

Learning Outcome: Students will gain experience auditing source code to verify compliance with an objective standard.

Description:

Your security firm has been contracted to perform a source code audit of an open source web application. The client has indicated that they want to determine the extent to which the open source application complies with parts of OWASP ASVS and the NIST Cybersecurity Framework. The sections of ASVS that your client is concerned about are listed below. For auditing compliance with the NIST Cybersecurity Framework, you are tasked with identifying the parts of the framework (as listed in the provided Expel.io spreadsheet) that are related to the application selected.

Sections of ASVS to audit:

1. V2: Authentication
2. V3: Session Management
3. V4: Access Control
4. V5: Malicious Input Handling
5. V7: Cryptography at Rest
6. V9: Data Protection

Deliverables:

1. A written report in PDF form including:
 - a. A cover page that includes:
 - i. A logo for your fake company
 - ii. A title for the report
 - iii. The names of the investigators producing the report
 - iv. The date the report is submitted
 - b. An executive summary that's approximately one page geared towards C-level executives
 - c. A summary of results section geared towards managers that provides an overview of the extent to which the software is in compliance with each standard.
 - i. A summary of the application's compliance with ASVS
 - ii. A summary of the application's compliance with the relevant parts of the NIST Cybersecurity Framework.
 - d. A detailed results section that provides an in-depth explanation of each finding in the audit. This section should be geared towards developers Each finding should include:
 - i. A description of the check-list item
 - ii. An explanation of how your group evaluated compliance with the checklist item.
 - iii. The rating assigned to the check-list item
 - iv. An explanation of why your group assigned the rating given.
 - v. A recommendation for how to bring the software into compliance.