	Needs further analysis
	Possibly failing, look for better options

Next Look out ?
Better Subdomain resolution/ filtering
Vulnerability Testing/ Detection
More security checks

SECURITY_CHECKS_ANALYSIS

Sr No	Security Check Name	Category	Tool/Technology/API Used	Pass/Fail Conditions	Depth Assessment	Cost (Free/ Paid)	Gaps/Recommendations
1	Server Information Header	Application Security	Axios HTTP Headers	PASS: HTTP response headers['server'] is undefined/null/empty | FAIL: 'Server' header present with value (e.g., 'Apache/2.4.41', 'nginx/1.18.0', 'Microsoft-IIS/10.0') exposing server technology and version	Deep enough - checks HTTP response headers	Free	Add checks for version disclosure in server headers and fingerprinting resistance
2	X-Powered-By Header	Application Security	Axios HTTP Headers	PASS: HTTP response headers['x-powered-by'] is undefined/ null/empty | FAIL: 'X-Powered-By' header present with technology disclosure (e.g., 'PHP/7.4.3', 'ASP.NET', 'Express') revealing backend technology stack	Deep enough - checks HTTP response headers	Free	Add detection of other technology disclosure headers (X-AspNet-Version etc.)
3	Referrer Policy Header	Application Security	Axios HTTP Headers	PASS: headers['referrer-policy'] !== 'unsafe-url' (including undefined, 'strict-origin', 'no-referrer') | FAIL: headers['referrer-policy'] === 'unsafe-url' which sends full URL in referrer to all destinations	Simplified - only checks for unsafe-url	Free	Should validate all referrer policy values and recommend secure configurations
4	ASP.NET Version Headers	Application Security	Axios HTTP Headers	PASS: All ASP.NET headers (X-AspNet-Version, X-AspNetMvc-Version, X-Powered-By: ASP.NET) are absent from response | FAIL: Any ASP.NET version header present revealing framework version (e.g., 'X-AspNet-Version: 4.0.30319')	Deep enough - checks specific ASP.NET headers	Free	Add detection of other framework version disclosures
5	WordPress XML-RPC	Application Security	Axios HTTP requests to /xmlrpc.php	PASS: XML-RPC disabled | FAIL: XML-RPC enabled	Deep enough - tests actual endpoint	Free	Add brute force protection testing and method enumeration
6	WordPress Version	Application Security	Axios HTTP requests parsing HTML/ headers	PASS: Version not exposed | FAIL: Version exposed in meta tags/headers	Deep enough - multiple detection methods	Free	Add plugin/theme version enumeration and vulnerability cross-referencing
7	Insecure WordPress	Application Security	Axios requests to wp-admin without auth	PASS: wp-admin protected | FAIL: wp-admin accessible	Simplified - basic access test	Free	Add weak credential testing and security plugin detection
8	MoveIt Transfer Detection	Application Security	Axios requests with User-Agent fingerprinting	PASS: MoveIt not detected | FAIL: MoveIt Transfer detected	Deep enough - HTTP fingerprinting	Free	Add version detection and CVE correlation for known vulnerabilities
9	FortiOS VPN Detection	Application Security	Axios requests to FortiGate login pages	PASS: FortiOS not detected | FAIL: FortiOS VPN detected	Simplified - basic endpoint detection	Free	Add version fingerprinting and vulnerability assessment
10	Citrix Products Detection	Application Security	Axios requests to multiple Citrix endpoints	PASS: Citrix not detected | FAIL: Citrix products detected	Deep enough - multiple product detection	Free	Add version detection and recent CVE correlation
11	Cisco IOS Detection	Application Security	Axios requests to Cisco management interfaces	PASS: Cisco IOS not detected | FAIL: Cisco IOS detected	Simplified - basic interface detection	Free	Add SNMP detection and version fingerprinting
12	Ivanti Connect Detection	Application Security	Axios requests to Ivanti endpoints	PASS: Ivanti not detected | FAIL: Ivanti Connect detected	Simplified - basic endpoint detection	Free	Add comprehensive Ivanti product detection and CVE correlation
13	GitLab Detection	Application Security	Axios requests to GitLab paths and headers	PASS: GitLab not detected | FAIL: GitLab detected	Deep enough - multiple detection methods	Free	Add version detection and security configuration analysis
14	Polyfill Sources	Application Security	HTML content parsing for polyfill.io references	PASS: No malicious polyfill sources | INFO: Polyfill sources found	Deep enough - content analysis	Free	Add comprehensive CDN security analysis and SRI validation
15	Meta Pixel Detection	Application Security	HTML content parsing for Facebook tracking	PASS: No Meta Pixel | FAIL: Meta Pixel detected	Deep enough - content and JavaScript analysis	Free	Add comprehensive tracking pixel detection for all major platforms
16	TikTok Pixel Detection	Application Security	HTML content parsing for TikTok tracking	PASS: No TikTok Pixel | FAIL: TikTok Pixel detected	Deep enough - content analysis	Free	Add privacy compliance analysis and tracking disclosure validation
17	Directory Listing	Application Security	Axios requests to common directory paths	PASS: Directory listing disabled | FAIL: Directory listing enabled	Deep enough - tests multiple paths	Free	Add sensitive file detection and comprehensive path enumeration
18	Cloud Storage Detection	Application Security	HTML parsing and header analysis	PASS: No exposed cloud storage | FAIL: Cloud storage detected	Deep enough - multiple cloud provider detection	Free	Add bucket/container permission testing and data exposure analysis
19	WordPress Plugin Versions	Application Security	Axios requests to plugin paths and parsing	PASS: Plugin versions not exposed | FAIL: Plugin versions exposed	Deep enough - multiple detection methods	Free	Add vulnerability database correlation and plugin security analysis
20	WordPress User List	Application Security	Axios requests to user enumeration endpoints	PASS: User list not exposed | FAIL: User list exposed	Deep enough - multiple enumeration methods	Free	Add user role analysis and privilege escalation testing
21	Leaked Data Detection	Application Security	Axios requests to sensitive file paths	PASS: No leaked data | FAIL: Sensitive files detected	Simplified - comprehensive file detection	Free	Add content analysis and credential extraction testing
22	Cookie Security Flags	Application Security	HTTP response header parsing	PASS: Secure cookies used | FAIL: Insecure cookies detected	Deep enough - analyzes all cookie flags	Free	Add SameSite attribute validation and cookie scope analysis
23	Fourth-Party Integration Detection	Application Security	Multiple methods: Headers/DNS/Content/ JS; WhatWeb	PASS: WhatWeb detection, Specific hardcoded patterns detected (e.g., content.includes('google-analytics.com'), headers['cf-ray'], script src contains 'stripe.com') | Detection uses 4 methods: 1) HTTP Headers (cf-ray for Cloudflare, x-amz-cf-id for AWS), 2) DNS CNAME analysis, 3) HTML content string matching, 4) JavaScript src URL parsing with predefined vendor list (~15 vendors)	Medium - WhatWeb and Hardcoded pattern matching for known vendors only	Free	Very limited vendor coverage; should implement dynamic detection
24	HTTP Strict Transport Security (HSTS)	Application Security	HTTP response header parsing	PASS: HSTS properly enforced | FAIL: HSTS not enforced	Deep enough - HSTS header validation	Free	Add max-age validation and includeSubDomains checking
25	X-Frame-Options Header	Application Security	HTTP response header parsing	PASS: X-Frame-Options set to DENY/SAMEORIGIN | FAIL: X-Frame-Options missing or unsafe	Deep enough - clickjacking protection	Free	Add CSP frame-ancestors directive validation
26	Content Security Policy (CSP)	Application Security	HTTP response header parsing	PASS: CSP implemented | WARNING: CSP not implemented	Deep enough - CSP header analysis	Free	Add comprehensive CSP directive validation and unsafe policies detection
27	X-Content-Type-Options Header	Application Security	HTTP response header parsing	PASS: X-Content-Type-Options set to nosniff | FAIL: Header missing	Deep enough - MIME type sniffing protection	Free	Add comprehensive security header analysis
28	Directory Listing - Root	Application Security	HTTP requests to / with directory listing detection	PASS: Directory listing disabled | FAIL: Directory listing enabled	Deep enough - directory traversal testing	Free	Add comprehensive directory enumeration and sensitive path detection
29	Directory Listing - Admin	Application Security	HTTP requests to /admin with directory listing detection	PASS: Admin directory protected | FAIL: Admin directory listing enabled	Deep enough - admin interface protection	Free	Add authentication requirement validation
30	Directory Listing - Backup	Application Security	HTTP requests to /backup with directory listing detection	PASS: Backup directory protected | FAIL: Backup directory listing enabled	Deep enough - backup file exposure	Free	Add backup file detection and data exposure analysis
31	Directory Listing - Config	Application Security	HTTP requests to /config with directory listing detection	PASS: Config directory protected | FAIL: Config directory listing enabled	Deep enough - configuration file exposure	Free	Add configuration file content analysis
32	Directory Listing - Database	Application Security	HTTP requests to /database with directory listing detection	PASS: Database directory protected | FAIL: Database directory listing enabled	Deep enough - database file exposure	Free	Add database backup detection and credential exposure analysis
33	Secure Cookie Flag	Application Security	HTTP response header parsing	PASS: Cookies use Secure flag | FAIL: Insecure cookies detected	Deep enough - cookie security analysis	Free	Add comprehensive cookie attribute validation
34	HttpOnly Cookie Flag	Application Security	HTTP response header parsing	PASS: Cookies use HttpOnly flag | FAIL: Cookies without HttpOnly detected	Deep enough - XSS protection via cookies	Free	Add SameSite attribute validation and cookie scope analysis
35	MoveIt Transfer HTTPS Detection	Application Security	HTTP endpoint fingerprinting	PASS: MoveIt not detected via HTTPS | FAIL: MoveIt Transfer detected via HTTPS	Deep enough - product detection	Free	Add version detection and vulnerability correlation
36	MoveIt Transfer HTTP Detection	Application Security	HTTP endpoint fingerprinting	PASS: MoveIt not detected via HTTP | FAIL: MoveIt Transfer detected via HTTP	Deep enough - product detection	Free	Add insecure deployment detection and security configuration analysis
37	Citrix Gateway Detection	Application Security	HTTP endpoint fingerprinting	PASS: Citrix Gateway not detected | FAIL: Citrix Gateway detected	Deep enough - product detection	Free	Add version detection and recent vulnerability correlation
38	Citrix ADC Detection	Application Security	HTTP endpoint fingerprinting	PASS: Citrix ADC not detected | FAIL: Citrix ADC detected	Deep enough - product detection	Free	Add configuration analysis and security hardening validation
39	Citrix ShareFile Detection	Application Security	HTTP endpoint fingerprinting	PASS: Citrix ShareFile not detected | FAIL: Citrix ShareFile detected	Deep enough - product detection	Free	Add access control validation and data exposure analysis
40	Domain Expiration	DNS Health	WHOIS data via whois-json package	PASS: Domain expiry date > 30 days from current date | WARNING: Domain expires between 7-30 days | FAIL: Domain expires in <7 days or expiry date parsing fails | Calculated as: (expiryDate - Date.now()) / (1000*60*60*24) days	Deep enough - uses official WHOIS data	Free	Add monitoring for registrar protection and auto-renewal status
41	MX Records	DNS Health	Node.js DNS resolution	PASS: Valid MX records found | FAIL: No MX records or DNS resolution fails	Deep enough - uses native DNS resolution	Free	Add DMARC/SPF validation and email security posture analysis
42	Subdomain Takeover	DNS Health	Axios HTTP requests to common patterns	PASS: No takeover detected | FAIL: Potential takeover detected	Simplified - checks for common error messages	Free	Should implement comprehensive CNAME validation and service fingerprinting
43	SPF Record Validation	DNS Health	Node.js DNS TXT record parsing	PASS: Valid SPF record | WARNING: Soft fail (~all) | FAIL: Invalid/ missing SPF	Deep enough - parses SPF mechanisms	Free	Add SPF record syntax validation and mechanism analysis

44	DMARC Policy	DNS Health	Node.js DNS TXT record parsing	PASS: DMARC policy exists and not p=none | FAIL: No DMARC or p=none	Deep enough - parses DMARC directives	Free	Add RUA/RUF validation and policy effectiveness analysis
45	CAA Records	DNS Health	Node.js DNS CAA record lookup	PASS: CAA records configured | FAIL: No CAA records	Deep enough - DNS CAA validation	Free	Add certificate authority validation and issuance monitoring
46	DNSSEC Validation	DNS Health	Node.js DNS with DNSSEC flags	PASS: DNSSEC enabled | FAIL: DNSSEC not configured	Deep enough - validates DNSSEC chain	Free	Add key rollover monitoring and algorithm strength analysis
47	Domain Registrar Protection	DNS Health	WHOIS data analysis	Multiple checks for registrar lock and privacy	Deep enough - registrar security analysis	Free	Add transfer protection validation and registrar security rating
48	Subdomain Discovery	DNS Health	Subfinder + crt.sh + AlienVault OTX	Discovers subdomains from multiple sources	Deep enough - multiple OSINT sources	Free	Add additional apis/tools for better discovery
49	Subdomain Validation	DNS Health	httpx tool for HTTP probing	PASS: Subdomain active | FAIL: Subdomain inactive	Deep enough - actual HTTP probing	Free	Add response analysis and technology fingerprinting
50	Domain Delete Protection	DNS Health	WHOIS data analysis	PASS: Domain has deletion protection | WARNING: No deletion protection	Deep enough - registrar protection settings	Free	Add comprehensive domain protection status monitoring
51	Domain Update Protection	DNS Health	WHOIS data analysis	PASS: Domain has update protection | WARNING: No update protection	Deep enough - registrar protection settings	Free	Add transfer protection and privacy protection validation
52	SPF Record Enabled	DNS Health	DNS TXT record parsing	PASS: SPF enabled | FAIL: SPF record not found	Deep enough - email authentication	Free	Add SPF record syntax validation and mechanism analysis
53	SPF Record Syntax Validation	DNS Health	DNS TXT record parsing	PASS: SPF syntax correct | FAIL: Invalid SPF syntax	Deep enough - SPF record validation	Free	Add comprehensive SPF mechanism validation
54	SPF Strict Filtering	DNS Health	DNS TXT record parsing	PASS: SPF policy does not use +all | FAIL: SPF policy uses +all	Deep enough - SPF policy analysis	Free	Add soft fail vs hard fail policy analysis
55	SPF Neutral Policy Check	DNS Health	DNS TXT record parsing	PASS: SPF policy not neutral | WARNING: SPF policy uses ?all	Deep enough - SPF enforcement level	Free	Add SPF record optimization recommendations
56	DMARC Policy Exists	DNS Health	DNS TXT record parsing	PASS: DMARC policy exists | FAIL: DMARC policy not found	Deep enough - email authentication	Free	Add DMARC record validation and policy effectiveness analysis
57	DMARC Policy Not None	DNS Health	DNS TXT record parsing	PASS: DMARC policy enforced | FAIL: DMARC policy set to none	Deep enough - DMARC policy enforcement	Free	Add quarantine vs reject policy analysis
58	DMARC Policy Not Quarantine	DNS Health	DNS TXT record parsing	PASS: DMARC policy not quarantine | WARNING: DMARC policy set to quarantine	Deep enough - DMARC policy analysis	Free	Add RUA/RUF reporting validation
59	DMARC Percentage Coverage	DNS Health	DNS TXT record parsing	PASS: Full DMARC coverage | WARNING: Partial DMARC coverage	Deep enough - DMARC enforcement percentage	Free	Add gradual DMARC deployment analysis
60	Malicious Activity Check	IP Reputation	AbuseIPDB API	PASS: No malicious reports | FAIL: Malicious activity detected	Very deep - external threat intelligence	Free with API key limits	Requires AbuseIPDB API key; add multiple threat intelligence sources
61	IP Reputation	IP Reputation	Multiple threat intelligence sources	Comprehensive threat analysis	Deep enough - multiple data sources	Free/Paid APIs	Add geolocation analysis and hosting provider reputation
62	Google Safe Browsing Malware Check	IP Reputation	Google Safe Browsing API	PASS: No malware detected | FAIL: Malware detected	Deep enough - Google threat intelligence	Free	Add integration with multiple threat intelligence sources
63	Phishing Activity Detection	IP Reputation	AbuseIPDB API	PASS: No phishing reports | FAIL: Phishing activity detected	Deep enough - threat intelligence	Free with API limits	Add multiple threat intelligence source correlation
64	Malware Distribution Detection	IP Reputation	AbuseIPDB API	PASS: No malware reports | FAIL: Malware distribution detected	Deep enough - threat intelligence	Free with API limits	Add malware family identification and IOC correlation
65	Botnet Activity Detection	IP Reputation	AbuseIPDB API	PASS: No botnet reports | FAIL: Botnet activity detected	Deep enough - threat intelligence	Free with API limits	Add botnet family identification and C&C analysis
66	Spam Activity Detection	IP Reputation	AbuseIPDB API	PASS: No spam reports | FAIL: Spam activity detected	Deep enough - threat intelligence	Free with API limits	Add spam campaign analysis and volume assessment
67	Unsolicited Scanning Detection	IP Reputation	AbuseIPDB API	PASS: No scanning reports | FAIL: Scanning activity detected	Deep enough - threat intelligence	Free with API limits	Add scan pattern analysis and target assessment
68	Brute Force Attack Detection	IP Reputation	AbuseIPDB API	PASS: No brute force reports | FAIL: Brute force attacks detected	Deep enough - threat intelligence	Free with API limits	Add attack pattern analysis and credential stuffing detection
69	Heartbleed Vulnerability	Network Security	Node.js TLS/Axios HTTPS requests	PASS: TLS connection to port 443 completes successfully with status 200-399 response | FAIL: TLS connection throws specific error containing 'ECONNRESET', 'EPROTO', or timeout indicating potential Heartbleed | INFO: Unable to establish connection for testing	Simplified - Only checks basic TLS connection	Free	Should implement actual Heartbleed exploit test using dedicated CVE scanners like OpenVAS or Nessus
70	POODLE Vulnerability	Network Security	Node.js TLS/Axios HTTPS requests	PASS: HTTPS GET request succeeds without SSLv3-related errors | FAIL: Connection fails with SSL3_GET_RECORD errors or protocol downgrade detected | INFO: Unable to test due to connection issues	Simplified - Only checks basic TLS connection	Free	Should implement SSLv3 protocol testing and cipher suite analysis
71	FREAK Vulnerability	Network Security	Node.js TLS/Axios HTTPS requests	PASS: TLS handshake completes without export-grade cipher negotiation | FAIL: Connection fails with export cipher related errors or weak encryption detected | INFO: Unable to complete vulnerability assessment	Simplified - Only checks basic TLS connection	Free	Should implement export-grade cipher detection and protocol downgrade testing
72	Logjam Vulnerability	Network Security	Node.js TLS/Axios HTTPS requests	PASS: TLS connection succeeds without DHE_RSA key exchange vulnerabilities | FAIL: Weak Diffie-Hellman parameters detected or connection fails with DH-related errors | INFO: Vulnerability test inconclusive	Simplified - Only checks basic TLS connection	Free	Should implement DH parameter strength testing and weak prime detection
73	HTTPS Support	Network Security	Axios HTTPS request	PASS: axios.get(`https://${domain}`) returns status 200-399 within 5s timeout | FAIL: HTTPS request throws ENOTFOUND, ECONNREFUSED, certificate errors, or times out indicating no HTTPS support	Simplified - basic connectivity test	Free	Should test TLS version support and cipher suite preferences
74	HSTS Header	Network Security	Axios HTTP Headers	PASS: headers['strict-transport-security'] exists with max-age >= 31536000 (1 year) | WARNING: HSTS header present but max-age < 31536000 seconds | FAIL: headers['strict-transport-security'] undefined/null. Regex: /max-age=(\d+)/ to extract seconds	Deep enough - parses HSTS directives	Free	Add validation of includeSubDomains and preload directives
75	SSL Certificate Revocation	Network Security	Node.js TLS certificate parsing	PASS: tlsSocket.authorized === true and certificate validity flags show not revoked | FAIL: tlsSocket.authorized === false due to certificate revocation | INFO: Unable to determine revocation status from TLS handshake	Simplified - checks certificate validity flag	Free	Should implement actual OCSP/CRL checking for real-time revocation status
76	SSL Availability	Network Security	Node.js TLS connection	PASS: tls.connect({host: domain, port: 443}) succeeds and socket.authorized === true | FAIL: TLS connection fails with ECONNREFUSED, ENOTFOUND, or certificate validation errors	Simplified - basic TLS handshake	Free	Should test for protocol version support and cipher suite analysis
77	HTTPS Redirect	Network Security	Axios HTTP requests	PASS: HTTP redirects to HTTPS | FAIL: No HTTPS redirect	Deep enough - follows redirects	Free	Add validation of redirect chains and HSTS implementation
78	SSL Certificate Validation	Network Security	Node.js TLS certificate inspection	Multiple checks for expiry/hostname/CA/self-signed	Very deep - comprehensive certificate analysis	Free	Add certificate transparency log validation and CAA record checking
79	Port Scans (MySQL/SSH/SMTP etc.)	Network Security	Nmap via child_process	PASS: Ports closed | FAIL: Sensitive ports open	Deep enough - actual port scanning	Free	Add service version detection and banner grabbing
80	SSL/TLS Parameters	Network Security	Node.js TLS socket analysis	Multiple checks for cipher suites and protocols	Very deep - TLS configuration analysis	Free	Add perfect forward secrecy validation and TLS 1.3 support analysis
81	HSTS Preload List	Network Security	External API to hstspreload.org	PASS: Domain in preload list | WARNING: Not in preload list	Deep enough - official preload list check	Free	Add preload eligibility validation and submission guidance
82	HSTS includeSubDomains	Network Security	HTTP header parsing	PASS: includeSubDomains present | WARNING: includeSubDomains missing	Deep enough - header directive analysis	Free	Add subdomain coverage analysis and policy inheritance validation
83	Weak TLS Ciphers	Network Security	Node.js TLS cipher suite enumeration	PASS: No weak ciphers | FAIL: Weak ciphers detected	Deep enough - cipher suite analysis	Free	Add cipher preference order analysis and PFS validation
84	Port Scanning	Network Security	Nmap with multiple scan types	Comprehensive port and service detection	Very deep - multiple scan techniques	Free	Add vulnerability scanning integration and service enumeration
85	SSL Certificate Chain Present	Network Security	Node.js TLS certificate inspection	PASS: SSL certificate chain present | FAIL: Certificate chain missing	Deep enough - certificate chain validation	Free	Add complete chain validation and intermediate certificate checks
86	SSL Certificate Hostname Validation	Network Security	Node.js TLS certificate inspection	PASS: Certificate hostname matches domain | FAIL: Hostname mismatch	Deep enough - hostname verification	Free	Add wildcard certificate validation and SAN analysis
87	SSL Certificate Expiry Check	Network Security	Node.js TLS certificate inspection	PASS: Certificate not expired | FAIL: Certificate expired or expires soon	Deep enough - certificate validity period	Free	Add expiry warning thresholds and renewal monitoring
88	SSL Certificate CA Validation	Network Security	Node.js TLS certificate inspection	PASS: Certificate issued by trusted CA | FAIL: Self-signed or untrusted CA	Deep enough - CA trust validation	Free	Add certificate transparency log verification
89	SSL Certificate Self-Signed Check	Network Security	Node.js TLS certificate inspection	PASS: Certificate not self-signed | FAIL: Self-signed certificate detected	Deep enough - certificate issuer validation	Free	Add certificate path validation and trust chain analysis
90	SSL Certificate Weak Signature	Network Security	Node.js TLS certificate inspection	PASS: Strong signature algorithm | FAIL: Weak signature algorithm	Deep enough - signature algorithm analysis	Free	Add comprehensive cryptographic algorithm strength assessment
91	SSL Certificate Key Length	Network Security	Node.js TLS certificate inspection	PASS: Strong key length (>=2048 bits) | FAIL: Weak key length	Deep enough - key strength validation	Free	Add support for different key types and recommended lengths

92	SSL Certificate Wild Card Usage	Network Security	Node.js TLS certificate inspection	PASS: Appropriate wildcard usage | WARNING: Wildcard certificate in use	Deep enough - wildcard certificate analysis	Free	Add wildcard scope validation and security implications analysis
93	Insecure SSL/TLS Versions	Network Security	Node.js TLS socket analysis	PASS: No insecure versions | FAIL: Insecure SSL/TLS versions detected	Deep enough - protocol version analysis	Free	Add comprehensive protocol support enumeration
94	Strong Certificate Key Length	Network Security	Node.js TLS socket analysis	PASS: Strong key length (>=2048 bits) | FAIL: Weak key length	Deep enough - cryptographic strength	Free	Add elliptic curve key support and future-proof recommendations
95	Insecure Cipher Suites	Network Security	Node.js TLS socket analysis	PASS: No insecure ciphers | FAIL: Insecure cipher suites detected	Deep enough - cipher suite analysis	Free	Add cipher preference order and perfect forward secrecy validation
96	Secure TLS Version	Network Security	Node.js TLS socket analysis	PASS: Secure TLS version | WARNING: Consider upgrading TLS version	Deep enough - TLS version validation	Free	Add TLS 1.3 support validation and deprecation timeline awareness
97	MySQL Port Exposure	Network Security	Port scanning via nmap	PASS: MySQL port closed | FAIL: MySQL port (3306) exposed	Deep enough - port scanning	Free	Add service version detection and authentication analysis
98	Port Mapper Service	Network Security	Port scanning via nmap	PASS: Port mapper service not detected | FAIL: Port mapper service (111) exposed	Deep enough - port scanning	Free	Add RPC service enumeration and exposure analysis
99	NTP Service Exposure	Network Security	Port scanning via nmap	PASS: NTP service not exposed | FAIL: NTP service (123) exposed	Deep enough - port scanning	Free	Add NTP amplification attack potential assessment
100	PPTP VPN Service	Network Security	Port scanning via nmap	PASS: PPTP service not detected | FAIL: PPTP service (1723) exposed	Deep enough - port scanning	Free	Add VPN security assessment and protocol analysis
101	SMTP Service Exposure	Network Security	Port scanning via nmap	PASS: SMTP service properly configured | FAIL: SMTP service (25) exposed	Deep enough - port scanning	Free	Add open relay testing and email security validation
102	SSH Service Exposure	Network Security	Port scanning via nmap	PASS: SSH service properly secured | WARNING: SSH service (22) exposed	Deep enough - port scanning	Free	Add SSH configuration analysis and key-based authentication validation
103	DNS Service Exposure	Network Security	Port scanning via nmap	PASS: DNS service properly configured | WARNING: DNS service (53) exposed	Deep enough - port scanning	Free	Add DNS configuration analysis and recursive query testing
104	HTTP Service Status	Network Security	Port scanning via nmap	PASS: HTTP service properly configured | INFO: HTTP service (80) detected	Deep enough - port scanning	Free	Add HTTPS redirection validation and security header analysis
105	HTTPS Service Status	Network Security	Port scanning via nmap	PASS: HTTPS service active | FAIL: HTTPS service (443) not available	Deep enough - port scanning	Free	Add TLS configuration analysis and certificate validation
106	IOTA Node Port	Network Security	Port scanning via nmap	PASS: IOTA node port not exposed | FAIL: IOTA node port (14265) exposed	Deep enough - port scanning	Free	Add blockchain service security analysis
107	RTMP Streaming Port	Network Security	Port scanning via nmap	PASS: RTMP port not exposed | FAIL: RTMP port (1935) exposed	Deep enough - port scanning	Free	Add streaming service security analysis
108	Cisco SCCP Port	Network Security	Port scanning via nmap	PASS: Cisco SCCP port not exposed | FAIL: Cisco SCCP port (2000) exposed	Deep enough - port scanning	Free	Add Cisco service security analysis
109	MySQL X Protocol Port	Network Security	Port scanning via nmap	PASS: MySQL X port not exposed | FAIL: MySQL X Protocol port (33060) exposed	Deep enough - port scanning	Free	Add database service security analysis
110	STUN/TURN Port	Network Security	Port scanning via nmap	PASS: STUN port not exposed | FAIL: STUN/TURN port (3478) exposed	Deep enough - port scanning	Free	Add WebRTC service security analysis
111	Redis Port Exposure	Network Security	Port scanning via nmap	PASS: Redis port not exposed | FAIL: Redis port (6379) exposed	Deep enough - port scanning	Free	Add Redis security configuration analysis
112	Unauthorized Ports Summary	Network Security	Comprehensive port analysis	PASS: No unauthorized ports | FAIL: Unauthorized ports detected	Deep enough - comprehensive port assessment	Free	Add service enumeration and attack surface analysis
113	Outdated WordPress	Patching Cadence	WordPress version comparison against latest	PASS: Current version | FAIL: Outdated version	Deep enough - version comparison logic	Free	Add vulnerability database correlation and patch management analysis
114	Unmaintained Page Detection	Patching Cadence	HTML content analysis for indicators	PASS: Site appears maintained | FAIL: Unmaintained indicators found	Simplified - basic content analysis	Free	Add CMS update detection and security patch status analysis