TFT
think future technologies

Application Security Program for RSSOFT Client

Process Overview and Case study

Share your website/application with us & your security concerns.
Our consultants will perform a pilot scan and will get back to you with minimum 2 critical security gaps -> **www.tftus.com**

We have been helping companies across different industries uncover critical bugs.

About

Client is a global logistics company headquartered in India. They provide freight forwarding, transportation, warehousing and supply chain management services to businesses, governments, international institutions and relief agancies worldwide.

Challenges

- ✓ Client wanted to launch a new product in USA. The product needed to pass vigorous tests in order to comply with standards of the federal agencies.
- ✓ After initial testing, client was asked to redesign the product as it was not considered secure by the authorities. In addition to that, the client required to perform a third party security audit.

Key Highlights

Half a Million
Lines of code reviewed

4 Weeks
Time allotted to complete the audit

3 Sides
Performing penetration testing for the same app

28
Vulnerabilities pointed out by us in addition to the 13 uncovered by 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

Application Security Program for RSSOFT

Highlights

- ✓ High urgency of tasks.
- ✓ Tremendous financial risk involved, if stored data was to be compromised.
- ✓ Lots of evaluation to identify risks involved.
- ✓ 3 parties had performed penetration testing on the same application at same time. Client's in-house team of 40 security experts and the Malaysian Authorities had uncovered 13 vulnerabilities. We found 28 more.
- ✓ Each module was tested by 4 or more hackers.
- ✓ Each bug found was fixed in an hour.
- ✓ Reviewed remediated software to assure quality of the repair and verify no additional flaws had been introduced.

Security Program for RSSOFT

think future technologies

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 inauthorized 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 attackers will try to trick the user to perform an action without the users knowledge.

Data 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 scenario wherein a user could add multiple individuals or organizations with the same information.

Time Based SQL Injection

When the value of a cooker 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.

Share your website/application with us & your security concerns.

Our consultants will perform a pilot scan and will get back to you with minimum 2 critical security gaps. -> **www.tftus.com**