Security Scanning of Web Application

Introduction:

Security scanning of web applications is a critical component of modern cybersecurity practices. As businesses and individuals increasingly rely on web-based services, the need to protect sensitive data and ensure the integrity of online platforms has never been greater. Web application security scanning is a proactive approach to identifying and addressing vulnerabilities and threats that could compromise the confidentiality, availability, or integrity of web applications.

This process involves the systematic examination of web applications, both from a code and runtime perspective, to uncover potential weaknesses that malicious actors could exploit. These vulnerabilities may include issues like SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and many others.

The primary goals of security scanning for web applications are:

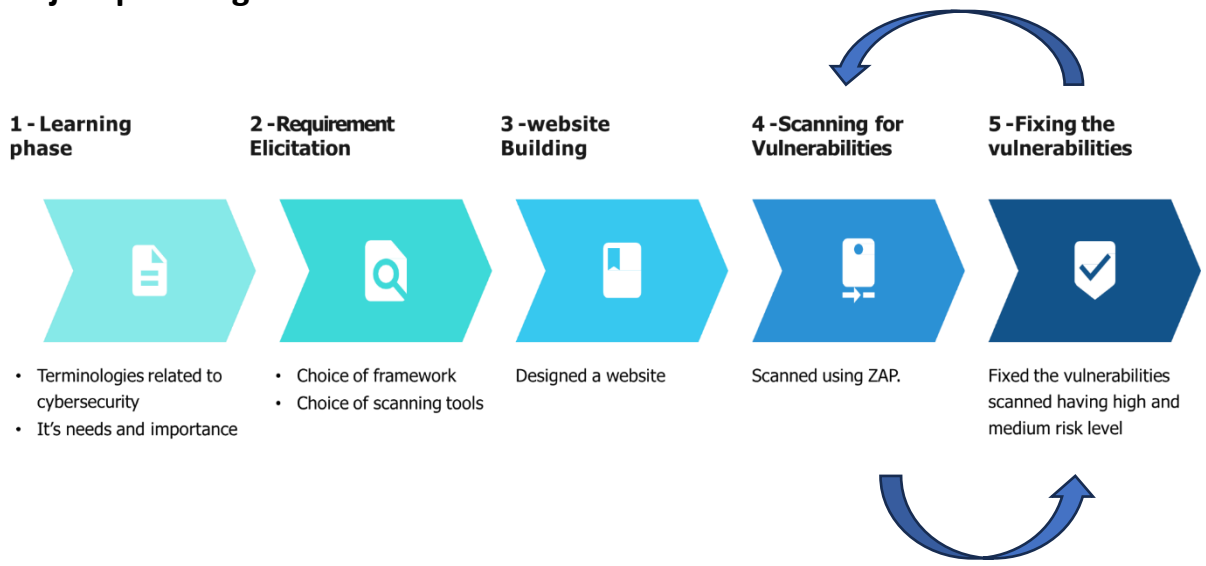
- **Vulnerability Detection**: Identifying and assessing vulnerabilities within the application code, configuration, and infrastructure that may be exploited by attackers.
- **Risk Assessment**: Evaluating the severity and potential impact of identified vulnerabilities to prioritize remediation efforts.
- **Compliance**: Ensuring that the web application complies with industry standards, regulations, and security best practices.
- **Continuous Monitoring**: Implementing ongoing scanning and monitoring to detect new vulnerabilities that may arise as the application evolves.
- **Protection**: Preventing security breaches and data breaches by proactively addressing vulnerabilities before they can be exploited by cybercriminals.

Security scanning techniques can vary and may include automated tools, manual testing by ethical hackers (penetration testing), code review, and configuration audits. The results of these scans provide valuable insights to developers, system administrators, and security teams, enabling them to fix vulnerabilities, strengthen defences, and ultimately safeguard web applications from potential threats.

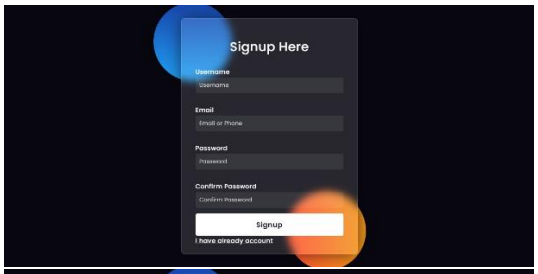
Technology Used:

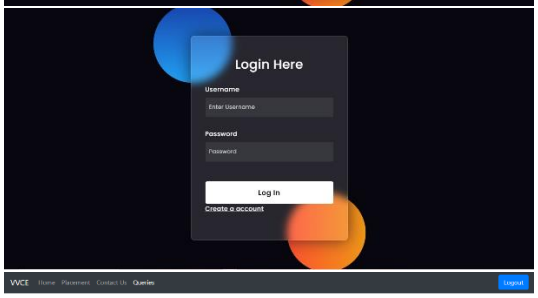
1. **Bootstrap**: It is a popular open-source front-end framework for building responsive and visually appealing web applications, providing pre-designed CSS and JavaScript components for streamlined web development.
2. **Django**: It is an open-source web framework that follows the Model-View-Controller (MVC) architectural pattern and promotes rapid development of web applications with built-in features like an ORM (Object-Relational Mapping), authentication, and templating.
3. **ZAP Scanning Tool**: ZAP (Zed Attack Proxy) is an open-source web application security scanning tool used for identifying vulnerabilities and potential security issues in web applications through automated and manual testing techniques. It helps developers and security professionals proactively assess and improve the security of web applications.

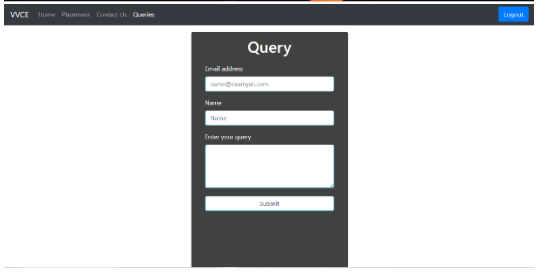
Project planning:

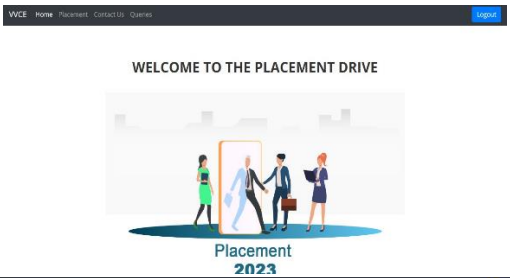


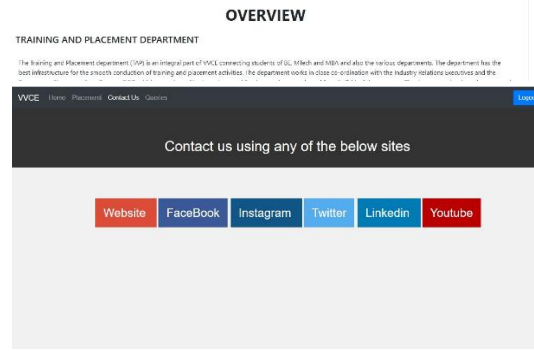
Website Snapshots:











Vulnerabilities Found:

Alerts

Name	Risk Level	Number of Instances
SQL Injection - SQLite	High	1
Absence of Anti-CSRF Tokens	Medium	8
Content Security Policy (CSP) Header Not Set	Medium	11
Cross-Domain Misconfiguration	Medium	1
Missing Anti-clickjacking Header	Medium	8
Cookie Without Secure Flag	Low	1
Strict-Transport-Security Header Not Set	Low	14
X-Content-Type-Options Header Missing	Low	11
Re-examine Cache-control Directives	Informational	8
Retrieved from Cache	Informational	2
User Agent Fuzzer	Informational	192

After Removing Vulnerabilities:

Alerts

Name	Risk Level	Number of Instances
Strict-Transport-Security Header Not Set	Low	6
X-Content-Type-Options Header Missing	Low	2
Re-examine Cache-control Directives	Informational	3
User Agent Fuzzer	Informational	228

Conclusion:

In conclusion, security scanning of web applications is an integral part of modern cybersecurity strategies. It not only protects organizations from potential threats but also demonstrates a commitment to the security and privacy of users and customers. To ensure the effectiveness of security scanning, it should be integrated into the development lifecycle and regularly updated to address evolving security challenges.