Escaneo Intrusivo

Report generated by Nessus™ Thu, 07 Mar 2024 06:03:12 EST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.56.101

10	14	19	6	67
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 116

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	81510	PHP 5.4.x < 5.4.38 Multiple Vulnerabilities (GHOST)
CRITICAL	9.8	-	82025	PHP 5.4.x < 5.4.39 Multiple Vulnerabilities
CRITICAL	9.8	-	83033	PHP 5.4.x < 5.4.40 Multiple Vulnerabilities
CRITICAL	9.8	-	83517	PHP 5.4.x < 5.4.41 Multiple Vulnerabilities
CRITICAL	9.8	-	84362	PHP 5.4.x < 5.4.42 Multiple Vulnerabilities
CRITICAL	9.8	-	84671	PHP 5.4.x < 5.4.43 Multiple Vulnerabilities (BACKRONYM)
CRITICAL	9.8	-	84215	ProFTPD mod_copy Information Disclosure
CRITICAL	9.8	-	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
CRITICAL	10.0	-	58987	PHP Unsupported Version Detection
CRITICAL	10.0*	-	92626	Drupal Coder Module Deserialization RCE
HIGH	7.5	-	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.5	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.3	-	66585	PHP 5.4.x < 5.4.13 Information Disclosure
HIGH	7.3	-	69401	PHP 5.4.x < 5.4.19 Multiple Vulnerabilities
HIGH	7.3	-	81080	PHP 5.4.x < 5.4.37 Multiple Vulnerabilities
HIGH	7.3	-	85298	PHP 5.4.x < 5.4.44 Multiple Vulnerabilities
HIGH	7.3	-	85885	PHP 5.4.x < 5.4.45 Multiple Vulnerabilities
HIGH	7.5*	-	78515	Drupal Database Abstraction API SQLi
HIGH	9.3*	-	67260	PHP 5.4.x < 5.4.17 Buffer Overflow

HIGH	7.5*	-	71427	PHP 5.4.x < 5.4.23 OpenSSL openssl_x509_parse() Memory Corruption
HIGH	7.2*	-	73862	PHP 5.4.x < 5.4.28 FPM Unix Socket Insecure Permission Escalation
HIGH	7.5*	-	76281	PHP 5.4.x < 5.4.30 Multiple Vulnerabilities
HIGH	7.5*	-	78545	PHP 5.4.x < 5.4.34 Multiple Vulnerabilities
HIGH	7.5*	-	80330	PHP 5.4.x < 5.4.36 'process_nested_data' RCE
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	5.9	-	187315	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)
MEDIUM	5.3	-	40984	Browsable Web Directories
MEDIUM	5.3	-	64993	PHP 5.4.x < 5.4.12 Information Disclosure
MEDIUM	5.3	-	152853	PHP < 7.3.28 Email Header Injection
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	5.0*	-	66843	PHP 5.4.x < 5.4.16 Multiple Vulnerabilities
MEDIUM	5.0*	-	71927	PHP 5.4.x < 5.4.24 Multiple Vulnerabilities
MEDIUM	5.0*	-	72881	PHP 5.4.x < 5.4.26 Multiple Vulnerabilities
MEDIUM	5.0*	-	73338	PHP 5.4.x < 5.4.27 awk Magic Parsing BEGIN DoS
MEDIUM	5.0*	-	74291	PHP 5.4.x < 5.4.29 'src/cdf.c' Multiple Vulnerabilities
MEDIUM	6.8*	-	77402	PHP 5.4.x < 5.4.32 Multiple Vulnerabilities
MEDIUM	5.0*	-	79246	PHP 5.4.x < 5.4.35 'donote' DoS
MEDIUM	5.0*	-	46803	PHP expose_php Information Disclosure
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	-	85582	Web Application Potentially Vulnerable to Clickjacking
LOW	3.7	-	70658	SSH Server CBC Mode Ciphers Enabled

LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	-	76791	PHP 5.4.x < 5.4.31 CLI Server 'header' DoS
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
LOW	N/A	-	42057	Web Server Allows Password Auto-Completion
LOW	2.6*	-	26194	Web Server Transmits Cleartext Credentials
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	39519	Backported Security Patch Detection (FTP)
INFO	N/A	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	39521	Backported Security Patch Detection (WWW)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	18638	Drupal Software Detection
INFO	N/A	-	19689	Embedded Web Server Detection
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	49704	External URLs
INFO	N/A	-	10092	FTP Server Detection
INFO	N/A	-	69826	HTTP Cookie 'secure' Property Transport Mismatch
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
INFO	N/A	-	17651	Microsoft Windows SMB : Obtains the Password Policy

INFO	N/A	-	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	60119	Microsoft Windows SMB Share Permissions Enumeration
INFO	N/A	-	10395	Microsoft Windows SMB Shares Enumeration
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	-	50345	Missing or Permissive X-Frame-Options HTTP Response Header
INFO	N/A	-	10719	MySQL Server Detection
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	181418	OpenSSH Detection
INFO	N/A	-	48243	PHP Version Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	56984	SSL / TLS Versions Supported

INFO	N/A	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	25240	Samba Server Detection
INFO	N/A	-	104887	Samba Version
INFO	N/A	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	66293	Unix Operating System on Extended Support
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	85601	Web Application Cookies Not Marked HttpOnly
INFO	N/A	-	85602	Web Application Cookies Not Marked Secure
INFO	N/A	-	91815	Web Application Sitemap
INFO	N/A	-	20108	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	-	11032	Web Server Directory Enumeration
INFO	N/A	-	10662	Web mirroring
INFO	N/A	-	24004	WebDAV Directory Enumeration
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	17219	phpMyAdmin Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.56.102

19	23	30	8	83
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 163

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	100995	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities
CRITICAL	9.8	-	101787	Apache 2.2.x < 2.2.34 Multiple Vulnerabilities
CRITICAL	9.8	-	158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL	9.8	-	161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
CRITICAL	9.8	-	172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
CRITICAL	9.8	-	153584	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.8	-	95438	Apache Tomcat 6.0.x < 6.0.48 / 7.0.x < 7.0.73 / 8.0.x < 8.0.39 / 8.5.x < 8.5.8 / 9.0.x < 9.0.0.M13 Multiple Vulnerabilities
CRITICAL	9.8	-	111067	Apache Tomcat 8.0.0 < 8.0.53 Security Constraint Weakness
CRITICAL	9.8	-	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
CRITICAL	9.1	-	121120	Apache Tomcat 7.0.x < 7.0.76 / 8.0.x < 8.0.42 / 8.5.x < 8.5.12 / 9.0.x < 9.0.0.M18 Improper Access Control
CRITICAL	9.0	-	170113	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities
CRITICAL	9.0	-	153583	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	10.0	-	171342	Apache Tomcat SEoL (8.0.x)
CRITICAL	10.0	-	171356	Apache httpd SEoL (2.1.x <= x <= 2.2.x)
CRITICAL	10.0	-	58987	PHP Unsupported Version Detection
CRITICAL	10.0	-	108797	Unsupported Windows OS (remote)

CRITICAL	10.0*	-	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
CRITICAL	10.0*	-	60085	PHP 5.3.x < 5.3.15 Multiple Vulnerabilities
HIGH	8.1	-	103697	Apache Tomcat 8.0.0.RC1 < 8.0.47 Multiple Vulnerabilities
HIGH	8.1	-	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	7.5	-	183391	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities
HIGH	7.5	-	96003	Apache Tomcat 6.0.16 < 6.0.50 / 7.0.x < 7.0.75 / 8.0.x < 8.0.41 / 8.5.x < 8.5.9 / 9.0.x < 9.0.0.M15 NIO HTTP Connector Information Disclosure
HIGH	7.5	-	94578	Apache Tomcat 6.0.x < 6.0.47 / 7.0.x < 7.0.72 / 8.0.x < 8.0.37 / 8.5.x < 8.5.5 / 9.0.x < 9.0.0.M10 Multiple Vulnerabilities
HIGH	7.5	-	99367	Apache Tomcat 6.0.x < 6.0.53 / 7.0.x < 7.0.77 / 8.0.x < 8.0.43 Pipelined Requests Information Disclosure
HIGH	7.5	-	121119	Apache Tomcat 7.0.x < 7.0.70 / 8.0.x < 8.0.36 / 8.5.x < 8.5.3 / 9.0.x < 9.0.0.M8 Denial of Service
HIGH	7.5	-	100681	Apache Tomcat 7.0.x < 7.0.78 / 8.0.x < 8.0.44 / 8.5.x < 8.5.15 / 9.0.x < 9.0.0.M21 Remote Error Page Manipulation
HIGH	7.5	-	121124	Apache Tomcat 8.0.x < 8.0.52 / 8.5.x < 8.5.31 / 9.0.x < 9.0.8 Denial of Service
HIGH	7.5	-	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.5	-	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.3	-	77531	Apache 2.2.x < 2.2.28 Multiple Vulnerabilities
HIGH	7.3	-	66584	PHP 5.3.x < 5.3.23 Multiple Vulnerabilities
HIGH	7.3	-	71426	PHP 5.3.x < 5.3.28 Multiple OpenSSL Vulnerabilities
HIGH	7.3	-	77285	PHP 5.3.x < 5.3.29 Multiple Vulnerabilities
HIGH	7.0	-	62101	Apache 2.2.x < 2.2.23 Multiple Vulnerabilities

HIGH	9.3*	-	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)
HIGH	7.5*	-	59056	PHP 5.3.x < 5.3.13 CGI Query String Code Execution
HIGH	7.5*	-	59529	PHP 5.3.x < 5.3.14 Multiple Vulnerabilities
HIGH	7.5*	-	64992	PHP 5.3.x < 5.3.22 Multiple Vulnerabilities
HIGH	7.5*	-	58988	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution
HIGH	7.5*	-	41028	SNMP Agent Default Community Name (public)
MEDIUM	6.8	-	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	6.5	-	18405	Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	5.9	-	187315	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)
MEDIUM	5.9	-	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.6	-	68915	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities
MEDIUM	5.3	-	57791	Apache 2.2.x < 2.2.22 Multiple Vulnerabilities
MEDIUM	5.3	-	64912	Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities
MEDIUM	5.3	-	73405	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities
MEDIUM	5.3	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	-	40984	Browsable Web Directories
MEDIUM	5.3	-	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	10546	Microsoft Windows LAN Manager SNMP LanMan Users Disclosure
MEDIUM	5.3	-	152853	PHP < 7.3.28 Email Header Injection
MEDIUM	5.3	-	57608	SMB Signing not required

MEDIUM	5.3	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	4.3	-	102588	Apache Tomcat 8.0.0.RC1 < 8.0.45 Cache Poisoning
MEDIUM	4.0	-	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	5.0*	-	66842	PHP 5.3.x < 5.3.26 Multiple Vulnerabilities
MEDIUM	6.8*	-	67259	PHP 5.3.x < 5.3.27 Multiple Vulnerabilities
MEDIUM	6.8*	-	58966	PHP < 5.3.11 Multiple Vulnerabilities
MEDIUM	5.0*	-	73289	PHP PHP_RSHUTDOWN_FUNCTION Security Bypass
MEDIUM	5.0*	-	46803	PHP expose_php Information Disclosure
MEDIUM	4.3*	-	57690	Terminal Services Encryption Level is Medium or Low
MEDIUM	4.3*	-	85582	Web Application Potentially Vulnerable to Clickjacking
MEDIUM	5.0*	-	90067	WordPress User Enumeration
LOW	3.7	-	106976	Apache Tomcat 8.0.0.RC1 < 8.0.50 Security Constraint Weakness
LOW	3.7	-	159462	Apache Tomcat 8.x < 8.5.78 Spring4Shell (CVE-2022-22965) Mitigations
LOW	3.7	-	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	N/A	-	10547	Microsoft Windows LAN Manager SNMP LanMan Services Disclosure
LOW	2.6*	-	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
LOW	N/A	-	42057	Web Server Allows Password Auto-Completion
LOW	2.6*	-	26194	Web Server Transmits Cleartext Credentials
LOW	2.6*	-	34850	Web Server Uses Basic Authentication Without HTTPS
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	21186	AJP Connector Detection
INFO	N/A	-	46739	Apache Axis2 Detection
INFO	N/A	-	48204	Apache HTTP Server Version

INFO	N/A	-	39446	Apache Tomcat Detection
INFO	N/A	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10736	DCE Services Enumeration
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	49704	External URLs
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	-	50345	Missing or Permissive X-Frame-Options HTTP Response Header
INFO	N/A	-	14274	Nessus SNMP Scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	-	11936	OS Identification

INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	181418	OpenSSH Detection
INFO	N/A	-	50845	OpenSSL Detection
INFO	N/A	-	48243	PHP Version Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	40665	Protected Web Page Detection
INFO	N/A	-	66173	RDP Screenshot
INFO	N/A	-	10940	Remote Desktop Protocol Service Detection
INFO	N/A	-	35296	SNMP Protocol Version Detection
INFO	N/A	-	19763	SNMP Query Installed Software Disclosure
INFO	N/A	-	34022	SNMP Query Routing Information Disclosure
INFO	N/A	-	10550	SNMP Query Running Process List Disclosure
INFO	N/A	-	10800	SNMP Query System Information Disclosure
INFO	N/A	-	10551	SNMP Request Network Interfaces Enumeration
INFO	N/A	-	185519	SNMP Server Detection
INFO	N/A	-	40448	SNMP Supported Protocols Detection
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported

INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	-	51891	SSL Session Resume Supported
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	17975	Service Detection (GET request)
INFO	N/A	-	11153	Service Detection (HELP Request)
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	64814	Terminal Services Use SSL/TLS
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	85601	Web Application Cookies Not Marked HttpOnly
INFO	N/A	-	85602	Web Application Cookies Not Marked Secure
INFO	N/A	-	91815	Web Application Sitemap
INFO	N/A	-	20108	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	-	11032	Web Server Directory Enumeration
INFO	N/A	-	49705	Web Server Harvested Email Addresses
INFO	N/A	-	11419	Web Server Office File Inventory
INFO	N/A	-	11422	Web Server Unconfigured - Default Install Page Present

INFO	N/A	-	10662	Web mirroring
INFO	N/A	-	11424	WebDAV Detection
INFO	N/A	-	24004	WebDAV Directory Enumeration
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	18297	WordPress Detection
INFO	N/A	-	101841	WordPress Outdated Plugin Detection
INFO	N/A	-	101842	WordPress Plugin Detection

* indicates the v3.0 score was not available; the v2.0 score is shown