



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://agid.internetsoluzioni.it |
| Scan date | 7/29/2015 4:54:35 AM |
| Duration | 7 hours, 27 minutes |
| Profile | High_Risk_Alerts |

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: 15
- [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: 15

- [Application Information Disclosure \(3.13\)](#)

Total number of alerts in this category: 12

Compliance According to Categories: A Detailed Report

This section is a detailed report that explains each vulnerability found according to individual compliance categories.

(3.5.1) Secure Defaults

The practice of secure defaults helps to ensure the application is deployed in a secure state. This practice implies unneeded or potentially unsafe functionality is disabled by default, and the user must explicitly enable the functionality when required.

Total number of alerts in this category: 1

Alerts in this category

Broken links

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

| | |
|--------------------|---|
| CVSS | Base Score: 0.0 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: None- Integrity Impact: None- Availability Impact: None |
| CWE | CWE-16 |
| Affected item | /media/_ |
| Affected parameter | |
| Variants | 1 |

(3.6.2) NSA Approved Cryptography

Cryptographic equipment, assembly or component classified or certified by NSA for encrypting and decrypting classified and sensitive national security information when appropriately keyed. Developed using established NSA business processes and containing NSA approved algorithms are used to protect systems requiring the most stringent protection mechanisms.

No alerts in this category.

(3.7.4) Data Transmission

Classified data transmitted through a network, which is cleared to a lower level than the data being transmitted, is separately encrypted using NSA-approved cryptography.

No alerts in this category.

(3.8.4.2) Password Transmission

In general, password use is highly discouraged in favor of PKI authentication. However, if applications transmit account passwords, they must be transmitted in an encrypted format.

No alerts in this category.

(3.9.3) Excessive Privileges

An application executing with more privileges than are required for it to function is considered to have excessive privileges and is violating the "Principle of Least Privilege." Applications. An application with excessive privileges greatly increases the risk to the system in the event the application suffers a security breach. The type of attack performed will vary based on the privileges granted to the application account.

Total number of alerts in this category: 1

Alerts in this category

Broken links

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

| | |
|--------------------|---|
| CVSS | Base Score: 0.0 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: None- Integrity Impact: None- Availability Impact: None |
| CWE | CWE-16 |
| Affected item | /media/_ |
| Affected parameter | |
| Variants | 1 |

(3.10) Input Validation

A major cause of software vulnerabilities is failure to validate un-trusted input. Any data crossing a trust boundary, as identified in the threat modeling process, will be checked to ensure validity before being used. Input may come from a user, data store, network socket, or other source.

Total number of alerts in this category: 15

Alerts in this category

Clickjacking: X-Frame-Options header missing

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

| | |
|--------------------|---|
| CVSS | Base Score: 6.8 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Medium- Authentication: None- Confidentiality Impact: Partial- Integrity Impact: Partial- Availability Impact: Partial |
| CWE | CWE-693 |
| Affected item | Web Server |
| Affected parameter | |
| Variants | 1 |

Possible relative path overwrite

Manual confirmation is required for this alert.

Gareth Heyes introduced a technique to take advantage of CSS imports with relative URLs by overwriting their target file. This technique can be used by an attacker to trick browsers into importing HTML pages as CSS stylesheets. If the attacker can control a part of the imported HTML pages he can abuse this issue to inject arbitrary CSS rules.

| | |
|--------------------|--|
| CVSS | Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None |
| CWE | CWE-20 |
| Affected item | /index.php |
| Affected parameter | |
| Variants | 1 |

Broken links

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

| | |
|--------------------|--|
| CVSS | Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None |
| CWE | CWE-16 |
| Affected item | /media/_ |
| Affected parameter | |
| Variants | 1 |

Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| | |
|--------------------|---|
| CVSS | Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None |
| CWE | CWE-200 |
| Affected item | /archivio13_strutture-organizzative_0_9861_0.html |
| Affected parameter | |
| Variants | 1 |
| Affected item | /archivio13_strutture-organizzative_0_9864_0.html |
| Affected parameter | |
| Variants | 1 |
| Affected item | /archivio13_strutture-organizzative_0_9882_0.html |
| Affected parameter | |
| Variants | 1 |
| Affected item | /archivio13_strutture-organizzative_0_9892_0.html |
| Affected parameter | |
| Variants | 1 |

| | |
|--------------------|---|
| Affected item | /archivio13_strutture-organizzative_0_9902_0.html |
| Affected parameter | |
| Variants | 1 |

| | |
|--------------------|---|
| Affected item | /archivio13_strutture-organizzative_0_9908_0.html |
| Affected parameter | |
| Variants | 1 |

| | |
|--------------------|--|
| Affected item | /archivio3_personale-ente_0_40509_0.html |
| Affected parameter | |
| Variants | 1 |

| | |
|--------------------|--|
| Affected item | /archivio3_personale-ente_0_40510_0.html |
| Affected parameter | |
| Variants | 1 |

| | |
|--------------------|--|
| Affected item | /archivio3_personale-ente_0_40511_0.html |
| Affected parameter | |
| Variants | 1 |

| | |
|--------------------|--|
| Affected item | /archivio3_personale-ente_0_40512_0.html |
| Affected parameter | |
| Variants | 1 |

| | |
|--------------------|--|
| Affected item | /archivio3_personale-ente_0_40514_0.html |
| Affected parameter | |
| Variants | 1 |

| | |
|--------------------|--|
| Affected item | /archivio3_personale-ente_0_40517_0.html |
| Affected parameter | |
| Variants | 1 |

(3.10.1) SQL Injection Vulnerabilities

A SQL Injection vulnerability allows an attacker to modify a database query to access or modify data to which they are not permitted. SQL Injection vulnerabilities are exploited through un-validated user input.

No alerts in this category.

(3.10.4) Command Injection Vulnerabilities

Command injection attacks are attempts to inject unwanted data into an application for the purpose of executing operating system shell commands. This can allow an attacker to execute code, possibly at a higher privilege level, resulting in system compromise. Command injection vulnerabilities are most often exploited through unvalidated input.

No alerts in this category.

(3.10.5) Cross Site Scripting (XSS) Vulnerabilities

XSS is a vulnerability where input is accepted by a website and then sent back through a web page. This input can include code, such as JavaScript, to be executed by the user's browser. Since this code is seen as originating from the web server it can access data from the server's domain such as a cookie, or modify the behavior of the webpage by modifying links and other malicious actions. A cross site scripting vulnerability can lead to an attacker gaining personal information or directing a user to a site of the attacker's choice.

No alerts in this category.

(3.12) Hidden Fields in Web Pages

A "hidden" field vulnerability results when hidden fields on a web page, values in a cookie, or variables included in the URL can be used for malicious purposes. While these fields are not normally visible or editable by the user of a web browser, they can be viewed and/or modified by looking at the source.

Total number of alerts in this category: 15

Alerts in this category

Clickjacking: X-Frame-Options header missing

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

| | |
|--------------------|---|
| CVSS | Base Score: 6.8 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Medium- Authentication: None- Confidentiality Impact: Partial- Integrity Impact: Partial- Availability Impact: Partial |
| CWE | CWE-693 |
| Affected item | Web Server |
| Affected parameter | |
| Variants | 1 |

Possible relative path overwrite

Manual confirmation is required for this alert.

Gareth Heyes introduced a technique to take advantage of CSS imports with relative URLs by overwriting their target file. This technique can be used by an attacker to trick browsers into importing HTML pages as CSS stylesheets. If the attacker can control a part of the imported HTML pages he can abuse this issue to inject arbitrary CSS rules.

| | |
|--------------------|---|
| CVSS | Base Score: 0.0 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: None- Integrity Impact: None- Availability Impact: None |
| CWE | CWE-20 |
| Affected item | /index.php |
| Affected parameter | |
| Variants | 1 |

Broken links

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

| | |
|--------------------|---|
| CVSS | Base Score: 0.0 <ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: None- Integrity Impact: None- Availability Impact: None |
| CWE | CWE-16 |
| Affected item | /media/_ |
| Affected parameter | |
| Variants | 1 |

Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| | |
|------|---|
| CVSS | Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None |
| CWE | CWE-200 |

| | |
|--------------------|--|
| Affected item | /archivio13_strutture-organizzative_0_9861_0.html |
| Affected parameter | |
| Variants | 1 |

| | |
|--------------------|--|
| Affected item | /archivio13_strutture-organizzative_0_9864_0.html |
| Affected parameter | |
| Variants | 1 |

| | |
|--------------------|--|
| Affected item | /archivio13_strutture-organizzative_0_9882_0.html |
| Affected parameter | |
| Variants | 1 |

| | |
|--------------------|--|
| Affected item | /archivio13_strutture-organizzative_0_9892_0.html |
| Affected parameter | |
| Variants | 1 |

| | |
|--------------------|--|
| Affected item | /archivio13_strutture-organizzative_0_9902_0.html |
| Affected parameter | |
| Variants | 1 |

| | |
|--------------------|--|
| Affected item | /archivio13_strutture-organizzative_0_9908_0.html |
| Affected parameter | |
| Variants | 1 |

| | |
|--------------------|---|
| Affected item | /archivio3_personale-ente_0_40509_0.html |
| Affected parameter | |
| Variants | 1 |

| | |
|--------------------|---|
| Affected item | /archivio3_personale-ente_0_40510_0.html |
| Affected parameter | |
| Variants | 1 |

| | |
|--------------------|---|
| Affected item | /archivio3_personale-ente_0_40511_0.html |
| Affected parameter | |
| Variants | 1 |

| | |
|--------------------|---|
| Affected item | /archivio3_personale-ente_0_40512_0.html |
| Affected parameter | |
| Variants | 1 |

| | |
|--------------------|---|
| Affected item | /archivio3_personale-ente_0_40514_0.html |
| Affected parameter | |
| Variants | 1 |

| | |
|--------------------|---|
| Affected item | /archivio3_personale-ente_0_40517_0.html |
| Affected parameter | |
| Variants | 1 |

(3.13) Application Information Disclosure

Information disclosure vulnerabilities are leaks of information from an application which are used by the attacker to perform a malicious attack against the application. This information itself may be the target of an attacker, or the information could provide an attacker with data needed to compromise the application or system in a subsequent attack. Information disclosure vulnerabilities are most often the result of programming errors, insufficient authentication, poor error handling, or inadequate data protection.

Total number of alerts in this category: 12

Alerts in this category

Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

| | |
|--------------------|---|
| CVSS | Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None |
| CWE | CWE-200 |
| Affected item | /archivio13_strutture-organizzative_0_9861_0.html |
| Affected parameter | |
| Variants | 1 |
| Affected item | /archivio13_strutture-organizzative_0_9864_0.html |
| Affected parameter | |
| Variants | 1 |
| Affected item | /archivio13_strutture-organizzative_0_9882_0.html |
| Affected parameter | |
| Variants | 1 |
| Affected item | /archivio13_strutture-organizzative_0_9892_0.html |
| Affected parameter | |
| Variants | 1 |
| Affected item | /archivio13_strutture-organizzative_0_9902_0.html |
| Affected parameter | |
| Variants | 1 |
| Affected item | /archivio13_strutture-organizzative_0_9908_0.html |
| Affected parameter | |
| Variants | 1 |
| Affected item | /archivio3_personale-ente_0_40509_0.html |
| Affected parameter | |
| Variants | 1 |
| Affected item | /archivio3_personale-ente_0_40510_0.html |
| Affected parameter | |
| Variants | 1 |
| Affected item | /archivio3_personale-ente_0_40511_0.html |
| Affected parameter | |
| Variants | 1 |

| | |
|--------------------|---|
| Affected item | /archivio3_personale-ente_0_40512_0.html |
| Affected parameter | |
| Variants | 1 |

| | |
|--------------------|---|
| Affected item | /archivio3_personale-ente_0_40514_0.html |
| Affected parameter | |
| Variants | 1 |

| | |
|--------------------|---|
| Affected item | /archivio3_personale-ente_0_40517_0.html |
| Affected parameter | |
| Variants | 1 |