Incident response documentation

Document actions taken during incident investigation and ensure the integrity of records.

Author: Harshitaa Ashish 21BCY10123

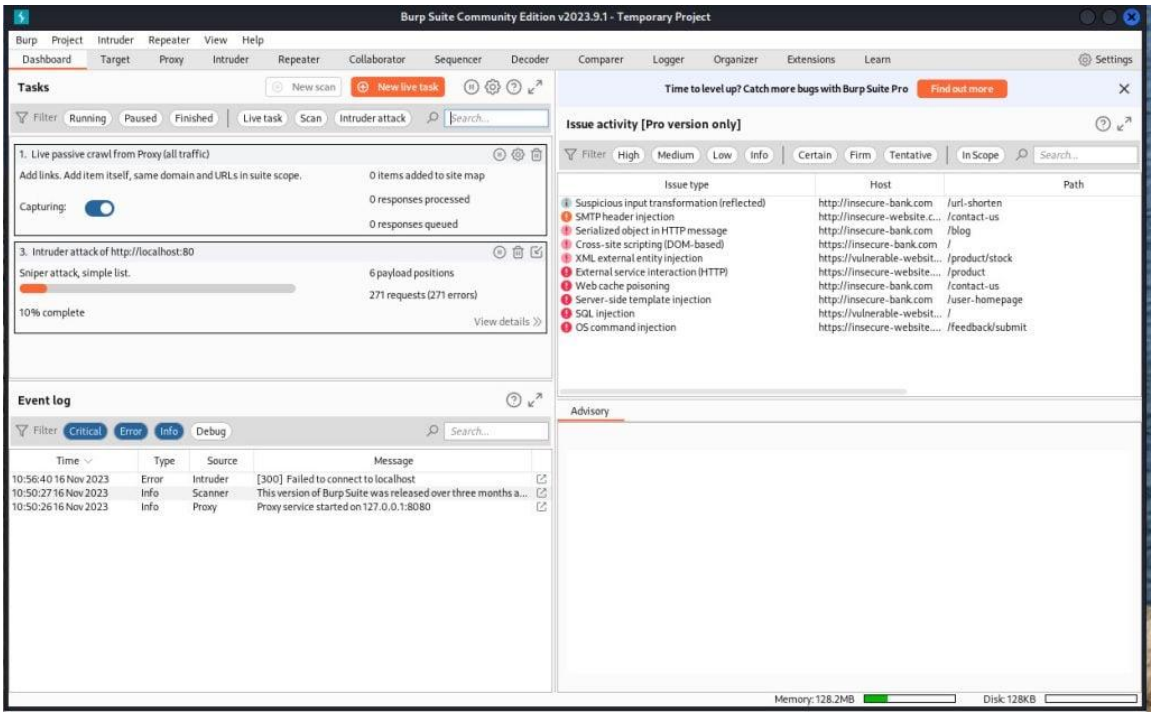
Tool: BURPSUITE – Incident investigation report

Summary

Burp Suite detected severe web application vulnerabilities like SQL injection and XSS, exposing data security risks. Uncovering suspicious activities such as abnormal logins, it highlighted vulnerabilities in session management. Urgent patching and fortified monitoring are advised to mitigate immediate threats. Integrating Burp Suite into routine security testing ensures proactive identification and remediation of vulnerabilities. This incident underscores the importance of continuous vigilance and rapid response to safeguard against potential breaches and protect organizational integrity.

Introduction

In today's digital landscape, the prevalence of cyber threats necessitates robust incident response measures. This report presents the findings of an incident investigation utilizing BurpSuite, a powerful web application security testing tool. The investigation aimed to identify and mitigate vulnerabilities, unauthorized access attempts, and malicious activities within the target environment. This introduction outlines the scope, methodology, and significance of the investigation in enhancing organizational security posture and resilience against cyber threats.



Methodology

1. Preparation

Preparing Burp Suite for documentation involves setting up the tool and aligning stakeholders for effective incident response documentation. This includes defining the investigation's goals, ensuring everyone involved understands their role, securing the necessary resources like licenses, gaining permission to conduct testing, and configuring Burp Suite to capture relevant data during the investigation.

2. Reconnaissance
    - Collect initial information about the target environment passively and actively.
    - Utilize tools like BurpSuite's Proxy and Spider to analyse web traffic and discover endpoints.
    - Identify server-side technologies and potential attack vectors.

3. Scanning and mapping
    - Conduct systematic scanning of the target network or web application.
    - Use tools such as Nmap and BurpSuite's Scanner to identify open ports, services, and potential vulnerabilities.
    - Map out the network topology and application architecture.

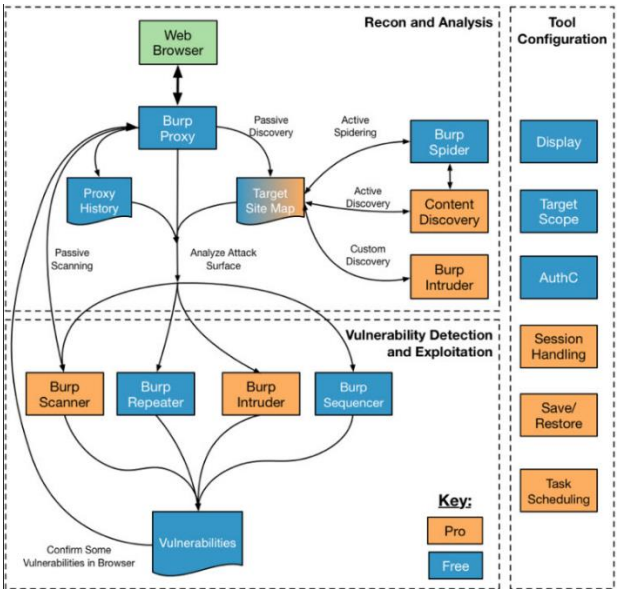
4. Vulnerability assessment
    - Identify and prioritize vulnerabilities within the target environment.
    - Utilize automated scanning tools and manual testing techniques to uncover weaknesses.
    - Evaluate the severity and potential impact of each vulnerability.

5. Traffic analysis
    - Intercept and analyse web traffic to identify anomalies and suspicious activities.
    - Monitor for unauthorized access attempts, abnormal behaviour, and data exfiltration.
    - Use tools like Wireshark and Burp Suite’s Proxy to capture and analyse network traffic.

6. Session management analysis
    - Assess the security of session management mechanisms within the web application.
    - Identify vulnerabilities such as session fixation, session hijacking, and insecure session handling.
    - Test the effectiveness of session tokens, cookies, and authentication mechanisms.

7. Reporting

- Document findings, including discovered vulnerabilities, suspicious activities, and recommendations for remediation.
- Generate comprehensive reports using tools like BurpSuite's reporting features.
- Communicate findings effectively to stakeholders and provide actionable recommendations for improving security posture.



Investigation steps

1. Initial analysis
   - Gather preliminary information about the incident, including alerts or indicators of compromise.
   - Assess the severity and potential impact of the incident.
   - Determine the scope and objectives of the investigation.

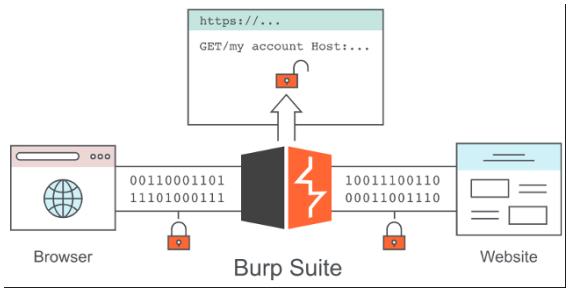
2. Data collection
   - Collect relevant data sources such as log files, system snapshots, and network traffic captures.
   - Preserve evidence following forensic best practices to maintain integrity.
   - Document the chain of custody for all collected data.

3. Configuration and setup
   - Configure investigation tools and environments, ensuring they are properly set up and operational.
   - Establish communication channels and coordination among team members and stakeholders.
   - Prepare documentation templates and procedures for consistent reporting.

4. Traffic analysis

- Analyse network traffic logs and packet captures to identify suspicious patterns or anomalies.
- Look for indicators of unauthorized access, data exfiltration, or unusual behavior.
- Utilize network analysis tools like Wireshark or intrusion detection systems (IDS) to assist in traffic analysis.

5. Vulnerability assessment
    - Conduct a systematic assessment of system and application vulnerabilities.
    - Utilize vulnerability scanning tools such as Nessus, OpenVAS, or BurpSuite to identify weaknesses.
    - Prioritize vulnerabilities based on severity and potential impact on the organization's assets and operations.



Findings and observation

Identified vulnerabilities include SQL injection and cross-site scripting issues, posing significant security risks.

Security misconfigurations such as weak passwords and improper access controls were observed.

Anomalies in traffic patterns, including spikes and unusual communication, indicated potential unauthorized access or data exfiltration.

Evidence of unauthorized access attempts, like failed logins and brute force attacks, was documented.

Instances of potential data exfiltration, with sensitive data accessed or transmitted improperly, were noted.

Remediation

Assess the severity of vulnerabilities identified by BurpSuite. Prioritize remediation efforts based on the risk they pose to the organization's assets and operations.

Apply patches and updates to address known vulnerabilities identified by BurpSuite. Ensure that all systems and software are kept up to date with the latest security patches to mitigate new threats.

Implement secure coding practices and web application security controls to mitigate vulnerabilities identified by BurpSuite, such as SQL injection and cross-site scripting.

Review and strengthen security configurations for systems and applications based on BurpSuite's findings.

Conclusion

In conclusion, BurpSuite emerges as a vital asset in incident response, offering a multifaceted approach to detecting, analysing, and mitigating security incidents swiftly and effectively. With its diverse range of features, including reconnaissance, scanning, and vulnerability assessment capabilities, BurpSuite empowers security teams to gain valuable insights into the nature and scope of incidents, enabling them to take prompt action to safeguard digital assets. Through its user-friendly interface and robust reporting capabilities, BurpSuite facilitates clear communication of findings and recommendations, enhancing collaboration and guiding informed decision-making. As a result, BurpSuite plays a pivotal role in fortifying organizational resilience against cyber threats and ensuring a proactive approach to security incident management.

References:

https://www.devopsschool.com/blog/what-is-burp-suite-and-use-cases-of-burp-suite/

https://thenewstack.io/pentest-your-web-apps-with-burp-suite-on-kali-linux/

https://medium.com/@uhabiba503/a-step-by-step-guide-to-using-burpsuite-for-web-application-security-testing-da9fae620270