Complete Test Results

ID	Security Check	Status	Occurrences	Affected URLs
0	Directory Browsing	PASS	-	-
2	Private IP Disclosure	PASS	-	-
3	Session ID in URL Rewrite	PASS	-	-
6	Path Traversal	PASS	-	-
7	Remote File Inclusion	PASS	-	-
10003	Vulnerable JS Library (Powered by Retire.js)	PASS	-	-
10009	In Page Banner Information Leak	PASS	-	-
10010	Cookie No HttpOnly Flag	PASS	-	-
10011	Cookie Without Secure Flag	PASS	-	-
10015	Re-examine Cache-control Directives	PASS	-	-
10017	Cross-Domain JavaScript Source File Inclusion	PASS	-	-
10019	Content-Type Header Missing	PASS	-	-

10020	Missing Anti-clickjacking Header	WARN	2	https://davfds89h1pfc.cloudfront.net/, https://davfds89h1pfc.cloudfront.net
10021	X-Content-Type-Options Header Missing	WARN	8	Homepage and multiple static assets (favicon.ico, logo192.png, robots.txt, etc.)
10023	Information Disclosure - Debug Error Messages	PASS	-	-
10024	Information Disclosure - Sensitive Information in URL	PASS	-	-
10025	Information Disclosure - Sensitive Information in HTTP Referrer Header	PASS	-	-
10026	HTTP Parameter Override	PASS	-	-
10027	Information Disclosure - Suspicious Comments	PASS	-	-
10028	Open Redirect	PASS	-	-
10029	Cookie Poisoning	PASS	-	-

10030	User Controllable Charset	PASS	-	-
10031	User Controllable HTML Element Attribute (Potential XSS)	PASS	-	-
10032	Viewstate	PASS	-	-
10033	Directory Browsing	PASS	-	-
10034	Heartbleed OpenSSL Vulnerability (Indicative)	PASS	-	-
10035	Strict-Transport-Security Header Not Set	WARN	9	Homepage and multiple resources (favicon.ico, logo192.png, manifest.json, etc.)
10036	Server Leaks Version Information via "Server" HTTP Response Header Field	WARN	9	Homepage and multiple resources (favicon.ico, logo192.png, manifest.json, etc.)
10037	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	PASS	-	
10038	Content Security Policy (CSP) Header Not Set	WARN	3	https://davfds89h1pfc.cloudfront.net/, https://davfds89h1pfc.cloudfront.net,

				https://davfds89h1pfc.cloudfront.net/sitemap.xml
10039	X-Backend-Server Header Information Leak	PASS	-	
10040	Secure Pages Include Mixed Content	PASS	-	
10041	HTTP to HTTPS Insecure Transition in Form Post	PASS	-	
10042	HTTPS to HTTP Insecure Transition in Form Post	PASS	-	
10043	User Controllable JavaScript Event (XSS)	PASS	-	
10044	Big Redirect Detected (Potential Sensitive Information Leak)	PASS	-	
10045	Source Code Disclosure - /WEB-INF Folder	PASS	-	
10047	HTTPS Content Available via HTTP	WARN	8	Homepage and multiple resources (robots.txt, manifest.json, favicon.ico, etc.)

10048	Remote Code Execution - Shell Shock	PASS	-	
10049	Content Cacheability	PASS	-	
10050	Retrieved from Cache	PASS	-	
10051	Relative Path Confusion	PASS	-	
10052	X-ChromeLogger-Data (XCOLD) Header Information Leak	PASS	-	
10054	Cookie without SameSite Attribute	PASS	-	
10055	CSP	PASS	-	
10056	X-Debug-Token Information Leak	PASS	-	
10057	Username Hash Found	PASS	-	
10058	GET for POST	PASS	-	
10061	X-AspNet-Version Response Header	PASS	-	
10062	PII Disclosure	PASS	-	

10063	Permissions Policy Header Not Set	WARN	4	Homepage, sitemap.xml, and JavaScript files (static/js/main.86ec999b.js)
10095	Backup File Disclosure	PASS	-	
10096	Timestamp Disclosure - Unix	WARN	13	Multiple instances in https://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js
10097	Hash Disclosure	PASS	-	
10098	Cross-Domain Misconfiguration	PASS	-	
10099	Source Code Disclosure	PASS	-	
10104	User Agent Fuzzer	PASS	-	
10105	Weak Authentication Method	PASS	-	
10106	HTTP Only Site	PASS	-	
10107	Httpoxy - Proxy Header Misuse	PASS	-	
10108	Reverse Tabnabbing	PASS	-	
10109	Modern Web Application	PASS	-	
10110	Dangerous JS Functions	PASS	-	-
10111	Authentication Request Identified	PASS	-	-

10112	Session Management Response Identified	PASS	-	-
10113	Verification Request Identified	PASS	-	-
10115	Script Served From Malicious Domain (polyfill)	PASS	-	-
10202	Absence of Anti-CSRF Tokens	PASS	-	-
20012	Anti-CSRF Tokens Check	PASS	-	-
20014	HTTP Parameter Pollution	PASS	-	-
20015	Heartbleed OpenSSL Vulnerability	PASS	-	-
20016	Cross-Domain Misconfiguration	PASS	-	-
20017	Source Code Disclosure - CVE-2012-1823	PASS	-	-
20018	Remote Code Execution - CVE-2012-1823	PASS	-	-
20019	External Redirect	PASS	-	-
30001	Buffer Overflow	PASS	-	-

30002	Format String Error	PASS	-	-
30003	Integer Overflow Error	PASS	-	-
40003	CRLF Injection	PASS	-	-
40008	Parameter Tampering	PASS	-	-
40009	Server Side Include	PASS	-	-
40012	Cross Site Scripting (Reflected)	PASS	-	-
40013	Session Fixation	PASS	-	-
40014	Cross Site Scripting (Persistent)	PASS	-	-
40016	Cross Site Scripting (Persistent) - Prime	PASS	-	-
40017	Cross Site Scripting (Persistent) - Spider	PASS	-	-
40018	SQL Injection	PASS	-	-
40019	SQL Injection - MySQL	PASS	-	-
40020	SQL Injection - Hypersonic SQL	PASS	-	-

40021	SQL Injection - Oracle	PASS	-	-
40022	SQL Injection - PostgreSQL	PASS	-	-
40023	Possible Username Enumeration	PASS	-	-
40024	SQL Injection - SQLite	PASS	-	-
40025	Proxy Disclosure	PASS	-	-
40026	Cross Site Scripting (DOM Based)	PASS	-	-
40027	SQL Injection - MsSQL	PASS	-	-
40028	ELMAH Information Leak	PASS	-	-
40029	Trace.axd Information Leak	PASS	-	-
40031	Out of Band XSS	PASS	-	-
40032	.htaccess Information Leak	PASS	-	-
40034	.env Information Leak	PASS	-	-
40035	Hidden File Finder	PASS	-	-
40038	Bypassing 403	PASS	-	-

40040	CORS Header	PASS	-	-
40042	Spring Actuator Information Leak	PASS	-	-
40043	Log4Shell	PASS	-	-
40044	Exponential Entity Expansion (Billion Laughs Attack)	PASS	-	-
40045	Spring4Shell	PASS	-	
40046	Server Side Request Forgery	PASS	-	
40047	Text4shell (CVE-2022-42889)	PASS	-	
41	Source Code Disclosure - Git	PASS	-	
42	Source Code Disclosure - SVN	PASS	-	
43	Source Code Disclosure - File Inclusion	PASS	-	
50000	Script Active Scan Rules	PASS	-	
50001	Script Passive Scan Rules	PASS	-	
90001	Insecure JSF ViewState	PASS	-	

90002	Java Serialization Object	PASS	-	
90003	Sub Resource Integrity Attribute Missing	PASS	-	
90004	Insufficient Site Isolation Against Spectre Vulnerability	WARN	10	Multiple instances on homepage URLs
90011	Charset Mismatch	PASS	-	
90017	XSLT Injection	PASS	-	
90019	Server Side Code Injection	PASS	-	
90020	Remote OS Command Injection	PASS	-	
90021	XPath Injection	PASS	-	-
90022	Application Error Disclosure	PASS	-	-
90023	XML External Entity Attack	PASS	-	-
90024	Generic Padding Oracle	PASS	-	-
90025	Expression Language Injection	PASS	-	-

90026	SOAP Action Spoofing	PASS	-	-
90027	Cookie Slack Detector	PASS	-	-
90028	Insecure HTTP Method	PASS	-	-
90029	SOAP XML Injection	PASS	-	-
90030	WSDL File Detection	PASS	-	-
90033	Loosely Scoped Cookie	PASS	-	-
90034	Cloud Metadata Potentially Exposed	PASS	-	-
90035	Server Side Template Injection	PASS	-	-
90036	Server Side Template Injection (Blind)	PASS	-	-

Summary Statistics

Status	Count	Percentage
PASS	128	93.4%
WARN-NEW	9	6.6%
FAIL-NEW	0	0%
FAIL-INPROG	0	0%
WARN-INPROG	0	0%
INFO	0	0%

IGNORE	0	0%
TOTAL	**137**	**100%**