

The Health Insurance Portability and Accountability Act (HIPAA)

Compliance Report

26 June 2023

Generated by Acunetix

Description

The Department of Health and Human Services (HHS) Medicare Program, other Federal agencies operating health plans or providing health care, State Medicaid agencies, private health plans, health care providers, and health care clearinghouses must assure their customers (for example, patients, insured individuals, providers, and health plans) that the integrity, confidentiality, and availability of electronic protected health information they collect, maintain, use, or transmit is protected. The confidentiality of health information is threatened not only by the risk of improper access to stored information, but also by the risk of interception during electronic transmission of the information. The purpose of this final rule is to adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information.

This final rule adopts standards as required under title II, subtitle F, sections 261 through 264 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191. These standards require measures to be taken to secure this information while in the custody of entities covered by HIPAA (covered entities) as well as in transit between covered entities and from covered entities to others.

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.

Scan

URL	http://sdcinstitution.com
Scan date	26/06/2023, 01:09:11
Duration	1337 minutes, 40 seconds
Profile	Full Scan

Compliance at a Glance

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

- General requirements(164.306 (a)(1))

Total number of alerts in this category: 32

- General requirements(164.306 (a)(2))

Total number of alerts in this category: 34

- General requirements(164.306 (a)(3))

Total number of alerts in this category: 33

- Standard: Security management process(164.308 (a)(1)(i))

Total number of alerts in this category: 32

- Risk management(164.308 (a)(1)(ii)(B))

Total number of alerts in this category: 34

- Protection from malicious software(164.308 (a)(5)(ii)(B))

No alerts in this category

- Password management(164.308 (a)(5)(ii)(D))

No alerts in this category

- Integrity(164.312 (c)(1))

No alerts in this category

- Person or entity authentication(164.312 (d))

No alerts in this category

- Transmission security(164.312 (e)(1))

No alerts in this category

- Safeguards(164.530 (c)(2)(i))
Total number of alerts in this category: 32

Compliance According to Categories: A Detailed Report

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

(164.306 (a)(1))General requirements

(a) General requirements. Covered entities must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.

Total number of alerts in this category: 32

Alerts in this category

Documentation file

A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-538
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Documentation file

A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-538

Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

	Base Score: 5.0
	Access Vector: Network_accessible
	Access Complexity: Low
	Authentication: None
	Confidentiality Impact: Partial
	Integrity Impact: None
	Availability Impact: None
CVSS2	Exploitability: Not_defined
	Remediation Level: Not_defined
	Report Confidence: Not_defined
	Availability Requirement: Not_defined
	Collateral Damage Potential: Not_defined
	Confidentiality Requirement: Not_defined
	Integrity Requirement: Not_defined
	Target Distribution: Not_defined
	Base Score: 7.5

CVSS3	Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None
--	--

CVSS2	Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None

CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined	CVSS2	Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined
--	-------	--

CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined
	Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined Base Score: 7.5 Attack Vector: Network
CVSS3	Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None
Confidentiality Impact: Partial Integrity Impact: None

CVSS2	Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None

CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined	CVSS2	Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined
--	-------	--

CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined
	Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined Base Score: 7.5 Attack Vector: Network
CVSS3	Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None
Confidentiality Impact: Partial Integrity Impact: None

CVSS2	Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None

CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined	CVSS2	Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined
--	-------	--

CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined
	Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined Base Score: 7.5 Attack Vector: Network
CVSS3	Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None
Confidentiality Impact: Partial Integrity Impact: None

CVSS2	Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None

CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Password type input with auto-complete enabled

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible username or password disclosure

A username and/or password was found in this file. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined
-------	---

	Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

(164.306 (a)(2))General requirements

(a) General requirements. Covered entities must do the following: (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of all electronic protected health information.

Total number of alerts in this category: 34

Alerts in this category

HTML form without CSRF protection

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.

CVSS2	Base Score: 2.6 Access Vector: Network_accessible Access Complexity: High Authentication: None Confidentiality Impact: None Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 4.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-352
Affected item	Web Server

Affected parameter	
Variants	Not available in the free trial

HTML form without CSRF protection

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.

CVSS2	Base Score: 2.6 Access Vector: Network_accessible Access Complexity: High Authentication: None Confidentiality Impact: None Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 4.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-352
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Documentation file

A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined
-------	---

	Target Distribution: Not_defined
CWE	CWE-538
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Documentation file

A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-538
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined
CVSS3	Target Distribution: Not_defined Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None

	Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined
	Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined

	Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None	
--	---	--

CVSS2	Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None

	Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial
	Integrity Impact: None Availability Impact: None
CVSS2	Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined
	Integrity Requirement: Not_defined

	Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None	
--	---	--

CVSS2	Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Confidentiality Impact: Partial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None

CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined

CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial	
---	--

CVSS2	Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None

CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined	CVSS2	Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined
--	-------	--

CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined
	Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined Base Score: 7.5 Attack Vector: Network
CVSS3	Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None
Confidentiality Impact: Partial Integrity Impact: None

CVSS2	Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Password type input with auto-complete enabled

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None

CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible username or password disclosure

A username and/or password was found in this file. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

(164.306 (a)(3))General requirements

(a) General requirements. Covered entities must do the following: (3) Protect against any reasonably anticipated uses or disclosures of all electronic protected health information that are not permitted or required under subpart E of this part.

Total number of alerts in this category: 33

Alerts in this category

Documentation file

A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

Base Score: 5.0 Access Vector: Network_accessible

CVSS2	Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-538
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Documentation file

A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-538
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Login page password-guessing attack

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.

Base Score: 5.0	
Access Vector: Network_accessible	
Access Complexity: Low	
Authentication: None	
Confidentiality Impact: Partial	
Integrity Impact: None	
Availability Impact: None	

CVSS2	Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: Low
CWE	CWE-307
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None

CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined	CVSS2	Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined
--	-------	--

CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial
Integrity Impact: None

CVSS2	Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None

CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined	CVSS2	Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined
--	-------	--

CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined
	Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined Base Score: 7.5 Attack Vector: Network
CVSS3	Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None
Confidentiality Impact: Partial Integrity Impact: None

CVSS2	Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None

CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined	CVSS2	Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined
--	-------	--

CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined
	Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined Base Score: 7.5 Attack Vector: Network
CVSS3	Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None
Confidentiality Impact: Partial Integrity Impact: None

CVSS2	Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None

CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined	CVSS2	Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined
--	-------	--

CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

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.

Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None
Confidentiality Impact: None

CVSS2	Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Password type input with auto-complete enabled

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A username and/or password was found in this file. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

(164.308 (a)(1)(i))Standard: Security management process

(a) A covered entity must, in accordance with 164.306: (1)(i) Implement policies and procedures to prevent, detect, contain, and correct security violations.

Total number of alerts in this category: 32

Alerts in this category

Documentation file

A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined
CVSS2	
	Report Confidence: Not_defined Availability Requirement: Not_defined
	Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined

	Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-538
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Documentation file

A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-538
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High

	Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None
	Confidentiality Impact: Partial Integrity Impact: None
0) (000	Availability Impact: None
CVSS2	Exploitability: Not_defined Remediation Level: Not_defined
	Report Confidence: Not_defined Availability Requirement: Not_defined
	Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined

	Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low
--	--

CVSS2	Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High

	Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None
CVSS2	Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined

	Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low
--	--

CVSS2	Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High

	Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None
CVSS2	Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined

	Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low
--	--

CVSS2	Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High

	Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None
CVSS2	Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined

	Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low
--	--

CVSS2	Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Password type input with auto-complete enabled

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Integrity Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged

	Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible username or password disclosure

A username and/or password was found in this file. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

(164.308 (a)(1)(ii)(B))Risk management

Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).

Total number of alerts in this category: 34

Alerts in this category

Cookie(s) without HttpOnly flag set

This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Login page password-guessing attack

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: Low
CWE	CWE-307
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

It's recommended to restrict access to the WordPress administration dashboard using HTTP authentication. Password protecting your WordPress admin dashboard through a layer of HTTP authentication is an effective measure to thwart attackers attempting to guess user's passwords. Additionally, if attackers manage to steal a user's password, they will need to get past HTTP authentication in order to gain access to WordPress login form.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Broken links

	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None
--	---

CVSS2	Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Broken links

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Broken links

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Broken links

	Base Score: 0.0
	Access Vector: Network_accessible
	Access Complexity: Low
	Authentication: None
	Confidentiality Impact: None
	Integrity Impact: None
	Availability Impact: None
CVSS2	Exploitability: Not_defined
	Remediation Level: Not_defined
	Report Confidence: Not_defined
	Availability Requirement: Not_defined

	Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Broken links

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Broken links

CVSS2	Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Broken links

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Broken links

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Broken links

	Base Score: 0.0
	Access Vector: Network_accessible
	Access Complexity: Low
	Authentication: None
	Confidentiality Impact: None
	Integrity Impact: None
	Availability Impact: None
CVSS2	Exploitability: Not_defined
	Remediation Level: Not_defined
	Report Confidence: Not_defined
	Availability Requirement: Not_defined

	Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Broken links

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Broken links

Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None
Integrity Impact: None

CVSS2	Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Broken links

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Broken links

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

(164.308 (a)(5)(ii)(B))Protection from malicious software

Procedures for guarding against, detecting, and reporting malicious software.

No alerts in this category.

(164.308 (a)(5)(ii)(D))Password management

Procedures for creating, changing, and safeguarding passwords.

No alerts in this category.

(164.312 (c)(1))Integrity

Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

No alerts in this category.

(164.312 (d))Person or entity authentication

Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

No alerts in this category.

(164.312 (e)(1))Transmission security

Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

No alerts in this category.

(164.530 (c)(2)(i))Safeguards

A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.

Total number of alerts in this category: 32

Alerts in this category

Documentation file

A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-538
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Documentation file

A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-538
Affected item	Web Server

Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low

CVSS3	Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

	Base Score: 5.0
	Access Vector: Network_accessible
	Access Complexity: Low
	Authentication: None
	Confidentiality Impact: Partial
	Integrity Impact: None
	Availability Impact: None
CVSS2	Exploitability: Not defined
	Remediation Level: Not_defined

	Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Affected parameter	
Affected item	Web Server
CWE	CWE-200
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None

CVSS3	User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

	Base Score: 5.0
	Access Vector: Network_accessible
	Access Complexity: Low
	Authentication: None
	Confidentiality Impact: Partial
	Integrity Impact: None
	Availability Impact: None
CVSS2	Exploitability: Not_defined
3,032	Remediation Level: Not_defined

	Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None

CVSS3	User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

	Base Score: 5.0
	Access Vector: Network accessible
	Access Complexity: Low
	Authentication: None
	Confidentiality Impact: Partial
	Integrity Impact: None
	Availability Impact: None
CVSS2	Exploitability: Not defined
0.002	Remediation Level: Not defined
	Report Confidence: Not_defined

	Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None

CVSS3	User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive directories

	Base Score: 5.0
	Access Vector: Network_accessible
	Access Complexity: Low
	Authentication: None
	Confidentiality Impact: Partial
	Integrity Impact: None
	Availability Impact: None
CVSS2	Exploitability: Not defined
	Remediation Level: Not defined
	Report Confidence: Not defined

	Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined Base Score: 0.0
CVSS3	Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server

Affected parameter	
Variants	Not available in the free trial

Password type input with auto-complete enabled

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Possible username or password disclosure

A username and/or password was found in this file. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
	Base Score: 7.5 Attack Vector: Network

CVSS3	Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Affected Items: A Detailed Report

This section provides full details of the types of vulnerabilities found according to individual affected items.

Web Server

HTML form without CSRF protection

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.

This alert belongs to the following categories: 164.306 (a)(2)

CVSS2	Base Score: 2.6 Access Vector: Network_accessible Access Complexity: High Authentication: None Confidentiality Impact: None Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 4.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-352
Parameter	Variations

HTML form without CSRF protection

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.

Base Score: 2.6 Access Vector: Network_accessible Access Complexity: High Authentication: None Confidentiality Impact: None Integrity Impact: Partial

CVSS2	Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 4.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-352
Parameter	Variations

Cookie(s) without HttpOnly flag set

This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

This alert belongs to the following categories: 164.308 (a)(1)(ii)(B)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

Documentation file

A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None
--	--

CVSS2	Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-538
Parameter	Variations

Documentation file

A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

This alert belongs to the following categories: 164.306 (a)(1), 164.306 (a)(2), 164.306 (a)(3), 164.308 (a)(1)(i), 164.530 (c)(2)(i)

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-538
Parameter	Variations

Login page password-guessing attack

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.

This alert belongs to the following categories: 164.306 (a)(3), 164.308 (a)(1)(ii)(B)

	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low	
	Authentication: None	
	Confidentiality Impact: Partial	
	Integrity Impact: None	
	Availability Impact: None	
CVSS2	Exploitability: Not_defined	
	Remediation Level: Not_defined	
	Report Confidence: Not_defined	
	Availability Requirement: Not_defined	
	Collateral Damage Potential: Not_defined	

	Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: Low
CWE	CWE-307
Parameter	Variations

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

This alert belongs to the following categories: 164.306 (a)(1), 164.306 (a)(2), 164.306 (a)(3), 164.308 (a)(1)(i), 164.530 (c)(2)(i)

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

Access Vector: Network_accessible Access Complexity: Low
--

CVSS2	Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

This alert belongs to the following categories: 164.306 (a)(1), 164.306 (a)(2), 164.306 (a)(3), 164.308 (a)(1)(i), 164.530 (c)(2)(i)

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

This alert belongs to the following categories: 164.306 (a)(1), 164.306 (a)(2), 164.306 (a)(3), 164.308 (a)(1)(i), 164.530 (c)(2)(i)

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined	
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None	

	Availability Impact: None
CWE	CWE-200
Parameter	Variations

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

This alert belongs to the following categories: 164.306 (a)(1), 164.306 (a)(2), 164.306 (a)(3), 164.308 (a)(1)(i), 164.530 (c)(2)(i)

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined
-------	---

	Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

This alert belongs to the following categories: 164.306 (a)(1), 164.306 (a)(2), 164.306 (a)(3), 164.308 (a)(1)(i), 164.530 (c)(2)(i)

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authenticin: None
Confidentiality Impact: Partial

CVSS2	Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

This alert belongs to the following categories: 164.306 (a)(1), 164.306 (a)(2), 164.306 (a)(3), 164.308 (a)(1)(i), 164.530 (c)(2)(i)

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

This alert belongs to the following categories: 164.306 (a)(1), 164.306 (a)(2), 164.306 (a)(3), 164.308 (a)(1)(i), 164.530 (c)(2)(i)

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None

	Availability Impact: None
CWE	CWE-200
Parameter	Variations

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

This alert belongs to the following categories: 164.306 (a)(1), 164.306 (a)(2), 164.306 (a)(3), 164.308 (a)(1)(i), 164.530 (c)(2)(i)

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined
-------	---

	Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

This alert belongs to the following categories: 164.306 (a)(1), 164.306 (a)(2), 164.306 (a)(3), 164.308 (a)(1)(i), 164.530 (c)(2)(i)

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authenticin: None
Confidentiality Impact: Partial

CVSS2	Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

This alert belongs to the following categories: 164.306 (a)(1), 164.306 (a)(2), 164.306 (a)(3), 164.308 (a)(1)(i), 164.530 (c)(2)(i)

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

This alert belongs to the following categories: 164.306 (a)(1), 164.306 (a)(2), 164.306 (a)(3), 164.308 (a)(1)(i), 164.530 (c)(2)(i)

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None

	Availability Impact: None
CWE	CWE-200
Parameter	Variations

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

This alert belongs to the following categories: 164.306 (a)(1), 164.306 (a)(2), 164.306 (a)(3), 164.308 (a)(1)(i), 164.530 (c)(2)(i)

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined
-------	---

	Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

This alert belongs to the following categories: 164.306 (a)(1), 164.306 (a)(2), 164.306 (a)(3), 164.308 (a)(1)(i), 164.530 (c)(2)(i)

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None
Confidentiality Impact: Partial

CVSS2	Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

This alert belongs to the following categories: 164.306 (a)(1), 164.306 (a)(2), 164.306 (a)(3), 164.308 (a)(1)(i), 164.530 (c)(2)(i)

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

This alert belongs to the following categories: 164.306 (a)(1), 164.306 (a)(2), 164.306 (a)(3), 164.308 (a)(1)(i), 164.530 (c)(2)(i)

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

Possible sensitive directories

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None

	Availability Impact: None
CWE	CWE-200
Parameter	Variations

Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

This alert belongs to the following categories: 164.306 (a)(1), 164.306 (a)(2), 164.306 (a)(3), 164.308 (a)(1)(i), 164.530 (c)(2)(i)

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

WordPress admin accessible without HTTP authentication

It's recommended to restrict access to the WordPress administration dashboard using HTTP authentication. Password protecting your WordPress admin dashboard through a layer of HTTP authentication is an effective measure to thwart attackers attempting to guess user's passwords. Additionally, if attackers manage to steal a user's password, they will need to get past HTTP authentication in order to gain access to WordPress login form.

	Base Score: 0.0
	Access Vector: Network accessible
	Access Complexity: Low
	Authentication: None
	Confidentiality Impact: None
	Integrity Impact: None
CVSS2	Availability Impact: None
	Exploitability: Not defined
	Remediation Level: Not defined
	Report Confidence: Not defined
	Availability Requirement: Not_defined
	Collateral Damage Potential: Not defined
	Confidentiality Requirement: Not defined

	Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

This alert belongs to the following categories: 164.308 (a)(1)(ii)(B)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

This alert belongs to the following categories: 164.308 (a)(1)(ii)(B)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

This alert belongs to the following categories: 164.308 (a)(1)(ii)(B)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

This alert belongs to the following categories: 164.308 (a)(1)(ii)(B)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

Base Score: 0.0	
Access Vector: Network_accessible	
Access Complexity: Low	
Authentication: None	
Confidentiality Impact: None	
Integrity Impact: None	
Availability Impact: None	

CVSS2	Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

This alert belongs to the following categories: 164.308 (a)(1)(ii)(B)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

This alert belongs to the following categories: 164.308 (a)(1)(ii)(B)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

This alert belongs to the following categories: 164.308 (a)(1)(ii)(B)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

Base Score: 0.0

CVSS2	Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

This alert belongs to the following categories: 164.308 (a)(1)(ii)(B)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

	Base Score: 0.0
	Access Vector: Network accessible
	Access Complexity: Low
	Authentication: None
	Confidentiality Impact: None
	Integrity Impact: None
	Availability Impact: None
CVSS2	Exploitability: Not_defined
	Remediation Level: Not_defined
	Report Confidence: Not_defined
	Availability Requirement: Not_defined
	Collateral Damage Potential: Not_defined
	Confidentiality Requirement: Not_defined

	Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

This alert belongs to the following categories: 164.308 (a)(1)(ii)(B)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

This alert belongs to the following categories: 164.308 (a)(1)(ii)(B)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

This alert belongs to the following categories: 164.308 (a)(1)(ii)(B)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

This alert belongs to the following categories: 164.308 (a)(1)(ii)(B)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

Base Score: 0.0	
Access Vector: Network_accessible	
Access Complexity: Low	
Authentication: None	
Confidentiality Impact: None	
Integrity Impact: None	
Availability Impact: None	

CVSS2	Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

This alert belongs to the following categories: 164.308 (a)(1)(ii)(B)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

This alert belongs to the following categories: 164.308 (a)(1)(ii)(B)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

This alert belongs to the following categories: 164.308 (a)(1)(ii)(B)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

Base Score: 0.0

CVSS2	Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

This alert belongs to the following categories: 164.308 (a)(1)(ii)(B)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

	Base Score: 0.0	
	Access Vector: Network accessible	
	Access Complexity: Low	
	Authentication: None	
	Confidentiality Impact: None	
	Integrity Impact: None	
	Availability Impact: None	
CVSS2	Exploitability: Not_defined	
	Remediation Level: Not_defined	
	Report Confidence: Not_defined	
	Availability Requirement: Not_defined	
	Collateral Damage Potential: Not_defined	
	Confidentiality Requirement: Not_defined	

	Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

This alert belongs to the following categories: 164.308 (a)(1)(ii)(B)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

This alert belongs to the following categories: 164.308 (a)(1)(ii)(B)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

This alert belongs to the following categories: 164.308 (a)(1)(ii)(B)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

This alert belongs to the following categories: 164.308 (a)(1)(ii)(B)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

Base Score: 0.0	
Access Vector: Network_accessible	
Access Complexity: Low	
Authentication: None	
Confidentiality Impact: None	
Integrity Impact: None	
Availability Impact: None	

CVSS2	Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

This alert belongs to the following categories: 164.308 (a)(1)(ii)(B)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Parameter	Variations

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.

This alert belongs to the following categories: 164.306 (a)(1), 164.306 (a)(2), 164.306 (a)(3), 164.308 (a)(1)(i), 164.530 (c)(2)(i)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

Password type input with auto-complete enabled

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

This alert belongs to the following categories: 164.306 (a)(1), 164.306 (a)(2), 164.306 (a)(3), 164.308 (a)(1)(i), 164.530 (c)(2)(i)

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
	Base Score: 7.5 Attack Vector: Network

CVSS3	Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

Possible username or password disclosure

A username and/or password was found in this file. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

This alert belongs to the following categories: 164.306 (a)(1), 164.306 (a)(2), 164.306 (a)(3), 164.308 (a)(1)(i), 164.530 (c)(2)(i)

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

Scanned items (coverage report)

http://sdcinstitution.com/

http://sdcinstitution.com/ Copy of

http://sdcinstitution.com/ (copy

http://sdcinstitution.com/a

http://sdcinstitution.com/a/14384091

http://sdcinstitution.com/a/8935649

http://sdcinstitution.com/achievements

http://sdcinstitution.com/activities

http://sdcinstitution.com/admin

http://sdcinstitution.com/admin (copy

http://sdcinstitution.com/admissions

http://sdcinstitution.com/aids-awarness-program-at-sdc-kolar

http://sdcinstitution.com/anti-ragging-cell

http://sdcinstitution.com/anti-sexual-harassment

http://sdcinstitution.com/auditorium http://sdcinstitution.com/canteen

http://sdcinstitution.com/cells-forums

http://sdcinstitution.com/cgi-bin

http://sdcinstitution.com/cgi-bin/atom

http://sdcinstitution.com/cgi-bin/cgi-bin (copy

http://sdcinstitution.com/cgi-bin/download

http://sdcinstitution.com/cgi-bin/feed

http://sdcinstitution.com/cgi-bin/feed/atom

http://sdcinstitution.com/cgi-bin/image

http://sdcinstitution.com/cgi-bin/m

http://sdcinstitution.com/cgi-bin/New folder (2

http://sdcinstitution.com/comments

http://sdcinstitution.com/comments/feed

http://sdcinstitution.com/commerce-forum

http://sdcinstitution.com/computer-lab

http://sdcinstitution.com/conferences

http://sdcinstitution.com/counselling-cell

http://sdcinstitution.com/equal-opportunity-cell

http://sdcinstitution.com/events

http://sdcinstitution.com/examination-committee

http://sdcinstitution.com/faculty-welfare

http://sdcinstitution.com/favicon.ico

http://sdcinstitution.com/feed

http://sdcinstitution.com/grievance-cell

http://sdcinstitution.com/home

http://sdcinstitution.com/home/about

http://sdcinstitution.com/home/about/management-desk

http://sdcinstitution.com/home/about/principal-desk

http://sdcinstitution.com/home/about/vision-and-mission

http://sdcinstitution.com/home/alumni

http://sdcinstitution.com/home/blog

http://sdcinstitution.com/home/blog/page

http://sdcinstitution.com/home/blog/page/2

http://sdcinstitution.com/home/blog/page/3

http://sdcinstitution.com/home/blog/page/4

http://sdcinstitution.com/home/blog/page/5

http://sdcinstitution.com/home/blog/page/6

http://sdcinstitution.com/home/blog/page/7

http://sdcinstitution.com/home/blog/page/8

http://sdcinstitution.com/home/branches

http://sdcinstitution.com/home/branches/bangarapet-branch

http://sdcinstitution.com/home/branches/bangarapet-branch/download

http://sdcinstitution.com/home/branches/bangarapet-branch/download/feed

http://sdcinstitution.com/home/branches/k-q-f-branch

http://sdcinstitution.com/home/branches/kolar-branch

http://sdcinstitution.com/home/branches/mulbagal-branch

http://sdcinstitution.com/home/branches/srinivaspur-branch

http://sdcinstitution.com/home/contact

http://sdcinstitution.com/home/gallery

http://sdcinstitution.com/home/infrastructure

http://sdcinstitution.com/home/infrastructure/business-lab

http://sdcinstitution.com/home/naac

```
http://sdcinstitution.com/home/naac/about
http://sdcinstitution.com/home/naac/about-2
http://sdcinstitution.com/home/naac/agar
http://sdcinstitution.com/home/naac/complienesaction-report
http://sdcinstitution.com/home/naac/minutes-of-meeting
http://sdcinstitution.com/home/naac/naac-certificate
http://sdcinstitution.com/home/programmes
http://sdcinstitution.com/home/programmes/b-b-a
http://sdcinstitution.com/home/programmes/b-c-a
http://sdcinstitution.com/home/programmes/b-com
http://sdcinstitution.com/home/programmes/b-s-c
http://sdcinstitution.com/home/programmes/m-com
http://sdcinstitution.com/home/programmes/m-s-c
http://sdcinstitution.com/home/programmes/pre-university
http://sdcinstitution.com/home/programmes/school
http://sdcinstitution.com/kannada-activity-program
http://sdcinstitution.com/language-class
http://sdcinstitution.com/lib
http://sdcinstitution.com/lib/uploadify
http://sdcinstitution.com/lib/uploadify/custom.php
http://sdcinstitution.com/library
http://sdcinstitution.com/license.txt
http://sdcinstitution.com/magazine-committee
http://sdcinstitution.com/national-public-school-kolar
http://sdcinstitution.com/New folder (2
http://sdcinstitution.com/outreach-program
http://sdcinstitution.com/placements
http://sdcinstitution.com/playground
http://sdcinstitution.com/readme.html
http://sdcinstitution.com/robots.txt
http://sdcinstitution.com/sales-day-and-food-fest-at-sdc-kolar
http://sdcinstitution.com/scholarships
http://sdcinstitution.com/science-forum
http://sdcinstitution.com/science-lab
http://sdcinstitution.com/sdc-bangarpet-spoorthi-archana-got-felicitated-by-kannada-sangha-for-being-selected-to-speak-in-
parliament
http://sdcinstitution.com/sdc-has-bagged-5-ranks-in-bca-and-b-sc-2023
http://sdcinstitution.com/seminar-hall
http://sdcinstitution.com/seminars
http://sdcinstitution.com/sports
http://sdcinstitution.com/student-life-and-support
http://sdcinstitution.com/student-welfare
http://sdcinstitution.com/student-welfare/image
http://sdcinstitution.com/student-welfare/image/feed
http://sdcinstitution.com/swaraswathi-puja-at-sdc-bangarpet
http://sdcinstitution.com/third-party
http://sdcinstitution.com/third-party/uploadify
http://sdcinstitution.com/third-party/uploadify/uploadify.php
http://sdcinstitution.com/traffic-rules-awarness-program-at-sdc-kolar
http://sdcinstitution.com/value-added-program
http://sdcinstitution.com/women-empowerment
http://sdcinstitution.com/workshop
http://sdcinstitution.com/workshop-on-advanced-programing
http://sdcinstitution.com/wp-admin
http://sdcinstitution.com/wp-admin/admin-ajax.php
http://sdcinstitution.com/wp-admin/atom
http://sdcinstitution.com/wp-admin/css
http://sdcinstitution.com/wp-admin/css/atom
http://sdcinstitution.com/wp-admin/css/css (copy
http://sdcinstitution.com/wp-admin/css/feed
http://sdcinstitution.com/wp-admin/css/feed/atom
http://sdcinstitution.com/wp-admin/css/forms.min.css
http://sdcinstitution.com/wp-admin/css/install.css
http://sdcinstitution.com/wp-admin/css/install.min.css
http://sdcinstitution.com/wp-admin/css/l10n.min.css
```

http://sdcinstitution.com/wp-admin/css/login.min.css http://sdcinstitution.com/wp-admin/css/New folder (2

http://sdcinstitution.com/wp-admin/download

```
http://sdcinstitution.com/wp-admin/feed
http://sdcinstitution.com/wp-admin/feed/atom
http://sdcinstitution.com/wp-admin/image
http://sdcinstitution.com/wp-admin/images
http://sdcinstitution.com/wp-admin/images/atom
http://sdcinstitution.com/wp-admin/images/feed
http://sdcinstitution.com/wp-admin/images/feed/atom
http://sdcinstitution.com/wp-admin/images/images (copy
http://sdcinstitution.com/wp-admin/images/New folder (2
http://sdcinstitution.com/wp-admin/import.php
http://sdcinstitution.com/wp-admin/includes
http://sdcinstitution.com/wp-admin/includes (copy
http://sdcinstitution.com/wp-admin/includes/atom
http://sdcinstitution.com/wp-admin/includes/feed
http://sdcinstitution.com/wp-admin/includes/feed/atom
http://sdcinstitution.com/wp-admin/includes/includes (copy
http://sdcinstitution.com/wp-admin/includes/New folder (2
http://sdcinstitution.com/wp-admin/install.php
http://sdcinstitution.com/wp-admin/js
http://sdcinstitution.com/wp-admin/js/atom
http://sdcinstitution.com/wp-admin/is/feed
http://sdcinstitution.com/wp-admin/is/feed/atom
http://sdcinstitution.com/wp-admin/js/js (copy
http://sdcinstitution.com/wp-admin/js/New folder (2
http://sdcinstitution.com/wp-admin/js/password-strength-meter.min.js
http://sdcinstitution.com/wp-admin/js/user-profile.min.js
http://sdcinstitution.com/wp-admin/m
http://sdcinstitution.com/wp-admin/New folder (2
http://sdcinstitution.com/wp-admin/update-core.php
http://sdcinstitution.com/wp-admin/upgrade.php
http://sdcinstitution.com/wp-admin/user
http://sdcinstitution.com/wp-admin/wp-admin (copy
http://sdcinstitution.com/wp-comments-post.php
http://sdcinstitution.com/wp-content
http://sdcinstitution.com/wp-content/atom
http://sdcinstitution.com/wp-content/download
http://sdcinstitution.com/wp-content/feed
http://sdcinstitution.com/wp-content/feed/atom
http://sdcinstitution.com/wp-content/image
http://sdcinstitution.com/wp-content/languages
http://sdcinstitution.com/wp-content/languages/atom
http://sdcinstitution.com/wp-content/languages/feed
http://sdcinstitution.com/wp-content/languages/feed/atom
http://sdcinstitution.com/wp-content/languages/languages (copy
http://sdcinstitution.com/wp-content/languages/New folder (2
http://sdcinstitution.com/wp-content/m
http://sdcinstitution.com/wp-content/New folder (2
http://sdcinstitution.com/wp-content/plugins
http://sdcinstitution.com/wp-content/plugins/atom
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/assets
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/assets/assets (copy
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/assets/images
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/assets/images/images (copy
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/assets/images/New folder (2
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/assets/legacy
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/assets/legacy/frontend.css
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/assets/legacy/frontend.min.js
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/assets/legacy/images
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/assets/legacy/images/images (copy
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/assets/legacy/images/New folder (2
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/assets/legacy/images/templates
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/assets/legacy/images/templates/New folder (2
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/assets/legacy/images/templates/copy
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/assets/legacy/legacy (copy
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/assets/legacy/New folder (2
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/assets/legacy/templates
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/assets/legacy/templates/New folder (2
```

```
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/assets/legacy/templates/templates (copy
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/assets/New folder (2
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/buttonizer-multifunctional-button (copy
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/languages
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/languages/languages (copy
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/languages/New folder (2
http://sdcinstitution.com/wp-content/plugins/buttonizer-multifunctional-button/New folder (2
http://sdcinstitution.com/wp-content/plugins/coblocks
http://sdcinstitution.com/wp-content/plugins/coblocks/assets
http://sdcinstitution.com/wp-content/plugins/coblocks/assets/assets (copy
http://sdcinstitution.com/wp-content/plugins/coblocks/assets/list
http://sdcinstitution.com/wp-content/plugins/coblocks/assets/list/list (copy
http://sdcinstitution.com/wp-content/plugins/coblocks/assets/list/New folder (2
http://sdcinstitution.com/wp-content/plugins/coblocks/assets/New folder (2
http://sdcinstitution.com/wp-content/plugins/coblocks/coblocks (copy
http://sdcinstitution.com/wp-content/plugins/coblocks/dist
http://sdcinstitution.com/wp-content/plugins/coblocks/dist/dist (copy
http://sdcinstitution.com/wp-content/plugins/coblocks/dist/images
http://sdcinstitution.com/wp-content/plugins/coblocks/dist/images/images (copy
http://sdcinstitution.com/wp-content/plugins/coblocks/dist/images/New folder (2
http://sdcinstitution.com/wp-content/plugins/coblocks/dist/js
http://sdcinstitution.com/wp-content/plugins/coblocks/dist/js/coblocks-animation.js
http://sdcinstitution.com/wp-content/plugins/coblocks/dist/js/coblocks-gist.js
http://sdcinstitution.com/wp-content/plugins/coblocks/dist/js/coblocks-lightbox.js
http://sdcinstitution.com/wp-content/plugins/coblocks/dist/js/coblocks-services.js
http://sdcinstitution.com/wp-content/plugins/coblocks/dist/js/coblocks-tinyswiper-initializer.js
http://sdcinstitution.com/wp-content/plugins/coblocks/dist/js/js (copy
http://sdcinstitution.com/wp-content/plugins/coblocks/dist/js/New folder (2
http://sdcinstitution.com/wp-content/plugins/coblocks/dist/js/vendors
http://sdcinstitution.com/wp-content/plugins/coblocks/dist/js/vendors/New folder (2
http://sdcinstitution.com/wp-content/plugins/coblocks/dist/js/vendors/tiny-swiper.js
http://sdcinstitution.com/wp-content/plugins/coblocks/dist/js/vendors/vendors (copy
http://sdcinstitution.com/wp-content/plugins/coblocks/dist/New folder (2
http://sdcinstitution.com/wp-content/plugins/coblocks/dist/style-coblocks-1.css
http://sdcinstitution.com/wp-content/plugins/coblocks/includes
http://sdcinstitution.com/wp-content/plugins/coblocks/includes (copy
http://sdcinstitution.com/wp-content/plugins/coblocks/includes/admin
http://sdcinstitution.com/wp-content/plugins/coblocks/includes/admin (copy
http://sdcinstitution.com/wp-content/plugins/coblocks/includes/admin/admin (copy
http://sdcinstitution.com/wp-content/plugins/coblocks/includes/admin/New folder (2
http://sdcinstitution.com/wp-content/plugins/coblocks/includes/Dependencies
http://sdcinstitution.com/wp-content/plugins/coblocks/includes/Dependencies/Dependencies (copy
http://sdcinstitution.com/wp-content/plugins/coblocks/includes/Dependencies/GoDaddy
http://sdcinstitution.com/wp-content/plugins/coblocks/includes/Dependencies/GoDaddy/GoDaddy (copy
http://sdcinstitution.com/wp-content/plugins/coblocks/includes/Dependencies/GoDaddy/New folder (2
http://sdcinstitution.com/wp-content/plugins/coblocks/includes/Dependencies/GoDaddy/Styles
http://sdcinstitution.com/wp-content/plugins/coblocks/includes/Dependencies/GoDaddy/Styles/build
http://sdcinstitution.com/wp-content/plugins/coblocks/includes/Dependencies/GoDaddy/Styles/build/build (copy
http://sdcinstitution.com/wp-content/plugins/coblocks/includes/Dependencies/GoDaddy/Styles/build/latest.css
http://sdcinstitution.com/wp-content/plugins/coblocks/includes/Dependencies/GoDaddy/Styles/build/New folder (2
http://sdcinstitution.com/wp-content/plugins/coblocks/includes/Dependencies/GoDaddy/Styles/New folder (2
http://sdcinstitution.com/wp-content/plugins/coblocks/includes/Dependencies/GoDaddy/Styles/Styles (copy
http://sdcinstitution.com/wp-content/plugins/coblocks/includes/Dependencies/New folder (2
http://sdcinstitution.com/wp-content/plugins/coblocks/includes/includes (copy
http://sdcinstitution.com/wp-content/plugins/coblocks/includes/New folder (2
http://sdcinstitution.com/wp-content/plugins/coblocks/New folder (2
http://sdcinstitution.com/wp-content/plugins/coblocks/src
http://sdcinstitution.com/wp-content/plugins/coblocks/src (copy
http://sdcinstitution.com/wp-content/plugins/coblocks/src/New folder (2
http://sdcinstitution.com/wp-content/plugins/coblocks/src/src (copy
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/admin
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/admin (copy
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/admin/admin (copy
http://sdcinstitution.com/wp-content/plugins/content-views-guery-and-display-post-page/admin/assets
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/admin/assets/assets (copy
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/admin/assets/images
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/admin/assets/images/images (copy
```

```
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/admin/assets/images/New folder (2
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/admin/assets/js
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/admin/assets/js/js (copy
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/admin/assets/js/New folder (2
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/admin/assets/New folder (2
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/admin/includes
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/admin/includes (copy
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/admin/includes/includes (copy
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/admin/includes/New folder (2
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/admin/includes/templates
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/admin/includes/templates/New folder (2
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/admin/includes/templates/templates (copy
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/admin/New folder (2
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/assets
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/assets/assets (copy
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/assets/New folder (2
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/content-views-query-and-display-post-
page (copy
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/includes
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/includes (copy
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/includes/includes (copy
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/includes/New folder (2
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/includes/settings.php
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/languages
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/languages/languages (copy
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/languages/New folder (2
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/New folder (2
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/public
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/public/assets
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/public/assets/assets (copy
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/public/assets/css
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/public/assets/css/css (copy
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/public/assets/css/cv.css
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/public/assets/css/New folder (2
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/public/assets/fonts
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/public/assets/fonts/fonts (copy
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/public/assets/fonts/glyphicons-halflings-
regular.woff2
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/public/assets/fonts/New folder (2
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/public/assets/js
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/public/assets/js/cv.js
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/public/assets/js/js (copy
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/public/assets/js/New folder (2
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/public/assets/New folder (2
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/public/New folder (2
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/public/public (copy
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/public/templates
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/public/templates/New folder (2
http://sdcinstitution.com/wp-content/plugins/content-views-query-and-display-post-page/public/templates/templates (copy
http://sdcinstitution.com/wp-content/plugins/feed
http://sdcinstitution.com/wp-content/plugins/feed/atom
http://sdcinstitution.com/wp-content/plugins/mystickyelements
http://sdcinstitution.com/wp-content/plugins/mystickyelements/admin
http://sdcinstitution.com/wp-content/plugins/mystickyelements/admin (copy
http://sdcinstitution.com/wp-content/plugins/mystickyelements/admin/admin (copy
http://sdcinstitution.com/wp-content/plugins/mystickyelements/admin/New folder (2
http://sdcinstitution.com/wp-content/plugins/mystickyelements/css
http://sdcinstitution.com/wp-content/plugins/mystickyelements/css/css (copy
http://sdcinstitution.com/wp-content/plugins/mystickyelements/css/font-awesome.min.css
http://sdcinstitution.com/wp-content/plugins/mystickyelements/css/mystickyelements-front.min.css
http://sdcinstitution.com/wp-content/plugins/mystickyelements/css/New folder (2
http://sdcinstitution.com/wp-content/plugins/mystickyelements/fonts
http://sdcinstitution.com/wp-content/plugins/mystickyelements/fonts/fonts (copy
http://sdcinstitution.com/wp-content/plugins/mystickyelements/fonts/New folder (2
http://sdcinstitution.com/wp-content/plugins/mystickyelements/images
http://sdcinstitution.com/wp-content/plugins/mystickyelements/images/images (copy
http://sdcinstitution.com/wp-content/plugins/mystickyelements/images/New folder (2
http://sdcinstitution.com/wp-content/plugins/mystickyelements/img
```

```
http://sdcinstitution.com/wp-content/plugins/mystickyelements/img/img (copy
http://sdcinstitution.com/wp-content/plugins/mystickyelements/img/New folder (2
http://sdcinstitution.com/wp-content/plugins/mystickyelements/includes
http://sdcinstitution.com/wp-content/plugins/mystickyelements/includes (copy
http://sdcinstitution.com/wp-content/plugins/mystickyelements/includes/includes (copy
http://sdcinstitution.com/wp-content/plugins/mystickyelements/includes/New folder (2
http://sdcinstitution.com/wp-content/plugins/mystickyelements/intl-tel-input-src
http://sdcinstitution.com/wp-content/plugins/mystickyelements/intl-tel-input-src/build
http://sdcinstitution.com/wp-content/plugins/mystickyelements/intl-tel-input-src/build/build (copy
http://sdcinstitution.com/wp-content/plugins/mystickyelements/intl-tel-input-src/build/css
http://sdcinstitution.com/wp-content/plugins/mystickyelements/intl-tel-input-src/build/css/css (copy
http://sdcinstitution.com/wp-content/plugins/mystickyelements/intl-tel-input-src/build/css/intlTelInput.css
http://sdcinstitution.com/wp-content/plugins/mystickyelements/intl-tel-input-src/build/css/New folder (2
http://sdcinstitution.com/wp-content/plugins/mystickyelements/intl-tel-input-src/build/imq
http://sdcinstitution.com/wp-content/plugins/mystickyelements/intl-tel-input-src/build/img/img (copy
http://sdcinstitution.com/wp-content/plugins/mystickyelements/intl-tel-input-src/build/img/New folder (2
http://sdcinstitution.com/wp-content/plugins/mystickyelements/intl-tel-input-src/build/js
http://sdcinstitution.com/wp-content/plugins/mystickyelements/intl-tel-input-src/build/js/intlTelInput.js
http://sdcinstitution.com/wp-content/plugins/mystickyelements/intl-tel-input-src/build/is/is (copy
http://sdcinstitution.com/wp-content/plugins/mystickyelements/intl-tel-input-src/build/is/New folder (2
http://sdcinstitution.com/wp-content/plugins/mystickyelements/intl-tel-input-src/build/New folder (2
http://sdcinstitution.com/wp-content/plugins/mystickyelements/intl-tel-input-src/intl-tel-input-src (copy
http://sdcinstitution.com/wp-content/plugins/mystickyelements/intl-tel-input-src/New folder (2
http://sdcinstitution.com/wp-content/plugins/mystickyelements/js
http://sdcinstitution.com/wp-content/plugins/mystickyelements/js/jquery.cookie.js
http://sdcinstitution.com/wp-content/plugins/mystickyelements/js/js (copy
http://sdcinstitution.com/wp-content/plugins/mystickyelements/js/mystickyelements-fronted.min.js
http://sdcinstitution.com/wp-content/plugins/mystickyelements/js/New folder (2
http://sdcinstitution.com/wp-content/plugins/mystickyelements/languages
http://sdcinstitution.com/wp-content/plugins/mystickyelements/languages/languages (copy
http://sdcinstitution.com/wp-content/plugins/mystickyelements/languages/New folder (2
http://sdcinstitution.com/wp-content/plugins/mystickyelements/mystickyelements (copy
http://sdcinstitution.com/wp-content/plugins/mystickyelements/New folder (2
http://sdcinstitution.com/wp-content/plugins/New folder (2
http://sdcinstitution.com/wp-content/plugins/pdf-embedder
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/assets (copy
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/css
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/css/css (copy
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/css/New folder (2
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/css/pdfemb-embed-pdf.css
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/img
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/img/img (copy
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/img/New folder (2
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/js
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/js/admin
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/js/admin (copy
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/js/admin/admin (copy
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/js/admin/New folder (2
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/js/js (copy
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/js/min
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/js/min/all-pdfemb-min.js
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/js/min/min (copy
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/js/min/New folder (2
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/js/New folder (2
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/js/pdfjs
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/js/pdfjs/New folder (2
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/js/pdfjs/pdf.min.js
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/js/pdfjs/pdfjs (copy
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/assets/New folder (2
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/core
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/core/core (copy
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/core/New folder (2
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/New folder (2
http://sdcinstitution.com/wp-content/plugins/pdf-embedder/pdf-embedder (copy
http://sdcinstitution.com/wp-content/plugins/plugins (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/New folder (2
```

```
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/New folder (2
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/Public (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application/Admin
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application/Admin (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application/Admin/Admin (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application/Admin/New folder (2
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application/Application (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application/Frontend
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application/Frontend/Assets
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application/Frontend/Assets/Assets (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application/Frontend/Assets/dist
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application/Frontend/Assets/dist/dist (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application/Frontend/Assets/dist/n2.min.js
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application/Frontend/Assets/dist/New folder (2
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application/Frontend/Assets/dist/smartslider-
http://sdcinstitution.com/wp-content/plugins/smart-slider-
3/Public/SmartSlider3/Application/Frontend/Assets/dist/smartslider.min.css
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application/Frontend/Assets/images
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application/Frontend/Assets/images/images (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application/Frontend/Assets/images/New folder (2
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application/Frontend/Assets/js
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application/Frontend/Assets/js/js (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application/Frontend/Assets/js/New folder (2
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application/Frontend/Assets/New folder (2
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application/Frontend/Frontend (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application/Frontend/New folder (2
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Application/New folder (2
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/New folder (2
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Slider
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Slider/New folder (2
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Slider/Slider (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Slider/SliderType
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Slider/SliderType/New folder (2
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider/SliderType/Simple
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider/SliderType/Simple/Assets
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Slider/SliderType/Simple/Assets/Assets (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider/Slider/SliderType/Simple/Assets/dist
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider/Slider/SliderType/Simple/Assets/dist/dist (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider/Slider/SliderType/Simple/Assets/dist/New folder (2
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider/Slider/SliderType/Simple/Assets/dist/smartslider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Public/SmartSlider-3/Publi
backgroundanimation.min.js
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Slider/SpiderType/Simple/Assets/dist/ss-
simple.min.js
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider/Slider/SliderType/Simple/Assets/New folder (2
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Slider/SliderType/Simple/New folder (2
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider/Slider/SliderType/Simple/Simple (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/SliderType/SliderType (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/SmartSlider3 (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Arrow
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Arrow/Arrow (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Arrow/ArrowImage
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Arrow/Arrow/mage/Arrow/mage (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Arrow/ArrowImage/Assets
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Arrow/Arrow/mage/Assets/Assets (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Arrow/Arrow/mage/Assets/dist
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Arrow/Arrow/mage/Assets/dist/dist (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Arrow/Arrow/mage/Assets/dist/New folder
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Arrow/ArrowImage/Assets/dist/w-arrow-
image.min.js
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Arrow/Arrow/mage/Assets/New folder (2
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Arrow/Arrow/mage/New folder (2
```

http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Arrow/New folder (2

http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public

```
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Bullet
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Bullet/Assets
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Bullet/Assets/Assets (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Bullet/Assets/dist
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Bullet/Assets/dist/dist (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Bullet/Assets/dist/New folder (2
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Bullet/Assets/dist/w-bullet.min.js
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Bullet/Assets/New folder (2
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Bullet/Bullet (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Bullet/New folder (2
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/New folder (2
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/Public/SmartSlider3/Widget/Widget (copy
http://sdcinstitution.com/wp-content/plugins/smart-slider-3/smart-slider-3 (copy
http://sdcinstitution.com/wp-content/plugins/updraftplus
http://sdcinstitution.com/wp-content/plugins/updraftplus/admin.php
http://sdcinstitution.com/wp-content/plugins/updraftplus/images
http://sdcinstitution.com/wp-content/plugins/updraftplus/images/icons
http://sdcinstitution.com/wp-content/plugins/updraftplus/images/icons/icons (copy
http://sdcinstitution.com/wp-content/plugins/updraftplus/images/icons/New folder (2
http://sdcinstitution.com/wp-content/plugins/updraftplus/images/images (copy
http://sdcinstitution.com/wp-content/plugins/updraftplus/images/New folder (2
http://sdcinstitution.com/wp-content/plugins/updraftplus/includes
http://sdcinstitution.com/wp-content/plugins/updraftplus/includes (copy
http://sdcinstitution.com/wp-content/plugins/updraftplus/includes/images
http://sdcinstitution.com/wp-content/plugins/updraftplus/includes/images/images (copy
http://sdcinstitution.com/wp-content/plugins/updraftplus/includes/images/New folder (2
http://sdcinstitution.com/wp-content/plugins/updraftplus/includes/includes (copy
http://sdcinstitution.com/wp-content/plugins/updraftplus/includes/New folder (2
http://sdcinstitution.com/wp-content/plugins/updraftplus/js
http://sdcinstitution.com/wp-content/plugins/updraftplus/js/js (copy
http://sdcinstitution.com/wp-content/plugins/updraftplus/js/New folder (2
http://sdcinstitution.com/wp-content/plugins/updraftplus/languages
http://sdcinstitution.com/wp-content/plugins/updraftplus/languages/languages (copy
http://sdcinstitution.com/wp-content/plugins/updraftplus/languages/New folder (2
http://sdcinstitution.com/wp-content/plugins/updraftplus/New folder (2
http://sdcinstitution.com/wp-content/plugins/updraftplus/templates
http://sdcinstitution.com/wp-content/plugins/updraftplus/templates/New folder (2
http://sdcinstitution.com/wp-content/plugins/updraftplus/templates/templates (copy
http://sdcinstitution.com/wp-content/plugins/updraftplus/templates/wp-admin
http://sdcinstitution.com/wp-content/plugins/updraftplus/templates/wp-admin/New folder (2
http://sdcinstitution.com/wp-content/plugins/updraftplus/templates/wp-admin/settings
http://sdcinstitution.com/wp-content/plugins/updraftplus/templates/wp-admin/settings (copy
http://sdcinstitution.com/wp-content/plugins/updraftplus/templates/wp-admin/settings/New folder (2
http://sdcinstitution.com/wp-content/plugins/updraftplus/templates/wp-admin/settings/settings (copy
http://sdcinstitution.com/wp-content/plugins/updraftplus/templates/wp-admin/wp-admin (copy
http://sdcinstitution.com/wp-content/plugins/updraftplus/updraftplus (copy
http://sdcinstitution.com/wp-content/plugins/updraftplus/vendor
http://sdcinstitution.com/wp-content/plugins/updraftplus/vendor/New folder (2
http://sdcinstitution.com/wp-content/plugins/updraftplus/vendor/vendor (copy
http://sdcinstitution.com/wp-content/plugins/visual-footer-credit-remover
http://sdcinstitution.com/wp-content/plugins/visual-footer-credit-remover/New folder (2
http://sdcinstitution.com/wp-content/plugins/visual-footer-credit-remover/script.js
http://sdcinstitution.com/wp-content/plugins/visual-footer-credit-remover/visual-footer-credit-remover (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/assets (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/css
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/css/admin
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/css/admin (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/css/admin/admin (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/css/admin/New folder (2
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/css/choices.min.css
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/css/css (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/css/New folder (2
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/css/wpforms-full.min.css
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/fonts
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/fonts/fonts (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/fonts/New folder (2
```

```
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/images
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/images/images (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/images/New folder (2
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/js
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/js/js (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/js/New folder (2
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/js/utils.min.js
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/js/wpforms.min.js
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/languages
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/languages/languages (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/languages/New folder (2
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/lib
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/lib/choices.min.js
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/lib/jquery.validate.min.js
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/lib/lib (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/lib/mailcheck.min.js
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/lib/New folder (2
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/lib/punycode.min.js
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/assets/New folder (2
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/includes
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/includes (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/includes/admin
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/includes/admin (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/includes/admin/admin (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/includes/admin/New folder (2
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/includes/includes (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/includes/New folder (2
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/includes/templates
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/includes/templates/New folder (2
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/includes/templates/templates (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/libs
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/libs/libs (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/libs/New folder (2
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/New folder (2
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/src
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/src (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/src/Admin
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/src/Admin (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/src/Admin/Admin (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/src/Admin/New folder (2
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/src/New folder (2
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/src/src (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/templates
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/templates/admin
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/templates/admin (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/templates/admin/admin (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/templates/admin/forms
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/templates/admin/forms/forms (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/templates/admin/forms/New folder (2
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/templates/admin/New folder (2
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/templates/admin/settings
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/templates/admin/settings (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/templates/admin/settings/New folder (2
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/templates/admin/settings/settings (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/templates/New folder (2
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/templates/templates (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/vendor
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/vendor/New folder (2
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/vendor/vendor (copy
http://sdcinstitution.com/wp-content/plugins/wpforms-lite/wpforms-lite (copy
http://sdcinstitution.com/wp-content/themes
http://sdcinstitution.com/wp-content/themes/atom
http://sdcinstitution.com/wp-content/themes/feed
http://sdcinstitution.com/wp-content/themes/feed/atom
http://sdcinstitution.com/wp-content/themes/go
http://sdcinstitution.com/wp-content/themes/go/dist
http://sdcinstitution.com/wp-content/themes/go/dist/css
http://sdcinstitution.com/wp-content/themes/go/dist/css/admin
```

```
http://sdcinstitution.com/wp-content/themes/go/dist/css/admin (copy
http://sdcinstitution.com/wp-content/themes/go/dist/css/admin/admin (copy
http://sdcinstitution.com/wp-content/themes/go/dist/css/admin/New folder (2
http://sdcinstitution.com/wp-content/themes/go/dist/css/css (copy
http://sdcinstitution.com/wp-content/themes/go/dist/css/design-styles
http://sdcinstitution.com/wp-content/themes/go/dist/css/design-styles/design-styles (copy
http://sdcinstitution.com/wp-content/themes/go/dist/css/design-styles/New folder (2
http://sdcinstitution.com/wp-content/themes/go/dist/css/design-styles/style-playful.min.css
http://sdcinstitution.com/wp-content/themes/go/dist/css/New folder (2
http://sdcinstitution.com/wp-content/themes/go/dist/css/style-shared.min.css
http://sdcinstitution.com/wp-content/themes/go/dist/dist (copy
http://sdcinstitution.com/wp-content/themes/go/dist/images
http://sdcinstitution.com/wp-content/themes/go/dist/images/admin
http://sdcinstitution.com/wp-content/themes/go/dist/images/admin (copy
http://sdcinstitution.com/wp-content/themes/go/dist/images/admin/admin (copy
http://sdcinstitution.com/wp-content/themes/go/dist/images/admin/New folder (2
http://sdcinstitution.com/wp-content/themes/go/dist/images/design-styles
http://sdcinstitution.com/wp-content/themes/go/dist/images/design-styles/design-styles (copy
http://sdcinstitution.com/wp-content/themes/go/dist/images/design-styles/New folder (2
http://sdcinstitution.com/wp-content/themes/go/dist/images/design-styles/playful
http://sdcinstitution.com/wp-content/themes/go/dist/images/design-styles/playful/New folder (2
http://sdcinstitution.com/wp-content/themes/go/dist/images/design-styles/playful/playful (copy
http://sdcinstitution.com/wp-content/themes/go/dist/images/images (copy
http://sdcinstitution.com/wp-content/themes/go/dist/images/New folder (2
http://sdcinstitution.com/wp-content/themes/go/dist/js
http://sdcinstitution.com/wp-content/themes/go/dist/js/admin
http://sdcinstitution.com/wp-content/themes/go/dist/js/admin (copy
http://sdcinstitution.com/wp-content/themes/go/dist/js/admin/admin (copy
http://sdcinstitution.com/wp-content/themes/go/dist/js/admin/New folder (2
http://sdcinstitution.com/wp-content/themes/go/dist/js/frontend.min.js
http://sdcinstitution.com/wp-content/themes/go/dist/js/js (copy
http://sdcinstitution.com/wp-content/themes/go/dist/js/New folder (2
http://sdcinstitution.com/wp-content/themes/go/dist/New folder (2
http://sdcinstitution.com/wp-content/themes/go/dist/shared
http://sdcinstitution.com/wp-content/themes/go/dist/shared/images
http://sdcinstitution.com/wp-content/themes/go/go (copy
http://sdcinstitution.com/wp-content/themes/go/images
http://sdcinstitution.com/wp-content/themes/go/includes
http://sdcinstitution.com/wp-content/themes/go/includes (copy
http://sdcinstitution.com/wp-content/themes/go/includes/classes
http://sdcinstitution.com/wp-content/themes/go/includes/classes/classes (copy
http://sdcinstitution.com/wp-content/themes/go/includes/classes/New folder (2
http://sdcinstitution.com/wp-content/themes/go/includes/includes (copy
http://sdcinstitution.com/wp-content/themes/go/includes/New folder (2
http://sdcinstitution.com/wp-content/themes/go/New folder (2
http://sdcinstitution.com/wp-content/themes/go/partials
http://sdcinstitution.com/wp-content/themes/go/partials/layouts
http://sdcinstitution.com/wp-content/themes/go/partials/layouts/images
http://sdcinstitution.com/wp-content/themes/go/partials/layouts/images/images (copy
http://sdcinstitution.com/wp-content/themes/go/partials/layouts/images/New folder (2
http://sdcinstitution.com/wp-content/themes/go/partials/layouts/layouts (copy
http://sdcinstitution.com/wp-content/themes/go/partials/layouts/New folder (2
http://sdcinstitution.com/wp-content/themes/go/partials/New folder (2
http://sdcinstitution.com/wp-content/themes/go/partials/partials (copy
http://sdcinstitution.com/wp-content/themes/New folder (2
http://sdcinstitution.com/wp-content/themes/themes (copy
http://sdcinstitution.com/wp-content/upgrade
http://sdcinstitution.com/wp-content/upgrade/atom
http://sdcinstitution.com/wp-content/upgrade/feed
http://sdcinstitution.com/wp-content/upgrade/feed/atom
http://sdcinstitution.com/wp-content/upgrade/New folder (2
http://sdcinstitution.com/wp-content/upgrade/upgrade (copy
http://sdcinstitution.com/wp-content/uploads
http://sdcinstitution.com/wp-content/uploads (copy
http://sdcinstitution.com/wp-content/uploads/2021
http://sdcinstitution.com/wp-content/uploads/2021/03
http://sdcinstitution.com/wp-content/uploads/2021/03/03 (copy
http://sdcinstitution.com/wp-content/uploads/2021/03/New folder (2
```

```
http://sdcinstitution.com/wp-content/uploads/2021/04
http://sdcinstitution.com/wp-content/uploads/2021/04/04 (copy
http://sdcinstitution.com/wp-content/uploads/2021/04/New folder (2
http://sdcinstitution.com/wp-content/uploads/2021/06
http://sdcinstitution.com/wp-content/uploads/2021/06/06 (copy
http://sdcinstitution.com/wp-content/uploads/2021/06/New folder (2
http://sdcinstitution.com/wp-content/uploads/2021/07
http://sdcinstitution.com/wp-content/uploads/2021/07/07 (copy
http://sdcinstitution.com/wp-content/uploads/2021/07/New folder (2
http://sdcinstitution.com/wp-content/uploads/2021/08
http://sdcinstitution.com/wp-content/uploads/2021/08/08 (copy
http://sdcinstitution.com/wp-content/uploads/2021/08/New folder (2
http://sdcinstitution.com/wp-content/uploads/2021/09
http://sdcinstitution.com/wp-content/uploads/2021/09/09 (copy
http://sdcinstitution.com/wp-content/uploads/2021/09/New folder (2
http://sdcinstitution.com/wp-content/uploads/2021/10
http://sdcinstitution.com/wp-content/uploads/2021/10/10 (copy
http://sdcinstitution.com/wp-content/uploads/2021/10/New folder (2
http://sdcinstitution.com/wp-content/uploads/2021/2021 (copy
http://sdcinstitution.com/wp-content/uploads/2021/New folder (2
http://sdcinstitution.com/wp-content/uploads/2022
http://sdcinstitution.com/wp-content/uploads/2022/03
http://sdcinstitution.com/wp-content/uploads/2022/03/03 (copy
http://sdcinstitution.com/wp-content/uploads/2022/03/New folder (2
http://sdcinstitution.com/wp-content/uploads/2022/05
http://sdcinstitution.com/wp-content/uploads/2022/05/05 (copy
http://sdcinstitution.com/wp-content/uploads/2022/05/New folder (2
http://sdcinstitution.com/wp-content/uploads/2022/06
http://sdcinstitution.com/wp-content/uploads/2022/06/06 (copy
http://sdcinstitution.com/wp-content/uploads/2022/06/New folder (2
http://sdcinstitution.com/wp-content/uploads/2022/07
http://sdcinstitution.com/wp-content/uploads/2022/07/07 (copy
http://sdcinstitution.com/wp-content/uploads/2022/07/New folder (2
http://sdcinstitution.com/wp-content/uploads/2022/08
http://sdcinstitution.com/wp-content/uploads/2022/08/08 (copy
http://sdcinstitution.com/wp-content/uploads/2022/08/New folder (2
http://sdcinstitution.com/wp-content/uploads/2022/09
http://sdcinstitution.com/wp-content/uploads/2022/09/09 (copy
http://sdcinstitution.com/wp-content/uploads/2022/09/New folder (2
http://sdcinstitution.com/wp-content/uploads/2022/10
http://sdcinstitution.com/wp-content/uploads/2022/10/10 (copy
http://sdcinstitution.com/wp-content/uploads/2022/10/New folder (2
http://sdcinstitution.com/wp-content/uploads/2022/11
http://sdcinstitution.com/wp-content/uploads/2022/11/11 (copy
http://sdcinstitution.com/wp-content/uploads/2022/11/New folder (2
http://sdcinstitution.com/wp-content/uploads/2022/12
http://sdcinstitution.com/wp-content/uploads/2022/12/12 (copy
http://sdcinstitution.com/wp-content/uploads/2022/12/New folder (2
http://sdcinstitution.com/wp-content/uploads/2022/2022 (copy
http://sdcinstitution.com/wp-content/uploads/2022/New folder (2
http://sdcinstitution.com/wp-content/uploads/2023
http://sdcinstitution.com/wp-content/uploads/2023/01
http://sdcinstitution.com/wp-content/uploads/2023/01/01 (copy
http://sdcinstitution.com/wp-content/uploads/2023/01/New folder (2
http://sdcinstitution.com/wp-content/uploads/2023/02
http://sdcinstitution.com/wp-content/uploads/2023/02/02 (copy
http://sdcinstitution.com/wp-content/uploads/2023/02/New folder (2
http://sdcinstitution.com/wp-content/uploads/2023/04
http://sdcinstitution.com/wp-content/uploads/2023/04/04 (copy
http://sdcinstitution.com/wp-content/uploads/2023/04/New folder (2
http://sdcinstitution.com/wp-content/uploads/2023/05
http://sdcinstitution.com/wp-content/uploads/2023/05/05 (copy
http://sdcinstitution.com/wp-content/uploads/2023/05/New folder (2
http://sdcinstitution.com/wp-content/uploads/2023/06
http://sdcinstitution.com/wp-content/uploads/2023/06/06 (copy
http://sdcinstitution.com/wp-content/uploads/2023/06/New folder (2
http://sdcinstitution.com/wp-content/uploads/2023/2023 (copy
http://sdcinstitution.com/wp-content/uploads/2023/New folder (2
```

```
http://sdcinstitution.com/wp-content/uploads/atom
http://sdcinstitution.com/wp-content/uploads/feed
http://sdcinstitution.com/wp-content/uploads/feed/atom
http://sdcinstitution.com/wp-content/uploads/New folder (2
http://sdcinstitution.com/wp-content/uploads/slider
http://sdcinstitution.com/wp-content/uploads/slider/cache
http://sdcinstitution.com/wp-content/uploads/slider/cache/3f164cc78530550cc3cf2b6f0f86efc4
http://sdcinstitution.com/wp-
content/uploads/slider/cache/3f164cc78530550cc3cf2b6f0f86efc4/3f164cc78530550cc3cf2b6f0f86efc4 (copy
http://sdcinstitution.com/wp-content/uploads/slider/cache/3f164cc78530550cc3cf2b6f0f86efc4/New folder (2
http://sdcinstitution.com/wp-content/uploads/slider/cache/5a0c94c4fd93b5d478d3d927e684e3fd
http://sdcinstitution.com/wp-
content/uploads/slider/cache/5a0c94c4fd93b5d478d3d927e684e3fd/5a0c94c4fd93b5d478d3d927e684e3fd (copy
http://sdcinstitution.com/wp-content/uploads/slider/cache/5a0c94c4fd93b5d478d3d927e684e3fd/New folder (2
http://sdcinstitution.com/wp-content/uploads/slider/cache/7bd84ae4c0ddd1e4d06886b9b7f7c6db
http://sdcinstitution.com/wp-
content/uploads/slider/cache/7bd84ae4c0ddd1e4d06886b9b7f7c6db/7bd84ae4c0ddd1e4d06886b9b7f7c6db (copy
http://sdcinstitution.com/wp-content/uploads/slider/cache/7bd84ae4c0ddd1e4d06886b9b7f7c6db/New folder (2
http://sdcinstitution.com/wp-content/uploads/slider/cache/abad4872f453234069c4f38568ff8922
http://sdcinstitution.com/wp-
content/uploads/slider/cache/abad4872f453234069c4f38568ff8922/abad4872f453234069c4f38568ff8922 (copy
http://sdcinstitution.com/wp-content/uploads/slider/cache/abad4872f453234069c4f38568ff8922/New folder (2
http://sdcinstitution.com/wp-content/uploads/slider/cache/cache (copy
http://sdcinstitution.com/wp-content/uploads/slider/cache/d35191358dc4289beb4e02eb4a12007e
http://sdcinstitution.com/wp-
content/uploads/slider/cache/d35191358dc4289beb4e02eb4a12007e/d35191358dc4289beb4e02eb4a12007e (copy
http://sdcinstitution.com/wp-content/uploads/slider/cache/d35191358dc4289beb4e02eb4a12007e/New folder (2
http://sdcinstitution.com/wp-content/uploads/slider/cache/e2e18329d187962bbcaaa799c4acd997
http://sdcinstitution.com/wp-
content/uploads/slider/cache/e2e18329d187962bbcaaa799c4acd997/e2e18329d187962bbcaaa799c4acd997 (copy
http://sdcinstitution.com/wp-content/uploads/slider/cache/e2e18329d187962bbcaaa799c4acd997/New folder (2
http://sdcinstitution.com/wp-content/uploads/slider/cache/f5abfd4e11d21d1f5a3f1b429bb8d123
http://sdcinstitution.com/wp-
content/uploads/slider/cache/f5abfd4e11d21d1f5a3f1b429bb8d123/f5abfd4e11d21d1f5a3f1b429bb8d123 (copy
http://sdcinstitution.com/wp-content/uploads/slider/cache/f5abfd4e11d21d1f5a3f1b429bb8d123/New folder (2
http://sdcinstitution.com/wp-content/uploads/slider/cache/fed161314dfa96389c95790a2052175f
http://sdcinstitution.com/wp-
content/uploads/slider/cache/fed161314dfa96389c95790a2052175f/fed161314dfa96389c95790a2052175f (copy
http://sdcinstitution.com/wp-content/uploads/slider/cache/fed161314dfa96389c95790a2052175f/New folder (2
http://sdcinstitution.com/wp-content/uploads/slider/cache/New folder (2
http://sdcinstitution.com/wp-content/uploads/slider/New folder (2
http://sdcinstitution.com/wp-content/uploads/slider/slider (copy
http://sdcinstitution.com/wp-content/uploads/uploads (copy
http://sdcinstitution.com/wp-content/wp-content (copy
http://sdcinstitution.com/wp-download.php
http://sdcinstitution.com/wp-includes
http://sdcinstitution.com/wp-includes/assets
http://sdcinstitution.com/wp-includes/assets/assets (copy
http://sdcinstitution.com/wp-includes/assets/atom
http://sdcinstitution.com/wp-includes/assets/feed
http://sdcinstitution.com/wp-includes/assets/feed/atom
http://sdcinstitution.com/wp-includes/assets/New folder (2
http://sdcinstitution.com/wp-includes/atom
http://sdcinstitution.com/wp-includes/blocks
http://sdcinstitution.com/wp-includes/blocks/archives
http://sdcinstitution.com/wp-includes/blocks/archives/archives (copy
http://sdcinstitution.com/wp-includes/blocks/archives/New folder (2
http://sdcinstitution.com/wp-includes/blocks/atom
http://sdcinstitution.com/wp-includes/blocks/audio
http://sdcinstitution.com/wp-includes/blocks/audio/audio (copy
http://sdcinstitution.com/wp-includes/blocks/audio/New folder (2
http://sdcinstitution.com/wp-includes/blocks/blocks (copy
http://sdcinstitution.com/wp-includes/blocks/feed
http://sdcinstitution.com/wp-includes/blocks/feed/atom
http://sdcinstitution.com/wp-includes/blocks/file
http://sdcinstitution.com/wp-includes/blocks/file/file (copy
```

http://sdcinstitution.com/wp-includes/blocks/file/New folder (2 http://sdcinstitution.com/wp-includes/blocks/file/view.min.is

```
http://sdcinstitution.com/wp-includes/blocks/group
http://sdcinstitution.com/wp-includes/blocks/group/group (copy
http://sdcinstitution.com/wp-includes/blocks/group/New folder (2
http://sdcinstitution.com/wp-includes/blocks/html
http://sdcinstitution.com/wp-includes/blocks/html/html (copy
http://sdcinstitution.com/wp-includes/blocks/html/New folder (2
http://sdcinstitution.com/wp-includes/blocks/image
http://sdcinstitution.com/wp-includes/blocks/image/image (copy
http://sdcinstitution.com/wp-includes/blocks/image/New folder (2
http://sdcinstitution.com/wp-includes/blocks/list
http://sdcinstitution.com/wp-includes/blocks/list/list (copy
http://sdcinstitution.com/wp-includes/blocks/list/New folder (2
http://sdcinstitution.com/wp-includes/blocks/New folder (2
http://sdcinstitution.com/wp-includes/blocks/rss
http://sdcinstitution.com/wp-includes/blocks/search
http://sdcinstitution.com/wp-includes/blocks/search/New folder (2
http://sdcinstitution.com/wp-includes/blocks/search/search (copy
http://sdcinstitution.com/wp-includes/css
http://sdcinstitution.com/wp-includes/css/atom
http://sdcinstitution.com/wp-includes/css/buttons.min.css
http://sdcinstitution.com/wp-includes/css/classic-themes.min.css
http://sdcinstitution.com/wp-includes/css/css (copy
http://sdcinstitution.com/wp-includes/css/dashicons.min.css
http://sdcinstitution.com/wp-includes/css/dist
http://sdcinstitution.com/wp-includes/css/dist/block-library
http://sdcinstitution.com/wp-includes/css/dist/block-library/block-library (copy
http://sdcinstitution.com/wp-includes/css/dist/block-library/New folder (2
http://sdcinstitution.com/wp-includes/css/dist/block-library/style.min.css
http://sdcinstitution.com/wp-includes/css/dist/components
http://sdcinstitution.com/wp-includes/css/dist/components/components (copy
http://sdcinstitution.com/wp-includes/css/dist/components/New folder (2
http://sdcinstitution.com/wp-includes/css/dist/components/style.min.css
http://sdcinstitution.com/wp-includes/css/dist/dist (copy
http://sdcinstitution.com/wp-includes/css/dist/editor
http://sdcinstitution.com/wp-includes/css/dist/editor/editor (copy
http://sdcinstitution.com/wp-includes/css/dist/editor/New folder (2
http://sdcinstitution.com/wp-includes/css/dist/New folder (2
http://sdcinstitution.com/wp-includes/css/feed
http://sdcinstitution.com/wp-includes/css/feed/atom
http://sdcinstitution.com/wp-includes/css/New folder (2
http://sdcinstitution.com/wp-includes/download
http://sdcinstitution.com/wp-includes/feed
http://sdcinstitution.com/wp-includes/feed/atom
http://sdcinstitution.com/wp-includes/fonts
http://sdcinstitution.com/wp-includes/fonts/atom
http://sdcinstitution.com/wp-includes/fonts/feed
http://sdcinstitution.com/wp-includes/fonts/feed/atom
http://sdcinstitution.com/wp-includes/fonts/fonts (copy
http://sdcinstitution.com/wp-includes/fonts/New folder (2
http://sdcinstitution.com/wp-includes/image
http://sdcinstitution.com/wp-includes/images
http://sdcinstitution.com/wp-includes/images/atom
http://sdcinstitution.com/wp-includes/images/feed
http://sdcinstitution.com/wp-includes/images/feed/atom
http://sdcinstitution.com/wp-includes/images/images (copy
http://sdcinstitution.com/wp-includes/images/media
http://sdcinstitution.com/wp-includes/images/media/media (copy
http://sdcinstitution.com/wp-includes/images/media/New folder (2
http://sdcinstitution.com/wp-includes/images/New folder (2
http://sdcinstitution.com/wp-includes/js
http://sdcinstitution.com/wp-includes/js/atom
http://sdcinstitution.com/wp-includes/js/comment-reply.min.js
http://sdcinstitution.com/wp-includes/is/dist
http://sdcinstitution.com/wp-includes/js/dist/dist (copy
http://sdcinstitution.com/wp-includes/js/dist/hooks.min.js
http://sdcinstitution.com/wp-includes/js/dist/i18n.min.js
http://sdcinstitution.com/wp-includes/js/dist/New folder (2
http://sdcinstitution.com/wp-includes/js/dist/vendor
```

```
http://sdcinstitution.com/wp-includes/js/dist/vendor/New folder (2
http://sdcinstitution.com/wp-includes/js/dist/vendor/regenerator-runtime.min.js
http://sdcinstitution.com/wp-includes/js/dist/vendor/vendor (copy
http://sdcinstitution.com/wp-includes/js/dist/vendor/wp-polyfill.min.js
http://sdcinstitution.com/wp-includes/js/feed
http://sdcinstitution.com/wp-includes/js/feed/atom
http://sdcinstitution.com/wp-includes/js/jguery
http://sdcinstitution.com/wp-includes/js/jquery/jquery-migrate.min.js
http://sdcinstitution.com/wp-includes/js/jquery/jquery (copy
http://sdcinstitution.com/wp-includes/js/jquery/jquery.min.js
http://sdcinstitution.com/wp-includes/js/jquery/New folder (2
http://sdcinstitution.com/wp-includes/js/js (copy
http://sdcinstitution.com/wp-includes/js/New folder (2
http://sdcinstitution.com/wp-includes/js/plupload
http://sdcinstitution.com/wp-includes/js/plupload/New folder (2
http://sdcinstitution.com/wp-includes/js/plupload/plupload (copy
http://sdcinstitution.com/wp-includes/js/swfupload
http://sdcinstitution.com/wp-includes/js/swfupload/New folder (2
http://sdcinstitution.com/wp-includes/js/swfupload/swfupload (copy
http://sdcinstitution.com/wp-includes/js/underscore.min.js
http://sdcinstitution.com/wp-includes/is/wp-emoii-release.min.is
http://sdcinstitution.com/wp-includes/js/wp-util.min.js
http://sdcinstitution.com/wp-includes/js/zxcvbn-async.min.js
http://sdcinstitution.com/wp-includes/js/zxcvbn.min.js
http://sdcinstitution.com/wp-includes/m
http://sdcinstitution.com/wp-includes/New folder (2
http://sdcinstitution.com/wp-includes/wlwmanifest.xml
http://sdcinstitution.com/wp-includes/wp-includes (copy
http://sdcinstitution.com/wp-json
http://sdcinstitution.com/wp-json/oembed
http://sdcinstitution.com/wp-json/oembed/1.0
http://sdcinstitution.com/wp-json/oembed/1.0/embed
http://sdcinstitution.com/wp-json/wp
http://sdcinstitution.com/wp-json/wp/v2
http://sdcinstitution.com/wp-json/wp/v2/media
http://sdcinstitution.com/wp-json/wp/v2/media/1296
http://sdcinstitution.com/wp-json/wp/v2/media/900
http://sdcinstitution.com/wp-json/wp/v2/pages
http://sdcinstitution.com/wp-json/wp/v2/pages/100
http://sdcinstitution.com/wp-json/wp/v2/pages/102
http://sdcinstitution.com/wp-json/wp/v2/pages/104
http://sdcinstitution.com/wp-json/wp/v2/pages/106
http://sdcinstitution.com/wp-json/wp/v2/pages/113
http://sdcinstitution.com/wp-json/wp/v2/pages/115
http://sdcinstitution.com/wp-json/wp/v2/pages/118
http://sdcinstitution.com/wp-json/wp/v2/pages/12
http://sdcinstitution.com/wp-json/wp/v2/pages/120
http://sdcinstitution.com/wp-json/wp/v2/pages/13
http://sdcinstitution.com/wp-json/wp/v2/pages/131
http://sdcinstitution.com/wp-json/wp/v2/pages/134
http://sdcinstitution.com/wp-json/wp/v2/pages/138
http://sdcinstitution.com/wp-json/wp/v2/pages/140
http://sdcinstitution.com/wp-json/wp/v2/pages/169
http://sdcinstitution.com/wp-json/wp/v2/pages/261
http://sdcinstitution.com/wp-json/wp/v2/pages/264
http://sdcinstitution.com/wp-json/wp/v2/pages/270
http://sdcinstitution.com/wp-json/wp/v2/pages/273
http://sdcinstitution.com/wp-json/wp/v2/pages/276
http://sdcinstitution.com/wp-json/wp/v2/pages/279
http://sdcinstitution.com/wp-json/wp/v2/pages/282
http://sdcinstitution.com/wp-json/wp/v2/pages/285
http://sdcinstitution.com/wp-json/wp/v2/pages/290
http://sdcinstitution.com/wp-json/wp/v2/pages/293
http://sdcinstitution.com/wp-json/wp/v2/pages/296
http://sdcinstitution.com/wp-json/wp/v2/pages/299
http://sdcinstitution.com/wp-json/wp/v2/pages/302
http://sdcinstitution.com/wp-json/wp/v2/pages/305
http://sdcinstitution.com/wp-json/wp/v2/pages/308
```

http://sdcinstitution.com/wp-json/wp/v2/pages/311 http://sdcinstitution.com/wp-json/wp/v2/pages/314 http://sdcinstitution.com/wp-json/wp/v2/pages/317 http://sdcinstitution.com/wp-json/wp/v2/pages/320 http://sdcinstitution.com/wp-json/wp/v2/pages/323 http://sdcinstitution.com/wp-json/wp/v2/pages/326 http://sdcinstitution.com/wp-json/wp/v2/pages/329 http://sdcinstitution.com/wp-json/wp/v2/pages/332 http://sdcinstitution.com/wp-json/wp/v2/pages/335 http://sdcinstitution.com/wp-json/wp/v2/pages/338 http://sdcinstitution.com/wp-json/wp/v2/pages/341 http://sdcinstitution.com/wp-json/wp/v2/pages/344 http://sdcinstitution.com/wp-json/wp/v2/pages/347 http://sdcinstitution.com/wp-json/wp/v2/pages/350 http://sdcinstitution.com/wp-json/wp/v2/pages/353 http://sdcinstitution.com/wp-json/wp/v2/pages/356 http://sdcinstitution.com/wp-json/wp/v2/pages/359 http://sdcinstitution.com/wp-json/wp/v2/pages/362 http://sdcinstitution.com/wp-json/wp/v2/pages/365 http://sdcinstitution.com/wp-json/wp/v2/pages/368 http://sdcinstitution.com/wp-ison/wp/v2/pages/455 http://sdcinstitution.com/wp-json/wp/v2/pages/461 http://sdcinstitution.com/wp-json/wp/v2/pages/628 http://sdcinstitution.com/wp-json/wp/v2/pages/63 http://sdcinstitution.com/wp-json/wp/v2/pages/66 http://sdcinstitution.com/wp-json/wp/v2/pages/68 http://sdcinstitution.com/wp-json/wp/v2/pages/73 http://sdcinstitution.com/wp-json/wp/v2/pages/75 http://sdcinstitution.com/wp-json/wp/v2/pages/758 http://sdcinstitution.com/wp-json/wp/v2/pages/78 http://sdcinstitution.com/wp-json/wp/v2/pages/80 http://sdcinstitution.com/wp-json/wp/v2/pages/82 http://sdcinstitution.com/wp-json/wp/v2/pages/9 http://sdcinstitution.com/wp-json/wp/v2/pages/90 http://sdcinstitution.com/wp-json/wp/v2/pages/95 http://sdcinstitution.com/wp-json/wp/v2/pages/98 http://sdcinstitution.com/wp-json/wp/v2/posts http://sdcinstitution.com/wp-json/wp/v2/posts/1862 http://sdcinstitution.com/wp-json/wp/v2/posts/1865 http://sdcinstitution.com/wp-json/wp/v2/posts/1870 http://sdcinstitution.com/wp-json/wp/v2/posts/1892 http://sdcinstitution.com/wp-json/wp/v2/posts/1896 http://sdcinstitution.com/wp-json/wp/v2/posts/1901 http://sdcinstitution.com/wp-json/wp/v2/posts/1904 http://sdcinstitution.com/wp-json/wp/v2/posts/1908 http://sdcinstitution.com/wp-json/wp/v2/posts/1915 http://sdcinstitution.com/wp-login.php http://sdcinstitution.com/wp-sitemap.xml http://sdcinstitution.com/xmlrpc.php