Executive Summary Report

AppScan: Web Application Security Report

Table of Contents

Document Map 3

Introduction 4

Objectives 4

Executive Summary 5

Number of Issues (Total 203) 5

Numbers of Issues by Test Type 6

Vulnerable vs. Non-vulnerable URLs 9

Number of Remediation Tasks 10

Detailed Summary 11

Issue Types 11

Remediation Tasks 12

Vulnerable URLs 13

Document Map

This report consists of the following sections:

* **Introduction and Objectives**General information about the scan, including the project name, purpose of the scan, etc.
* **Executive Summary**   
  A high level view of the information gathered during the scan, usually using graphs or comparative numbers.This section is meant to provide a general understanding of the security status of the application.
* **Detailed Summary**  
  A detailed listing of the scan results, including all issue types found, all remediation tasks recommended, all vulnerable URLs, etc.This section is meant to provide a more detailed understanding of the security status of the application, as well as assist in scoping and prioritizing the work required to remedy the issues found.

Introduction

This report holds the results of a web application security scan performed on the [Assignment Name] application by the [Company Name] security team.The scan revealed 32 high severity security issues, 36 medium severity issues and 107 low severity issues in this application. The findings have been consolidated for this Executive Summary and Detailed Summary. Additional information is contained within the Detailed Vulnerability Information section of this report.

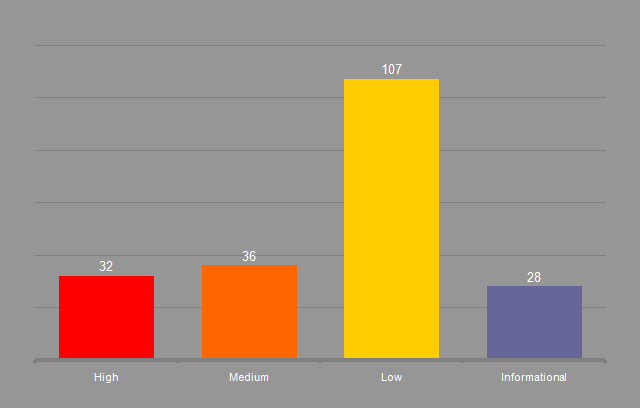
Objectives

The [Company Name] security team performs realtime security assessments on web applications. These assessments aim to unconver any security issues in the scanned web application, explain the impact and risks associated with the found issues, and provide guidance in the prioritization and remediation steps, The objective of this assignment was to perform controlled attack and penetration activities to assess the overall level of security of the [Assignment Name] web application. The [Company Name] security team was/was not provided with access credentials for the application and/or an overview of the application.This report relates to the testing against the [Assignment Name] application from the perspective of an authorised/unauthorised attacker.

Executive Summary

# Number of Issues (Total 203)

Number of Issues by Severity



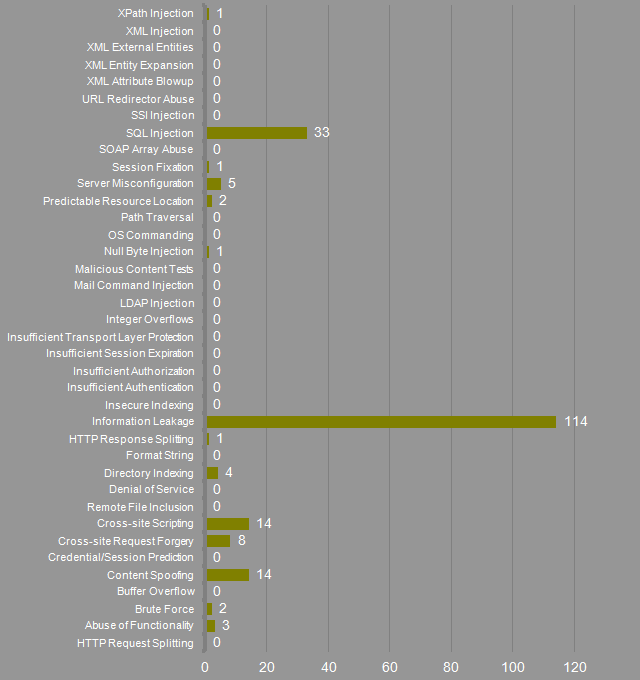
# Numbers of Issues by Test Type

| Type | Vulnerable URL |
| --- | --- |
| Application | 188 |
| Infrastructure | 15 |
| Third-Party Web Components | 0 |
| Total | 203 |

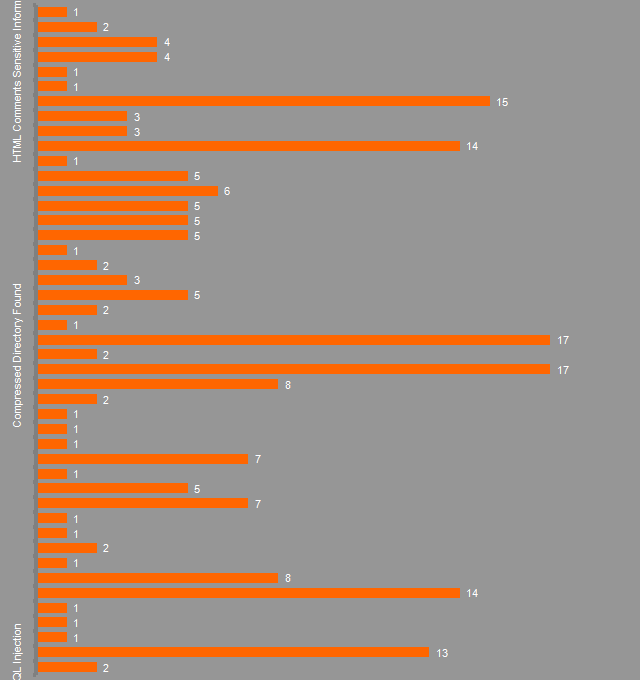
Security Issues by Classification

Security Issues by Issue Type

Security Issues by Threat Classification

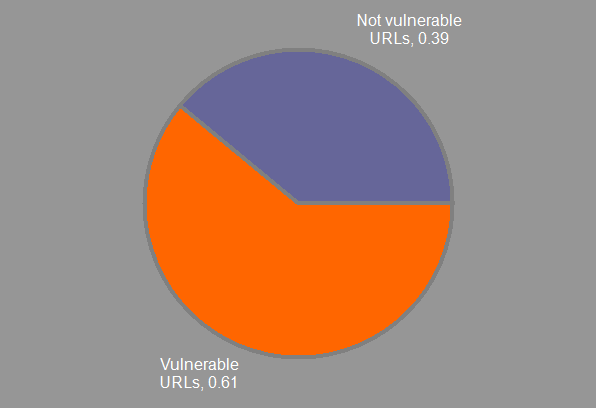


Security Issues by Issue Type



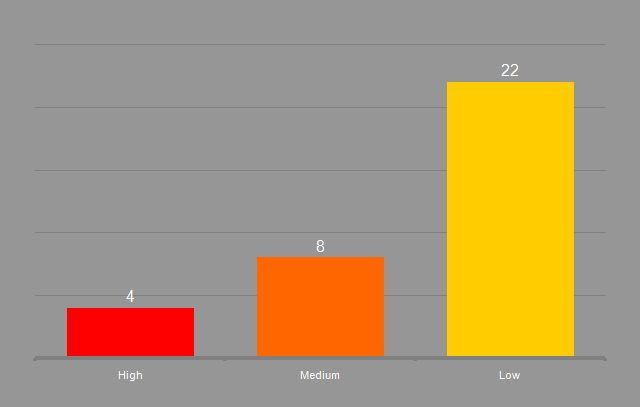
# Vulnerable vs. Non-vulnerable URLs

Vulnerable vs. Non-vulnerable URLs (%)



# Number of Remediation Tasks

Remediation Tasks by Priority



Detailed Summary

# High severity issues

|  | Issue Type | Issues (All Severities) |
| --- | --- | --- |
|  | Blind SQL Injection | 2 |
|  | Cross-Site Scripting | 13 |
|  | DOM Based Cross-Site Scripting | 1 |
|  | Poison Null Byte Windows Files Retrieval | 1 |
|  | Predictable Login Credentials | 1 |
|  | SQL Injection | 14 |

# Medium severity issues

|  | Issue Type | | Issues (All Severities) |
| --- | --- | --- | --- |
|  | Cross-Site Request Forgery | 8 | |
|  | Deprecated SSL Version is Supported | 1 | |
|  | Directory Listing | 2 | |
|  | HTTP Response Splitting | 1 | |
|  | Inadequate Account Lockout | 1 | |
|  | Link Injection (facilitates Cross-Site Request Forgery) | 7 | |
|  | Missing Secure Attribute in Encrypted Session (SSL) Cookie | 5 | |
|  | Padding Oracle On Downgraded Legacy Encryption (a.k.a. POODLE) | 1 | |
|  | Phishing Through Frames | 7 | |
|  | RC4 cipher suites were detected | 1 | |
|  | Session Identifier Not Updated | 1 | |
|  | XPath Injection | 1 | |

# Low severity issues

|  | Issue Type | Issues (All Severities) |
| --- | --- | --- |
|  | Autocomplete HTML Attribute Not Disabled for Password Field | 2 |
|  | Body Parameters Accepted in Query | 8 |
|  | Cacheable SSL Page Found | 17 |
|  | Compressed Directory Found | 2 |
|  | Database Error Pattern Found | 17 |
|  | Direct Access to Administration Pages | 1 |
|  | Directory Listing Pattern Found | 2 |
|  | Encryption Not Enforced | 5 |
|  | Hidden Directory Detected | 3 |
|  | Microsoft ASP.NET Debugging Enabled | 2 |
|  | Missing HttpOnly Attribute in Session Cookie | 1 |
|  | Missing or insecure "Content-Security-Policy" header | 5 |
|  | Missing or insecure "X-Content-Type-Options" header | 5 |
|  | Missing or insecure "X-XSS-Protection" header | 5 |
|  | Missing or insecure Cross-Frame Scripting Defence | 6 |
|  | Missing or insecure HTTP Strict-Transport-Security Header | 5 |
|  | Older TLS Version is Supported | 1 |
|  | Query Parameter in SSL Request | 14 |
|  | Unencrypted \_\_VIEWSTATE Parameter | 3 |
|  | Unsigned \_\_VIEWSTATE Parameter | 3 |

# Informational severity issues

|  | Issue Type | Issues (All Severities) |
| --- | --- | --- |
|  | Application Error | 15 |
|  | Application Test Script Detected | 1 |
|  | Browser Exploit Against SSL/TLS (a.k.a. BEAST) | 1 |
|  | Email Address Pattern Found | 4 |
|  | HTML Comments Sensitive Information Disclosure | 4 |
|  | Possible Server Path Disclosure Pattern Found | 2 |
|  | SHA-1 cipher suites were detected | 1 |

# Remediation Tasks

|  | Remediation Task | Count | Priority |
| --- | --- | --- | --- |
|  | Analyze client side code and sanitize its input sources | 1 | High |
|  | Change the login credentials to a stronger combination | 1 | High |
|  | Ensure that accessed files reside in the virtual path and have certain extensions; remove special characters from user input | 1 | High |
|  | Review possible solutions for hazardous character injection | 42 | High |
|  | Add the 'Secure' attribute to all sensitive cookies | 5 | Medium |
|  | Change server's supported ciphersuites | 1 | Medium |
|  | Change session identifier values after login | 1 | Medium |
|  | Enforce account lockout after several failed login attempts | 1 | Medium |
|  | Implement TLS\_FALLBACK\_SCSV. Additionally, either disable SSLv3 altogether, or disable all cipher suites that operate in CBC mode over SSLv3. | 1 | Medium |
|  | Modify the server configuration to deny directory listing, and install the latest security patches available | 4 | Medium |
|  | Use a different signature algorithm for the certificate. See "Fix Recommentation" for specific server instructions | 1 | Medium |
|  | Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form | 8 | Medium |
|  | Add the 'HttpOnly' attribute to all session cookies | 1 | Low |
|  | Always use SSL and POST (body) parameters when sending sensitive information. | 14 | Low |
|  | Apply proper authorization to administration scripts | 1 | Low |
|  | Config your server to use the "Content-Security-Policy" header with secure policies | 5 | Low |
|  | Config your server to use the "X-Content-Type-Options" header with "nosniff" value | 5 | Low |
|  | Config your server to use the "X-Frame-Options" header with DENY or SAMEORIGIN value | 6 | Low |
|  | Config your server to use the "X-XSS-Protection" header with value '1' (enabled) | 5 | Low |
|  | Correctly set the "autocomplete" attribute to "off" | 2 | Low |
|  | Disable Debugging on Microsoft ASP.NET | 2 | Low |
|  | Do not accept body parameters that are sent in the query string | 8 | Low |
|  | Download the relevant security patch for your web server or web application. | 2 | Low |
|  | Enforce the use of HTTPS when sending sensitive information | 5 | Low |
|  | Implement the HTTP Strict-Transport-Security policy with a long "max-age" | 5 | Low |
|  | Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely | 3 | Low |
|  | Modify the property of each ASP.NET page to sign the VIEWSTATE parameter | 3 | Low |
|  | Modify your Web.Config file to encrypt the VIEWSTATE parameter | 3 | Low |
|  | Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses. | 17 | Low |
|  | Remove e-mail addresses from the website | 4 | Low |
|  | Remove or restrict access to the compressed directory file | 2 | Low |
|  | Remove sensitive information from HTML comments | 4 | Low |
|  | Remove test scripts from the server | 1 | Low |
|  | Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions | 15 | Low |

# Vulnerable URLs

| URL | Issues (Types) | Remediation Tasks (Types) |
| --- | --- | --- |
| https://demo.testfire.net/static/ | 1 (1) | 1 (1) |
| https://demo.testfire.net/admin/application.aspx | 1 (1) | 1 (1) |
| https://demo.testfire.net/admin/admin.aspx | 4 (4) | 4 (4) |
| https://demo.testfire.net/admin/ | 2 (2) | 2 (2) |
| https://demo.testfire.net/pr/ | 2 (2) | 2 (1) |
| https://demo.testfire.net/bank/ws.asmx | 12 (5) | 12 (4) |
| https://demo.testfire.net/bank/transfer.aspx | 25 (15) | 19 (11) |
| https://demo.testfire.net/bank/transaction.aspx | 18 (12) | 18 (11) |
| https://demo.testfire.net/bank/servererror.aspx | 1 (1) | 1 (1) |
| https://demo.testfire.net/bank/queryxpath.aspx | 10 (7) | 9 (6) |
| https://demo.testfire.net/bank/mozxpath.js | 1 (1) | 1 (1) |
| https://demo.testfire.net/bank/main.aspx | 2 (2) | 2 (2) |
| https://demo.testfire.net/bank/login.aspx | 23 (18) | 22 (16) |
| https://demo.testfire.net/bank/customize.aspx | 12 (11) | 9 (8) |
| https://demo.testfire.net/bank/apply.aspx | 7 (7) | 7 (7) |
| https://demo.testfire.net/bank/account.aspx | 9 (7) | 9 (5) |
| https://demo.testfire.net/bank/ | 4 (4) | 4 (3) |
| https://demo.testfire.net/images/ | 2 (2) | 2 (2) |
| https://demo.testfire.net/survey\_questions.aspx | 4 (4) | 4 (4) |
| https://demo.testfire.net/survey\_complete.aspx | 6 (6) | 4 (4) |
| https://demo.testfire.net/subscribe.aspx | 8 (7) | 7 (5) |
| https://demo.testfire.net/security.htm | 1 (1) | 1 (1) |
| https://demo.testfire.net/search.aspx | 5 (5) | 3 (3) |
| https://demo.testfire.net/notfound.aspx | 4 (4) | 2 (2) |
| https://demo.testfire.net/feedback.aspx | 7 (7) | 7 (7) |
| https://demo.testfire.net/disclaimer.htm | 2 (2) | 2 (2) |
| https://demo.testfire.net/default.aspx | 6 (6) | 6 (6) |
| https://demo.testfire.net/comment.aspx | 6 (5) | 4 (3) |
| https://demo.testfire.net/Privacypolicy.aspx | 2 (1) | 2 (1) |
| https://demo.testfire.net/ | 16 (15) | 13 (12) |