Rapport de Test de Pénétration

Cible : Mahamadou

Date du scan : 2025-06-19 11:15 CEST

Outils utilisés : Nmap, ZAP

Résultats Nmap :

Système d'Exploitation détecté :

Linux 2.6.32, Linux 5.0 - 6.2

Port	Service	État	Info
80/tcp	http	open	syn-ack ttl 64 Apache httpd 2.4.63
443/tcp	ssl/http	open	syn-ack ttl 64 Apache httpd 2.4.63

Vulnérabilités détectées par ZAP :

WARN-NEW: In Page Banner Information Leak [10009] x 3

WARN-NEW: Missing Anti-clickjacking Header [10020] x 10

WARN-NEW: X-Content-Type-Options Header Missing [10021] x 11

WARN-NEW: User Controllable HTML Element Attribute (Potential XSS) [10031] x 3

WARN-NEW: Server Leaks Version Information via "Server" HTTP Response Header Field [10036] x 11

WARN-NEW: Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) [10037] x 11

WARN-NEW: Content Security Policy (CSP) Header Not Set [10038] x 10

WARN-NEW: Non-Storable Content [10049] x 11

WARN-NEW: Permissions Policy Header Not Set [10063] x 12

WARN-NEW: Modern Web Application [10109] x 9

WARN-NEW: Authentication Request Identified [10111] x 1

WARN-NEW: Absence of Anti-CSRF Tokens [10202] x 12

WARN-NEW: Insufficient Site Isolation Against Spectre Vulnerability [90004] x 9

WARN-NEW: Charset Mismatch (Header Versus Meta Content-Type Charset) [90011] x 13

FAIL-NEW: 0□FAIL-INPROG: 0□WARN-NEW: 14□WARN-INPROG: 0□INFO: 0□IGNORE: 0□PASS: 52

WARN-NEW: In Page Banner Information Leak [10009] x 3

WARN-NEW: Missing Anti-clickjacking Header [10020] x 10

WARN-NEW: X-Content-Type-Options Header Missing [10021] x 12

WARN-NEW: User Controllable HTML Element Attribute (Potential XSS) [10031] x 3

WARN-NEW: Server Leaks Version Information via "Server" HTTP Response Header Field [10036] x 11

WARN-NEW: Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) [10037] x 11

WARN-NEW: Content Security Policy (CSP) Header Not Set [10038] x 10

WARN-NEW: Non-Storable Content [10049] x 11

WARN-NEW: Permissions Policy Header Not Set [10063] x 11

WARN-NEW: Modern Web Application [10109] x 9

WARN-NEW: Authentication Request Identified [10111] x 1

WARN-NEW: Absence of Anti-CSRF Tokens [10202] x 11

WARN-NEW: Insufficient Site Isolation Against Spectre Vulnerability [90004] x 9

WARN-NEW: Charset Mismatch (Header Versus Meta Content-Type Charset) [90011] x 11

FAIL-NEW: 0␣FAIL-INPROG: 0␣WARN-NEW: 14␣WARN-INPROG: 0␣INFO: 0␣IGNORE: 0␣PASS: 52

WARN-NEW: In Page Banner Information Leak [10009] x 3

WARN-NEW: Missing Anti-clickjacking Header [10020] x 11

WARN-NEW: X-Content-Type-Options Header Missing [10021] x 11

WARN-NEW: User Controllable HTML Element Attribute (Potential XSS) [10031] x 3

WARN-NEW: Server Leaks Version Information via "Server" HTTP Response Header Field [10036] x 11

WARN-NEW: Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) [10037] x 11

WARN-NEW: Content Security Policy (CSP) Header Not Set [10038] x 9

WARN-NEW: Storable and Cacheable Content [10049] x 11

WARN-NEW: Permissions Policy Header Not Set [10063] x 11

WARN-NEW: Modern Web Application [10109] x 9

WARN-NEW: Authentication Request Identified [10111] x 1

WARN-NEW: Absence of Anti-CSRF Tokens [10202] x 14

WARN-NEW: Insufficient Site Isolation Against Spectre Vulnerability [90004] x 9

WARN-NEW: Charset Mismatch (Header Versus Meta Content-Type Charset) [90011] x 13

FAIL-NEW: 0␣FAIL-INPROG: 0␣WARN-NEW: 14␣WARN-INPROG: 0␣INFO: 0␣IGNORE: 0␣PASS: 52

WARN-NEW: In Page Banner Information Leak [10009] x 3

WARN-NEW: Missing Anti-clickjacking Header [10020] x 10

WARN-NEW: X-Content-Type-Options Header Missing [10021] x 11

WARN-NEW: User Controllable HTML Element Attribute (Potential XSS) [10031] x 2

WARN-NEW: Server Leaks Version Information via "Server" HTTP Response Header Field [10036] x 11

WARN-NEW: Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) [10037] x 11

WARN-NEW: Content Security Policy (CSP) Header Not Set [10038] x 10

WARN-NEW: Storable and Cacheable Content [10049] x 12

WARN-NEW: Permissions Policy Header Not Set [10063] x 12

WARN-NEW: Modern Web Application [10109] x 4

WARN-NEW: Absence of Anti-CSRF Tokens [10202] x 12

WARN-NEW: Insufficient Site Isolation Against Spectre Vulnerability [90004] x 15

WARN-NEW: Charset Mismatch (Header Versus Meta Content-Type Charset) [90011] x 11

FAIL-NEW: 0␣FAIL-INPROG: 0␣WARN-NEW: 13␣WARN-INPROG: 0␣INFO: 0␣IGNORE: 0␣PASS: 53

WARN-NEW: In Page Banner Information Leak [10009] x 3

WARN-NEW: Missing Anti-clickjacking Header [10020] x 11

WARN-NEW: X-Content-Type-Options Header Missing [10021] x 11

WARN-NEW: User Controllable HTML Element Attribute (Potential XSS) [10031] x 3

WARN-NEW: Server Leaks Version Information via "Server" HTTP Response Header Field [10036] x 11

WARN-NEW: Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) [10037] x 12

WARN-NEW: Content Security Policy (CSP) Header Not Set [10038] x 9

WARN-NEW: Storable and Cacheable Content [10049] x 11

WARN-NEW: Permissions Policy Header Not Set [10063] x 11

WARN-NEW: Modern Web Application [10109] x 9

WARN-NEW: Authentication Request Identified [10111] x 1

WARN-NEW: Absence of Anti-CSRF Tokens [10202] x 12

WARN-NEW: Insufficient Site Isolation Against Spectre Vulnerability [90004] x 12

WARN-NEW: Charset Mismatch (Header Versus Meta Content-Type Charset) [90011] x 11

FAIL-NEW: 0␣FAIL-INPROG: 0␣WARN-NEW: 14␣WARN-INPROG: 0␣INFO: 0␣IGNORE: 0␣PASS: 52

WARN-NEW: In Page Banner Information Leak [10009] x 3

WARN-NEW: Missing Anti-clickjacking Header [10020] x 10

WARN-NEW: X-Content-Type-Options Header Missing [10021] x 11

WARN-NEW: User Controllable HTML Element Attribute (Potential XSS) [10031] x 3

WARN-NEW: Server Leaks Version Information via "Server" HTTP Response Header Field [10036] x 11

WARN-NEW: Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) [10037] x 11

WARN-NEW: Content Security Policy (CSP) Header Not Set [10038] x 10

WARN-NEW: Non-Storable Content [10049] x 11

WARN-NEW: Permissions Policy Header Not Set [10063] x 11

WARN-NEW: Modern Web Application [10109] x 9

WARN-NEW: Authentication Request Identified [10111] x 1

WARN-NEW: Absence of Anti-CSRF Tokens [10202] x 11

WARN-NEW: Insufficient Site Isolation Against Spectre Vulnerability [90004] x 9

WARN-NEW: Charset Mismatch (Header Versus Meta Content-Type Charset) [90011] x 13

FAIL-NEW: 0␣FAIL-INPROG: 0␣WARN-NEW: 14␣WARN-INPROG: 0␣INFO: 0␣IGNORE: 0␣PASS: 52

WARN-NEW: In Page Banner Information Leak [10009] x 3

WARN-NEW: Missing Anti-clickjacking Header [10020] x 10

WARN-NEW: X-Content-Type-Options Header Missing [10021] x 11

WARN-NEW: User Controllable HTML Element Attribute (Potential XSS) [10031] x 3

WARN-NEW: Server Leaks Version Information via "Server" HTTP Response Header Field [10036] x 13

WARN-NEW: Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) [10037] x 11

WARN-NEW: Content Security Policy (CSP) Header Not Set [10038] x 10

WARN-NEW: Non-Storable Content [10049] x 11

WARN-NEW: Permissions Policy Header Not Set [10063] x 11

WARN-NEW: Modern Web Application [10109] x 9

WARN-NEW: Authentication Request Identified [10111] x 1

WARN-NEW: Absence of Anti-CSRF Tokens [10202] x 12

WARN-NEW: Insufficient Site Isolation Against Spectre Vulnerability [90004] x 9

WARN-NEW: Charset Mismatch (Header Versus Meta Content-Type Charset) [90011] x 12

FAIL-NEW: 0️⃣FAIL-INPROG: 0️⃣WARN-NEW: 14️⃣WARN-INPROG: 0️⃣INFO: 0️⃣IGNORE: 0️⃣PASS: 52