Adviesplan: Automated Web Scanner

Gemaakt door Jens Cornelius Gijsbertus van den Hurk

Datum: 5-1-2025

Voor: Fontys Hogescholen

In samenwerking met: FireBV

Inhoud

Target: Metasploitable 2

Service Enumeration

De handmatige service-enumeratie is bevestigd en uitgebreid door een Nmap full TCP service scan. Hierbij zijn meerdere legacy en onveilige services aangetroffen die typisch zijn voor een slecht gehard Linux-systeem.

Overzicht geopende services (selectie)

Poort	Service	Versie	Risico
21	FTP	vsftpd 2.3.4	Backdoor / plaintext
22	SSH	OpenSSH 4.7p1	Verouderd
23	Telnet	Linux telnetd	Geen encryptie
80	HTTP	Apache 2.2.8 + PHP 5.2.4	Meerdere CVE's
139 / 445	Samba	3.x – 4.x	Privilege escalation
1524	Bind shell	Root shell	Kritiek
3306	MySQL	Onbekend	DB exposure
5432	PostgreSQL	8.3.x	Verouderd
8180	Tomcat	Coyote 1.1	Default creds

Tabel 1 Services Metasploitable 2

Kwetsbaarheidsanalyse

Vulnerability #1

PHP CGI Remote Code Execution
CVE-2012-1823 – Critical (NIST: CVE-2012-1823, 2025)

Scanbewijs:
Nuclei bevestigde succesvolle remote code execution door injectie van PHP-parameters via de querystring. De payload resulteerde in server-side code execution, aantoonbaar door hash-output in de HTTP-response.

Impact

- Remote code execution zonder authenticatie
- Volledige overname van de webserver
- Directe pivot naar OS-level toegang

Mitigatie

- Upgrade PHP ≥ 5.4.2
- CGI-modus uitschakelen
- Gebruik PHP-FPM
- Input parsing hardenen

Vulnerability #2

Apache Tomcat Manager – Default Credentials
Severity: High / Critical

Scanbewijs:
Nikto en Gobuster identificeerden de Tomcat Manager interface (/manager/html) met actieve default credentials (tomcat:tomcat). Authenticatie was mogelijk zonder voorafgaande toegang. (Tomcat Apache - Documentation, 2025) (CWE 284 - Improper Access Control, 2025)

Impact

- Uploaden van WAR-bestanden (webshells)
- Volledige controle over Tomcat-applicaties
- Mogelijke privilege escalation naar root

Mitigatie

- Default credentials verwijderen
- Sterke wachtwoorden afdwingen
- Manager-interface beperken via IP-filtering
- Tomcat Manager uitschakelen indien niet noodzakelijk

Vulnerability #3

Root Bind Shell Open
Severity: Critical

Scanbewijs:
Nmap detecteerde een actieve bind shell op poort 1524 die directe root-toegang verschaft zonder enige vorm van authenticatie. (CWE 306 - Missing Authentication, 2025)

Impact

- Directe root shell
- Volledige systeemcompromittering
- Geen exploit of authenticatie vereist

Mitigatie

- Bind shell service volledig verwijderen
- Firewall-regels toepassen
- Hardening volgens Principle of Least Privilege

Vulnerability #4

vsftpd 2.3.4 Backdoor
CVE-2011-2523 – Critical (NIST: CVE-2011-2523, 2025)

Scanbewijs:
Nmap identificeerde vsftpd versie 2.3.4, een bekende kwetsbare versie waarin een backdoor aanwezig is die remote shell access mogelijk maakt.

Impact

- Remote shell toegang
- Ongeautoriseerde systeemtoegang
- Volledige compromittering van het systeem

Mitigatie

- vsftpd upgraden naar een veilige versie
- FTP-service verwijderen indien niet noodzakelijk
- Overstappen op SFTP

Vulnerability #5

rsh / rexec / rlogin Services Actief
Severity: Critical

Scanbewijs:
Nmap detecteerde actieve legacy r-services op poorten 512, 513 en 514, welke bekendstaan om zwakke of ontbrekende authenticatie. (CWE 306 - Missing Authentication, 2025) (Red Hat Enterprise - Documentation Security, 2025)

Impact

- Authenticatie-bypass
- Plaintext credentials
- Ongeautoriseerde remote toegang

Mitigatie

- r-services volledig uitschakelen
- SSH gebruiken als veilig alternatief

Vulnerability #6

Samba Service Onveilig Geconfigureerd
Severity: High

Scanbewijs:
Nmap identificeerde een Samba 3.x–4.x service met open shares, zonder duidelijke toegangsbeperkingen. (CWE 284 - Improper Access Control, 2025)

Impact

- Ongeautoriseerde toegang tot gedeelde bestanden
- Mogelijke privilege escalation
- Informatie-lekken

Mitigatie

- Samba upgraden
- Share-permissies beperken
- Toegang beperken via firewall en authenticatie

Vulnerability #7

NFS Service Publiek Bereikbaar
Severity: High

Scanbewijs:
Nmap detecteerde een actieve NFS-service op poort 2049 zonder zichtbare restricties. (CWE 284 - Improper Access Control, 2025)

Impact

- Remote filesystem mounting
- Inzicht in gevoelige bestanden
- Mogelijke privilege escalation

Mitigatie

- NFS uitschakelen indien niet nodig
- Exportrestricties toepassen
- IP-whitelisting configureren

Vulnerability #8

PostgreSQL 8.3 End-of-Life
Severity: High

Scanbewijs:
Nmap identificeerde PostgreSQL versie 8.3, een end-of-life versie met bekende kwetsbaarheden. (PostgreSQL - Version, 2025)

Impact

- Bekende exploits beschikbaar
- Brute-force en privilege escalation risico
- Databasediefstal

Mitigatie

- PostgreSQL upgraden naar ondersteunde versie
- Database alleen lokaal binden
- Sterke authenticatie afdwingen

Vulnerability #9

MySQL Service Publiek Toegankelijk
Severity: High

Scanbewijs:
MySQL werd gedetecteerd op poort 3306 zonder netwerkrestricties. (Development SQL - Security Tips, 2025)

Impact

- Brute-force aanvallen
- Mogelijke database-exfiltratie
- Credential harvesting

Mitigatie

- bind-address beperken tot localhost
- Firewall-regels toepassen
- Sterke wachtwoorden en least privilege gebruiken

Vulnerability #10

UnrealIRCd Backdoor Risico
CVE-2010-2075 – Critical (NIST CVE-2010-2075, 2025)

Scanbewijs:
Nmap detecteerde een actieve UnrealIRCd-service, een versie die historisch bekend staat om een ingebouwde backdoor.

Impact

- Remote command execution
- Volledige servercompromittering

Mitigatie

- UnrealIRCd verwijderen
- Service isoleren of upgraden

Vulnerability #11

phpMyAdmin Publiek Toegankelijk
Severity: Medium

Scanbewijs:
Nikto en Gobuster identificeerden een publiek toegankelijke phpMyAdmin-interface zonder aanvullende beveiligingsmaatregelen.

Impact

- Brute-force aanvallen
- Database-inzage
- Informatie-lekken

Mitigatie

- IP-restricties toepassen
- Extra authenticatie (MFA)
- phpMyAdmin verwijderen indien niet noodzakelijk

Vulnerability #12

phpinfo() Information Disclosure
Severity: Low

Scanbewijs:
Nikto detecteerde een publiek toegankelijke phpinfo()-pagina die uitgebreide server- en PHP-configuratiegegevens toont.

Impact

- Informatie-lekken
- Versimpelt exploit chaining

Mitigatie

- phpinfo()-pagina verwijderen
- expose_php = Off instellen

Vulnerability #13

Directory Listing Enabled
CVE-1999-0678 – Medium (NIST CVE-1999-0678, 2025)

Scanbewijs:
Nikto en Gobuster bevestigden browsable directories zoals /doc/, /test/ en /icons/.

Impact

- Inzicht in bestandsstructuur
- Mogelijke blootstelling van gevoelige bestanden

Mitigatie

- Directory listing uitschakelen (Options -Indexes)

Vulnerability #14

WebDAV Enabled
Severity: Medium

Scanbewijs:
Gobuster identificeerde een actieve WebDAV-directory (/dav/). (Apache - Security Tips, 2025) (CWE 284 - Improper Access Control, 2025)

Impact

- Bestandsupload en -overschrijving
- Mogelijke webshell plaatsing

Mitigatie

- WebDAV uitschakelen
- Authenticatie afdwingen

Vulnerability #15

HTTP PUT & DELETE Methods Enabled (Tomcat)
Severity: Medium

Scanbewijs:
Nikto bevestigde dat PUT en DELETE HTTP-methodes zijn toegestaan op de Tomcat-server. (Apache - Security Tips, 2025)

Impact

- Upload of verwijdering van bestanden
- Mogelijke code execution

Mitigatie

- HTTP-methodes beperken tot noodzakelijke methodes

Vulnerability #16

HTTP TRACE Enabled
Severity: Medium

Scanbewijs:
Nikto bevestigde dat de HTTP TRACE-methode is ingeschakeld. (Apache - Security Tips, 2025)

Impact

- Cross Site Tracing (XST)
- Cookie disclosure

Mitigatie

- TRACE uitschakelen (TraceEnable Off)

Vulnerability #17

Missing Security Headers
Severity: Low

Scanbewijs:
Nikto rapporteerde ontbrekende security headers zoals X-Frame-Options en X-Content-Type-Options. (Apache - Security Tips, 2025) (OWASP - Secure Headers Project, 2025)

Impact

- Clickjacking
- MIME sniffing aanvallen

Mitigatie

- OWASP Secure Headers implementeren

Vulnerability #18

Verouderde Software Stack
Severity: Medium

Scanbewijs:
Meerdere services draaien op end-of-life versies, waaronder Apache 2.2.8, PHP 5.2.4 en OpenSSH 4.7. (Apache, 2025) (OpenSSH - Security, 2025)

Impact

- Vergroot aanvalsoppervlak
- Bekende exploits beschikbaar

Mitigatie

- Software upgraden
- Systeem hardenen volgens CIS benchmarks

Vulnerability #19

SMTP Service Publiek Bereikbaar (Postfix)
Severity: Medium

Scanbewijs:
Nmap identificeerde een publiek toegankelijke SMTP-service (Postfix smtpd) op poort 25 zonder zichtbare netwerkrestricties. (Postfix - Basic Configuration, 2025)

Impact

- Misbruik als open relay (indien fout geconfigureerd)
- User enumeration via SMTP commands
- Faciliteert phishing en spamcampagnes

Mitigatie

- SMTP beperken tot interne hosts
- Relay-beperkingen afdwingen
- SMTP-authenticatie verplicht stellen

Vulnerability #20

DNS Service Publiek Bereikbaar (ISC BIND 9.4.2)
Severity: Medium

Scanbewijs:
Nmap detecteerde een actieve DNS-service op poort 53 met een sterk verouderde BIND-versie.

Impact

- Zone transfer aanvallen
- Informatie-lekken over interne infrastructuur
- Bekende kwetsbaarheden in legacy BIND-versies

Mitigatie

- DNS zone transfers beperken
- BIND upgraden
- DNS alleen intern beschikbaar maken

Vulnerability #21

VNC Service Open Zonder Zichtbare Beperkingen
Severity: High

Scanbewijs:
Nmap detecteerde een VNC-service op poort 5900 met protocolversie 3.3, wat duidt op een legacy configuratie. (CWE 306 - Missing Authentication, 2025) (Archive.org - TightVNC Security FAQ, 2025)

Impact

- Remote desktop toegang
- Mogelijke afwezigheid van authenticatie
- Volledige GUI-overname van het systeem

Mitigatie

- VNC uitschakelen indien niet nodig
- Sterke authenticatie configureren
- Toegang beperken via firewall

Vulnerability #22

X11 Service Publiek Bereikbaar
Severity: High

Scanbewijs:
Nmap identificeerde een actieve X11-service op poort 6000, ondanks dat toegang werd geweigerd. (CWE 306 - Missing Authentication, 2025) (Security Stack Exchange - X11 Forwarding, 2025) (Archive.org - XORG Documentation, 2025)

Impact

- Mogelijke screen capturing
- Keystroke logging
- Remote GUI-manipulatie

Mitigatie

- X11 netwerktoegang uitschakelen
- Gebruik SSH X11 forwarding indien noodzakelijk

Vulnerability #23

Apache JServ Protocol (AJP) Open
Severity: Medium

Scanbewijs:
Nmap detecteerde een actieve AJP-service op poort 8009 (Apache JServ Protocol). (Tomcat Apache AJP, 2025) (CWE - Administrative Paths available, 2025)

Impact

- Bekende misbruikscenario's (bijv. Ghostcat-achtige aanvallen)
- Informatie-lekken tussen Apache en Tomcat
- Mogelijke file disclosure

Mitigatie

- AJP uitschakelen indien niet strikt nodig
- AJP beperken tot localhost

Vulnerability #24

HTTP OPTIONS Method Enabled
Severity: Low

Scanbewijs:
Nikto rapporteerde dat de HTTP OPTIONS-methode actief is en ondersteunde methodes openbaar maakt. (HTTPD APACHE - Known Security tips v2.2, 2025)

Impact

- Informatie-lek over toegestane HTTP-methodes
- Vergemakkelijkt gerichte aanvallen

Mitigatie

- OPTIONS-response beperken
- Alleen noodzakelijke methodes toestaan

Vulnerability #25

Cookies Zonder HttpOnly Flag (Tomcat Admin)
Severity: Medium

Scanbewijs:
Nikto detecteerde dat de JSESSIONID-cookie wordt gezet zonder de HttpOnly-flag binnen de Tomcat admin interface.

Impact

- Cookie theft via XSS
- Session hijacking

Mitigatie

- HttpOnly en Secure flags afdwingen
- Session management hardenen

Vulnerability #26

Server-Status Endpoint Aanwezig
Severity: Low

Scanbewijs:
Gobuster identificeerde /server-status als bestaand endpoint (403), wat wijst op een actieve Apache status module. (HTTPD APACHE - Known Security tips v2.2, 2025)

Impact

- Inzicht in serverconfiguratie
- Mogelijke informatie-lekken bij misconfiguratie

Mitigatie

- server-status uitschakelen
- Toegang beperken tot localhost

Vulnerability #27

Gevoelige Apache Config Bestanden Detecteerbaar
Severity: Medium

Scanbewijs:
Gobuster detecteerde de aanwezigheid van .htpasswd, .htaccess en .hta bestanden (403 responses). (HTTPD APACHE - Known Security tips v2.2, 2025)

Impact

- Informatie-lek over authenticatiestructuur
- Doelwit voor brute-force en misconfiguratie

Mitigatie

- Toegang tot dotfiles blokkeren
- Apache configuratie hardenen

Vulnerability #28

Back-up / Config Bestandsindicatie (wp-config.php)
Severity: High

Scanbewijs:
Nikto rapporteerde een detectie van #wp-config.php#, wat kan duiden op een verkeerd geconfigureerd of tijdelijk back-upbestand.

Impact

- Mogelijke blootstelling van database credentials
- Volledige applicatiecompromittering

Mitigatie

- Back-upbestanden verwijderen
- Webroot controleren op gevoelige bestanden

Vulnerability #29

Verouderde OpenSSH Versie
Severity: Medium

Scanbewijs:
Nmap identificeerde OpenSSH versie 4.7p1, een end-of-life versie met bekende kwetsbaarheden. (OpenSSH - Security, 2025)

Impact

- Bekende exploits beschikbaar
- Brute-force en downgrade-aanvallen

Mitigatie

- OpenSSH upgraden
- SSH hardenen (key-based auth, rate limiting)

Vulnerability #30

Information Disclosure via HTTP Headers
Severity: Low

Scanbewijs:
Nikto identificeerde headers zoals X-Powered-By die PHP-versie-informatie prijsgeven. (OWASP - Secure Headers Project, 2025)

Impact

- Versimpelt fingerprinting
- Vergemakkelijkt exploit chaining

Mitigatie

- expose_php = Off
- ServerTokens en ServerSignature minimaliseren

Vulnerability #31

Apache Server Version Disclosure
Severity: Low

Scanbewijs:
HTTP-responses bevatten expliciete serverinformatie (Apache/2.2.8 (Ubuntu) DAV/2), zoals zichtbaar in meerdere Nuclei responses. (Apache, 2025) (OWASP - Secure Headers Project, 2025)

Impact

- Vergemakkelijkt fingerprinting
- Versnelt exploitselectie door aanvaller

Mitigatie

- ServerTokens Prod
- ServerSignature Off

Vulnerability #32

X-Powered-By Header Disclosure (PHP)
Severity: Low

Scanbewijs:
De HTTP-header X-Powered-By: PHP/5.2.4-2ubuntu5.10 werd aangetroffen in meerdere responses. (OWASP - Secure Headers Project, 2025)

Impact

- Exacte PHP-versie zichtbaar
- Verhoogt kans op gerichte exploits

Mitigatie

- expose_php = Off in php.ini

Vulnerability #33

PHP display_errors Enabled
Severity: Medium

Scanbewijs:
Uit de phpinfo()-pagina blijkt dat display_errors = On actief is. (PHP - Versions, 2025)

Impact

- Informatie-lek van stack traces
- Mogelijke blootstelling van paden en variabelen

Mitigatie

- display_errors = Off
- Logging via error_log configureren

Vulnerability #34

PHP allow_url_fopen Enabled
Severity: Medium

Scanbewijs:
phpinfo() toont dat allow_url_fopen = On actief is. (PHP - Versions, 2025)

Impact

- Faciliteert Remote File Inclusion (RFI)
- Vergemakkelijkt exploit chaining

Mitigatie

- allow_url_fopen = Off indien niet noodzakelijk

Vulnerability #35

PHP Functions Not Restricted
Severity: Medium

Scanbewijs:
phpinfo() toont dat disable_functions leeg is en geen gevaarlijke functies zijn uitgeschakeld. (PHP - Versions, 2025)

Impact

- Command execution eenvoudiger na exploit
- Vergroot impact van RCE

Mitigatie

- Functies zoals exec, system, shell_exec uitschakelen

Vulnerability #36

Apache DAV Module Enabled
Severity: Medium

Scanbewijs:
Server-header vermeldt DAV/2, wat wijst op een actieve WebDAV-module. (Apache - Security Tips, 2025)

Impact

- Bestandsmanipulatie mogelijk
- Vergroot risico op webshell uploads

Mitigatie

- DAV uitschakelen indien niet nodig
- Authenticatie afdwingen

Vulnerability #37

Tomcat Host Manager Publiek Toegankelijk
Severity: High

Scanbewijs:
Naast /manager/html is ook /host-manager/html toegankelijk met dezelfde default credentials. (Tomcat - Paths, 2025) (CWE - Administrative Paths available, 2025)

Impact

- Aanmaken/verwijderen van virtual hosts
- Manipulatie van serverconfiguratie

Mitigatie

- Host Manager uitschakelen
- Toegang beperken tot localhost

Vulnerability #38

Tomcat Server Status Endpoint Toegankelijk
Severity: Medium

Scanbewijs:
De Tomcat Manager interface toont een actieve link naar /manager/status. (Tomcat - Paths, 2025)

Impact

- Inzicht in threads, memory en requests
- Waardevolle informatie voor DoS of timing-aanvallen

Mitigatie

- Status endpoints uitschakelen
- Authenticatie + IP-restricties toepassen

Vulnerability #39

Tomcat Default Example Applications Enabled
Severity: Medium

Scanbewijs:
Applicaties zoals /jsp-examples, /servlets-examples en /tomcat-docs zijn actief. (Tomcat - Paths, 2025)

Impact

- Vergroot attack surface
- Historisch kwetsbare voorbeeldcode

Mitigatie

- Alle voorbeeldapplicaties verwijderen

Vulnerability #40

Tomcat Administrative Applications Active
Severity: High

Scanbewijs:
Applicaties zoals /admin, /manager, /host-manager draaien actief en zijn bereikbaar. (Tomcat - Paths, 2025) (CWE - Administrative Paths available, 2025)

Impact

- Volledige controle over applicatielaag
- Kans op WAR upload en RCE

Mitigatie

- Admin apps verwijderen of isoleren
- Sterke authenticatie afdwingen

Vulnerability #41

HTTP Methods Enumeration Exposure
Severity: Low

Scanbewijs:
De HTTP OPTIONS-methode onthult toegestane methodes.

Impact

- Inzicht in serverconfiguratie
- Versimpelt aanvalskeuze

Mitigatie

- OPTIONS responses minimaliseren

Vulnerability #42

Outdated PHP Version (End-of-Life)
Severity: High

Scanbewijs:
phpinfo() toont PHP versie 5.2.4, welke end-of-life is en meerdere bekende CVE's bevat.

Impact

- Meerdere publieke exploits beschikbaar
- Structureel onveilig platform

Mitigatie

- PHP upgraden naar ondersteunde versie
- Applicatie isoleren indien upgrade niet mogelijk

Vulnerability #43

Outdated Apache Version (End-of-Life)
Severity: High

Scanbewijs:
Apache versie 2.2.8 wordt gebruikt, een end-of-life release. (Apache, 2025)

Impact

- Bekende kwetsbaarheden
- Geen security updates beschikbaar

Mitigatie

- Apache upgraden
- Hardening volgens CIS benchmark

Vulnerability #44

Sensitive Application Enumeration (DVWA, Mutillidae, TWiki)
Severity: Medium

Scanbewijs:
De indexpagina toont expliciete links naar kwetsbare applicaties zoals DVWA, Mutillidae en TWiki. (OWASP - Mutillidae, 2025) (OWASP: DVWA, 2025)

Impact

- Opzettelijk kwetsbare applicaties
- Direct exploiteerbaar

Mitigatie

- Verwijderen in productie
- Segmentatie van testomgevingen

Automated scanner

Uitleg over de gemaakte scanner

Voor deze opdracht is een automatische webscanner ontwikkeld die meerdere security tools combineert tot een scanproces. Het doel van deze scanner is om op een geautomatiseerde manier kwetsbaarheden, configuratiefouten en security hardening issues te identificeren binnen een targetomgeving.

De scanner fungeert als een orchestrator: hij voert verschillende gespecialiseerde tools uit en verzamelt de resultaten in een JSON overzicht. Hierdoor wordt handmatig scannen verminderd en ontstaat een consistente aanpak voor het uitvoeren van een eerste technische beveiligingsanalyse. De broncode en opzet van de scanner zijn beschikbaar via de volgende repository: https://github.com/HurkieIT/AutomatedWebScanner

Conclusie

Uit dit adviesrapport blijkt dat de ontwikkelde automatische webscanner daadwerkelijk functioneert zoals bedoeld. De scanner is in staat gebleken om op consistente wijze zowel kritieke kwetsbaarheden, configuratiefouten als hardening-issues te identificeren binnen het onderzochte target (Metasploitable 2).

De resultaten in dit document tonen aan dat de scanner meerdere bekende CVE's, exposed managementinterfaces, verouderde services en onveilige configuraties correct heeft gedetecteerd, waaronder remote code execution, ontbrekende authenticatie en onvoldoende toegangscontrole. Deze bevindingen zijn bevestigd door scanbewijs uit tools zoals Nmap, Nikto, Gobuster en Nuclei, die geïntegreerd zijn binnen de automatische scanner.

Daarnaast laat de analyse zien dat de scanner niet alleen exploiteerbare kwetsbaarheden detecteert, maar ook bredere beveiligingsproblemen zoals informatielekken en ontbrekende security headers. Dit onderstreept dat de scanner geschikt is voor het uitvoeren van een eerste technische beveiligingsanalyse en het inzichtelijk maken van de algehele beveiligingsstatus van een systeem.

Bibliografie

Apache - Security Tips. (2025). Opgehaald van httpd.apache.org: https://httpd.apache.org/docs/2.2/misc/security_tips.html

Apache. (2025). Opgehaald van httpd.apache.org: https://httpd.apache.org/

Archive.org - TightVNC Security FAQ. (2025). Opgehaald van TightVNC.com: https://web.archive.org/web/20260104133835/https://www.tightvnc.com/faq.php

Archive.org - XORG Documentation. (2025). Opgehaald van Xorg: https://web.archive.org/web/20251231160916/https://www.x.org/wiki/Documentation/

CWE - Administrative Paths available. (2025). Opgehaald van cwe.mitre.org: https://cwe.mitre.org/data/definitions/284.html

CWE 284 - Improper Access Control. (2025). Opgehaald van cwe.mitre.org: https://cwe.mitre.org/data/definitions/284.html

CWE 306 - Missing Authentication. (2025). Opgehaald van cwe.mitre.org: https://cwe.mitre.org/data/definitions/306.html

Development SQL - Security Tips. (2025). Opgehaald van dev.sql.com: https://dev.mysql.com/doc/refman/8.0/en/security.html

HTTPD APACHE - Known Security tips v2.2. (2025). Opgehaald van httpd.apache.org: https://httpd.apache.org/docs/2.2/misc/security_tips.html

NIST CVE-1999-0678. (2025). Opgehaald van nvd.nist.gov: https://nvd.nist.gov/vuln/detail/CVE-1999-0678

NIST CVE-2010-2075. (2025). Opgehaald van nvd.nist.gov: https://nvd.nist.gov/vuln/detail/CVE-2010-2075

NIST: CVE-2011-2523. (2025). Opgehaald van nvd.nist.gov: https://nvd.nist.gov/vuln/detail/CVE-2011-2523

NIST: CVE-2012-1823. (2025). Opgehaald van nvd.nist.gov: https://nvd.nist.gov/vuln/detail/CVE-2012-1823

OpenSSH - Security. (2025). Opgehaald van Openssh.org: https://www.openssh.org/security.html

OWASP - Mutillidae. (2025). Opgehaald van OWASP.org: https://twiki.org/cgi-bin/view/Codev/SecurityAlert https://owasp.org/www-project-mutillidae/

OWASP - Secure Headers Project. (2025). Opgehaald van OWASP.org: https://owasp.org/www-project-secure-headers/

OWASP: DVWA. (2025). Opgehaald van owasp.org: https://owasp.org/www-project-damn-vulnerable-web-application/

PHP - Versions. (2025). Opgehaald van PHP.net: https://www.php.net/supported-versions.php

Postfix - Basic Configuration. (2025). Opgehaald van Postfix.org: https://www.postfix.org/BASIC_CONFIGURATION_README.html

PostgreSQL - Version. (2025). Opgehaald van PostgreSQL.com: https://www.postgresql.org/support/versioning/

Red Hat Enterprise - Documentation Security. (2025). Opgehaald van RHEL.com: https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/10#Security

Security Stack Exchange - X11 Forwarding. (2025). Opgehaald van Security.Stackexchange: https://security.stackexchange.com/questions/14815/security-concerns-with-x11-forwarding

Tomcat - Paths. (2025). Opgehaald van tomcat.apache.org: https://tomcat.apache.org/tomcat-6.0-doc/manager-howto.html

Tomcat Apache - Documentation. (2025). Opgehaald van tomcat.apache.org/: https://tomcat.apache.org/tomcat-6.0-doc/manager-howto.html

Tomcat Apache AJP. (2025). Opgehaald van Tomcat.apache: https://tomcat.apache.org/connectors-doc/ajp/ajpv13a.html

Gebruik van AI

Tijdens de ontwikkeling van dit document is er gebruik gemaakt van generatieve AI, in de vorm van OpenAI, ChatGPT 5.2. De mate van gebruik van AI is voor taalkundige en grammaticale verbeteringen. De validatiefase binnen dit document zijn zelfstandig uitgevoerd.