ENTERSOFT SECURITY

CASE STUDY

DELIVERING ABSOLUTE SECURITY, FAST

With estimated worldwide cyber crime losses each year touching $400 billion, it is of high importance for corporations, both large and small, to focus considerable attention towards the security of their physical infrastructures as well as their outward facing web applications

01 ABOUT

The client is a global logistics company headquartered in Kuwait. They provide freight forwarding, transportation, warehousing and supply chain management services to businesses, governments, international institutions and relief agencies worldwide. Client's primary business is commercial logistics.

02 THE CHALLENGE

Client wanted to launch a new product in Malaysia. For it to be considered 'protected' by the federal agencies, the product needed to pass vigorous tests performed by them.

After initial testing, the client was asked to redesign the product as it was not considered secure by the authorities. In addition to that, the client required a security audit to be completed by a third party, in this case, Entersoft.

03 HIGHLIGHTS

- High urgency in terms of delivery.
- Tremendous financial risk involved, if stored data was to be compromised.
- An evaluation of the application as well as conversations with the owners and developers of the web application provided detailed insights into the risk factors associated with the application.
- 3 parties performed Penetration Testing on the same application. Client's in-house team of 40 security experts and the Malaysian Authorities uncovered 13 vulnerabilities. Entersoft found 28 more.
- Each module was tested by 4 or more hackers to ensure each and every bug was found.
- Each bug found was fixed in under an hour. Instantaneous support was provided by a Project manager assigned by the client.
- Software developers (skilled in standard and security development techniques) reviewed the remediated software to assure the quality of the repair and verify no additional security flaws had been introduced.
- A retest verified the repair of the high-risk flaws as well as the fact that no additional vulnerabilities had been introduced.
- While security tests pointed out numerous critical security flaws, the immediate need was to identify those flaws that might be considered high-risk. These flaws were selected because of the relative ease of a successful security attack and the ‘protected’ status of the data that would be compromised.

04 QUICK OVERVIEW

Half a Million

Lines of code to be reviewed

1 Week

Time allotted to complete the audit

3 Sides

Performing Penetration Testing for the same app

28

Vulnerabilities pointed out by Entersoft in addition to the 13 uncovered by the client and federal authorities

1 Hour

Maximum time taken to fix a bug once it was identified

4 <

White Hat Hackers assigned to test each module

04 THE PROCESS

Automated Vulnerability Scanning

Automated security scanning tools are designed to simulate security attacks on targeted web applications. These scanners run a simulation of every known web application attack (updated frequently to keep pace with recently discovered security attack methods) over the entirety of the web application.

Manual Testing

Professional cyber criminals will often spend hours or days probing a web application for security flaws. Entersoft's white hat hackers will use the same skills and persistence to identify the same flaws, except with the goal of remediating the flaws, not compromising the data.

Code Review

While the majority of security testing can be done from the browser-side (automated scanning and manual reviews), a security code review will discover security issues that manifest themselves only after a web application has been compromised.

05 VULNERABILITIES FOUND / RESULTS

Owing to the urgency of the engagement, the client insisted that all found vulnerabilities were to be marked high

Null Byte Injection

Null Byte Injection is an exploitation technique which uses URL-encoded null byte characters (i.e. , or 0x00 in hex) to supplement the user-supplied data. This injection process can alter the intended logic of the application and allow malicious adversary to get unauthorized access to the system files.

User Session Recreation

Attacker could intercept user traffic and steal the user active session cookies to recreate the user active session and login to the application without authentication.

Response Caching

Unless directed otherwise, browsers may store a local cached copy of content received from web servers. If sensitive information in application responses is stored in the local cache, then this may be retrieved by other users who have access to the same computer at a future time.

Insecure HTTP Request Cookies

Application was using insecure request cookies. By adding additional HTTP headers like content type filtering, xss, http only and session cookie variables, the server can be protected from various threats.

CSRF Vulnerability

Implementing a CSRF token for every action makes the application more secure. CSRF is a vulnerability in which the attacker will try to trick the user to perform an action without the user's knowledge.

Date Boundary Validation

The database accepted expiry date value without validation.

In our test case we sent a date which is below the minimum value (1899) and the server accepted the value.

Database Allowing Duplicate Data

We observed a scenerio wherein a user could add multiple individuals or organisations with the same information.

Time Based SQL Injection

When the value of a cookie parameter was replaced with a time based SQL query, we observed a time delay that was specified in the payload.

The time based SQL queries results in the improper functioning of the database server.

Remote File Inclusion

The application had an upload functionality where the users could upload security documents.

An attacker could trick the web application to allow uploading malicious code in any file format. We were able to upload .exe and .jsp files.

BANGALORE

+91 80 4150 1408
info@entersoftsecurity.com
www.entersoftsecurity.com

BRISBANE

+61 7 3376 9381
info@entersoft.com.au
www.entersoft.com.au

SINGAPORE

+65 6519 0757
info-sg@entersoftsecurity.com
www.entersoftsecurity.com