SOFTSEQ

Phone/Fax: +1.307.31.65.777
E-mail: security@softseq.com
Visit us at www.softseq.com

Compliance Audit Report

OWASP
Application Security Verification Standard
version 3.0.1, Level 2

Object of Audit: {product}

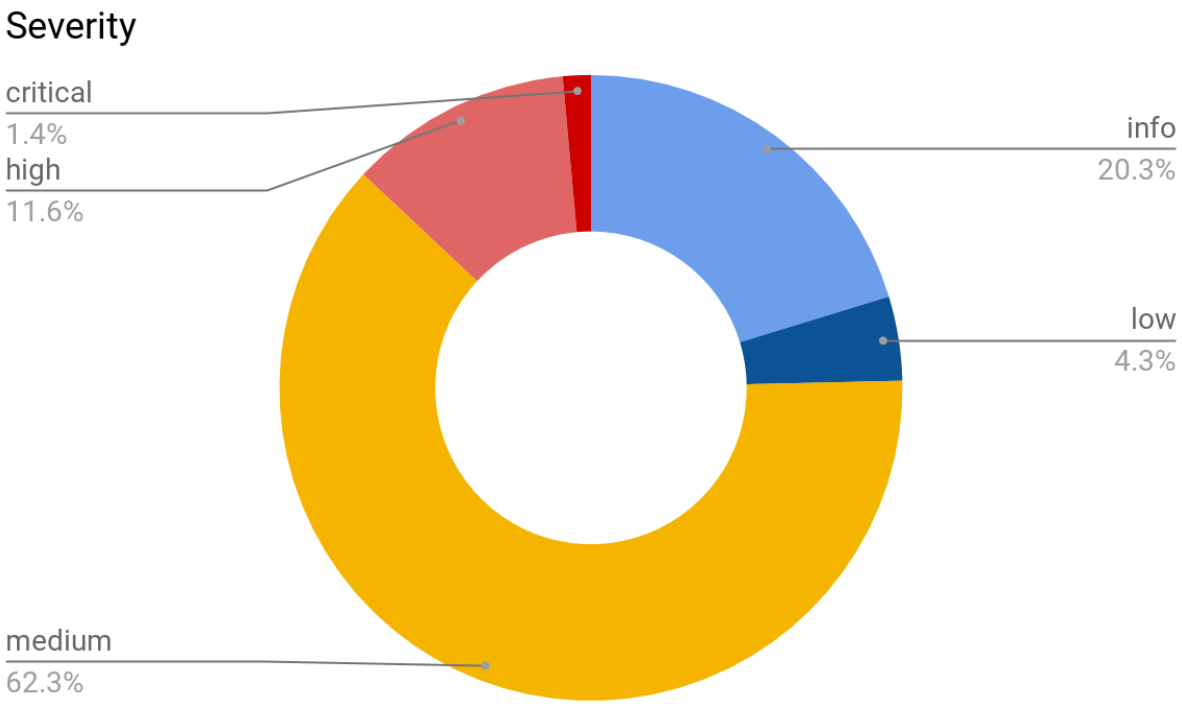
ver. 28250:853eec989233

Customer: {customer}

Date of issue: May 16th, 2018

Executive summary - audit findings

69 vulnerabilities were found. They are charted below by impact, calculated via CVSS standard:



3 examples of identified issues:

Instruction injections

> A way was found to download any files from {product} media server, including system files. This could allow a hacker to steal {product} users' data and obtain direct access to the media server.

Broken Access Control

> A way was found to modify other companies and users' data, to compromise accounts completely, and steal marketing strategies or users' personal data.

Cross-site scripting

> A way was found to inject hacker-supplied code in {product} application. An attacker could craft code to send him {product} users' data, perform unauthorized actions, and disclose passwords.

All identified issues have been fixed, and all fixes re-tested to ensure robustness of the final solution.

Detailed technical audit findings breakdown is available in Appendix B.

Introduction

{customer} retained the services of the SoftSeq LLC to perform application security audit of {customer} {product} solution according to the requirements of OWASP Application Security Verification Standard 3.0.1.

This document describes the timing, scope and methodologies taken during the security assessment and audit.

The assessment relies on information gathered from Q&A, additional meetings with technical staff, project's documentation, as well as on the results of manual and automatic testing of specific threat scenarios. It included theoretical and practical assessment methodologies, best practices used to mitigate potential threats and techniques of attacks performed by a malicious entity (e.g. hacker, internal attacker, spyware, virus, etc.).

OWASP ASVS 3.0.1 Level 2 had been chosen as an audit baseline, and is a superset of:

- OWASP Top 10 issue classes
- CWE-25
- PCI DSS technical requirements to security of developed applications

Security Assessment Objectives

The main objective of the security assessment was to perform an in-depth security review in order to identify security vulnerabilities in the application level that may jeopardize {customer} customers' systems and customers' information.

To this end, requirements of OWASP Application Security Verification Standard 3.0.1 Level 2 were strictly adhered to.

Other objectives include:

- Verifying that authentication & authorization controls are implemented properly in the application.
- Inspecting business logic at the design and implementation levels.
- Detecting security vulnerabilities at the application level, which could potentially jeopardize {customer} customers' systems and data that is processed and/or stored in {product}.
- Reviewing the security practices used in configuration of the databases, application servers, and other application-supporting components, modules, or integrated third party components.
- Providing mitigating controls for secured design, implementation and configuration of the product.

The Assessment Phases

The security assessment was performed by a team comprised of application security experts, and included the following activities:

1. Analysis of the product structure, interfaces, data flow, sensitive modules, infrastructure and architectural aspects, reliance on third party products or interfaces, and identifying classes of vulnerabilities.

2. Information gathering from various sources - human and technological. This included communicating with both technical people and management.
3. Hands-on testing of the product in various scenarios, with respect to previously obtained knowledge of the product and its data flow scenarios.
4. Analysis of gathered data and results from the previous security assessments. The analysis includes categorizing the detected vulnerabilities and prioritizing them according to the business and technical context of the application.
5. A final and comprehensive report of the security review activity, summarizing the entire review process, the methodology and the detailed findings.

The Assessed Components and Areas

The security assessment was based on the results of threat modeling and risk assessment (evaluated based on an unauthorized activity of both a legitimate user and a non-legitimate user).

SoftSeq security assessment addressed the review of security controls in different product layers such as the application architecture, design, implementation and secure deployment. The following product areas and mechanisms were assessed according to OWASP ASVS Level 2 categories:

ASVS Category	ASVS checks done	ASVS checks not applicable	Compliance status
V1. Architecture, design and threat modelling	1, 2, 3, 7, 8, 9, 10, 11		Compliant
V2: Authentication	1, 2, 4, 6, 7, 8, 9, 12, 13, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 31, 32, 33		Compliant
V3: Session Management	1, 2, 3, 4, 5, 6, 7, 10, 11, 12, 16, 17, 18		Compliant
V4: Access Control	1, 4, 5, 8, 9, 10, 12, 13, 14, 15, 16		Compliant
V5: Malicious input handling	1, 3, 5, 10, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26	11	Compliant
V7: Cryptography at rest	2, 6, 7, 9, 12, 13, 14		Compliant
V8: Error handling and logging	1, 2, 3, 4, 5, 6, 7, 10, 13		Compliant
V9: Data protection	1, 3, 4, 5, 7, 9, 10, 11		Compliant

V10: Communications security	1, 3, 6, 10, 11, 13, 14, 15, 16		Compliant
V11: HTTP security configuration	1, 2, 3, 4, 5, 6, 7, 8		Compliant
V13: Malicious controls	-		N/A
V15: Business logic	1, 2		Compliant
V16: Files and resources	1, 2, 3, 4, 5, 6, 7, 8, 9		Compliant
V17: Mobile	-		N/A
V18: Web services	1, 2, 3, 4, 5, 6, 8, 9, 10	7	Compliant
V19. Configuration	1, 2, 3	4, 5	Compliant

Each area/component was reviewed and inspected for potential and actual security flaws that might allow various attacks by external attackers, internal attackers or malicious system users, such as, but not limited to:

- Unauthorized access to sensitive information
- Unauthorized modifications of information
- Unauthorized deletion of information
- Unauthorized handling of audit information
- Performance of unauthorized operations or transactions
- Illegal or unauthorized impersonation to different users or entities
- Performance of unauthorized operations that may affect system's SLA
- Performance of unauthorized operations that may cause total DoS
- Exploitation of existing security controls to perform fraudulent activities

For a complete list of security requirements audited in scope of this engagement, please refer to OWASP Application Security Verification Standard 3.0.1, Level 2.

Audit Results

A number of corrective actions have been identified to resolve noncompliance of {customer} {product} with OWASP ASVS 3.0.1 Level 2 requirements.

The security audit findings were communicated by SoftSeq LLC to {customer} Software Architect and development team via a dedicated project tracking tool (Jira).

{customer} has taken meaningful steps to remediate all findings in order to improve the system's security posture, and eliminate noncompliance with OWASP ASVS 3.0.1 Level 2 requirements.

{customer} {product} version 28250:853eec989233 has been verified to comply with all OWASP ASVS 3.0.1 Level 2 requirements.

Limitations

The SoftSeq security engagement was based on past experiences, available information, and known threats at the time the work was conducted.

As technologies and risks change over time, the vulnerabilities associated with the operation of {customer} products included in the Security Review report, as well as the actions necessary to reduce the exposure to such vulnerabilities may change.

All information systems, which are designed by, and, therefore, dependent on human beings, are always vulnerable to some degree.

Confidentiality Notice

The provided information is considered {customer} confidential information and is subject to the confidentiality agreement signed between the parties.

The receiving party should keep the information within this document taking appropriate measures to avoid its disclosure to unauthorized persons.

About SoftSeq LLC:

SoftSeq LLC is a Boutique Security Consulting company providing Professional Services in the field of Application Security Engineering.

SoftSeq is specializing in Application Security Engineering and provides end to end solutions to enterprises of all sizes for building Secure Software Systems and Products.

For more information about SoftSeq LLC, please go to:

https://softseq.com/

Appendix A

Product Name	Product Version	Engagement period
{customer} {product}	28250:853eec989233	October 30, 2017 – December 11, 2017

Appendix B

An exhaustive listing of all OWASP ASVS 3.0.1 Level 2 requirements satisfied, their individual audit findings, and corrective actions implemented are presented in a separate spreadsheet supplied with this report.