

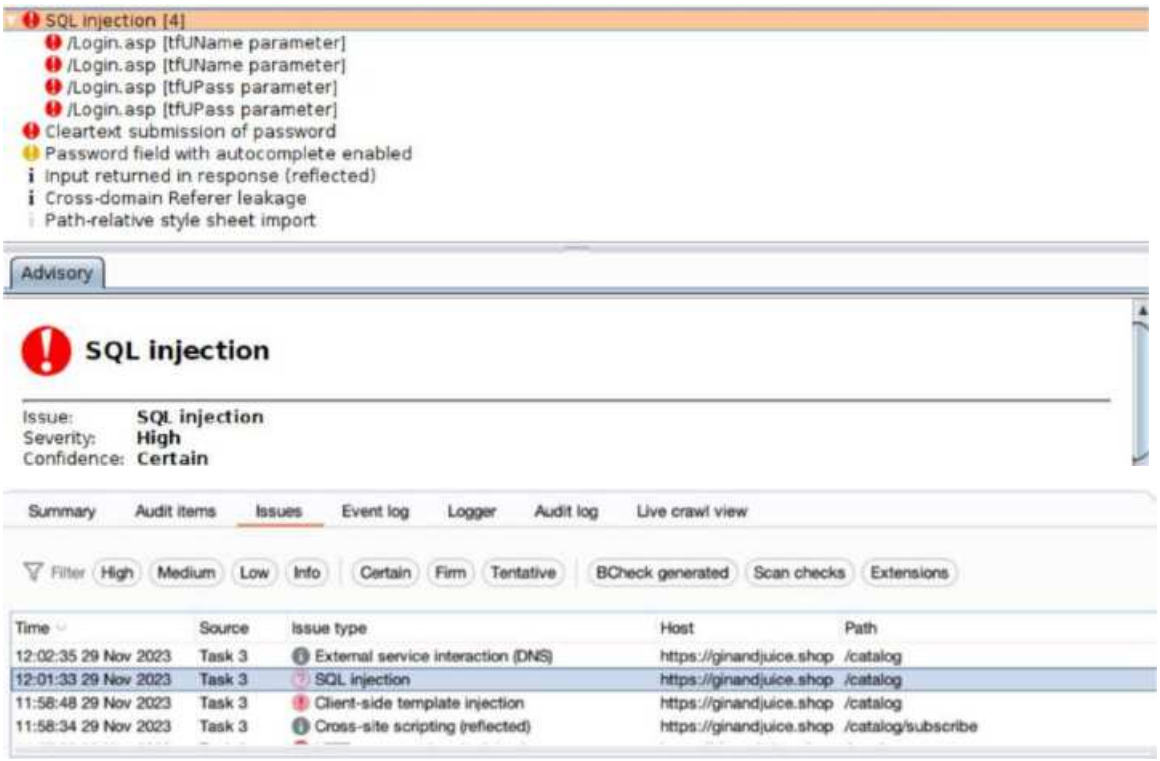


3. **Intruder Tool**: Use Burp's Intruder tool to modify parameters and observe SQL responses.

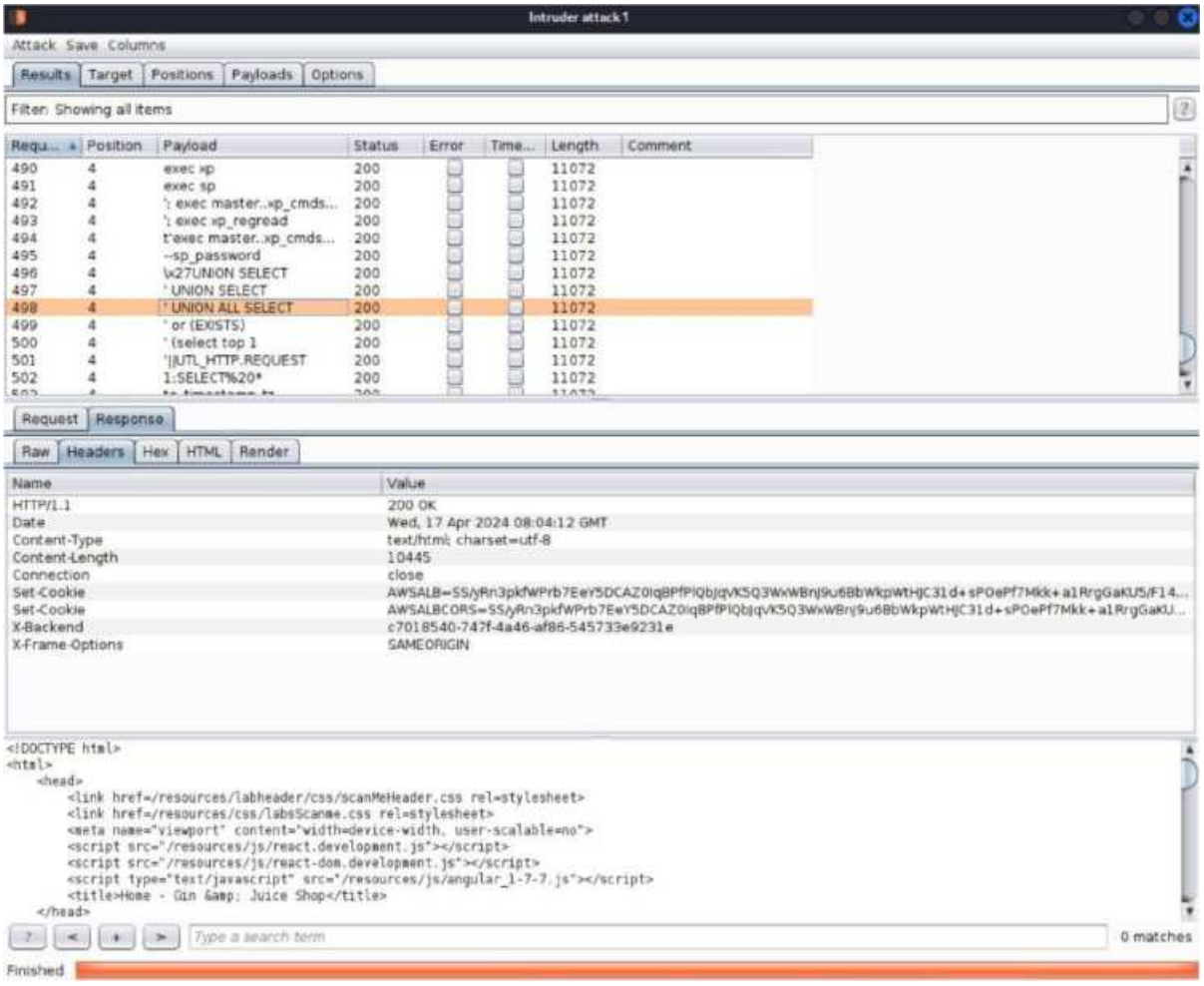


4. **Payload Crafting**: Craft SQL injection payloads and inject them through various input fields.

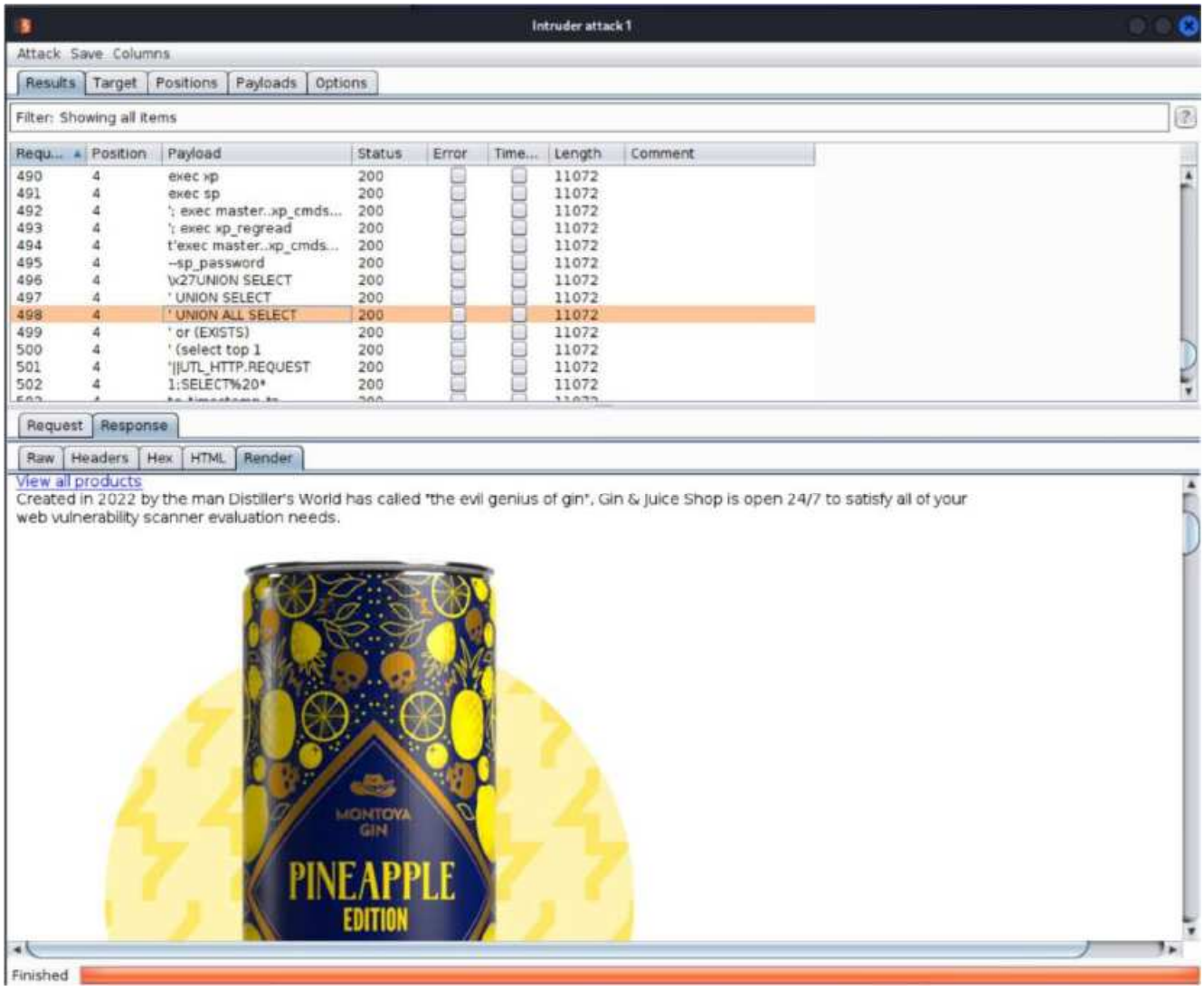
5. **Response Analysis**: Analyze server responses for any SQL errors or unusual behavior.



6. **Scanner**: Utilize Burp's Scanner to automate SQL injection testing and verify the findings.



- Utilize Burp Suite's Render tool to render the response in different formats (e.g., HTML, JSON).
- Examine the rendered response for any unexpected behavior or content that may indicate SQL injection vulnerabilities.



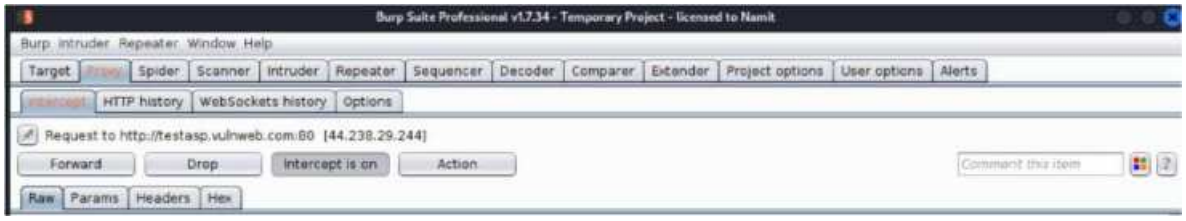
4. **Session Hijacking**:

Scenario Question: In what ways can Burp Suite be employed to assess the security of a web application against session hijacking attacks, and how would you document the results?

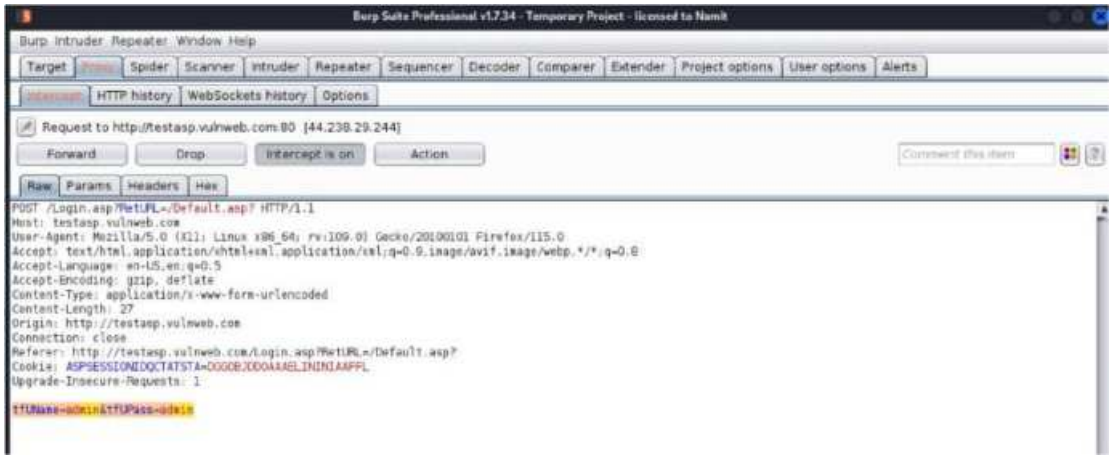
Scenario: We want to test the security of https://testasp.vulnweb.com/Login.asp?RetURL=/Default.asp? against session hijacking attacks.

- **Steps**:

1. **Interception**: Intercept a user's session token using Burp's Proxy.



2. **Session Handling Rules**: Copy the session token and use Burp's Session Handling Rules to set it as your own session.



3. **Browsing**: Browse the application to see if you gain unauthorized access to sensitive data or perform unauthorized actions.

4. **Monitoring**: Monitor for any session expiration or invalidation mechanisms.

5. **Documentation**: Document any successful or unsuccessful attempts and their implications.

5. **Sensitive Data Exposure**:

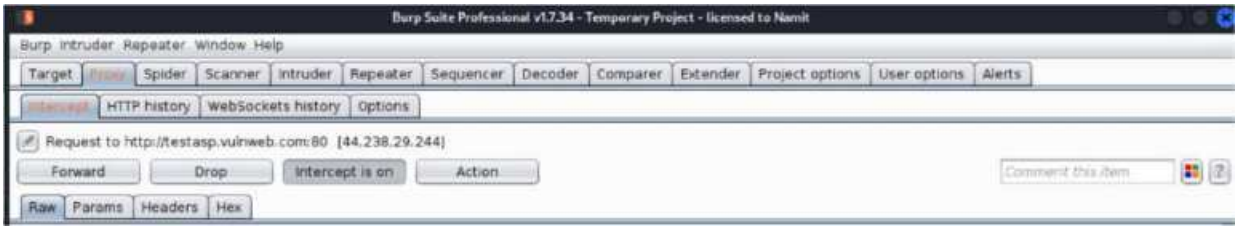
Scenario Question: Can you demonstrate how Burp Suite can be used to identify and mitigate sensitive data exposure vulnerabilities in the web application http://testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?

Scenario: You suspect that the web application testasp.vulnweb.com/Login.asp?RetURL=/Default.asp is exposing sensitive information

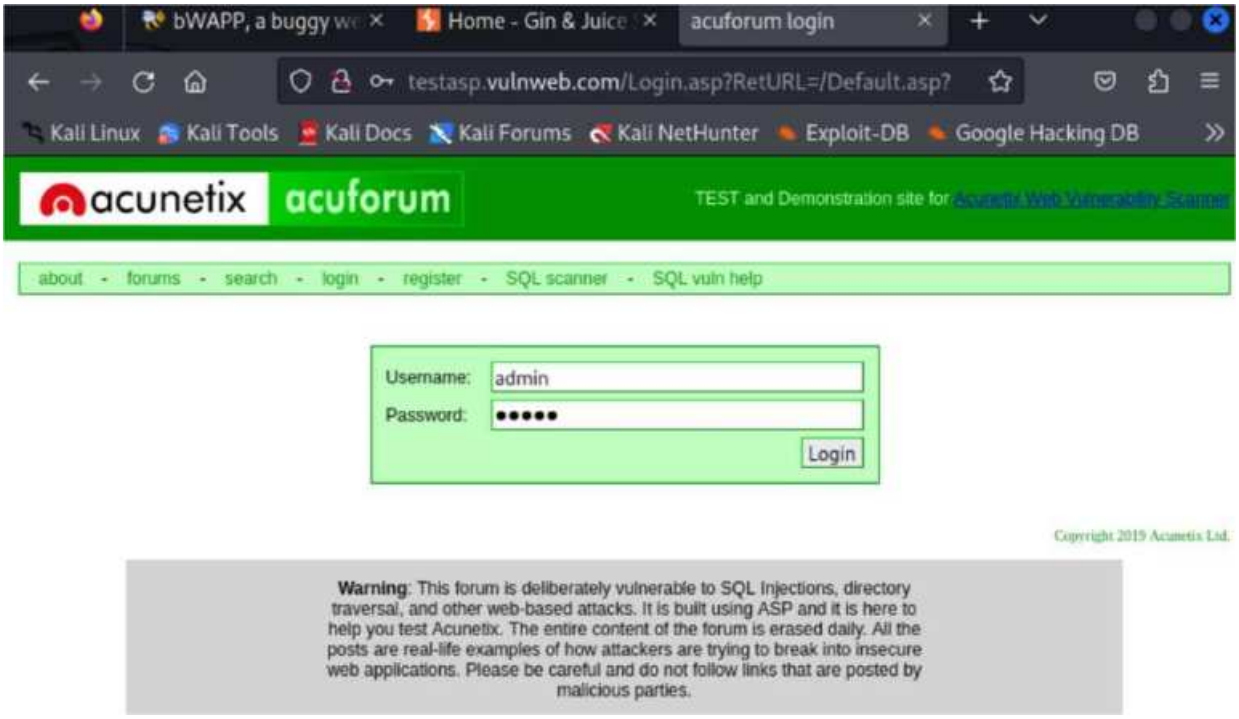
Steps:

1. **Interception:**

- Launch Burp Suite and configure it as a proxy.
- Navigate to testasp.vulnweb.com/Login.asp?RetURL=/Default.asp using your browser.
- Use Burp's Proxy tool to intercept traffic while browsing the application.

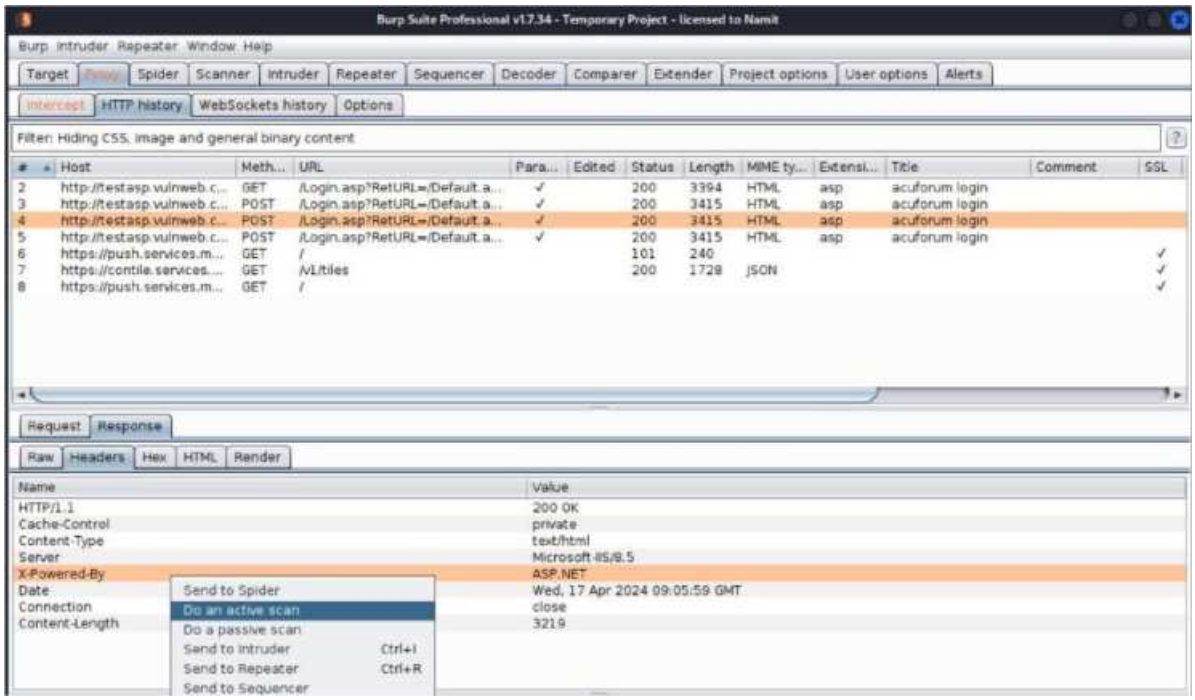


2. **Response Analysis**: Look for responses containing sensitive data such as passwords, API keys, or personal information.



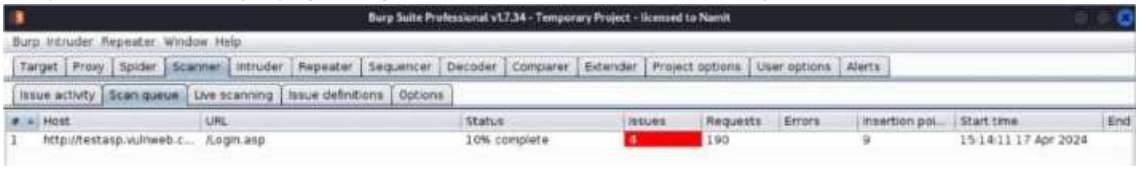
3. **Header Inspection:**

- Inspect the server's response headers for security-related headers such as X-Frame-Options or Content-Security-Policy.
- Look for proper security headers that help prevent sensitive data exposure, such as Content-Security-Policy directives restricting resource loading.

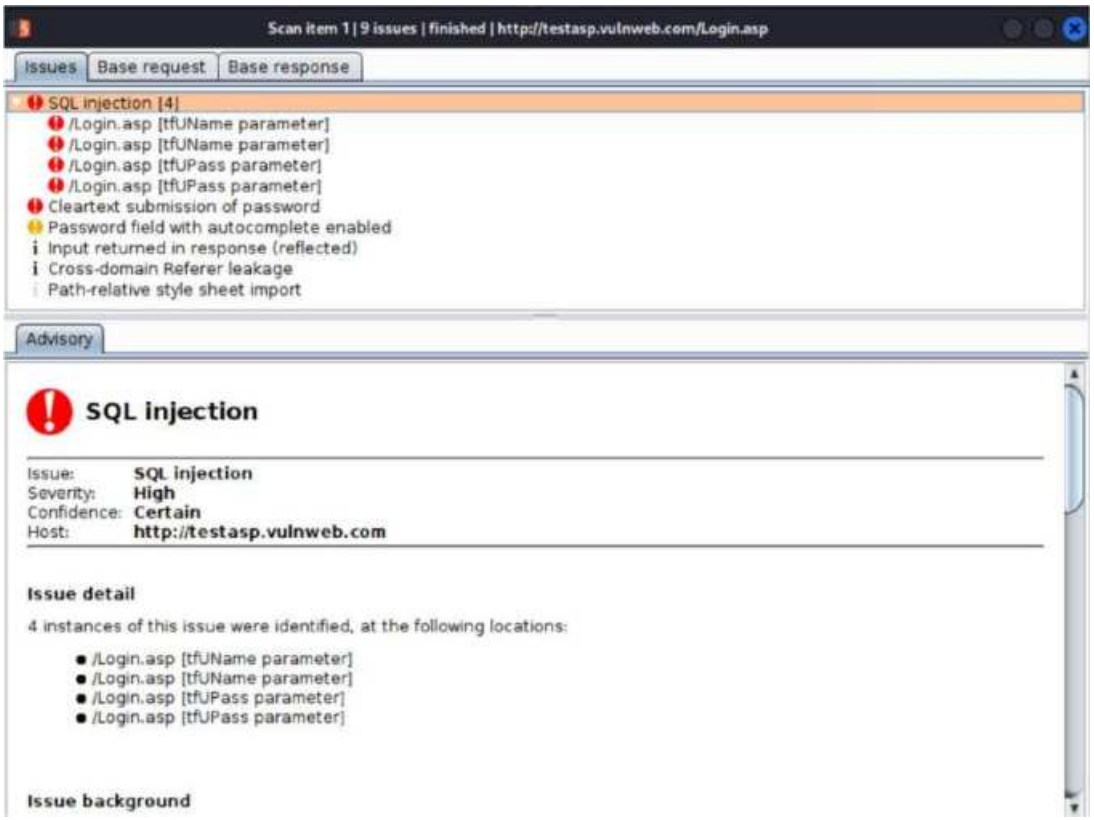


4. **Scanner:**

- Utilize Burp's Scanner to automate the detection of sensitive data exposure vulnerabilities.
- Configure the scanner to target areas of the application where sensitive information may be exposed, such as login pages, registration forms, or account management sections.



5. **Reporting**: Report any findings and suggest remediation measures to the development team.



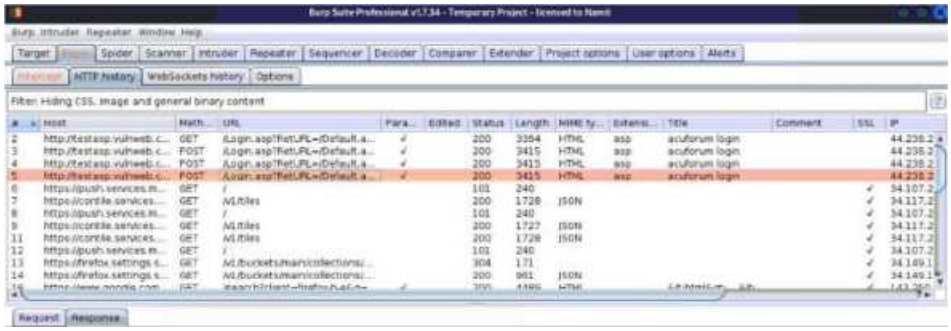
6. CSRF (Cross-Site Request Forgery) Vulnerabilities:

Scenario Question: Can you demonstrate how Burp Suite can be used to assess if the web application http://testasp.vulnweb.com/Login.asp?RetURL=/Default.asp is vulnerable to CSRF attacks?

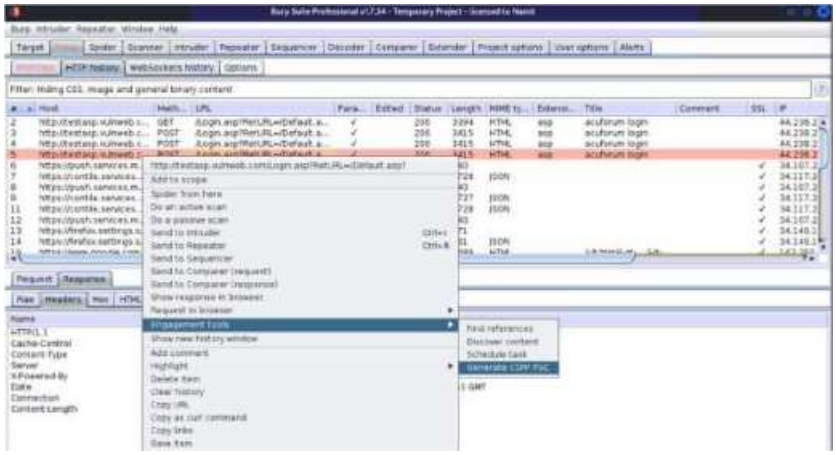
Scenario: You want to assess if the web application http://testasp.vulnweb.com/Login.asp?RetURL=/Default.asp is vulnerable to CSRF attacks.

- **Steps**:

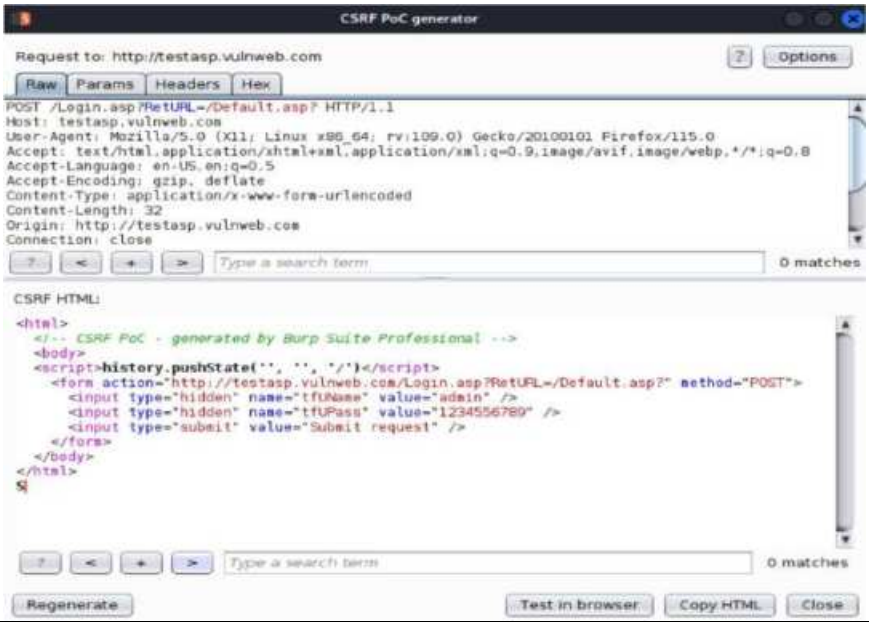
1. **Interception**: Use Burp's Proxy to intercept and modify requests while interacting with the application.



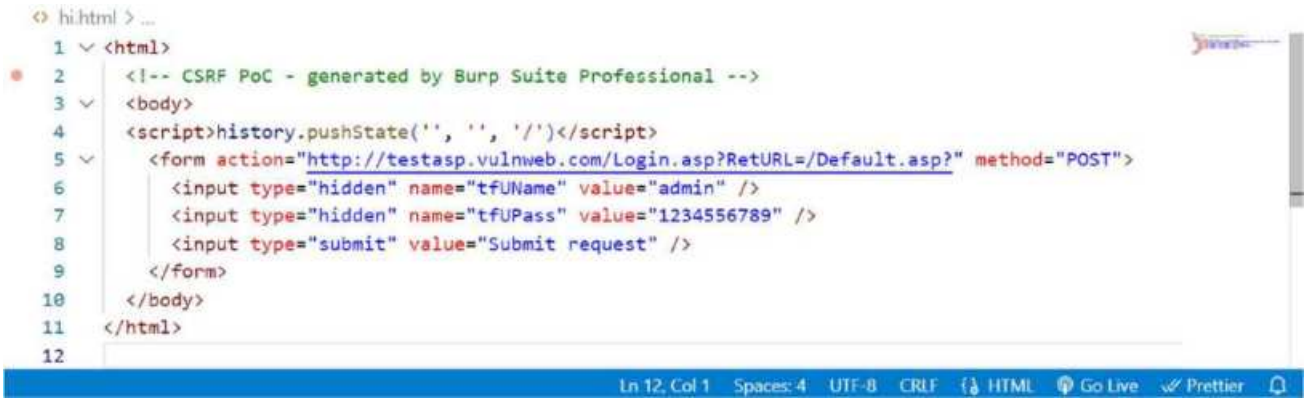
2. **Payload Crafting**: Craft a malicious HTML page containing CSRF payloads targeting the application's functionalities.



3. **Host the Page**: Host the malicious page and trick a logged-in user into visiting it by copying the HTML.



- Now paste html code in Vscode or any browser and host it or go live.
- Trick a logged-in user into visiting the malicious page by sending them a crafted link or embedding it within a legitimate website.

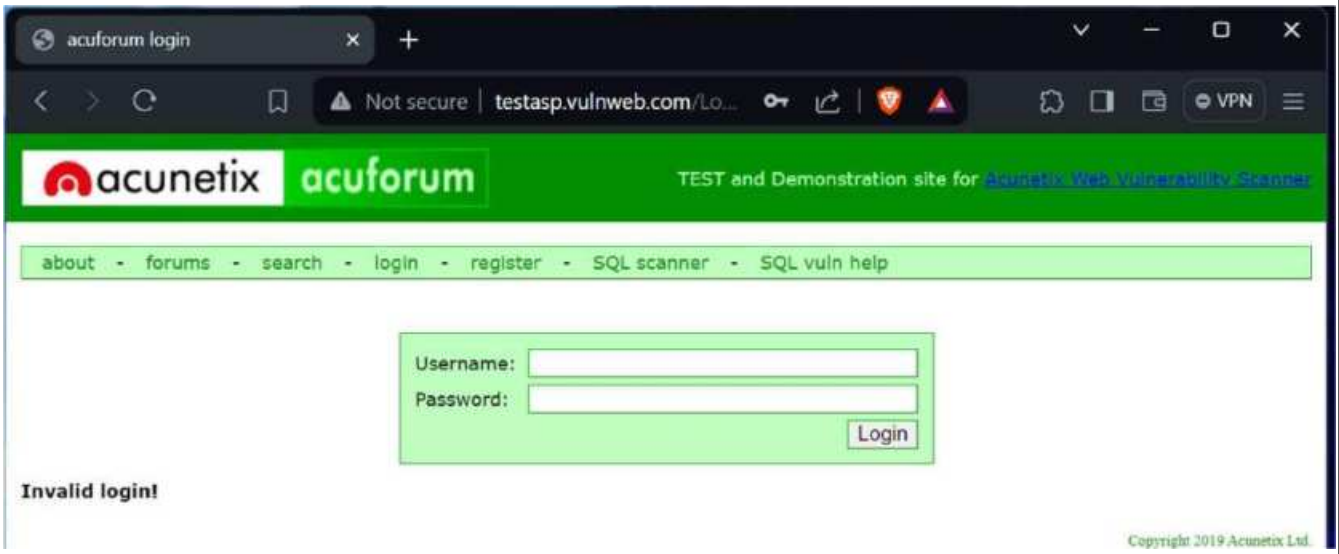


4. **Monitoring**: Monitor the intercepted requests in Burp Suite to see if the CSRF attack is successful.

    - Analyze the requests generated by the victim user's interaction with the malicious HTML page.
    - submit the request

5. **Assessment**: Assess the impact of the attack and recommend mitigations such as CSRF tokens.

    - Copy the HTML of the malicious page and test it by pasting it into a web browser or an editor like VSCode, then go live to observe the impact of the attack firsthand.



7. Traffic analysis Testing:

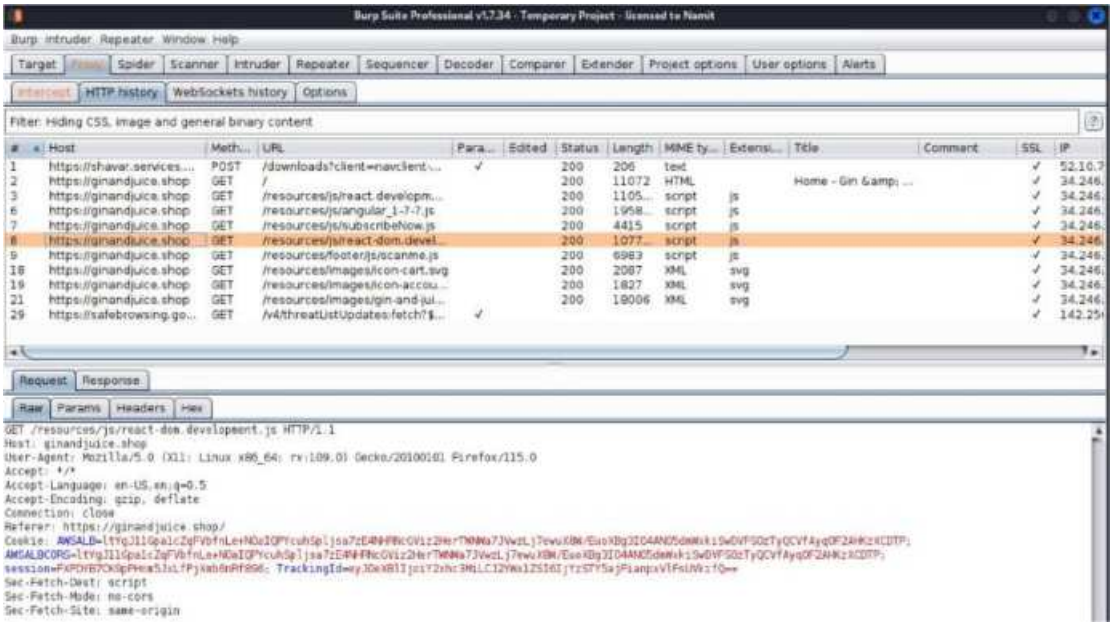
Scenario Question: How would you utilize Burp Suite to detect and mitigate suspicious or malicious activity in the web application https://ginandjuice.shop/ through traffic analysis?

Scenario: We suspect that the web application https://ginandjuice.shop/ may be under attack or compromised, and you want to perform traffic analysis to detect any suspicious or malicious activity.

Steps:

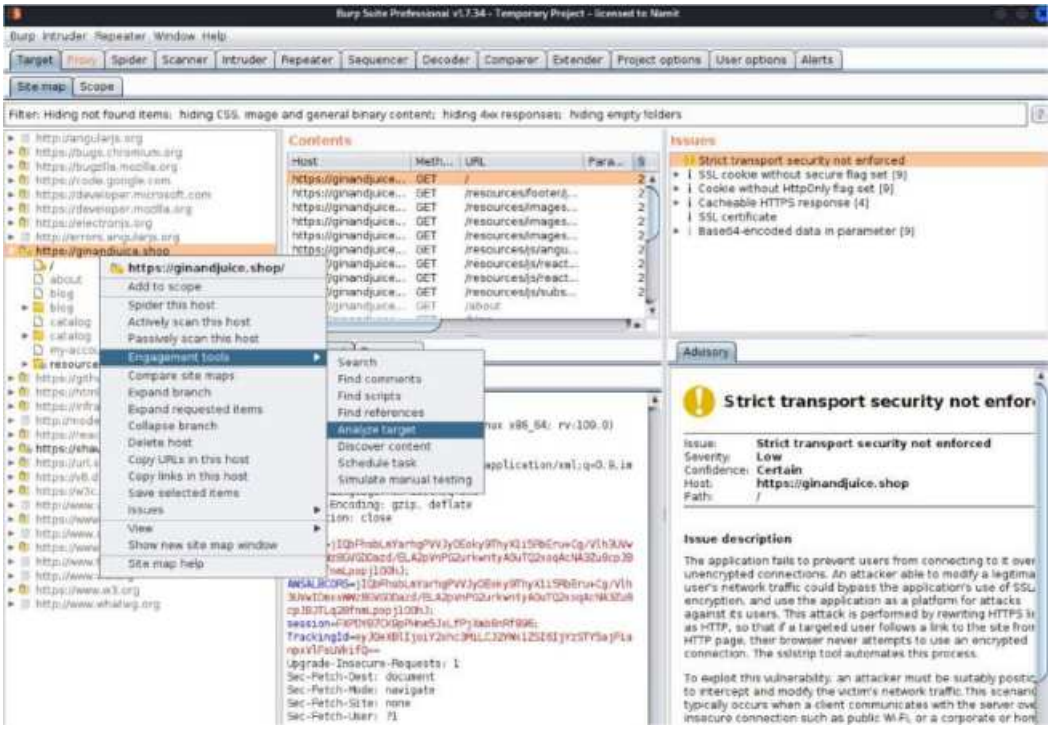
1. Proxy Setup: Configure Burp Suite as a proxy and ensure interception is enabled.

2. Intercept Traffic: Browse the target web application https://ginandjuice.shop/ using your browser allowing Burp Suite to intercept HTTP(S) requests and responses.



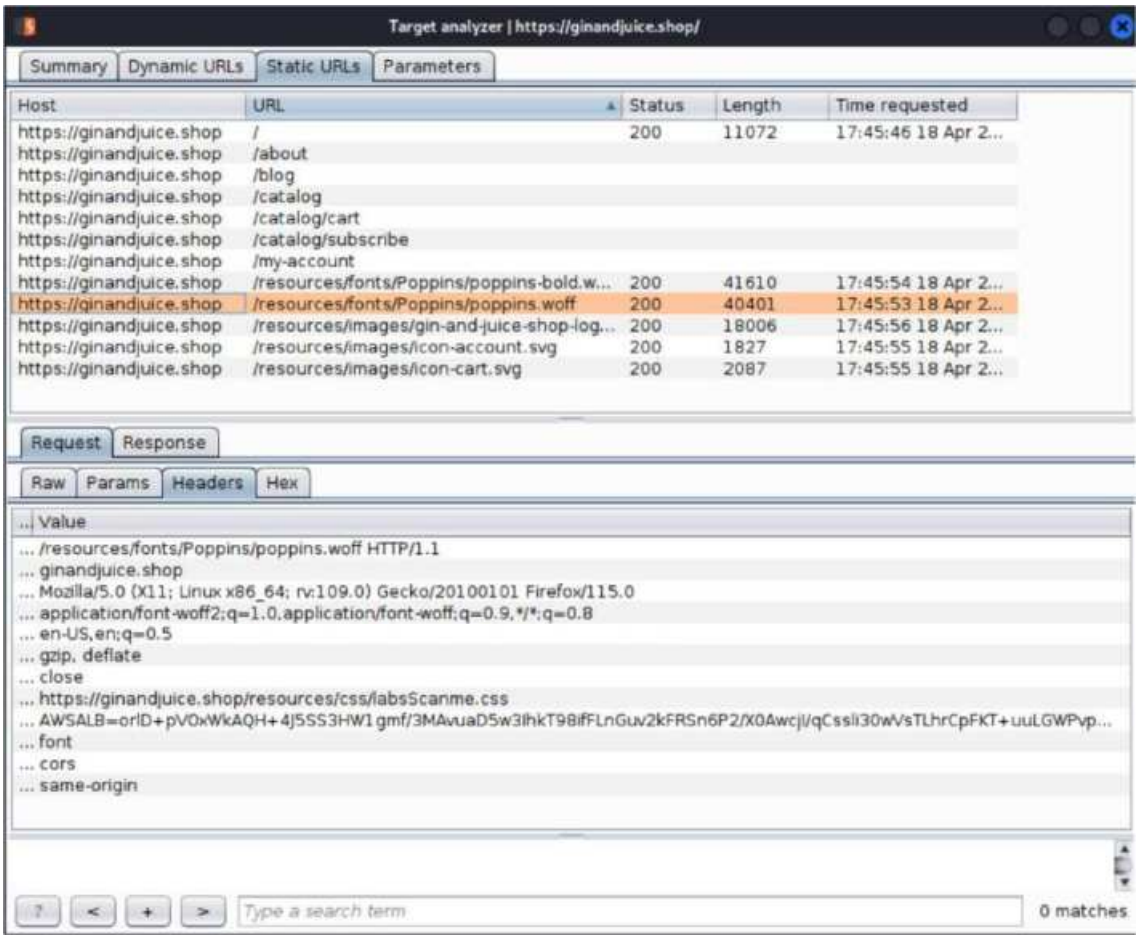
3. Analyze Request Patterns: Review intercepted requests for abnormal patterns or unexpected endpoints.

4. Inspect Response Content: Analyze response content for injected scripts or unexpected files.



5. Check HTTP Headers:

- Inspect the HTTP headers of intercepted requests and responses for suspicious user-agents, unusual cookies, or any other anomalies.
- Look for headers commonly used by attackers to fingerprint or exploit vulnerabilities in web applications.



6. Identify Outbound Connections: Monitor outbound connections for connections to known malicious domains or IP addresses.

- Use tools like Burp Suite's Collaborator or external threat intelligence feeds to identify suspicious outbound connections.

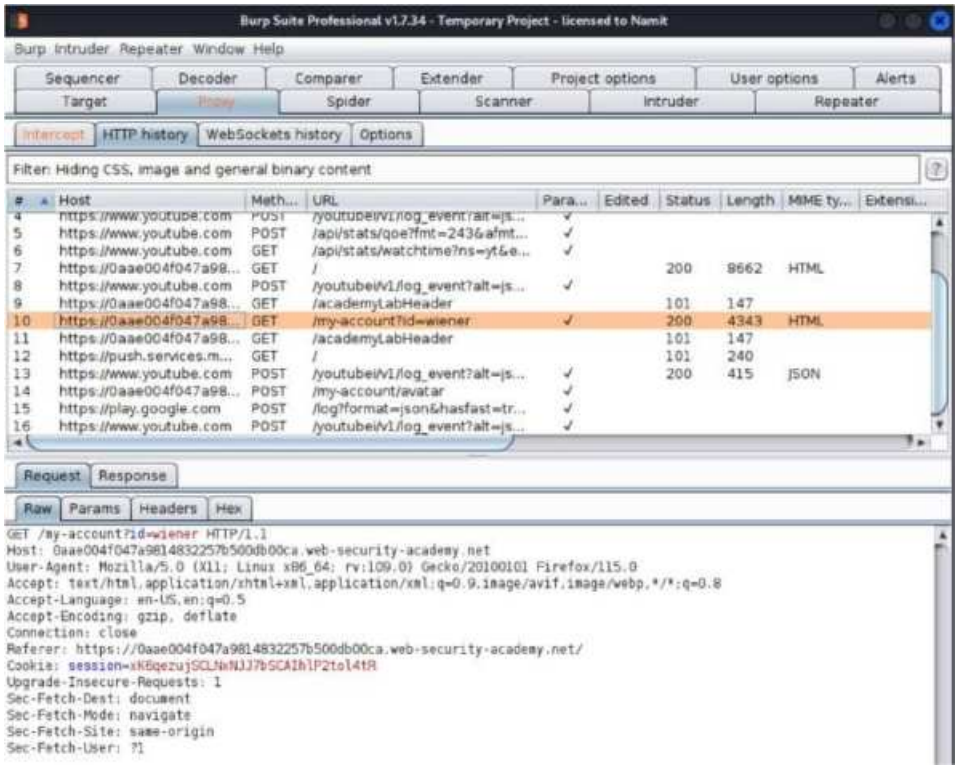
8. **File Upload Vulnerabilities**:

Scenario Question: How can Burp Suite be used to assess the security of a web application's file upload functionality and detect potential vulnerabilities leading to remote code execution?

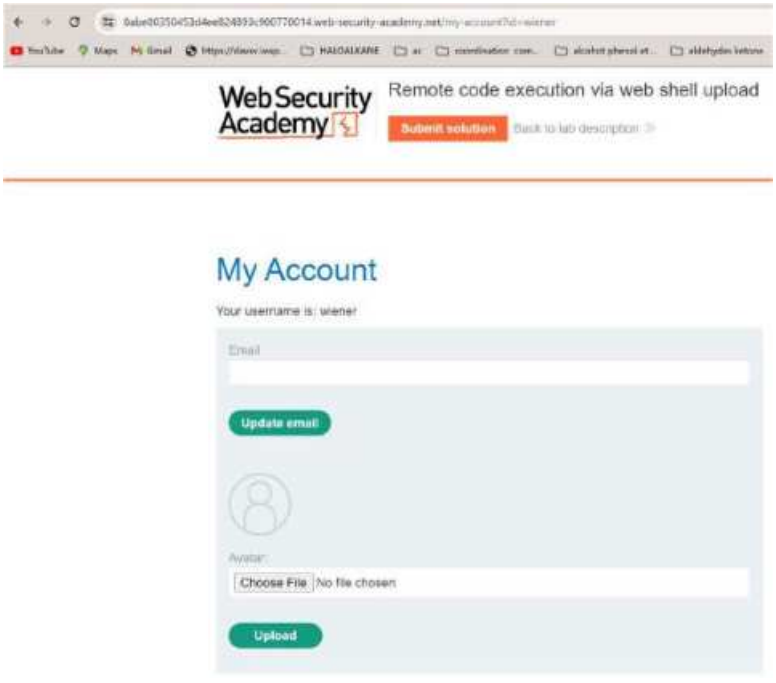
Scenario: We aim to evaluate the security of the file upload functionality on the web application located at https://portswigger.net/web-security/file-upload/lab-file-upload-remote-code-execution-via-web-shell-upload.

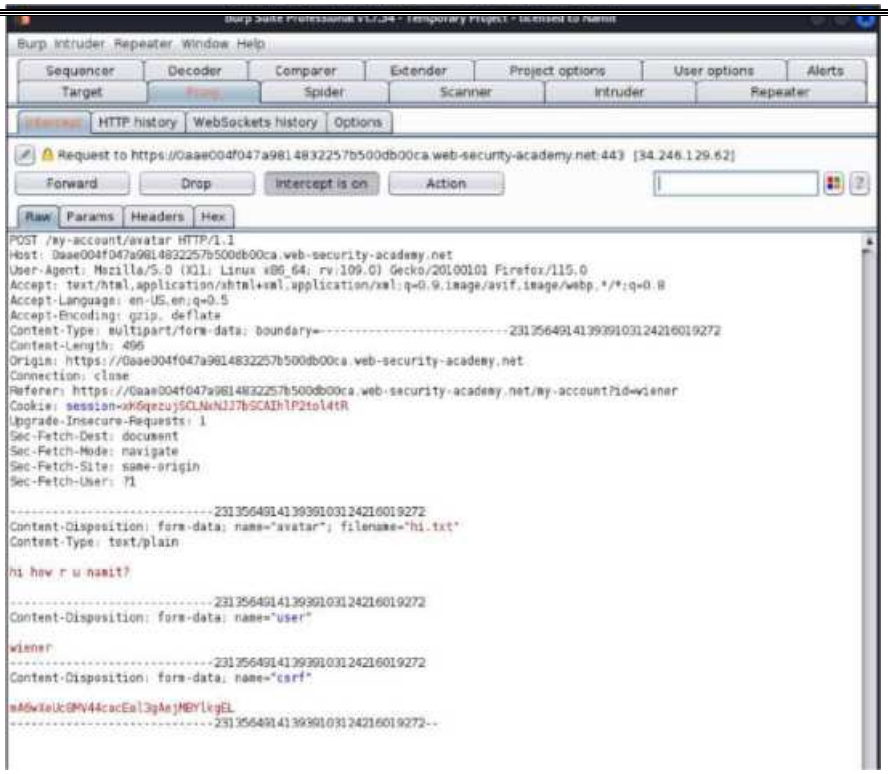
- **Steps**:

1. **Request Interception**: Upload various file types with different extensions using Burp's Repeater tool.



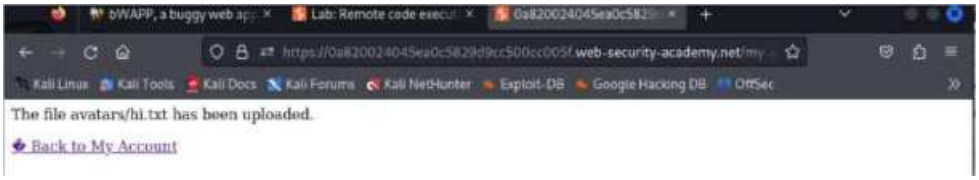
2. **Payload Modification**: Modify the file content to include malicious scripts or executable code.



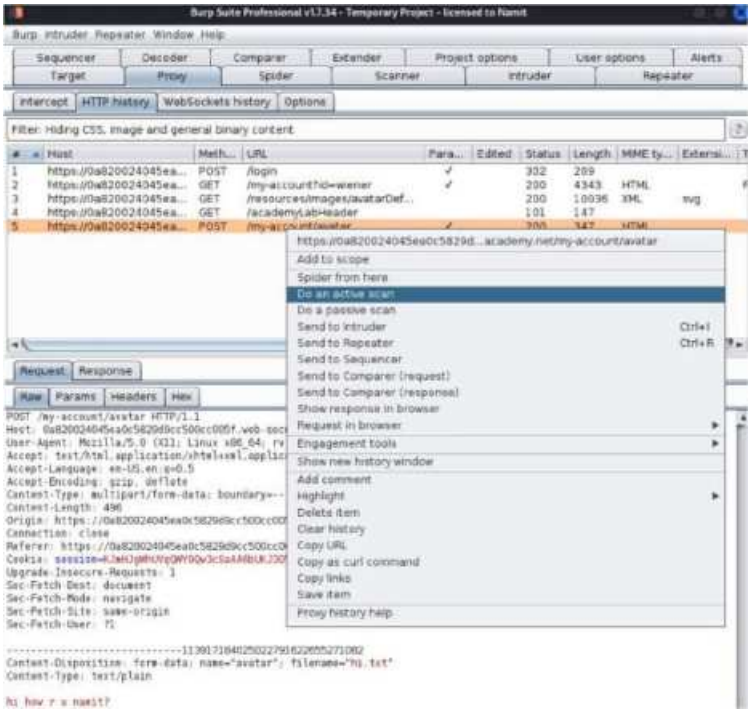


3. **Response Analysis**:

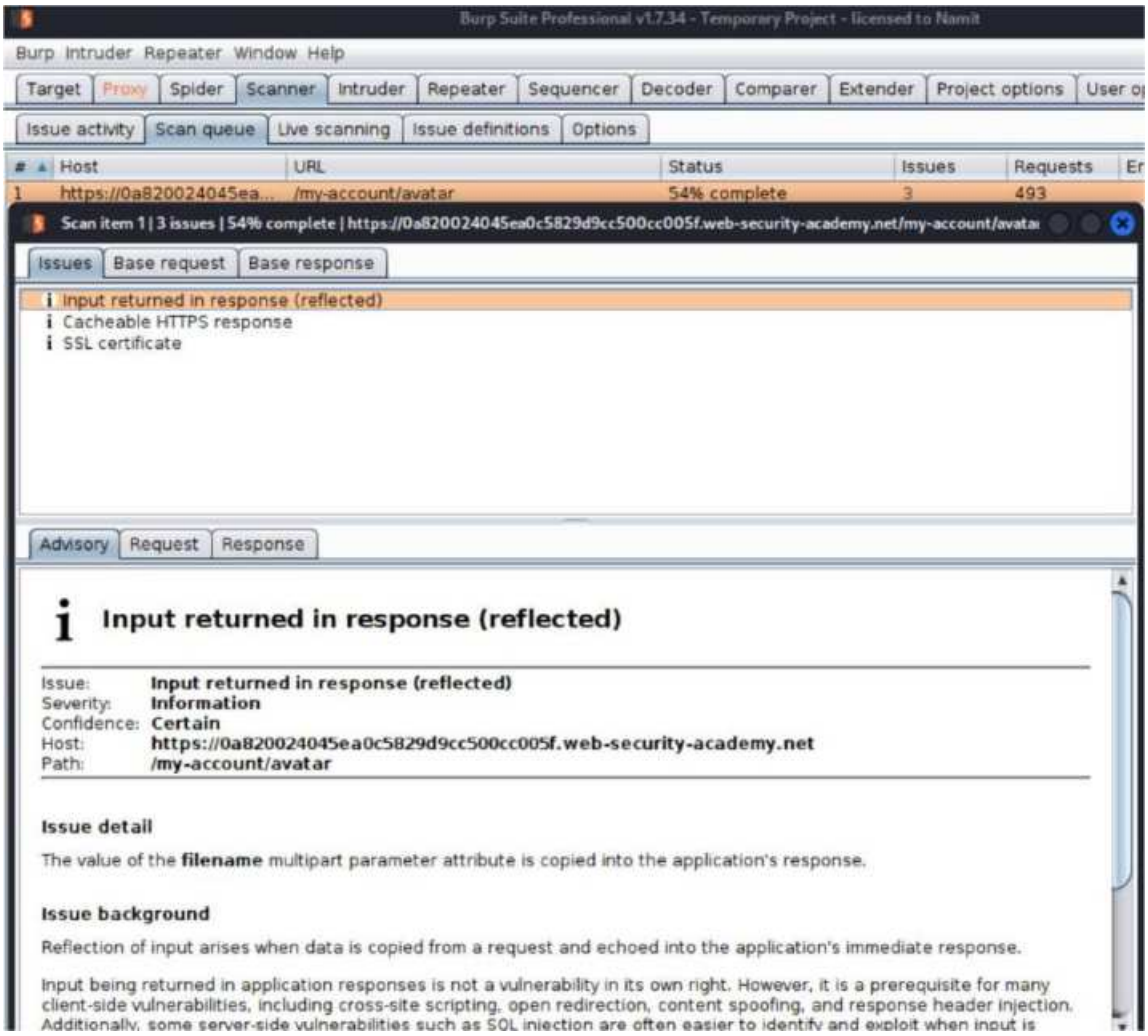
- Analyze the responses from the server to the file upload requests for any indications of validation errors or unexpected behaviors.
- Look for responses that may suggest successful execution of the injected payloads or bypassing of file type restrictions.



4. **Scanner Usage**: Use Burp's Scanner to automate file upload vulnerability testing.

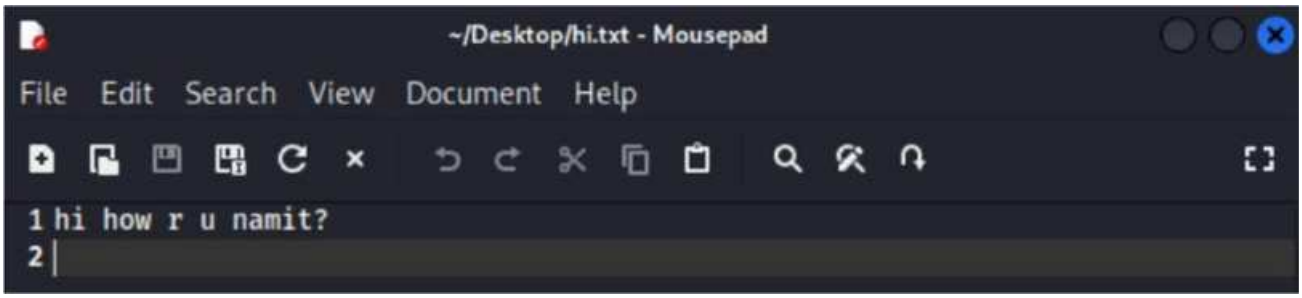


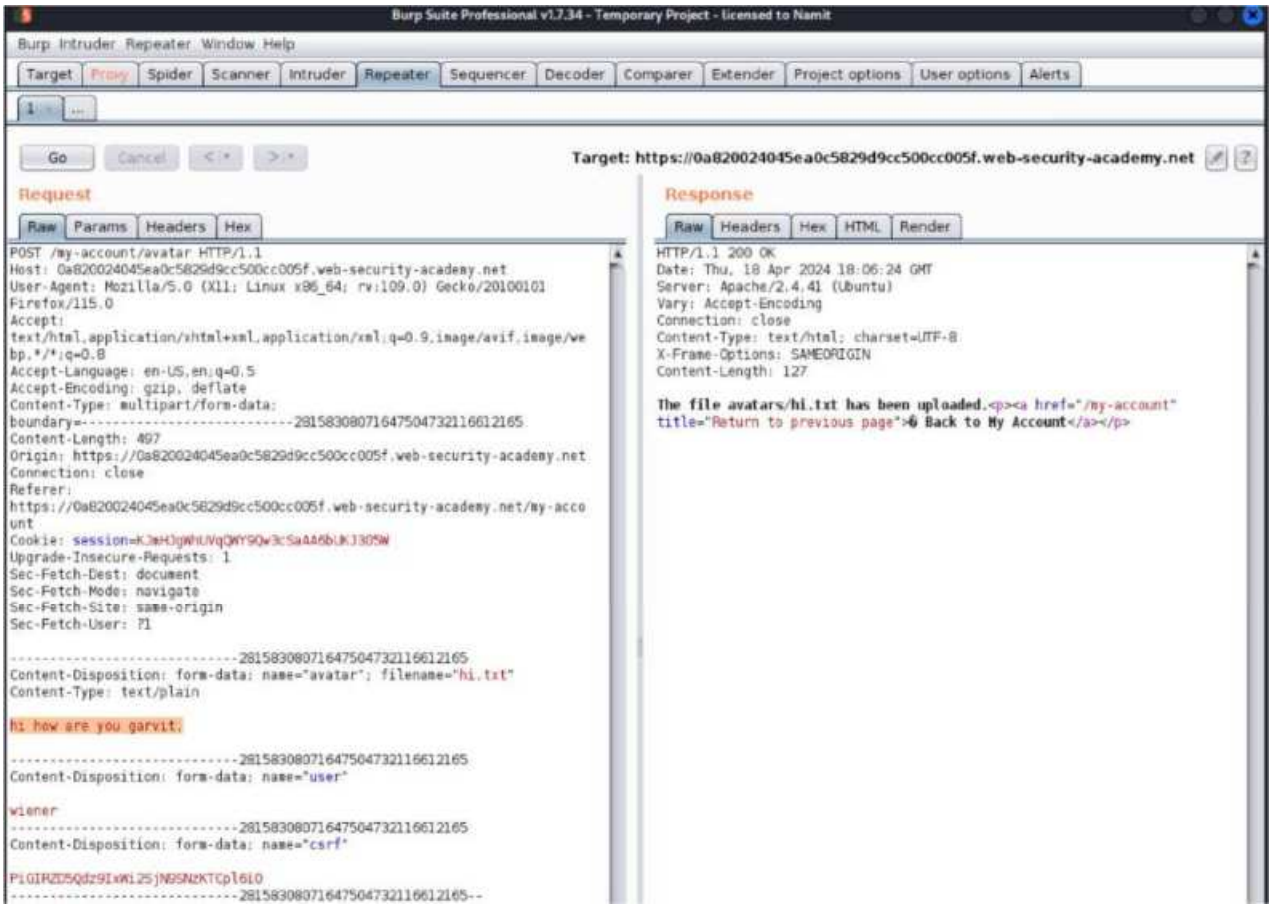
- Configure the scanner to target the file upload functionality and perform thorough testing to identify any potential security weaknesses.

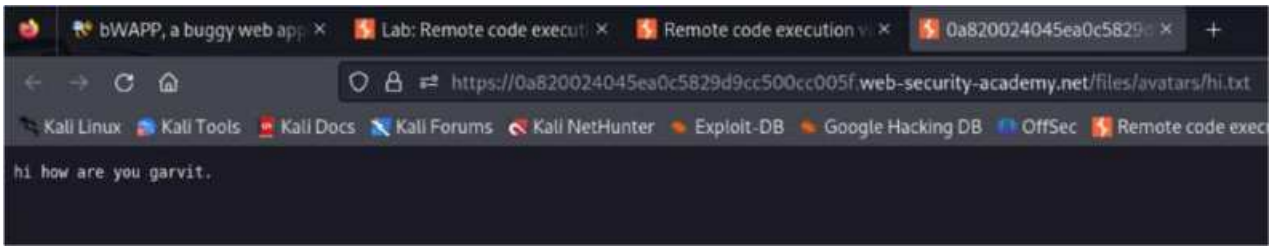


5. **Analyzes**: Analyze the findings and the changes made.

- Evaluate the impact and severity of any discovered vulnerabilities, particularly those leading to remote code execution.
- Document the changes made during the testing process and provide recommendations for remediation to enhance the security of the file upload functionality.




Burp Suite Professional v1.7.34 - Temporary Project - licensed to Namit
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go Cancel
Target: https://0a820024045ea0c5829d9cc500cc005f.web-security-academy.net
Request
Raw Params Headers Hex
POST /my-account/avatar HTTP/1.1
Host: 0a820024045ea0c5829d9cc500cc005f.web-security-academy.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------281583080716475047321166121 65
Content-Length: 497
Origin: https://0a820024045ea0c5829d9cc500cc005f.web-security-academy.net
Connection: close
Referer: https://0a820024045ea0c5829d9cc500cc005f.web-security-academy.net/my-account
Cookie: session=KJmHJgWhUVqQWY9Qw3cSaA46bUKJ3O5W
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
-----------------------------281583080716475047321166121 65
Content-Disposition: form-data; name="avatar"; filename="hi.txt"
Content-Type: text/plain
hi how are you garvit.
-----------------------------281583080716475047321166121 65
Content-Disposition: form-data; name="user"
wiener
-----------------------------281583080716475047321166121 65
Content-Disposition: form-data; name="csrf"
P1GIRZD5Qdz9IxWi2SjN9SNzKTCpl6L0
-----------------------------281583080716475047321166121 65--
Response
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Date: Thu, 18 Apr 2024 18:06:24 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 127
The file avatars/hi.txt has been uploaded. « Back to My Account


bWAPP, a buggy web ap
Lab: Remote code execut
Remote code execution v
0a820024045ea0c5829
https://0a820024045ea0c5829d9cc500cc005f.web-security-academy.net/files/avatars/hi.txt
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Remote code exec
hi how are you garvit.

9. **Information Disclosure via Error Messages**:

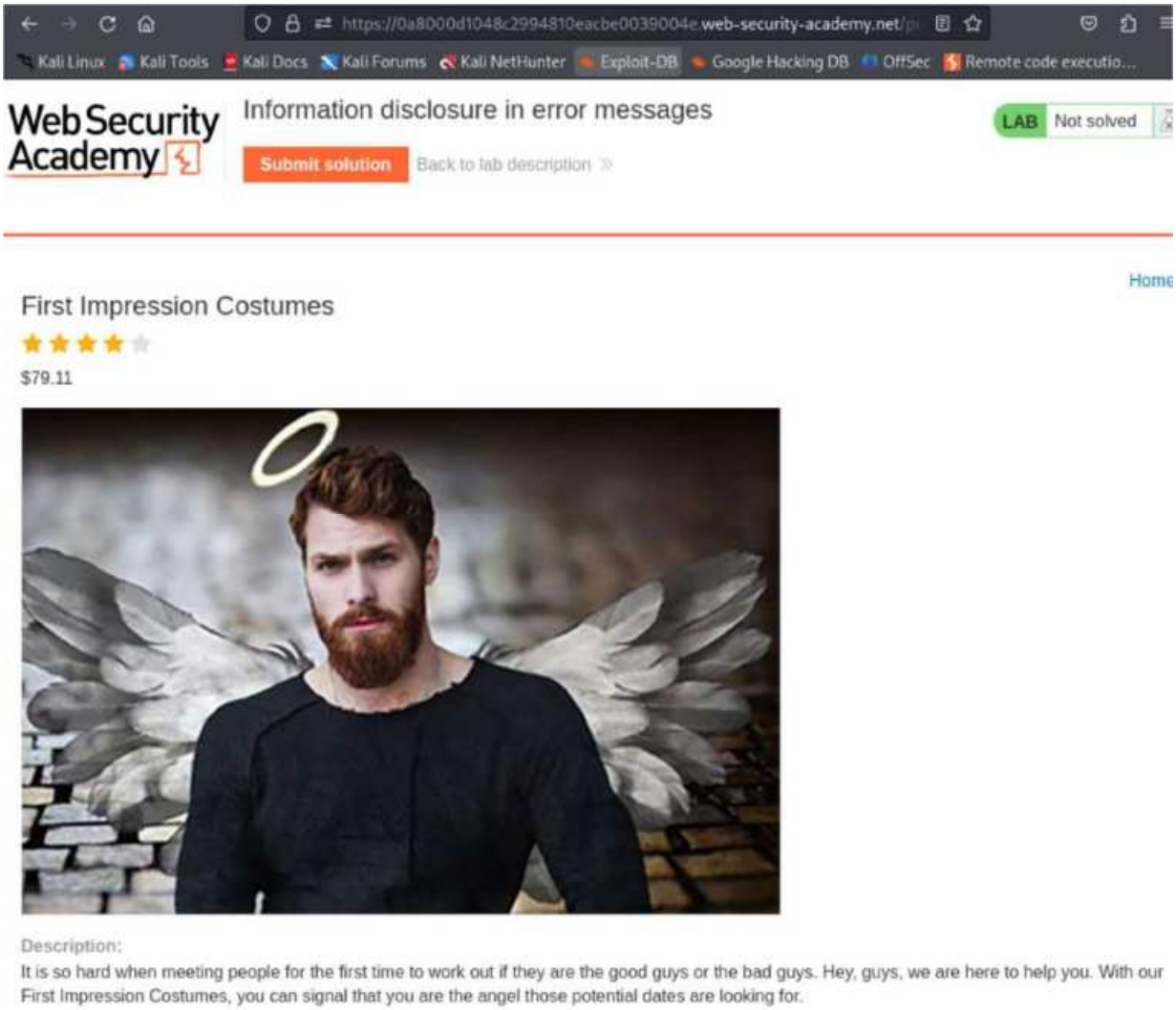
Scenario Question: How can Burp Suite be utilized to investigate and mitigate potential information disclosure vulnerabilities through error messages in a web application?

Scenario: We aim to assess the security of error messages in the web application located at https://portswigger.net/web-security/information-disclosure/exploiting/lab-infoleak-in-error-messages

- **Steps**:

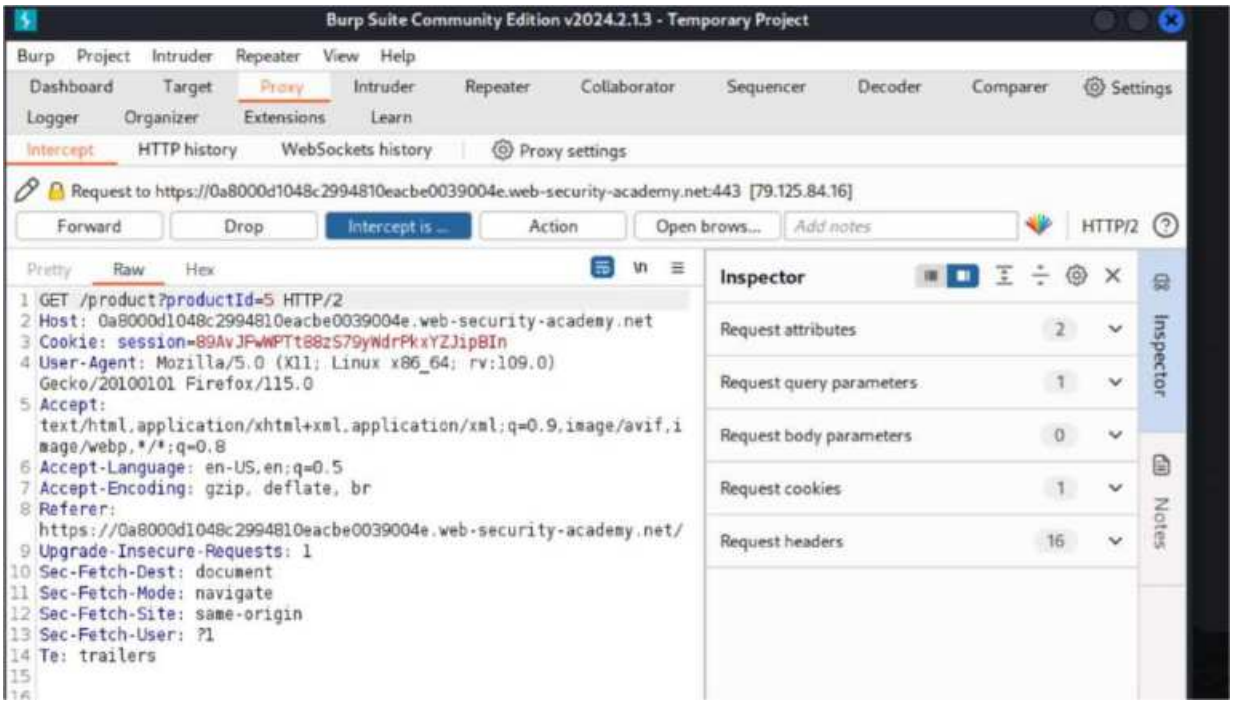
1. **Error Triggering**: Trigger various error conditions within the application.

- Navigate through various functionalities of the web application and intentionally trigger error conditions.
- Manipulate input fields or perform actions that may lead to the generation of error messages by the server.



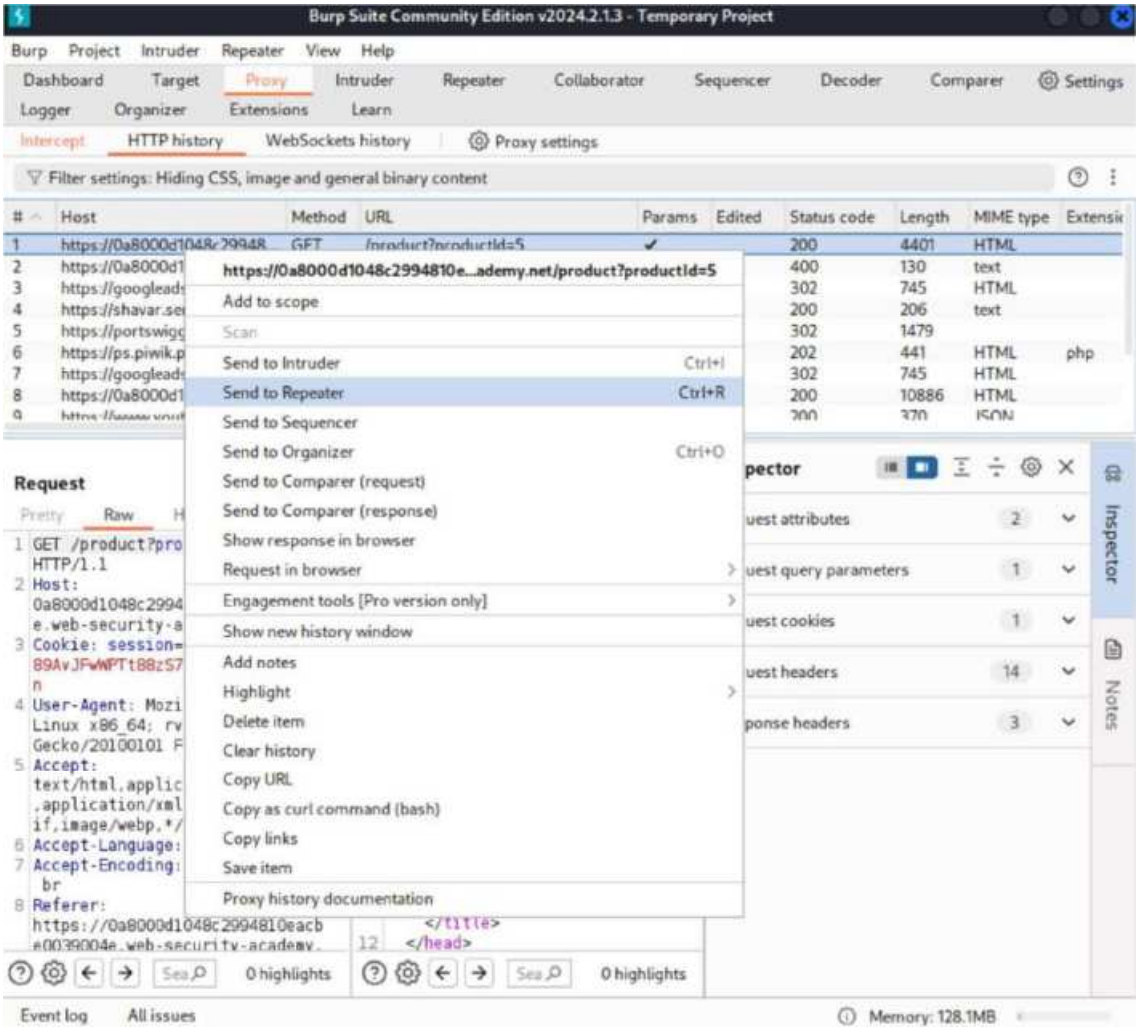
2. **Response Interception**:

- Use Burp's Proxy tool to intercept the server's responses to the error-triggering requests.
- Ensure that Burp Suite is configured to intercept both HTTP and HTTPS traffic.

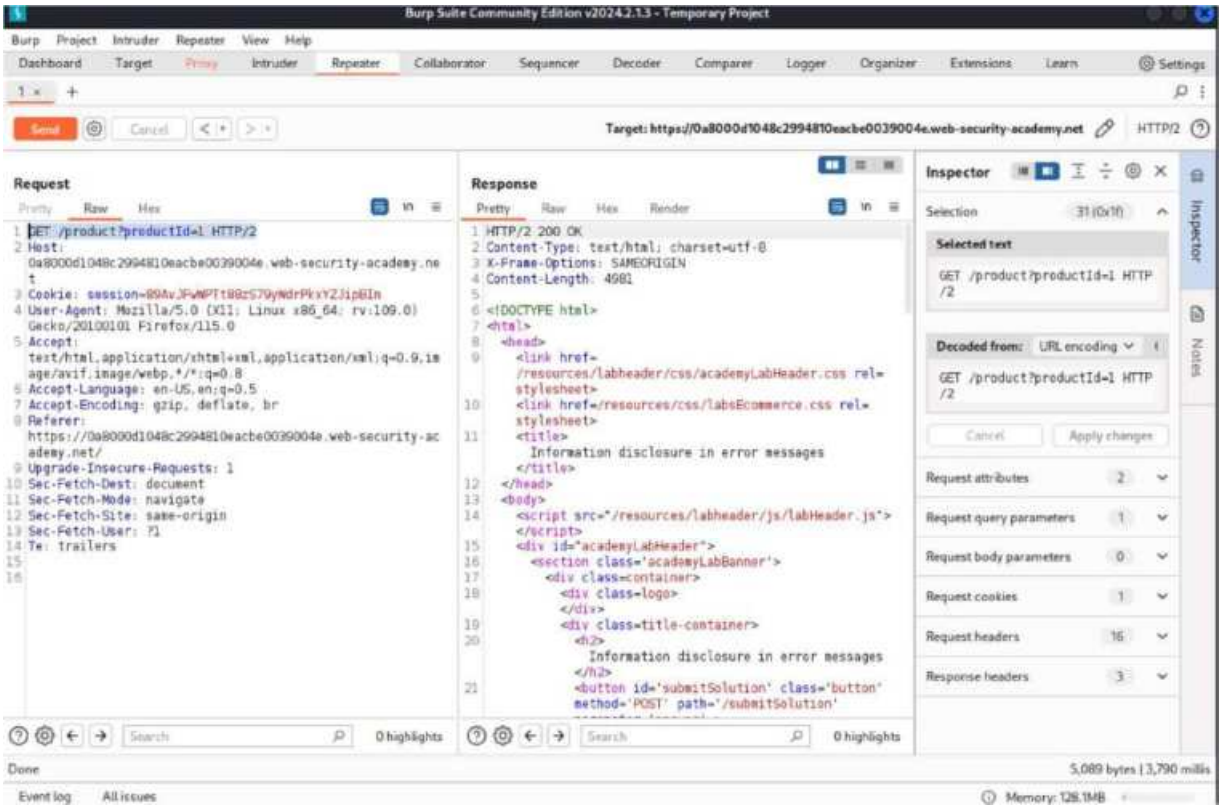


3. **Error Message Analysis**: Analyze the error messages for any hints or direct exposure of sensitive information.

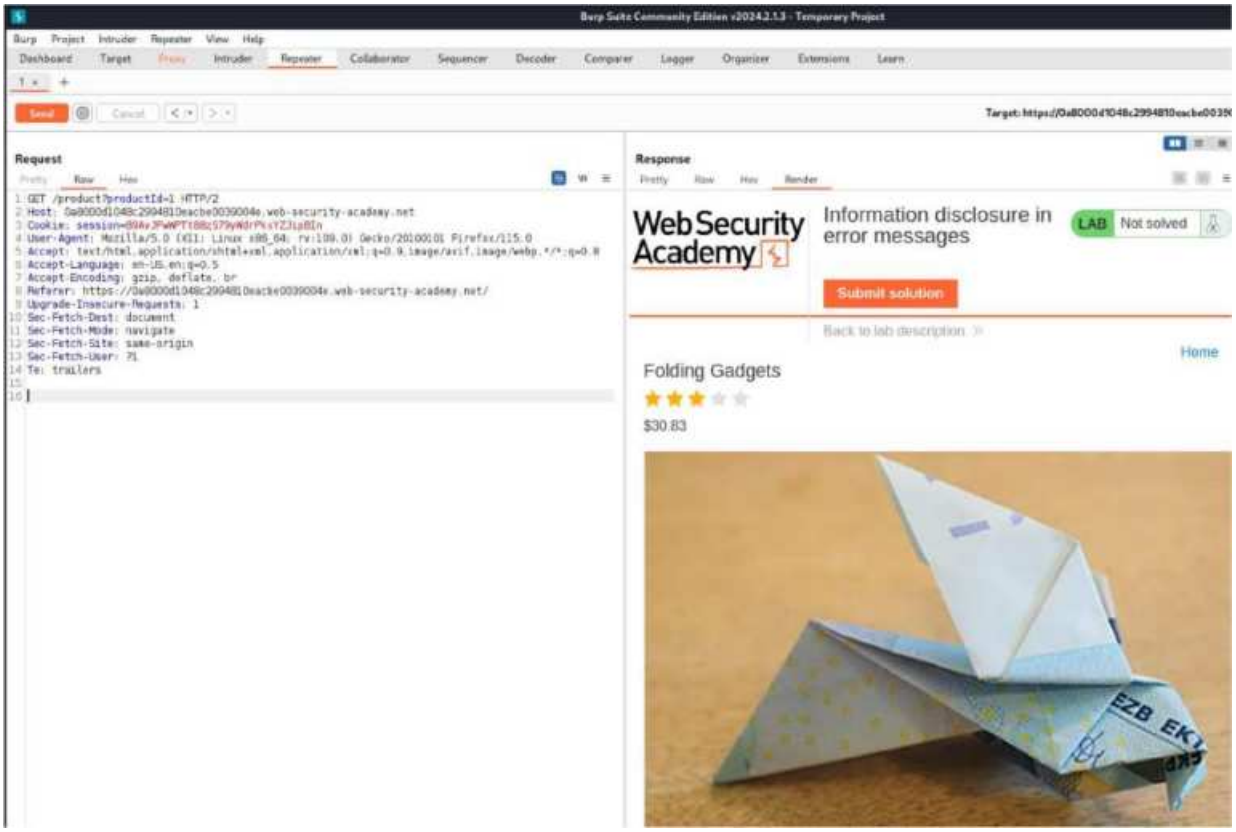
    - Look for details such as stack traces, file paths, database query fragments, or other sensitive data that may be inadvertently disclosed.



4. **Input Testing**: Test different input scenarios to see if error messages change based on the type of input.



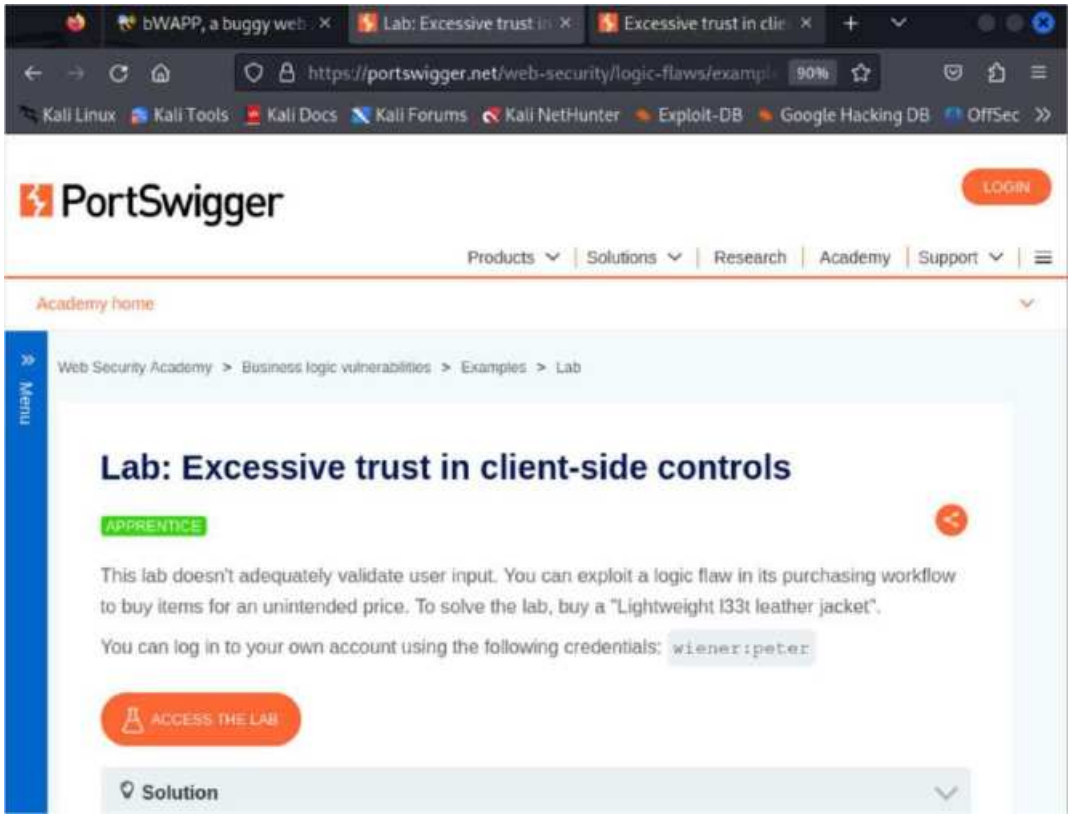
5. **Documentation**: Document any instances of information disclosure and recommend improvements in error handling.

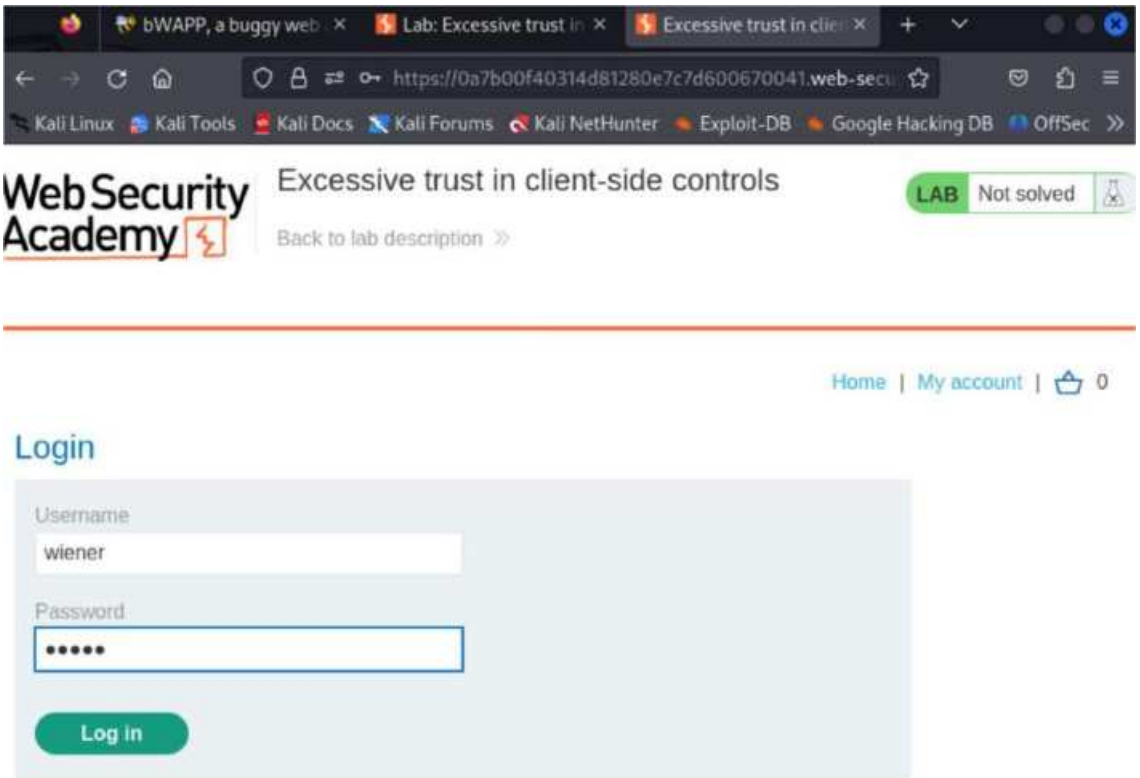


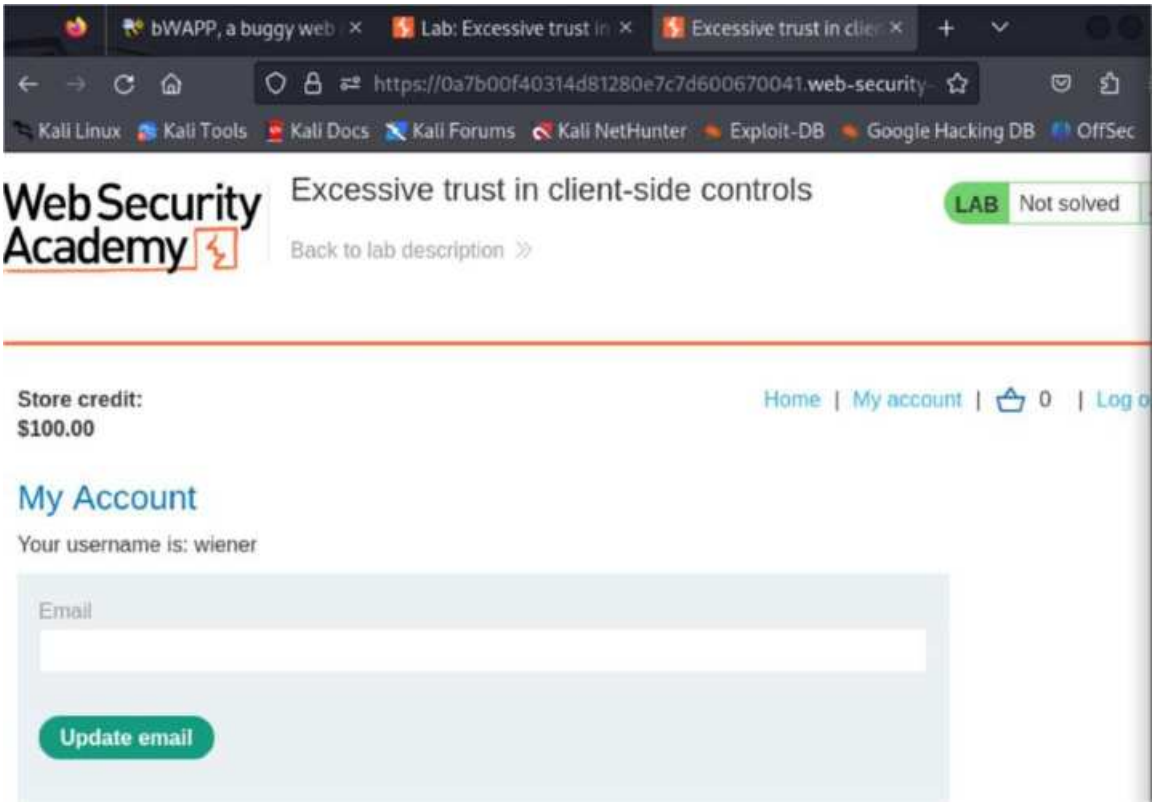
10. **HTTP Header Manipulation**:

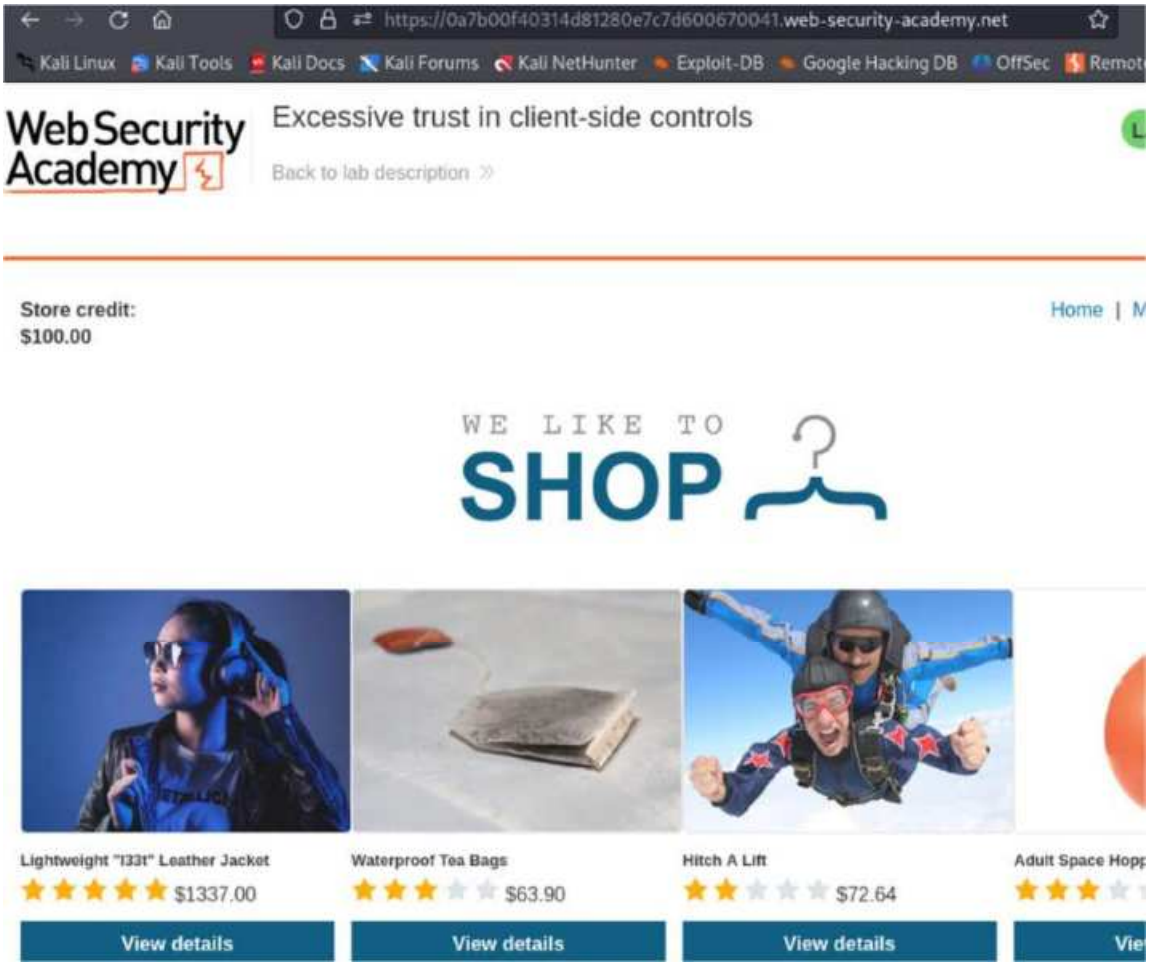
Scenario Question: How can Burp Suite be utilized to assess how a web application manages different HTTP headers?

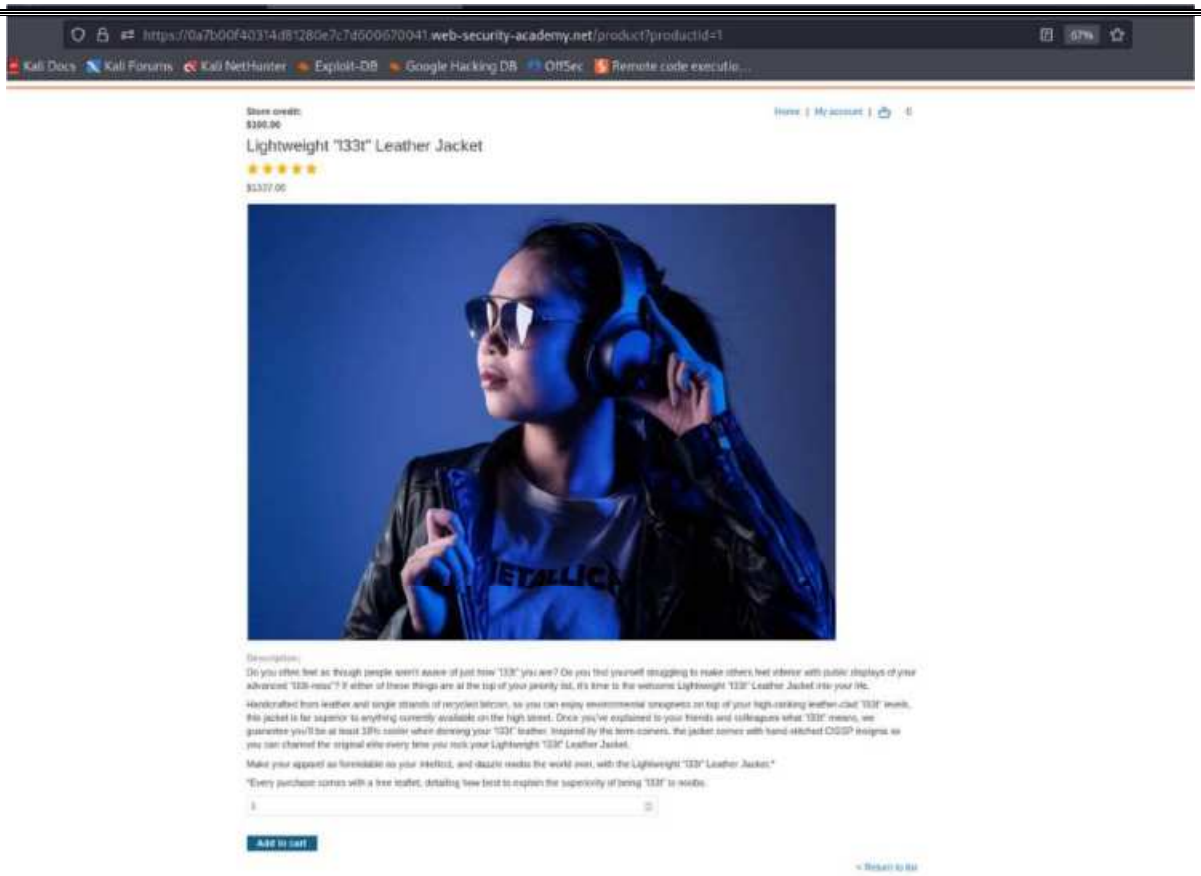
Scenario: We aim to evaluate how the web application handles various HTTP headers, specifically focusing on the lab located at https://portswigger.net/web-security/logic-flaws/examples/lab-logic-flaws-excessive-trust-in-client-side-controls





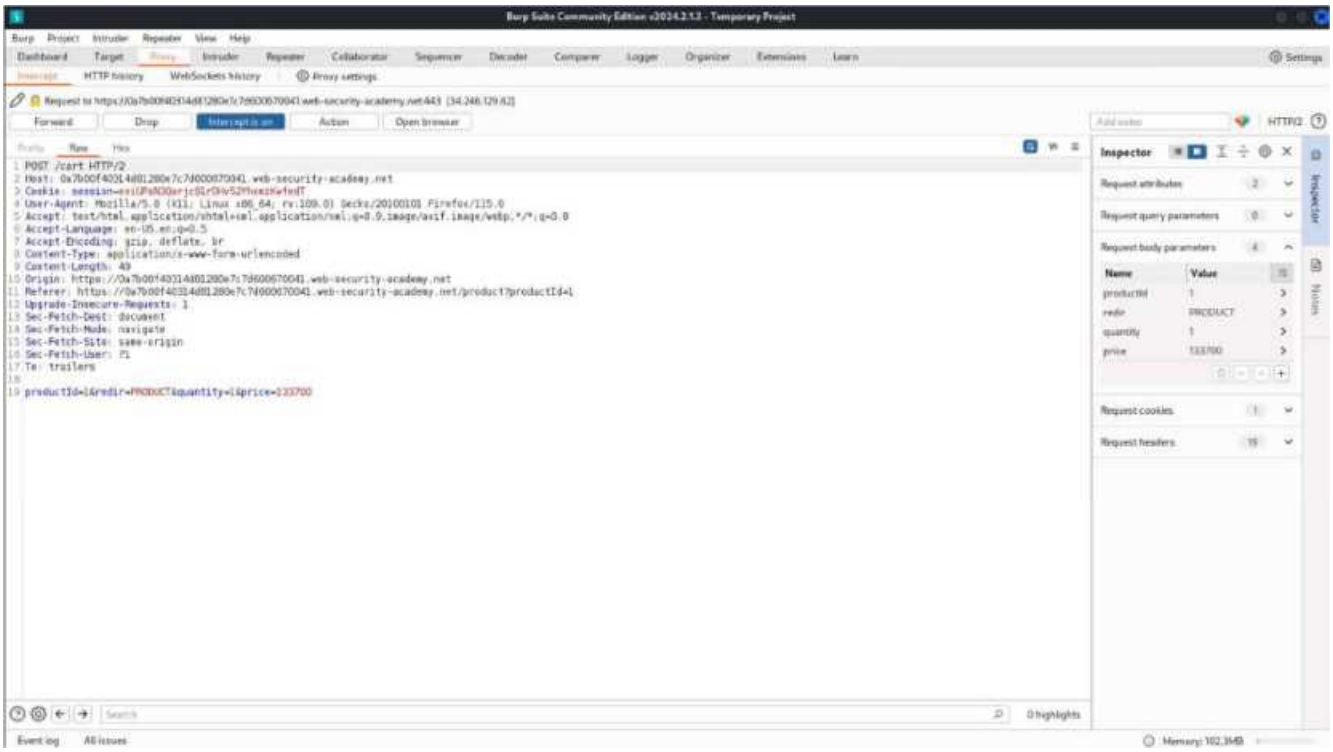

bWAPP, a buggy web
Lab: Excessive trust in
Excessive trust in clie
https://0a7b00f40314d81280e7c7d600670041.web-security
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Web Security Academy
Excessive trust in client-side controls
LAB
Not solved
Back to lab description
Store credit:
$100.00
Home | My account | 0 | Log o
My Account
Your username is: wiener
Email
Update email


https://0a7b00f40314d81280e7c7d600670041.web-security-academy.net
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Remot
Web Security Academy
Excessive trust in client-side controls
Back to lab description
Store credit:
$100.00
Home | M
WE LIKE TO
SHOP
Lightweight "l33t" Leather Jacket
$1337.00
View details
Waterproof Tea Bags
$63.90
View details
Hitch A Lift
$72.64
View details
Adult Space Hopp
View details

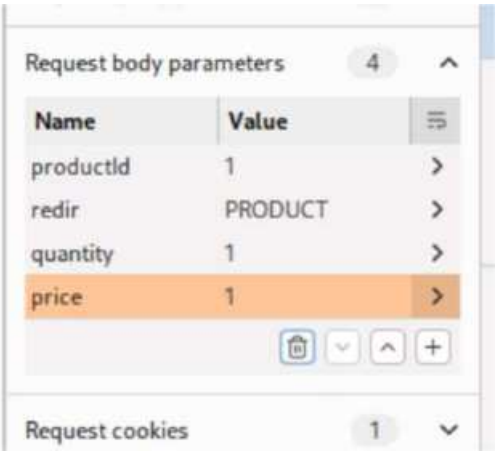


Steps:

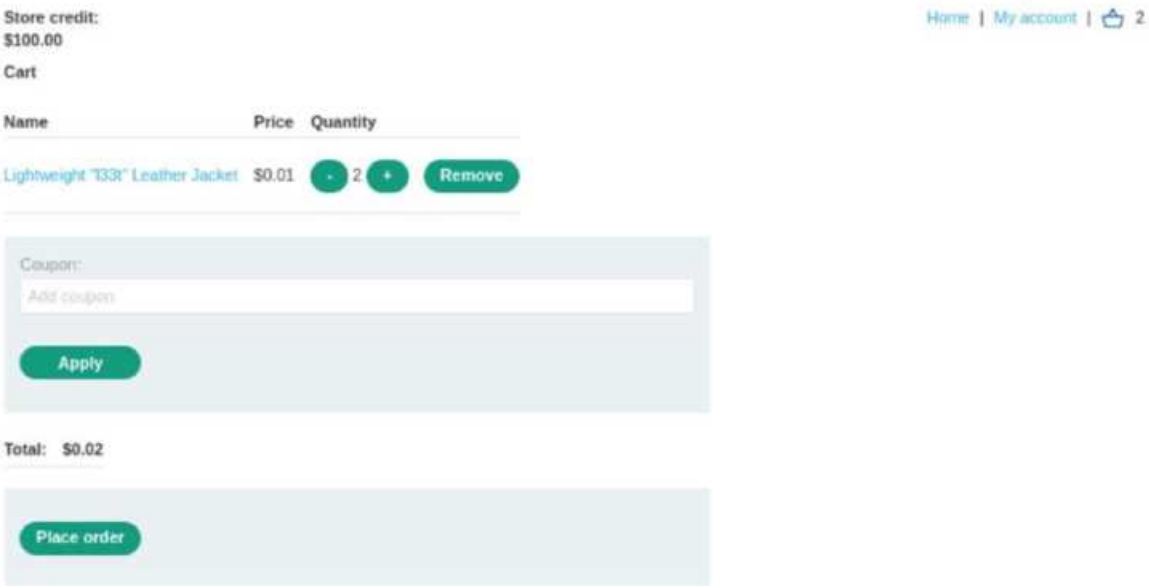
1. **Proxy Setup:**
    - Configure Burp Suite as a proxy and ensure interception is enabled.
    - Set up your browser to use Burp Suite as a proxy to intercept requests and responses.



2. **Interception and Inspector:**
    - Navigate to the target web application's URL provided in the scenario.
    - Perform various actions within the application while Burp Suite intercepts the traffic.
    - Observe the HTTP headers in both requests and responses to understand their handling by the application.



3. **Header Modification:**
    - Use Burp Suite to modify existing HTTP headers or inject new headers into intercepted requests.
    - Experiment with different header values and combinations to assess the application's response.



4. **Behavior Analysis:**
    - Analyze how the application behaves in response to modified HTTP headers.
    - Look for any changes in functionality, security controls, or application behavior triggered by manipulated headers.

5. **Security Mechanisms Testing:**
    - Test for the presence and effectiveness of security mechanisms such as HTTP Strict Transport Security (HSTS) or Content Security Policy (CSP).
    - Manipulate headers related to security controls to evaluate their impact on the application's security posture.
6. **Vulnerability Reporting:**
    - Document any vulnerabilities or weaknesses discovered during the testing process.
    - Provide recommendations for improving the application's handling of HTTP headers to enhance security and mitigate potential risks.

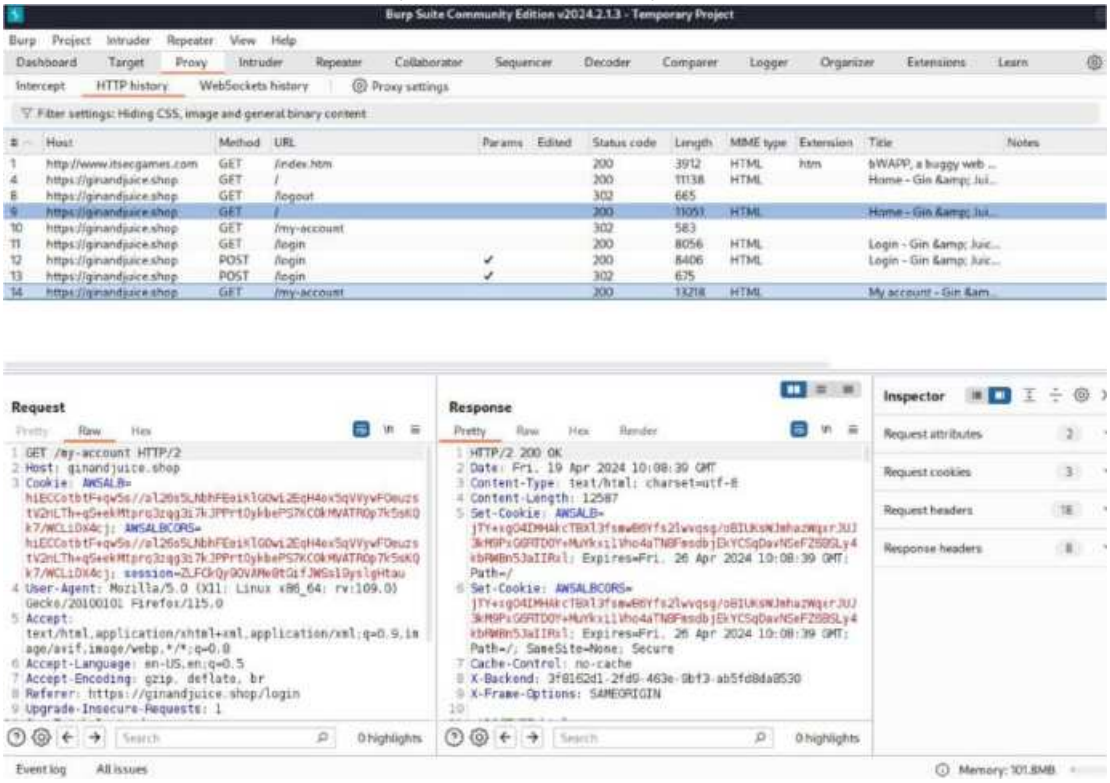
11. Determining the session timeout using Burp Suite

Scenario Question: How can Burp Suite be employed to determine the session timeout of a web application?

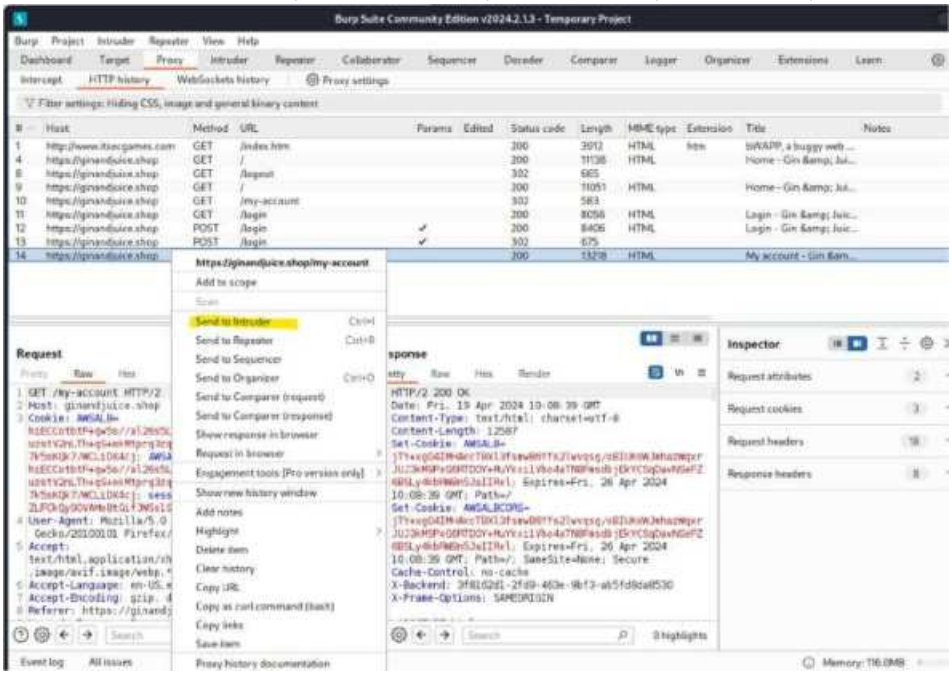
Scenario: We aim to determine the session timeout of the web application located at https://ginandjuice.shop/.

Steps:

1. **Proxy Setup:**
    - Launch Burp Suite and configure it as a proxy.
    - Ensure that interception is enabled in Burp Suite.

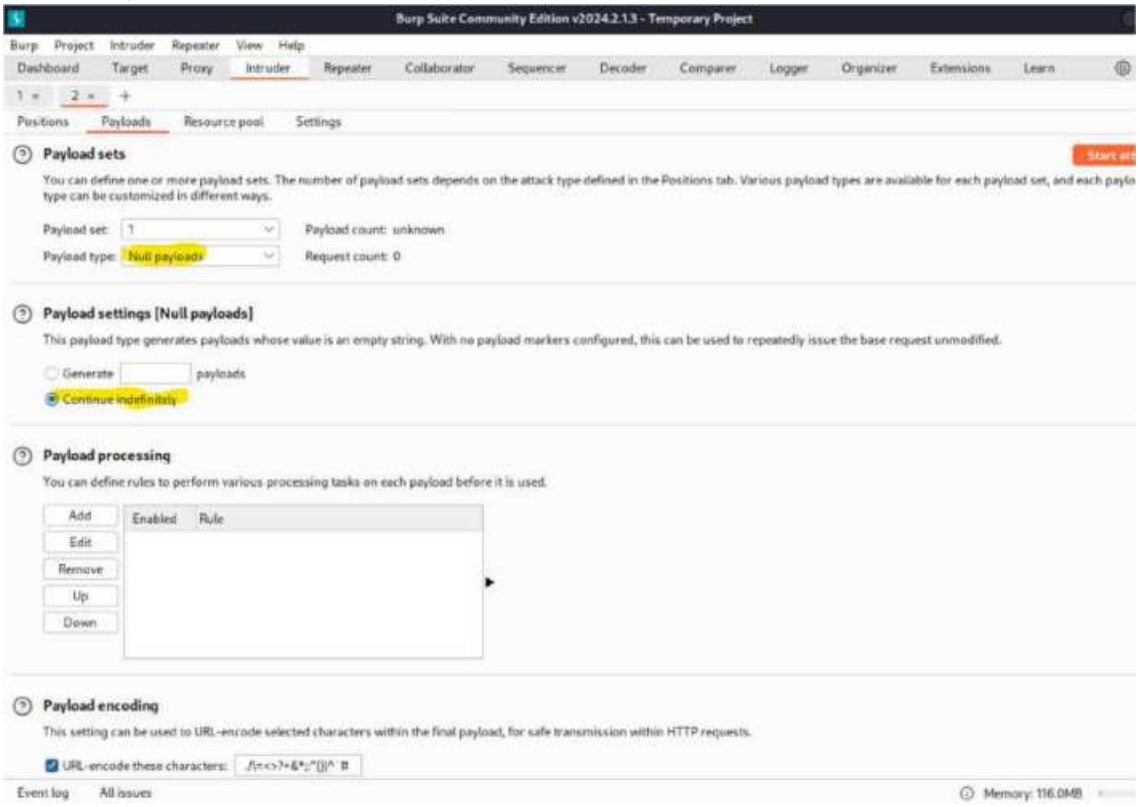


2. **Interception and Observation:**
    - Access the web application at https://ginandjuice.shop/ through your browser.
    - Allow Burp Suite to intercept the HTTP requests and responses.



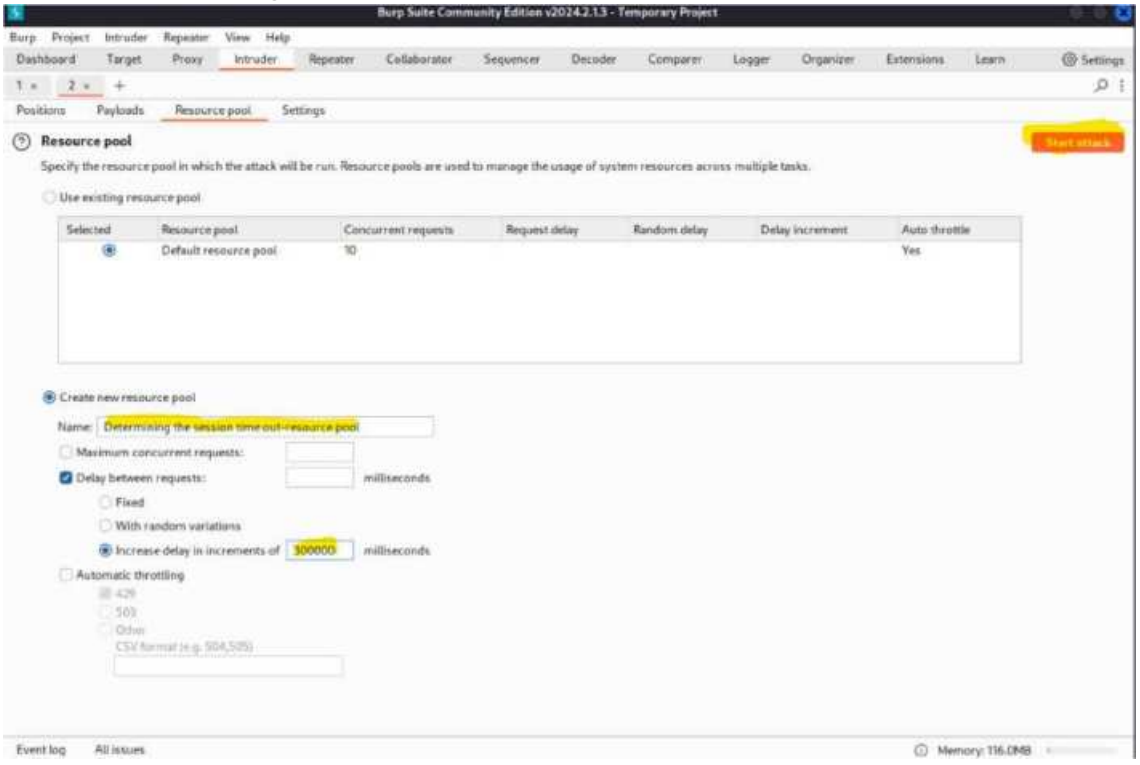
3. **Payload Injection:**

- Utilize Burp Suite's Intruder tool to perform automated session timeout testing with payloads.
- Configure the Intruder tool to send a series of requests with different payloads targeting session-related parameters.



4. **Session Timeout Testing with Payloads:**

- Execute the Intruder attack to send a sequence of requests with payloads designed to manipulate session-related parameters.
- Observe the responses from the web application to determine any changes in session behavior or session timeout settings.



5. **Session Persistence Testing:**

    - Keep the application idle for a period longer than the expected session timeout duration.
    - Observe how the session-related parameters change or if the session is terminated after the timeout duration.

6. **Documentation and Reporting:**

    - Document the observed session timeout behavior, including the duration of inactivity required for session expiration.
    - Provide recommendations for adjusting the session timeout settings, if necessary, to align with security best practices and user experience requirements.