DISA STIG Web Security

~ compliance report ~

DISA STIG Web Security

compliance report

Description

This Application Security and Development Security Technical Implementation Guide (STIG) provides security guidance for use throughout the application development lifecycle. This STIG provides the guidance needed to promote the development, integration, and updating of secure applications. Subjects covered in this document are: development, design, testing, conversions and upgrades for existing applications, maintenance, software configuration management, education, and training.

Disclaimer

This document or any of its content cannot account for, or be included in any form of legal advice. The outcome of a vulnerability scan (or security evaluation) should be utilized to ensure that diligent measures are taken to lower the risk of potential exploits carried out to compromise data.

Legal advice must be supplied according to its legal context. All laws and the environments in which they are applied, are constantly changed and revised. Therefore no information provided in this document may ever be used as an alternative to a qualified legal body or representative.

A portion of the information in this report is taken from Security Technical Implementation Guide, developed by Defense Information Systems Agency and can be found at http://iase.disa.mil/stigs/stig/application_security_and_development_stig_v2r1_final_20080724.pdf.

Scan

URL	**http://gsa-agile.digicon.com/demo/**
Scan date	7/2/2015 10:09:14 AM
Duration	6 minutes, 36 seconds
Profile	Default

Compliance at a Glance

This section of the report is a summary and lists the number of alerts found according to individual compliance categories.

- Secure Defaults (3.5.1)
  Total number of alerts in this category: 1
- NSA Approved Cryptography (3.6.2)
  ✔ **No alerts in this category**
- Data Transmission (3.7.4)
  ✔ **No alerts in this category**
- Password Transmission (3.8.4.2)
  ✔ **No alerts in this category**
- Excessive Privileges (3.9.3)
  Total number of alerts in this category: 1
- Input Validation (3.10)
  Total number of alerts in this category: 2
- SQL Injection Vulnerabilities (3.10.1)
  ✔ **No alerts in this category**
- Command Injection Vulnerabilities (3.10.4)
  ✔ **No alerts in this category**

- Cross Site Scripting (XSS) Vulnerabilities (3.10.5)
  ✔ **No alerts in this category**
- Hidden Fields in Web Pages (3.12)
  Total number of alerts in this category: 2
- Application Information Disclosure (3.13)
  Total number of alerts in this category: 1