Nama : Anak Agung Istri Istadewanti
NRP : 5026211143
Kelas : PAI (C)

Link Youtube:

https://youtu.be/4Z9Ajvo6f-g

acunetix

Developer Report

Acunetix Security Audit

04 June 2023

Generated by Acunetix

Scan of http://testphp.vulnweb.com

Scan details

Scan information	
Start time	04/06/2023, 04:42:09
Start url	http://testphp.vulnweb.com
Host	http://testphp.vulnweb.com
Scan time	50 minutes, 28 seconds
Profile	Full Scan

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	200
High	92
Medium	79
Low	9
Informational	20

Alerts summary

Blind SQL Injection

Classification	
CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation 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: 10.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-89

Affected items	Variation
Web Server	34

Cross site scripting

Classification	
CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial 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: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79

Affected items	Variation
Web Server	19

Directory traversal

Classification	
CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation 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: Low Integrity Impact: None Availability Impact: None
CWE	CWE-22

Affected items	Variation
Web Server	1

PHP allow_url_fopen enabled (AcuSensor)

Classification	
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 items	Variation
Web Server	1

Script source code disclosure

Classification	
	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
CWE	CWE-538

Affected items	Variation
Web Server	1

SQL injection

Classification	
CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation 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: 10.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-89

Affected items	Variation
Web Server	35

Weak password

Classification	
CVSS2	Base Score: 7.5 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation 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 items	Variation
Web Server	1

.htaccess file readable

Classification	
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-16

Affected items	Variation
Web Server	1

Application error message

Classification	
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: Low Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation

Web Server	7

Backup files

Classification	
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 items	Variation
Web Server	18

Backup files

Classification	
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 items	Variation
Web Server	2

CRLF injection/HTTP response splitting

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low 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: 5.4 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-113

Affected items	Variation
Web Server	1

Cross domain data hijacking

Classification	
CVSS2	Base Score: 4.3 Access Vector: Network_accessible Access Complexity: Medium 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
CWE	CWE-20

Affected items	Variation
Web Server	1

Cross site scripting (content-sniffing)

Classification	
CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial 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: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None

CWE	CWE-79

Affected items	Variation
Web Server	1

Directory listing

Classification	
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-538

Affected items	Variation
Web Server	15

Error message on page

Classification	
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: Low Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
Web Server	12

HTML form without CSRF protection

Classification	
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 items	Variation
Web Server	6

HTTP parameter pollution

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low 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: 9.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-88

Affected items	Variation

Web Server	2

Insecure crossdomain.xml file

Classification	
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: 6.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-284

Affected items	Variation
Web Server	1

JetBrains .idea project directory

Classification	
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 items	Variation
Web Server	1

PHP allow_url_fopen enabled

Classification	
	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: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CWE	CWE-16

Affected items	Variation
Web Server	1

PHP errors enabled

Classification	
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: Low Integrity Impact: None Availability Impact: None
CWE	CWE-16

Affected items	Variation
Web Server	1

PHP errors enabled (AcuSensor)

Classification	
	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
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CWE	CWE-16

Affected items	Variation
Web Server	1

PHP open_basedir is not set

Classification	
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: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CWE	CWE-16

Affected items	Variation
Web Server	1

PHP session.use_only_cookies disabled

Classification	
	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 items	Variation
Web Server	1

PHPinfo page

Classification	
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 items	Variation
Web Server	1

PHPinfo page found

Classification	
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 items	Variation
Web Server	1

URL redirection

Classification	
CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial 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: 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-601

Affected items	Variation
Web Server	1

User credentials are sent in clear text

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: High Remediation Level: Workaround Report Confidence: Confirmed Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
	Base Score: 9.1 Attack Vector: Network Attack Complexity: Low

CVSS3	Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-310

Affected items	Variation
Web Server	2

WS_FTP log file found

Classification	
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 items	Variation
Web Server	1

Clickjacking: X-Frame-Options header missing

Classification	
CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation 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-693

Affected items	Variation
Web Server	1

Hidden form input named price was found

Classification	
	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
CWE	CWE-16

Affected items	Variation
Web Server	1

Login page password-guessing attack

Classification	
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 items	Variation
Web Server	1

MySQL username disclosure

Classification	
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-538

Affected items	Variation
Web Server	6

Broken links

Classification	
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 items	Variation
Web Server	4

Email address found

Classification	
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 items	Variation
Web Server	1

Microsoft Office possible sensitive information

Classification	
	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
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 items	Variation
Web Server	1

Password type input with auto-complete enabled

Classification	
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 items	Variation
Web Server	2

Possible internal IP address disclosure

Classification	
	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 items	Variation
Web Server	3

Possible server path disclosure (Unix)

Classification	
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 items	Variation
Web Server	2

Possible username or password disclosure

Classification	
	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 items	Variation
Web Server	7

Alerts details

Blind SQL Injection

Severity	**High**
Reported by module	Scripting (Blind_Sql_Injection.script)

Description

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

Impact

An attacker can use SQL injection it to bypass a web application's authentication and authorization mechanisms and retrieve the contents of an entire database. SQLi can also be used to add, modify and delete records in a database, affecting data integrity. Under the right circumstances, SQLi can also be used by an attacker to execute OS commands, which may then be used to escalate an attack even further.

Recommendation

Use parameterized queries when dealing with SQL queries that contains user input. Parameterized queries allows the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.

References

SQL Injection (SQLi) - Acunetix (https://www.acunetix.com/websitesecurity/sql-injection/)
Types of SQL Injection (SQLi) - Acunetix (https://www.acunetix.com/websitesecurity/sql-injection2/)
Prevent SQL injection vulnerabilities in PHP applications and fix them - Acunetix (prevent-sql-injection-vulnerabilities-in-php-applications/)
SQL Injection - OWASP (https://www.owasp.org/index.php/SQL_Injection)
Bobby Tables: A guide to preventing SQL injection (http://bobby-tables.com/)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server

Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial

Request headers

`Not available in the free trial`

Web Server

Details

Not available in the free trial

Request headers

`Not available in the free trial`

Web Server

Details

Not available in the free trial

Request headers

`Not available in the free trial`

Web Server

Details

Not available in the free trial

Request headers

`Not available in the free trial`

Web Server

Details

Not available in the free trial

Request headers

`Not available in the free trial`

Web Server

Details

Not available in the free trial

Request headers

`Not available in the free trial`

Web Server

Details

Not available in the free trial

Request headers

`Not available in the free trial`

Web Server

Details

Not available in the free trial

Request headers

`Not available in the free trial`

Web Server

Details

Not available in the free trial

Request headers

`Not available in the free trial`

Web Server

Details

Not available in the free trial

Request headers

`Not available in the free trial`

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details

Not available in the free trial
Request headers
Not available in the free trial
Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial

Cross site scripting

Severity	**High**
Reported by module	Scripting (XSS.script)

Description

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

Impact

Malicious JavaScript has access to all the same objects as the rest of the web page, including access to cookies and local storage, which are often used to store session tokens. If an attacker can obtain a user's session cookie, they can then impersonate that user.

Furthermore, JavaScript can read and make arbitrary modifications to the contents of a page being displayed to a user. Therefore, XSS in conjunction with some clever social engineering opens up a lot of possibilities for an attacker.

Recommendation

Apply context-dependent encoding and/or validation to user input rendered on a page

References

Cross-site Scripting (XSS) Attack - Acunetix (https://www.acunetix.com/websitesecurity/cross-site-scripting/)
Types of XSS - Acunetix (https://www.acunetix.com/websitesecurity/xss/)
Cross-site Scripting - OWASP (http://www.owasp.org/index.php/Cross_Site_Scripting)
XSS Filter Evasion Cheat Sheet (https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
Excess XSS, a comprehensive tutorial on cross-site scripting (https://excess-xss.com/)
Cross site scripting (http://en.wikipedia.org/wiki/Cross-site_scripting)

Affected items

Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial
Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial
Web Server
Details

Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers

Not available in the free trial
Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial
Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial
Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial
Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial
Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial
Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial
Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial

Directory traversal

Severity	**High**
Reported by module	Scripting (Directory_Traversal.script)

Description

This script is possibly vulnerable to directory traversal attacks.

Directory Traversal is a vulnerability which allows attackers to access restricted directories and read files outside of the web server's root directory.

Impact

By exploiting directory traversal vulnerabilities, attackers step out of the root directory and access files in other directories. As a result, attackers might view restricted files or execute commands, leading to a full compromise of the Web server.

Recommendation

Your script should filter metacharacters from user input.

References

Acunetix Directory Traversal Attacks (http://www.acunetix.com/websitesecurity/directory-traversal/)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

PHP allow_url_fopen enabled (AcuSensor)

Severity	**High**
Reported by module	

Description

The PHP configuration directive allow_url_fopen is enabled. When enabled, this directive allows data retrieval from remote locations (web site or FTP server). A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling allow_url_fopen and bad input filtering.

allow_url_fopen is enabled by default.

Impact

Application dependant - possible remote file inclusion.

Recommendation

You can disable allow_url_fopen from either php.ini (for PHP versions newer than 4.3.4) or .htaccess (for PHP versions up to 4.3.4).

php.ini
allow_url_fopen = 'off'

.htaccess
php_flag allow_url_fopen off

References

Runtime Configuration (http://www.php.net/manual/en/filesystem.configuration.php)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

Script source code disclosure

Severity	**High**
Reported by module	Scripting (Script_Source_Code_Disclosure.script)

Description

It is possible to read the source code of this script by using script filename as a parameter. It seems that this script includes a file which name is determined using user-supplied data. This data is not properly validated before being passed to the include function.

Impact

An attacker can gather sensitive information (database connection strings, application logic) by analyzing the source code. This information can be used to launch further attacks.

Recommendation

Analyze the source code of this script and solve the problem.

References

Source Code Disclosure (http://www.imperva.com/resources/glossary?term=source_code_disclosure)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

SQL injection

Severity	**High**
Reported by module	Scripting (Sql_Injection.script)

Description

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

Impact

An attacker can use SQL injection it to bypass a web application's authentication and authorization mechanisms and retrieve the contents of an entire database. SQLi can also be used to add, modify and delete records in a database, affecting data integrity. Under the right circumstances, SQLi can also be used by an attacker to execute OS commands, which may then be used to escalate an attack even further.

Recommendation

Use parameterized queries when dealing with SQL queries that contains user input. Parameterized queries allows the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.

References

SQL Injection (SQLi) - Acunetix (https://www.acunetix.com/websitesecurity/sql-injection/)
Types of SQL Injection (SQLi) - Acunetix (https://www.acunetix.com/websitesecurity/sql-injection2/)
Prevent SQL injection vulnerabilities in PHP applications and fix them - Acunetix (https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/)

[SQL Injection - OWASP](https://www.owasp.org/index.php/SQL_Injection) (https://www.owasp.org/index.php/SQL_Injection)
[Bobby Tables: A guide to preventing SQL injection](http://bobby-tables.com/) (http://bobby-tables.com/)
[SQL Injection Cheet Sheets - Pentestmonkey](http://pentestmonkey.net/category/cheat-sheet/sql-injection) (http://pentestmonkey.net/category/cheat-sheet/sql-injection)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial

Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details

Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

Weak password

Severity	**High**
Reported by module	Scripting (Html_Authentication_Audit.script)

Description

This page is using a weak password. Acunetix was able to guess the credentials required to access this page. A weak password is short, common, a system default, or something that could be rapidly guessed by executing a brute force attack using a subset of all possible passwords, such as words in the dictionary, proper names, words based on the user name or common variations on these themes.

Impact

An attacker may access the contents of the password-protected page.

Recommendation

Enforce a strong password policy. Don't permit weak passwords or passwords based on dictionary words.

References

Wikipedia - Password strength (http://en.wikipedia.org/wiki/Password_strength)
Authentication Hacking Attacks (http://www.acunetix.com/websitesecurity/authentication/)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

.htaccess file readable

Severity	**Medium**
Reported by module	Scripting (htaccess_File_Readable.script)

Description

This directory contains an **.htaccess** file that is readable. This may indicate a server misconfiguration. htaccess files are designed to be parsed by web server and should not be directly accessible. These files could contain sensitive information that could help an attacker to conduct further attacks. It's recommended to restrict access to this file.

Impact

Possible sensitive information disclosure.

Recommendation

Restrict access to the .htaccess file by adjusting the web server configuration.

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

Application error message

Severity	**Medium**
Reported by module	Scripting (XSS.script)

Description

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

Impact

Error messages may disclose sensitive information which can be used to escalate attacks.

Recommendation

Verify that this page is disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.

References

PHP Runtime Configuration (http://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors)
Improper Error Handling (https://www.owasp.org/index.php/Improper_Error_Handling)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

Backup files

Severity	**Medium**
Reported by module	Scripting (Backup_Folder.script)

Description

A possible backup copy of a directory was found on your web server. These files are usually created by developers to backup their work.

Impact

Backup files can contain script sources, configuration files or other sensitive information that may help an malicious user to prepare more advanced attacks.

Recommendation

Remove the file(s) if they are not required on your website. As an additional step, it is recommended to implement a security policy within your organization to disallow creation of backup files in directories accessible from the web.

References

Testing for Old, Backup and Unreferenced Files (OWASP-CM-006) (https://www.owasp.org/index.php/Review_Old,_Backup_and_Unreferenced_Files_for_Sensitive_Information_(OTG-CONFIG-004))
Security Tips for Server Configuration (http://httpd.apache.org/docs/1.3/misc/security_tips.html)
Protecting Confidential Documents at Your Site (http://www.w3.org/Security/Faq/wwwsf5.html)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers

`Not available in the free trial`

Web Server

Details

Not available in the free trial

Request headers

`Not available in the free trial`

Web Server

Details

Not available in the free trial

Request headers

`Not available in the free trial`

Web Server

Details

Not available in the free trial

Request headers

`Not available in the free trial`

Web Server

Details

Not available in the free trial

Request headers

`Not available in the free trial`

Web Server

Details

Not available in the free trial

Request headers

`Not available in the free trial`

Web Server

Details

Not available in the free trial

Request headers

`Not available in the free trial`

Web Server

Details

Not available in the free trial

Request headers

`Not available in the free trial`

Web Server

Details

Not available in the free trial

Request headers

`Not available in the free trial`

Web Server

Details

Not available in the free trial

Request headers

`Not available in the free trial`

Web Server

Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

Backup files

Severity	**Medium**
Reported by module	Scripting (Backup_File.script)

Description

A possible backup file was found on your web-server. These files are usually created by developers to backup their work.

Impact

Backup files can contain script sources, configuration files or other sensitive information that may help an malicious user to prepare more advanced attacks.

Recommendation

Remove the file(s) if they are not required on your website. As an additional step, it is recommended to implement a security policy within your organization to disallow creation of backup files in directories accessible from the web.

References

Testing for Old, Backup and Unreferenced Files (OWASP-CM-006) (https://www.owasp.org/index.php/Review_Old,_Backup_and_Unreferenced_Files_for_Sensitive_Information_(OTG-CONFIG-004))
Security Tips for Server Configuration (http://httpd.apache.org/docs/1.3/misc/security_tips.html)
Protecting Confidential Documents at Your Site (http://www.w3.org/Security/Faq/wwwsf5.html)

Affected items

Web Server

Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

CRLF injection/HTTP response splitting

Severity	**Medium**
Reported by module	Scripting (CRLF_Injection.script)

Description

This script is possibly vulnerable to CRLF injection attacks.

HTTP headers have the structure "Key: Value", where each line is separated by the CRLF combination. If the user input is injected into the value section without properly escaping/removing CRLF characters it is possible to alter the HTTP headers structure.
HTTP Response Splitting is a new application attack technique which enables various new attacks such as web cache poisoning, cross user defacement, hijacking pages with sensitive user information and cross-site scripting (XSS). The attacker sends a single HTTP request that forces the web server to form an output stream, which is then interpreted by the target as two HTTP responses instead of one response.

Impact

Is it possible for a remote attacker to inject custom HTTP headers. For example, an attacker can inject session cookies or HTML code. This may conduct to vulnerabilities like XSS (cross-site scripting) or session fixation.

Recommendation

You need to restrict CR(0x13) and LF(0x10) from the user input or properly encode the output in order to prevent the injection of custom HTTP headers.

References

Acunetix CRLF Injection Attack (http://www.acunetix.com/websitesecurity/crlf-injection.htm)
Whitepaper - HTTP Response Splitting (http://packetstormsecurity.org/papers/general/whitepaper_httpresponse.pdf)
Introduction to HTTP Response Splitting (http://www.securiteam.com/securityreviews/5WP0E2KFGK.html)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

Cross domain data hijacking

Severity	**Medium**
Reported by module	Scripting (XSS.script)

Description

This page is possibly vulnerable to Cross domain data hijacking. If an attacker can create/upload a malicious Flash (SWF) file or control the top part of any page he can perform an attack known as **Cross domain data hijacking**. The Content-Type of the response doesn't matter. If the file is embedded using an <object> tag, it will be executed as a Flash file as long as the content of the file looks like a valid Flash file.

Here is the attack scenario:

- An attacker creates a malicious Flash (SWF) file
- The attacker changes the file extension to JPG
- The attacker uploads the file to victim.com
- The attacker embeds the file on attacker.com using an tag with type "application/x-shockwave-flash"
- The victim visits attacker.com, loads the file as embedded with the tag
- The attacker can now send and receive arbitrary requests to victim.com using the victims session
- The attacker sends a request to victim.com and extracts the CSRF token from the response

There are many ways to perform this attack. The attacker doesn't need to upload a file. The only requirement is that an attacker can control the data on a location of the target domain. One way is to abuse a JSONP API. Usually, the attacker can control the output of a JSONP API endpoint by changing the callback parameter. However, if an attacker uses an entire Flash file as callback, we can use it just like we would use an uploaded file in this attack.

A payload could look like this:

```
<object style="height:1px;width:1px;" data="http://victim.com/user/jsonp?callback=CWS%07%0E000
```

Impact

An attacker can read any secrets (such as CSRF tokens) from the affected domain.

Recommendation

For file uploads: It is recommended to check the file's content to have the correct header and format. If possible, use "Content-Disposition: attachment; filename=Filename.Extension;" header for the files that do not need to be served in the web browser. Isolating the domain of the uploaded files is also a good solution as long as the crossdomain.xml file of the main website does not include the isolated domain.

For other cases: For JSONP abuses or other cases when the attacker control the top part of the page, you need to perform proper input filtering to protect against this type of issues.

References

Cross Domain Data Hijacking (https://soroush.secproject.com/blog/2014/05/even-uploading-a-jpg-file-can-lead-to-cross-domain-data-hijacking-client-side-attack/)
The pitfalls of allowing file uploads on your website (http://labs.detectify.com/post/86302927946/the-lesser-known-pitfalls-of-allowing-file-uploads)

Affected items

Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial

Cross site scripting (content-sniffing)

Severity	**Medium**
Reported by module	Scripting (XSS.script)

Description

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

Impact

Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to fool a user in order to gather data from them. An attacker can steal the session cookie and take over the account, impersonating the user. It is also possible to modify the content of the page presented to the user.

Recommendation

Your script should filter metacharacters from user input.

References

Acunetix Cross Site Scripting Attack (http://www.acunetix.com/websitesecurity/cross-site-scripting.htm)
VIDEO: How Cross-Site Scripting (XSS) Works (http://www.acunetix.com/blog/web-security-zone/video-how-cross-site-scripting-xss-works/)
The Cross Site Scripting Faq (http://www.cgisecurity.com/xss-faq.html)
OWASP Cross Site Scripting (http://www.owasp.org/index.php/Cross_Site_Scripting)
XSS Filter Evasion Cheat Sheet (https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
Cross site scripting (http://en.wikipedia.org/wiki/Cross-site_scripting)
OWASP PHP Top 5 (http://www.owasp.org/index.php/PHP_Top_5)
How To: Prevent Cross-Site Scripting in ASP.NET (http://msdn.microsoft.com/en-us/library/ms998274.aspx)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

Directory listing

Severity	**Medium**
Reported by module	Scripting (Directory_Listing.script)

Description

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

Impact

A user can view a list of all files from this directory possibly exposing sensitive information.

Recommendation

You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration.

References

Directory Listing and Information Disclosure (http://www.acunetix.com/blog/web-security-zone/directory-listing-information-disclosure/)

Affected items

Web Server

Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial

Request headers
Not available in the free trial
Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial
Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial
Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial
Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial

Error message on page

Severity	**Medium**
Reported by module	Scripting (Text_Search_File.script)

Description

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

Impact

Error messages may disclose sensitive information which can be used to escalate attacks.

Recommendation

Verify that this page is disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.

References

PHP Runtime Configuration (http://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors)
Improper Error Handling (https://www.owasp.org/index.php/Improper_Error_Handling)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers

Not available in the free trial
Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial
Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial
Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial

HTML form without CSRF protection

Severity	**Medium**
Reported by module	Crawler

Description

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.

Impact

An attacker could use CSRF to trick a victim into accessing a website hosted by the attacker, or clicking a URL containing malicious or unauthorized requests.

CSRF is a type of 'confused deputy' attack which leverages the authentication and authorization of the victim when the forged request is being sent to the web server. Therefore, if a CSRF vulnerability could affect highly privileged users such as administrators full application compromise may be possible.

Recommendation

Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary.

The recommended and the most widely used technique for preventing CSRF attacks is know as an anti-CSRF token, also sometimes referred to as a synchronizer token. The characteristics of a well designed anti-CSRF system involve the following attributes.

- The anti-CSRF token should be unique for each user session
- The session should automatically expire after a suitable amount of time
- The anti-CSRF token should be a cryptographically random value of significant length
- The anti-CSRF token should be cryptographically secure, that is, generated by a strong Pseudo-Random Number Generator (PRNG) algorithm
- The anti-CSRF token is added as a hidden field for forms, or within URLs (only necessary if GET requests cause state changes, that is, GET requests are not idempotent)
- The server should reject the requested action if the anti-CSRF token fails validation

When a user submits a form or makes some other authenticated request that requires a Cookie, the anti-CSRF token should be included in the request. Then, the web application will then verify the existence and correctness of this token before processing the request. If the token is missing or incorrect, the request can be rejected.

References

What is Cross Site Reference Forgery (CSRF)? (https://www.acunetix.com/websitesecurity/csrf-attacks/)
Cross-Site Request Forgery (CSRF) Prevention Cheatsheet (https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet)
The Cross-Site Request Forgery (CSRF/XSRF) FAQ (http://www.cgisecurity.com/csrf-faq.html)
Cross-site Request Forgery (https://en.wikipedia.org/wiki/Cross-site_request_forgery)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

HTTP parameter pollution

Severity	**Medium**
Reported by module	Scripting (HTTP_Parameter_Pollution.script)

Description

This script is possibly vulnerable to HTTP Parameter Pollution attacks.

HPP attacks consist of injecting encoded query string delimiters into other existing parameters. If the web application does not properly sanitize the user input, a malicious user can compromise the logic of the application to perform either clientside or server-side attacks.

Impact

The impact depends on the affected web application. An attacker could

- Override existing hardcoded HTTP parameters
- Modify the application behaviors
- Access and, potentially exploit, uncontrollable variables
- Bypass input validation checkpoints and WAFs rules

Recommendation

The application should properly sanitize user input (URL encode) to protect against this vulnerability.

References

HTTP Parameter Pollution (https://www.owasp.org/images/b/ba/AppsecEU09_CarettoniDiPaola_v0.8.pdf)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

Insecure crossdomain.xml file

Severity	**Medium**
Reported by module	Scripting (Crossdomain_XML.script)

Description

The browser security model normally prevents web content from one domain from accessing data from another domain. This is commonly known as the "same origin policy". URL policy files grant cross-domain permissions for reading data. They permit operations that are not permitted by default. The URL policy file is located, by default, in the root directory of the target server, with the name crossdomain.xml (for example, at www.example.com/crossdomain.xml).

When a domain is specified in crossdomain.xml file, the site declares that it is willing to allow the operators of any servers in that domain to obtain any document on the server where the policy file resides. The crossdomain.xml file deployed on this website opens the server to all domains (use of a single asterisk "*" as a pure wildcard is supported) like so:

```
<cross-domain-policy>

<allow-access-from domain="*" />

</cross-domain-policy>
```

This practice is suitable for public servers, but should not be used for sites located behind a firewall because it could permit

access to protected areas. It should not be used for sites that require authentication in the form of passwords or cookies. Sites that use the common practice of authentication based on cookies to access private or user-specific data should be especially careful when using cross-domain policy files.

Impact

Using an insecure cross-domain policy file could expose your site to various attacks.

Recommendation

Carefully evaluate which sites will be allowed to make cross-domain calls. Consider network topology and any authentication mechanisms that will be affected by the configuration or implementation of the cross-domain policy.

References

Cross-domain policy file usage recommendations for Flash Player (http://www.adobe.com/devnet/flashplayer/articles/cross_domain_policy.html)
Cross-domain policy files (http://blogs.adobe.com/stateofsecurity/2007/07/crossdomain_policy_files_1.html)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

JetBrains .idea project directory

Severity	**Medium**
Reported by module	Scripting (JetBrains_Idea_Project_Directory.script)

Description

The .idea directory contains a set of configuration files (.xml) for your project. These configuration files contain information core to the project itself, such as names and locations of its component modules, compiler settings, etc. If you've defined a data source the file dataSources.ids contains information for connecting to the database and credentials. The workspace.xml file stores personal settings such as placement and positions of your windows, your VCS and History settings, and other data pertaining to the development environment. It also contains a list of changed files and other sensitive information. These files should not be present on a production system.

Impact

These files may expose sensitive information that may help an malicious user to prepare more advanced attacks.

Recommendation

Remove these files from production systems or restrict access to the .idea directory. To deny access to all the .idea folders you need to add the following lines in the appropriate context (either global config, or vhost/directory, or from .htaccess):

```
<Directory ~ "\.idea">

Order allow,deny

Deny from all

</Directory>
```

References

Apache Tips & Tricks: Deny access to some folders (http://www.ducea.com/2006/08/11/apache-tips-tricks-deny-access-to-some-folders/)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

PHP allow_url_fopen enabled

Severity	**Medium**
Reported by module	Scripting (PHPInfo.script)

Description

The PHP configuration directive allow_url_fopen is enabled. When enabled, this directive allows data retrieval from remote locations (web site or FTP server). A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling allow_url_fopen and bad input filtering.

allow_url_fopen is enabled by default.

Impact

Application dependant - possible remote file inclusion.

Recommendation

You can disable allow_url_fopen from either php.ini (for PHP versions newer than 4.3.4) or .htaccess (for PHP versions up to 4.3.4).

php.ini
allow_url_fopen = 'off'

.htaccess
php_flag allow_url_fopen off

References

Runtime Configuration (http://www.php.net/manual/en/filesystem.configuration.php)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

PHP errors enabled

Severity	**Medium**
Reported by module	Scripting (PHPInfo.script)

Description

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found that the PHP `display_errors` directive is enabled.

Impact

Application error messages may disclose sensitive information which can be used to escalate attacks.

Recommendation

Adjust `php.ini` or `.htaccess` (`mod_php` with Apache HTTP Server) to disable `display_errors` (refer to 'Detailed information' section).

References

PHP Runtime Configuration (display_errors) (http://php.net/manual/en/errorfunc.configuration.php#ini.display-errors)
PHP Runtime Configuration (log_errors) (http://php.net/manual/en/errorfunc.configuration.php#ini.log-errors)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

PHP errors enabled (AcuSensor)

Severity	**Medium**
Reported by module	

Description

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix AcuSensor found that the PHP `display_errors` directive is enabled.

Impact

Application error messages may disclose sensitive information which can be used to escalate attacks.

Recommendation

Adjust `php.ini` or `.htaccess` (`mod_php` with Apache HTTP Server) to disable `display_errors` (refer to 'Detailed information' section).

References

PHP Runtime Configuration (display_errors) (http://php.net/manual/en/errorfunc.configuration.php#ini.display-errors)
PHP Runtime Configuration (log_errors) (http://php.net/manual/en/errorfunc.configuration.php#ini.log-errors)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

PHP open_basedir is not set

Severity	**Medium**
Reported by module	Scripting (PHPInfo.script)

Description

The open_basedir configuration directive will limit the files that can be opened by PHP to the specified directory-tree. When a script tries to open a file with, for example, fopen() or gzopen(), the location of the file is checked. When the file is outside the specified directory-tree, PHP will refuse to open it. open_basedir is a good protection against remote file inclusion vulnerabilities. For a remote attacker it is not possible to break out of the open_basedir restrictions if he is only able to inject the name of a file to be included. Therefore the number of files he will be able to include with such a local file include vulnerability is limited.

Impact

Application dependant - possible remote code inclusion.

Recommendation

You can set open_basedir from php.ini

php.ini
open_basedir = your_application_directory

References

Description of core php.ini directives (http://php.net/ini.core)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

PHP session.use_only_cookies disabled

Severity	**Medium**
Reported by module	Scripting (PHPInfo.script)

Description

When use_only_cookies is disabled, PHP will pass the session ID via the URL. This makes the application more vulnerable to session hijacking attacks. Session hijacking is basically a form of identity theft wherein a hacker impersonates a legitimate user by stealing his session ID. When the session token is transmitted in a cookie, and the request is made on a secure channel (that is, it uses SSL), the token is secure.

Impact

Application dependant - possible session hijacking.

Recommendation

You can enabled session.use_only_cookies from php.ini or .htaccess.

php.ini
session.use_only_cookies = 'on'

.htaccess
php_flag session.use_only_cookies on

References

Runtime Configuration (http://www.php.net/session.configuration)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

PHPinfo page

Severity	**Medium**
Reported by module	Scripting (PHPInfo.script)

Description

PHPinfo page has been found in this directory. The PHPinfo page outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.

Impact

This file may expose sensitive information that may help an malicious user to prepare more advanced attacks.

Recommendation

Remove the file from production systems.

References

PHP phpinfo (http://www.php.net/manual/en/function.phpinfo.php)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

PHPinfo page found

Severity	**Medium**
Reported by module	Scripting (Text_Search_File.script)

Description

This script is using phpinfo() function. This function outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options,

HTTP headers, and the PHP License.

Impact

This file may expose sensitive information that may help an malicious user to prepare more advanced attacks.

Recommendation

Remove the file from production systems.

References

PHP phpinfo (http://www.php.net/manual/en/function.phpinfo.php)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

URL redirection

Severity	**Medium**
Reported by module	Scripting (XFS_and_Redir.script)

Description

This script is possibly vulnerable to URL redirection attacks.

URL redirection is sometimes used as a part of phishing attacks that confuse visitors about which web site they are visiting.

Impact

A remote attacker can redirect users from your website to a specified URL. This problem may assist an attacker to conduct phishing attacks, trojan distribution, spammers.

Recommendation

Your script should properly sanitize user input.

References

Unvalidated Redirects and Forwards Cheat Sheet
(https://www.owasp.org/index.php/Unvalidated_Redirects_and_Forwards_Cheat_Sheet)
HTTP Response Splitting, Web Cache Poisoning Attacks, and Related Topics
(http://packetstormsecurity.org/papers/general/whitepaper_httpresponse.pdf)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

User credentials are sent in clear text

Severity	**Medium**
Reported by module	Crawler

Description

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

Impact

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

Recommendation

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

WS_FTP log file found

Severity	**Medium**
Reported by module	Scripting (WS_FTP_log_file.script)

Description

WS_FTP is a popular FTP client. This application creates a log file named WS_FTP.LOG. This file contains sensitive data such as file source/destination and file name, date/time of upload etc.

Impact

This file may expose sensitive information that may help an malicious user to prepare more advanced attacks.

Recommendation

Remove this file from your website or change its permissions to remove access.

References

ws_ftp.log (http://archives.neohapsis.com/archives/fulldisclosure/2004-08/0663.html)

Affected items

Web Server
Details
Not available in the free trial
Request headers

```
Not available in the free trial
```

Clickjacking: X-Frame-Options header missing

Severity	**Low**
Reported by module	Scripting (Clickjacking_X_Frame_Options.script)

Description

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

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

Impact

The impact depends on the affected web application.

Recommendation

Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.

References

The X-Frame-Options response header (https://developer.mozilla.org/en-US/docs/HTTP/X-Frame-Options)
Clickjacking (http://en.wikipedia.org/wiki/Clickjacking)
OWASP Clickjacking (https://www.owasp.org/index.php/Clickjacking)
Defending with Content Security Policy frame-ancestors directive (https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet#Defending_with_Content_Security_Policy_frame-ancestors_directive)
Frame Buster Buster (http://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

Hidden form input named price was found

Severity	**Low**
Reported by module	Crawler

Description

A hidden form input named price was found. It's not recommended to hide sensitive information in hidden form fields.

Impact

User may change price information before submitting the form.

Recommendation

Check if the script inputs are properly validated.

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

Login page password-guessing attack

Severity	**Low**
Reported by module	Scripting (Html_Authentication_Audit.script)

Description

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.

Impact

An attacker may attempt to discover a weak password by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.

Recommendation

It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.

References

Blocking Brute Force Attacks (http://www.owasp.org/index.php/Blocking_Brute_Force_Attacks)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

MySQL username disclosure

Severity	**Low**
Reported by module	Scripting (Text_Search_File.script)

Description

For a client program to be able to connect to the MySQL server, it must use the proper connection parameters, such as the name of the host where the server is running and the user name and password of your MySQL account.

When the connection to the database cannot be established, the server returns an error message including the MySQL username and host that were used. This information should not be present on a production system.

Impact

This file may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Make sure the MySQL connection can be established and configure PHP not to display error messages.

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

Broken links

Severity	**Informational**
Reported by module	Crawler

Description

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.

Impact

Problems navigating the site.

Recommendation

Remove the links to this file or make it accessible.

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

Email address found

Severity	**Informational**
Reported by module	Scanner

Description

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.

Impact

Email addresses posted on Web sites may attract spam.

Recommendation

Check references for details on how to solve this problem.

References

Anti-spam techniques (https://en.wikipedia.org/wiki/Anti-spam_techniques)

Affected items

Web Server

Details
Not available in the free trial
Request headers
`Not available in the free trial`

Microsoft Office possible sensitive information

Severity	**Informational**
Reported by module	Scripting (Text_Search_File.script)

Description

This document has been converted to HTML using Microsoft Office. It seems that Office has included sensitive information during the conversion.

Impact

Possible sensitive information disclosure that may help an attacker to conduct social engineering attacks.

Recommendation

Inspect the source code of this document and remove the sensitive information.

References

iMPERVA Source Code Disclosure (http://www.imperva.com/resources/glossary?term=source_code_disclosure)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

Password type input with auto-complete enabled

Severity	**Informational**
Reported by module	Crawler

Description

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.

Impact

Possible sensitive information disclosure.

Recommendation

The password auto-complete should be disabled in sensitive applications.
To disable auto-complete, you may use a code similar to:

```
<INPUT TYPE="password" AUTOCOMPLETE="off">
```

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

Possible internal IP address disclosure

Severity	**Informational**
Reported by module	Scripting (Text_Search_File.script)

Description

A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

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

Impact

Possible sensitive information disclosure.

Recommendation

Prevent this information from being displayed to the user.

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

Possible server path disclosure (Unix)

Severity	**Informational**

Reported by module	Scripting (Text_Search_File.script)

Description

One or more fully qualified path names were found on this page. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

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

Impact

Possible sensitive information disclosure.

Recommendation

Prevent this information from being displayed to the user.

References

Full Path Disclosure (https://www.owasp.org/index.php/Full_Path_Disclosure)

Affected items

Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`
Web Server
Details
Not available in the free trial
Request headers
`Not available in the free trial`

Possible username or password disclosure

Severity	**Informational**
Reported by module	Scripting (Text_Search_File.script)

Description

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.

Impact

Possible sensitive information disclosure.

Recommendation

Remove this file from your website or change its permissions to remove access.

Affected items

Web Server
Details

Not available in the free trial
Request headers
Not available in the free trial
Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial
Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial
Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial
Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial
Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial
Web Server
Details
Not available in the free trial
Request headers
Not available in the free trial

Scanned items (coverage report)

http://testphp.vulnweb.com/
http://testphp.vulnweb.com/.idea
http://testphp.vulnweb.com/.idea/.name
http://testphp.vulnweb.com/.idea/acuart.iml
http://testphp.vulnweb.com/.idea/encodings.xml
http://testphp.vulnweb.com/.idea/misc.xml
http://testphp.vulnweb.com/.idea/modules.xml
http://testphp.vulnweb.com/.idea/scopes
http://testphp.vulnweb.com/.idea/scopes/scope_settings.xml
http://testphp.vulnweb.com/.idea/vcs.xml
http://testphp.vulnweb.com/.idea/workspace.xml
http://testphp.vulnweb.com/_mmServerScripts
http://testphp.vulnweb.com/_mmServerScripts/MMHTTPDB.php
http://testphp.vulnweb.com/_mmServerScripts/mysql.php
http://testphp.vulnweb.com/404.php
http://testphp.vulnweb.com/adm1nPan3l
http://testphp.vulnweb.com/adm1nPan3l/index.php
http://testphp.vulnweb.com/admin
http://testphp.vulnweb.com/admin/create.sql
http://testphp.vulnweb.com/AJAX
http://testphp.vulnweb.com/AJAX/artists.php
http://testphp.vulnweb.com/AJAX/categories.php
http://testphp.vulnweb.com/AJAX/htaccess.conf
http://testphp.vulnweb.com/AJAX/index.php
http://testphp.vulnweb.com/AJAX/infoartist.php
http://testphp.vulnweb.com/AJAX/infocateg.php
http://testphp.vulnweb.com/AJAX/infotitle.php
http://testphp.vulnweb.com/AJAX/showxml.php
http://testphp.vulnweb.com/AJAX/styles.css
http://testphp.vulnweb.com/AJAX/titles.php
http://testphp.vulnweb.com/artists.php
http://testphp.vulnweb.com/bxss
http://testphp.vulnweb.com/bxss/adminPan3l
http://testphp.vulnweb.com/bxss/adminPan3l/index.php
http://testphp.vulnweb.com/bxss/adminPan3l/style.css
http://testphp.vulnweb.com/bxss/cleanDatabase.php
http://testphp.vulnweb.com/bxss/database_connect.php
http://testphp.vulnweb.com/bxss/index.php
http://testphp.vulnweb.com/bxss/test.js
http://testphp.vulnweb.com/bxss/vuln.php
http://testphp.vulnweb.com/cart.php
http://testphp.vulnweb.com/categories.php
http://testphp.vulnweb.com/clearguestbook.php
http://testphp.vulnweb.com/clientaccesspolicy.xml
http://testphp.vulnweb.com/comment.php
http://testphp.vulnweb.com/Connections
http://testphp.vulnweb.com/Connections/DB_Connection.php
http://testphp.vulnweb.com/crossdomain.xml
http://testphp.vulnweb.com/CVS
http://testphp.vulnweb.com/CVS/Entries
http://testphp.vulnweb.com/CVS/Entries.Log
http://testphp.vulnweb.com/CVS/Repository
http://testphp.vulnweb.com/CVS/Root
http://testphp.vulnweb.com/database_connect.php
http://testphp.vulnweb.com/disclaimer.php
http://testphp.vulnweb.com/favicon.ico
http://testphp.vulnweb.com/Flash
http://testphp.vulnweb.com/Flash/add.fla
http://testphp.vulnweb.com/Flash/add.swf
http://testphp.vulnweb.com/guestbook.php
http://testphp.vulnweb.com/hpp
http://testphp.vulnweb.com/hpp/index.php
http://testphp.vulnweb.com/hpp/params.php
http://testphp.vulnweb.com/hpp/test.php
http://testphp.vulnweb.com/images
http://testphp.vulnweb.com/index.bak
http://testphp.vulnweb.com/index.php

http://testphp.vulnweb.com/index.zip
http://testphp.vulnweb.com/listproducts.php
http://testphp.vulnweb.com/login.php
http://testphp.vulnweb.com/logout.php
http://testphp.vulnweb.com/medias
http://testphp.vulnweb.com/medias/css
http://testphp.vulnweb.com/medias/css/main.css
http://testphp.vulnweb.com/medias/img
http://testphp.vulnweb.com/medias/js
http://testphp.vulnweb.com/medias/js/common_functions.js
http://testphp.vulnweb.com/Mod_Rewrite_Shop
http://testphp.vulnweb.com/Mod_Rewrite_Shop/.htaccess
http://testphp.vulnweb.com/Mod_Rewrite_Shop/buy.php
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1 - Copy
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1 (copy)
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1%20-%20Copy - Copy
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1%20-%20Copy (copy)
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1%20(copy) - Copy
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1%20(copy) (copy)
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2 - Copy
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2 (copy)
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2%20-%20Copy - Copy
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2%20-%20Copy (copy)
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2%20(copy) - Copy
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2%20(copy) (copy)
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3 - Copy
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3 (copy)
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3%20-%20Copy - Copy
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3%20-%20Copy (copy)
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3%20(copy) - Copy
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3%20(copy) (copy)
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
http://testphp.vulnweb.com/Mod_Rewrite_Shop/details.php
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
http://testphp.vulnweb.com/Mod_Rewrite_Shop/index.php
http://testphp.vulnweb.com/Mod_Rewrite_Shop/rate.php
http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html
http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html
http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html
http://testphp.vulnweb.com/pictures
http://testphp.vulnweb.com/pictures/1.jpg.tn
http://testphp.vulnweb.com/pictures/2.jpg.tn
http://testphp.vulnweb.com/pictures/3.jpg.tn
http://testphp.vulnweb.com/pictures/4.jpg.tn
http://testphp.vulnweb.com/pictures/5.jpg.tn
http://testphp.vulnweb.com/pictures/6.jpg.tn
http://testphp.vulnweb.com/pictures/7.jpg.tn
http://testphp.vulnweb.com/pictures/8.jpg.tn
http://testphp.vulnweb.com/pictures/credentials.txt
http://testphp.vulnweb.com/pictures/ipaddresses.txt
http://testphp.vulnweb.com/pictures/path-disclosure-unix.html
http://testphp.vulnweb.com/pictures/path-disclosure-win.html
http://testphp.vulnweb.com/pictures/wp-config.bak
http://testphp.vulnweb.com/pictures/WS_FTP.LOG
http://testphp.vulnweb.com/privacy.php
http://testphp.vulnweb.com/product.php
http://testphp.vulnweb.com/redir.php
http://testphp.vulnweb.com/search.php
http://testphp.vulnweb.com/secured

http://testphp.vulnweb.com/secured/database_connect.php
http://testphp.vulnweb.com/secured/index.php
http://testphp.vulnweb.com/secured/newuser.php
http://testphp.vulnweb.com/secured/office.htm
http://testphp.vulnweb.com/secured/office_files
http://testphp.vulnweb.com/secured/office_files/filelist.xml
http://testphp.vulnweb.com/secured/phpinfo.php
http://testphp.vulnweb.com/secured/style.css
http://testphp.vulnweb.com/sendcommand.php
http://testphp.vulnweb.com/showimage.php
http://testphp.vulnweb.com/signup.php
http://testphp.vulnweb.com/style.css
http://testphp.vulnweb.com/Templates
http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.php
http://testphp.vulnweb.com/userinfo.php
http://testphp.vulnweb.com/vendor
http://testphp.vulnweb.com/vendor/installed.json
http://testphp.vulnweb.com/wvstests
http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19
http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/scripts
http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/scripts/version.php