DRCBS Baseline Web Application Security Checklist - v2.0

S.No.	Vulnerability/Error	References	Severity (Critical/High/Medium/Low/Informational) CVSS Infomational = 0, Low = 0.1 to 3.9, Medium = 4.0 to 6.9, High = 7.0 to 8.9, Critical = 9.0 to 10.0			
			External Application	Range	Internal Application	Range
Authentication Related						
1	Weak Password Policy	CWE-521, 620, OWASP ASVS v4.0.3 – V2.1	Medium	4.0 to 6.9	Low	0.1 to 3.9
2	2FA Authentication Bypass	OWASP ASVS v4.0.3 – V2.6, OWASP Top 10 A07:2025, CAPEC-115	High	7.0 to 8.9	Medium	4.0 to 6.9
3	Missing Rate Limiting on Authentication / 2FA	OWASP ASVS v4.0.3 – V2.2	Medium	4.0 to 6.9	Medium	4.0 to 6.9
4	2FA Replay Attack	CWE-294, OWASP ASVS v4.0.3 – V2.7, NIST SP 800-53 Rev. 5.2.0 - IA-08	High	7.0 to 8.9	High	7.0 to 8.9
5	Authentication Bypass	OWASP Top 10 A07:2025, OWASP ASVS v4.0.3 – V2	Critical	9.0 to 10.0	High	7.0 to 8.9
6	Insecure OTP Implementation	CAPEC-121, CAPEC-49, CAPEC-60, CAPEC-55, OWASP ASVS v4.0.3 – V2.6	High to Medium (Depends on the attack)	4.0 to 8.9	Medium	4.0 to 6.9
7	Improper CAPTCHA Implementation	CWE-804, OWASP ASVS v4.0.3 – V2.2, OWASP Top 10 A07	High to Medium (Depends on the attack)	4.0 to 8.9	Medium	4.0 to 6.9
8	Use of Hard-Coded Credentials	CWE-798, OWASP ASVS v4.0.3 – V2.10	High	7.0 to 8.9	Medium	4.0 to 6.9
Session Related						
9	Session Management / Parallel Session Usage	CWE-613, OWASP ASVS v4.0.3 – V3	Medium	4.0 to 6.9	Low	0.1 to 3.9
10	Session Hijacking	CAPEC-593	Critical	9.0 to 10.0	Critical	9.0 to 10.0
11	Session Fixation	CWE-384, OWASP Top10:2025 A07:2025 Authentication Failures	High	7.0 to 8.9	High	7.0 to 8.9
12	Cross Site Request Frogery	CWE-352, OWASP Top10:2025 - A01:2025 Broken Access Control	High (Medium if not sensitive data is there)	4.0 to 8.9	High (Medium if not sensitive data is there)	4.0 to 8.9
13	Back & Refresh Attack	CWE-613, OWASP ASVS v4.0.3 – V3.3.1	Medium	4.0 to 6.9	Medium	4.0 to 6.9
14	Cookie Manipulation	CWE-565, CWE-565	Medium/High	4.0 to 8.9	Medium	4.0 to 6.9
15	Cookie without Secure Flag	CWE-614, OWASP ASVS v4.0.3 – V3.4.1	Low	0.1 to 3.9	Low	0.1 to 3.9
16	Cookie without Http-Only Flag	OWASP ASVS v4.0.3 – V3.4.2, CWE-1004 (In some case if session is only bind with cookie)	Low	0.1 to 3.9	Low	0.1 to 3.9
17	Cookie without Same-Site Attribute	OWASP ASVS v4.0.3 – V3.4.3	Low	0.1 to 3.9	Informational	0
Encryption Related						
18	Absence of SSL Certificate	CWE-319,OWASP ASVS v4.0.3 – V9.1.1	Critical	9.0 to 10.0	Low	0.1 to 3.9
19	Use of Insecure TLS Versions (TLS 1.0, TLS 1.1)	CWE-319,OWASP ASVS v4.0.3 – V9.1.1	High	7.0 to 8.9	Low	0.1 to 3.9
20	Insufficient Cryptography (TLS 1.2 with weak cipher suite)	CWE-326, OWASP ASVS v4.0.3 – V9.1.1	Medium	4.0 to 6.9	Low	0.1 to 3.9
21	Insecure Client-Side Encryption Mechanism	CWE-326, OWASP Top 10:2025 A04:2025 Cryptographic Failures	Medium	4.0 to 6.9	Low	0.1 to 3.9
22	Weak Encryption Method for Password Policy	CWE-261	Medium	4.0 to 6.9	Medium	4.0 to 6.9
Configuration Related						
23	HTTP Methods Allowed (OPTIONS, DELETE, PUT, TRACE, PATCH)	CWE-650, OWASP ASVS v4.0.3 – V14.1.3 and 14.5.1	Low (DELETE or more than 2 then Medium)	0.1 to 6.9	Low	0.1 to 3.9
24	HTTP Strict Transport Security	OWASP ASVS v4.0.3 – V14.1.5	Low	0.1 to 3.9	Low	0.1 to 3.9
25	Improper or No Cache-control Header Set	CWE-525	Low	0.1 to 3.9	Low	0.1 to 3.9
26	X-Frame Option header not set	OWASP ASVS v4.0.3 – V14.4.7	Low	0.1 to 3.9	Low	0.1 to 3.9
27	X-Content header missing	OWASP ASVS v4.0.3 – V14.4.4	Low	0.1 to 3.9	Low	0.1 to 3.9
28	Content Security Policy Bypass	OWASP ASVS v4.0.3 – V14.4.3	Medium	4.0 to 6.9	Low	0.1 to 3.9
29	X-Powered-By Version Disclosure	CWE-497	Low	0.1 to 3.9	Low	0.1 to 3.9
30	Cross-Origin Resource Sharing (CORS)	CWE-942, OWASP ASVS v4.0.3 – V14.5.3	Medium	4.0 to 6.9	Low	0.1 to 3.9
31	Absence of Anti-CSRF Tokens	CWE-352	Medium	4.0 to 6.9	Medium	4.0 to 6.9
32	Improper Input Validation	CWE-1287	Medium	4.0 to 6.9	Medium	4.0 to 6.9
33	Unrestricted Upload of File with Dangerous Type	CWE-434, OWASP ASVS v4.0.3 – V12	Medium	4.0 to 6.9	Medium	4.0 to 6.9
34	URL Redirection to Untrusted Site ('Open Redirect')	CWE-601	Medium	4.0 to 6.9	Low	0.1 to 3.9
35	Creation of Temporary File in Directory with Insecure Permissions	CWE-378/379	Medium	4.0 to 6.9	Medium	4.0 to 6.9
Injection Related						
36	SQL Injection	CWE-89, OWASP Top 10:2025 A05:2025 Injection	Critical/High	7.0 to 10.0	Critical/High	7.0 to 10.0
37	NoSQL injection	OWASP Top 10:2025 A05:2025 Injection, OWASP ASVS v4.0.3 – V5.3.4	Critical(Full Access)/High(Write&Read)/Medium(Read)	4.0 to 10.0	Critical(Full Access)/High(Write&Read)/Medium(Read)	4.0 to 10.0

38	OS Command Injection	CWE-78, OWASP Top 10:2025 A05:2025 Injection	Critical	9.0 to 10.0	Critical	9.0 to 10.0
39	Reflected / DOM / Stored Cross Site Scripting	CWE-79, OWASP Top 10:2025 A05:2025 Injection	Critical/High	7.0 to 10.0	Critical/High	7.0 to 10.0
40	HTML Injection	CWE-80, OWASP Top 10:2025 A05:2025 Injection	High	7.0 to 8.9	Medium	4.0 to 6.9
41	IFrame Injection	CWE-1021, OWASP Top 10:2025 A05:2025 Injection	High	7.0 to 8.9	Medium	4.0 to 6.9
42	LDAP Injection	CWE-90, OWASP Top 10:2025 A05:2025 Injection	Critical	9.0 to 10.0	Critical	9.0 to 10.0
43	XPath Injection	CWE-643, OWASP Top 10:2025 A05:2025 Injection, OWASP ASVS v4.0.3 – V5.3.10	High	7.0 to 8.9	High	7.0 to 8.9
44	XML Injection	OWASP Top 10:2025 A05:2025 Injection, OWASP ASVS v4.0.3 – V5.3.10	High	7.0 to 8.9	High	7.0 to 8.9
45	Server Side Template Injection (SSTI)	CWE-1336, OWASP Top 10:2025 A05:2025 Injection	High	7.0 to 8.9	High	7.0 to 8.9
46	CRLF Injection	CWE-93, OWASP Top 10:2025 A05:2025 Injection	High	7.0 to 8.9	High	7.0 to 8.9
47	XXE Injection	CWE-611, OWASP Top 10:2025 A05:2025 Injection	High	7.0 to 8.9	High	7.0 to 8.9
48	Server-Side Request Forgery (SSRF)	CWE-918	Critical	9.0 to 10.0	High	7.0 to 8.9
49	Directory Traversal/Path Traversal	CWE-22	High	7.0 to 8.9	Medium	4.0 to 6.9
Sensitive Data Exposure						
50	Cleartext Transmission of Credentials	OWASP Top 10:2025 A04:2025 Cryptographic Failures	Informational	0	Informational	0
51	Plaintext Storage of a Password (Memory or Files)	CWE-256	Medium	4.0 to 6.9	Medium	4.0 to 6.9
52	Exposure of Configuration Files	OWASP Top 10:2025 A02:2025 - Security Misconfiguration	Medium	4.0 to 6.9	Low	0.1 to 3.9
53	Private IP Disclosure	CWE-497, OWASP Top 10:2025 A02:2025 - Security Misconfiguration	Low	0.1 to 3.9	Informational	0
54	Source Code Disclosure	CWE-540, OWASP Top 10:2025 A02:2025 - Security Misconfiguration	Medium	4.0 to 6.9	Low	0.1 to 3.9
55	Sensitive Information Disclosure Through Error Messages	CWE-209, OWASP ASVS v4.0.3 – V7.4	Medium/Low	0.1 to 6.9	Low	0.1 to 3.9
56	Exposure of WSDL File Containing Sensitive Information	CWE-651, OWASP Top 10:2025 A02:2025 - Security Misconfiguration	Low	0.1 to 3.9	Low	0.1 to 3.9
57	Directory Listings	CWE-548, OWASP Top 10:2025 A02:2025 - Security Misconfiguration	Medium	4.0 to 6.9	Medium	4.0 to 6.9
58	Internal Path Disclosure	CWE-497	Low	0.1 to 3.9	Low	0.1 to 3.9
59	User Enumeration	CWE-497	Medium	4.0 to 6.9	Medium	4.0 to 6.9
60	Email Disclosure / Email Harvesting	CWE-359	Informational	0	Informational	0
Access Control Related						
61	Unprotected Admin Panel	CWE-419	Medium	4.0 to 6.9	Low	0.1 to 3.9
62	Incorrect Privilege Assignment	CWE-266	Medium	4.0 to 6.9	Medium	4.0 to 6.9
63	Improper Restriction of Excessive Authentication Attempts/Absence of Lockout Policy	CWE-307	Medium	4.0 to 6.9	Low	0.1 to 3.9
64	Insecure Direct Object Reference (IDOR)	CWE-639	High	7.0 to 8.9	High	7.0 to 8.9
Business Logic Flaws/Error						
65	Functional Error	OWASP ASVS v4.0.3 – V11	Low	0.1 to 3.9	Low	0.1 to 3.9
66	Concurrent Execution using Shared Resource with Improper Synchronization / Race Condition	CWE-362	Medium	4.0 to 6.9	Medium	4.0 to 6.9
67	Insecure Design	1348/657	Medium	4.0 to 6.9	Medium	4.0 to 6.9
68	Broken Link	OWASP Top 10:2025 A02:2025 Security Misconfiguration	Low	0.1 to 6.9	Low	0.1 to 6.9
Out-of-Band Management (OOBM)						
69	Out-of-bounds Write	CWE-787	High	7.0 to 8.9	High	7.0 to 8.9
70	Out-of-bounds Read	CWE-125	High	7.0 to 8.9	High	7.0 to 8.9
71	Host Header Injection	CWE-346	Medium	4.0 to 6.9	Medium	4.0 to 6.9
OTHERS						
72	Vulnerable/Outdated Components	CWE-1104	Medium/Low	0.1 to 6.9	Medium/Low	0.1 to 6.9
73	Server Related Issues (Sampe Files, Directories, Default Credentials)	CWE-550	Medium	4.0 to 6.9	Medium	4.0 to 6.9
74	Parameter Based Attacks	CWE-233	High	7.0 to 8.9	High	7.0 to 8.9
75	Insecure Storage of Cookies	CWE-922 / CWE-312	Medium	4.0 to 6.9	Medium	4.0 to 6.9
Privilage Escalation						
76	Privilage Escalation (Vertical / Horizontal)	CWE-639	Critical	9.0 to 10.0	Critical	9.0 to 10.0
77	Broken Access Control	OWASP ASVS v4.0.3 – V4, OWASP Top 10:2025 – A01: Broken Access Control	Critical to Low (Depends on the attack)	0.1 to 10.0	Critical to Low (Depends on the attack)	0.1 to 10.0