# ASSIGNMENT-4

BY:

NAME:OMKAR SANJAY NARKAR

REG.NO.:21BCE8412

# What is Burp Suite?

Burp Suite is an integrated platform for performing security testing of web applications. It provides a comprehensive set of tools for manually and automatically testing applications for vulnerabilities, including SQL injection, cross-site scripting, and broken authentication. Burp Suite is a popular tool among security professionals due to its ease of use and its powerful features.

**Benefits of using Burp Suite reports**

Burp Suite reports can provide a number of benefits to organizations, including:

- **Improved visibility into web application security:** Burp Suite reports can help organizations to identify and prioritize security vulnerabilities in their web applications. This information can then be used to develop remediation plans and improve the overall security of their applications.

- **Reduced risk of data breaches and other attacks:** By identifying and remediating security vulnerabilities in their web applications, organizations can reduce the risk of data breaches and other attacks. This can help to protect their reputation and financial resources.
- **Improved compliance:** Burp Suite reports can help organizations to comply with industry regulations and standards, such as PCI DSS and HIPAA. These regulations and standards often require organizations to perform regular security assessments of their web applications.

### Types of Burp Suite reports

Burp Suite can generate a variety of reports, including:

- **Standard reports:** Standard reports provide a general overview of scan details, such as the included URLs, scan configurations used, and the duration of the scan.
- **Compliance reports:** Compliance reports help to show whether a site meets a specific compliance standard or framework. Burp Suite currently offers compliance reporting for the OWASP Top 10 2021 list and the PCI DSS v3. 2 security compliance standard.
- **Custom reports:** Custom reports allow users to create reports that are tailored to their specific needs. For example, users can create reports that only include certain types of vulnerabilities or that are organized by severity.

### How to generate a Burp Suite report

To generate a Burp Suite report, follow these steps:

1. Go to the **Target** > **Site map** tab.
2. Right-click on the entry for the website that you want to generate a report for.
3. Select **Issues** > **Report issues for this host**.
4. In the **Report issues** dialog box, select the issues that you want to include in the report.
5. Click **Next**.
6. In the **Report options** dialog box, customize the report settings.
7. Click **Next**.
8. In the **Save report** dialog box, enter a filename and location for the report.
9. Click **Save**.

### Conclusion

Burp Suite reports can be a valuable tool for organizations that are looking to improve the security of their web applications. By generating and reviewing Burp Suite reports, organizations can identify and prioritize security vulnerabilities, reduce the risk of data breaches and other attacks, and improve compliance with industry regulations and standard.

### Features of Burp Suite

Burp Suite includes a wide range of features for performing web application security testing, including:

- **Interception:** Burp Suite can intercept all traffic between your browser and the web application under test. This allows you to modify requests and responses, and to view the raw data being exchanged.
- **Scanning:** Burp Suite can perform both manual and automated scanning of web applications for vulnerabilities. The manual scanner allows you to test individual requests and responses, while the automated scanner can scan entire websites and applications.
- **Intruder:** Burp Suite's Intruder tool allows you to perform fuzzing and brute-force attacks against web applications. This can be useful for finding vulnerabilities that are not detected by the scanner.
- **Repeater:** Burp Suite's Repeater tool allows you to resend requests to a web application with different values. This can be useful for testing different scenarios and for finding vulnerabilities that are only exploitable under certain conditions.
- **Sequencer:** Burp Suite's Sequencer tool can be used to analyze the behavior of web applications and to identify potential vulnerabilities. For example, it can be used to identify session management vulnerabilities and CSRF vulnerabilities.
- **Proxy:** Burp Suite can be used as a proxy server, which allows you to route all traffic between your browser and the internet through Burp Suite. This gives you the ability to inspect all traffic, including encrypted traffic.

### Use cases for Burp Suite

Burp Suite can be used for a variety of web application security testing tasks, including:

- **Penetration testing:** Burp Suite is a popular tool among penetration testers, who use it to identify and exploit vulnerabilities in web applications.
- **Bug bounty hunting:** Burp Suite is also a popular tool among bug bounty hunters, who use it to find and report vulnerabilities in web applications.
- **Compliance testing:** Burp Suite can be used to test web applications for compliance with industry regulations and standards, such as PCI DSS and HIPAA.
- **Application security testing:** Burp Suite can be used by developers and security professionals to test web applications for vulnerabilities during the development process.

### Getting started with Burp Suite

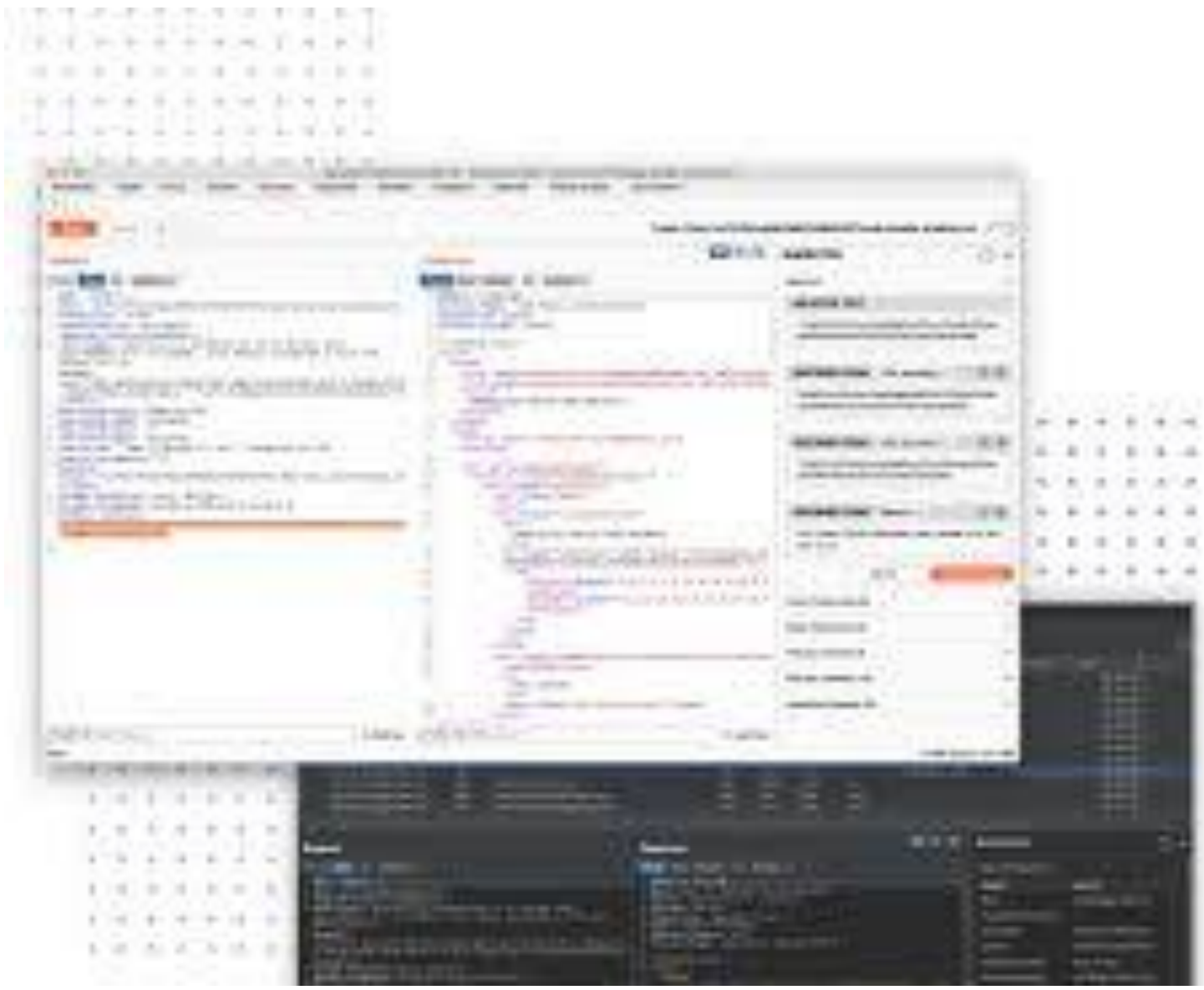
Burp Suite is available for download from the PortSwigger website. There is a free Community Edition of Burp Suite, as well as a paid Professional Edition. The Professional Edition includes additional features, such as automated scanning and reporting.

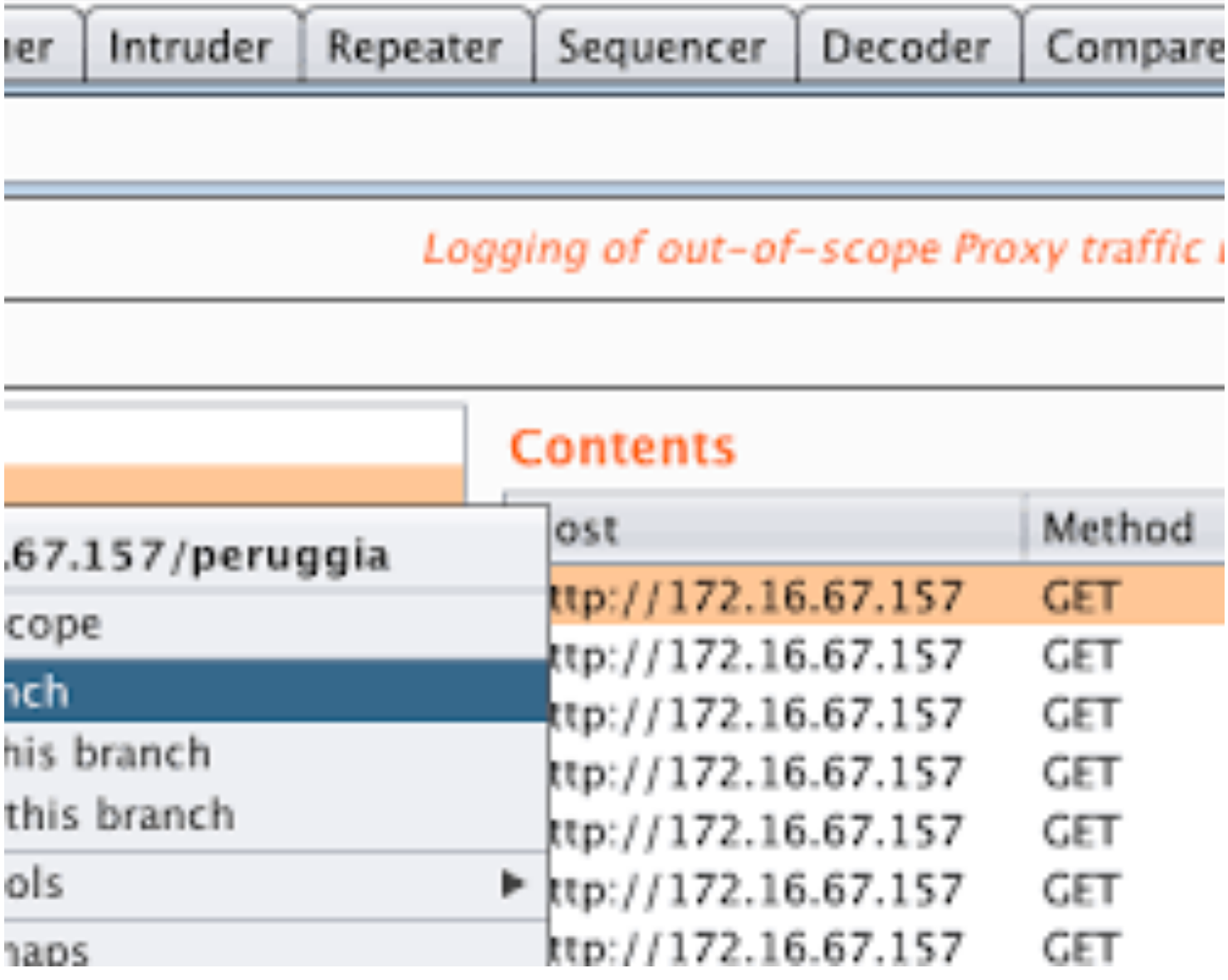
To get started with Burp Suite, you can follow the PortSwigger documentation: Burp Suite documentation: https://portswigger.net/burp/documentation

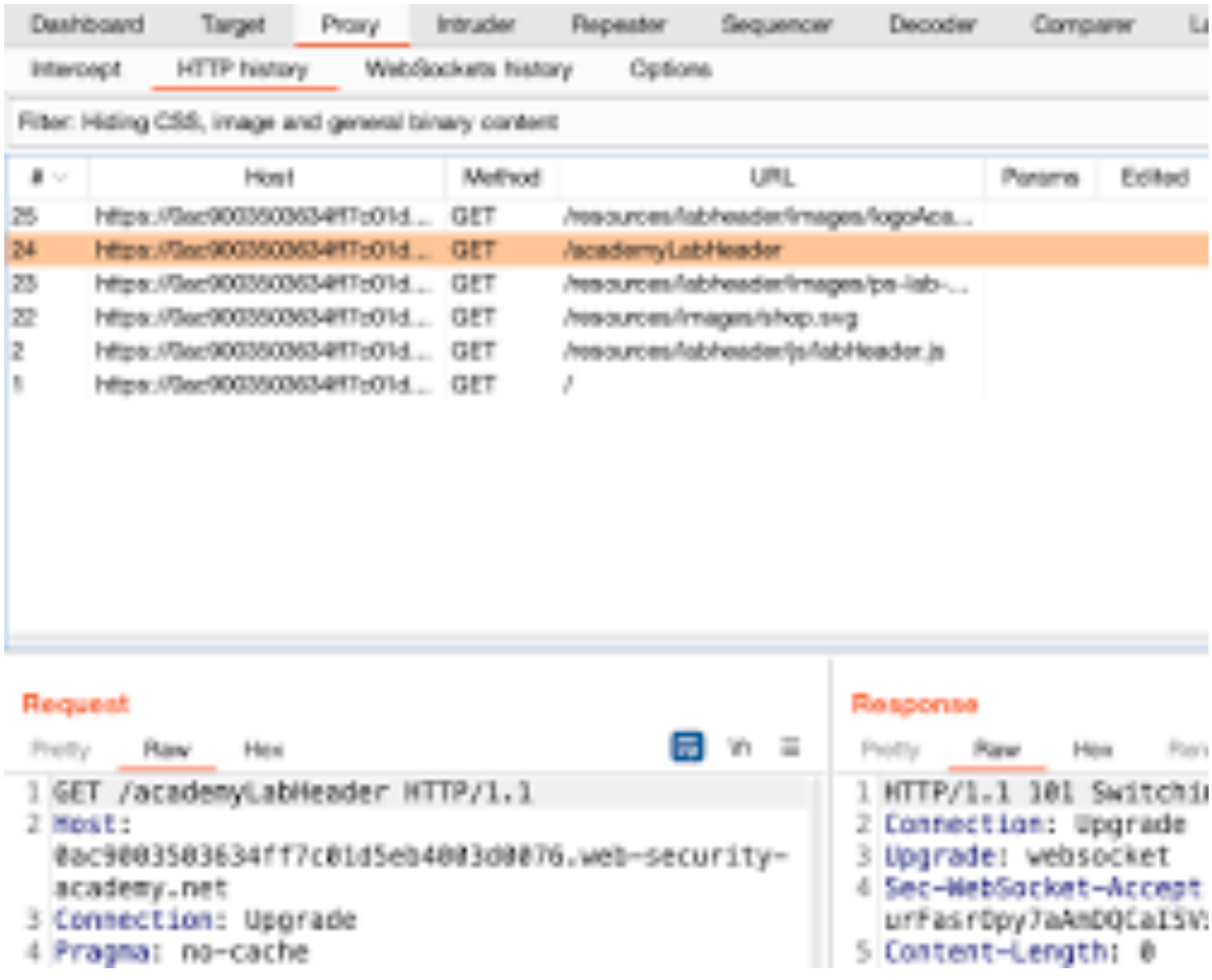
### Conclusion

Burp Suite is a powerful and versatile web application security testing tool. It can be used by security professionals, developers, and bug bounty hunters to identify and exploit vulnerabilities in web applications.

Here are some images of Burp Suite:




Intruder
Repeater
Sequencer
Decoder
Compare
Logging of out-of-scope Proxy traffic
Contents
.67.157/peruggia
cope
nch
his branch
this branch
ols
aps
ost
Method
ttp://172.16.67.157
GET


Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Intercept
HTTP history
WebSockets history
Options
Filter: Hiding CSS, image and general binary content
# Host Method URL Params Edited
25 https://0ac900350363 4ff7c01d... GET /resources/labheader/images/logoAca...
24 https://0ac900350363 4ff7c01d... GET /academyLabHeader
23 https://0ac900350363 4ff7c01d... GET /resources/labheader/images/ps-lab-...
22 https://0ac900350363 4ff7c01d... GET /resources/images/shop.svg
2 https://0ac900350363 4ff7c01d... GET /resources/labheader/js/labHeader.js
1 https://0ac900350363 4ff7c01d... GET /
Request
Pretty Raw Hex
1 GET /academyLabHeader HTTP/1.1
2 Host:
0ac900350363 4ff7c01d5eb4003d0076.web-security-
academy.net
3 Connection: Upgrade
4 Pragma: no-cache
Response
Pretty Raw Hex
1 HTTP/1.1 101 Switchi
2 Connection: Upgrade
3 Upgrade: websocket
4 Sec-WebSocket-Accept
urFasrDpy7aAmDQCaISV
5 Content-Length: 0