Red Team Report

Group – Sigma

Team Members

1) Shivam Dayama (0850964)
2) Jishnu ( )
3) Shreeji Ashokbai Patel ( )

Executive Summary

This report details the results of a Red Team exercise carried out on six different websites. The main goal was to assess the security of each site by simulating actual cyber attacks to find vulnerabilities. Key findings revealed significant security flaws, weaknesses in incident response, and areas where security measures can be enhanced. The report offers an in-depth analysis of the attack methods, the vulnerabilities that were exploited, and suggestions for reducing these risks.

URL'S we used to perform the test were :

1) .
2) .
3) .
4) .
5) .
6) .

Methodology and Approach

The Red Team exercise was carefully planned to assess the security of each target site. The process included several phases: gathering initial information, analyzing potential vulnerabilities, exploiting those weaknesses, assessing the extent of the breach, and finally, documenting the findings and recommendations. The approach included the following phases:

- Reconnaissance : Collecting information through open-source intelligence (OSINT) and active scanning.

- Attack Surface Analysis : Identifying potential entry points and vulnerabilities.

- Exploitation : Using various tools and techniques to exploit the identified vulnerabilities.

- Post-Exploitation : Assessing the extent of access, moving laterally within the network, and extracting sensitive data.

- Reporting : Documenting findings, assessing impacts, and providing recommendations.

Tools Used

- NMAP : For network mapping and port scanning.

- Metasploit : For automated exploitation and post-exploitation tasks.

- Hydra : For brute-force attacks on login credentials.

- John the Ripper : For password cracking.

This structured approach provided valuable insights into the security weaknesses of the target sites and led to actionable recommendations to improve their defenses.

Attack Surface Analysis

During our Attack Surface Analysis, we thoroughly examined the security status of each website to understand their vulnerability to potential cyber threats:

- We used tools like Nmap and DNS enumeration to gather essential information about IP addresses and server hosting details. This data is critical for attackers seeking to exploit specific server vulnerabilities.
- Our investigation uncovered multiple open ports, including HTTP (port 80), HTTPS (port 443), FTP (port 21), and SSH (port 22). These open ports expose the

websites to risks such as brute force attacks, exploitation of service vulnerabilities, and unauthorized access attempts.

- Many of the websites lacked a Web Application Firewall (WAF), leaving them susceptible to common web-based attacks like SQL injection, cross-site scripting (XSS), and distributed denial-of-service (DDoS) attacks.
- We carefully reviewed SSL/TLS configurations to identify any potential weaknesses. Inadequate SSL/TLS settings can expose sensitive data to interception and man-in-the-middle attacks.
- Additionally, vulnerability scans and penetration testing were conducted to detect and exploit potential weaknesses. This involved identifying unpatched vulnerabilities and misconfigurations that could be exploited by malicious actors to gain unauthorized access and compromise system integrity.

In essence, our analysis aimed to uncover vulnerabilities that could compromise the security and integrity of the websites, providing insights crucial for enhancing their defenses against cyber threats.

Site	Entry Points	Vulnerabilities Identified	Severity
Site 1	5	7	High
Site 2	3	5	Medium
Site 3	6	9	High
Site 4	4	6	Medium
Site 5	8	10	Critical
Site 6	7	8	High

Incident Response and Detection Analysis

During the Red Team exercise, we conducted a comprehensive assessment of the incident response and detection capabilities across all six sites to gauge their preparedness against simulated cyber threats.

Site	Detection Mechanisms	Response Time	Effectiveness
Site 1	Limited	45 mins	Poor
Site 2	Limited	1 hour	Poor
Site 3	Moderate	20 mins	Fair
Site 4	Moderate	25 mins	Fair
Site 5	Limited	30 mins	Poor
Site 6	Good	15 mins	Good

Overall, our findings underscore the critical importance of robust incident response and detection capabilities in safeguarding against cyber threats. Recommendations for all sites will focus on enhancing detection tools, reducing response times, and implementing proactive security measures to strengthen their overall security posture and resilience against evolving cyber threats.

Exploited Vulnerabilities