QASOURCE
Quality That Creates Value

CASE STUDY
Security Testing

The Challenge

Web application security testing is critical to ensure the security and reliability of web-based applications. Being a large size company, the customer possesses a large database of sensitive data including customer data and PII information which is an appealing target for hackers. To ensure that the existing security measures are effective enough to protect all the assets from unauthorized access, the customer decided to evaluate the level of security to eliminate any existing security issues.

Our Solutions

An expert team of security testing specialists was assigned to this project. All the sensitive areas were included in the scope and the team followed a four-step process:

- **Reconnaissance:** The team started by gathering information about the application and its environment. This includes identifying web server type, web application framework, database, and API.
- **Vulnerability Scanning:** In this step, a mix of tools was used to do different kinds of security scans and identify the loopholes in the application.
- **Exploitation:** Here, security engineers attempted to exploit any vulnerabilities identified in the previous steps. This involved attempts to gain unauthorized access to the application or its underlying systems or to escalate privileges.
- **Reporting:** Finally, the team documented all the identified vulnerabilities and provided recommendations for remediation. The report includes a description of the vulnerabilities, their potential impact, and a recommendation on ways to mitigate them.

About Our Client

The client is a leading tire manufacturer, whose focus is to develop and manufacture a diverse portfolio of tires that deliver social and customer value. Being an industry leader in transportation, the client has a large fleet of software deployed that they use for different operations. They excel at best-in-class offerings to consumers around the world.

Industry
Transportation

QASOURCE
Quality That Creates Value

The Results

The penetration testing identified several vulnerabilities in the application, including:

- **SQL injection vulnerability:** The application was found to be vulnerable to SQL injection attacks, which could allow an attacker to access the database and steal sensitive information.
- **Cross-site scripting (XSS) vulnerability:** The application was also found to be vulnerable to XSS attacks, which could allow an attacker to execute malicious code in the user's browser.
- **DOS - Denial-of-Service:** Testers were able to send thousands of requests from a single source resulting in taking down the application for some time which leads to financial losses, and reputational damage.
- **Unauthorized access to the application:** The application was also found to be vulnerable to unauthorized access resulting in security breaches, data leaks, unauthorized modifications, and other malicious activities that can compromise the confidentiality of the application.

Based on the results of the penetration testing, the following recommendations were made to the client:

- Implement input validation to prevent SQL injection attacks.
- Implement measures to prevent XSS attacks, such as input filtering and output encoding.
- Implement a stronger password policy, requiring users to choose complex passwords and enforcing password expiration policies.

Conclusion

The penetration testing was successful in identifying several vulnerabilities in the web application. By addressing these vulnerabilities, we improved the security of the application and protect sensitive information.

To speak with a specialist, please visit qasource.com