Network Security and Cryptography Lab [IIIT Allahabad]

Web Security – Preliminary Checklist

1	Avoid Iframe by doing X Options = Deny [Use Same Origin Policy]
2	Avoid Directory Listing
3	Use HTTPS
4	Use Symbolic Link whenever required
5	Avoid SQL injection - Use prepared statement and Sanitization
6	Avoid XSS vulnerability (Persistent, Reflected and DOM) - Sanitization
7	Avoid CSRF vulnerability with random tokens for each request
8	Keep the folder accessible only by apache and only respective folder
9	Allow to upload desired type of file. Use sandbox for the execution of the file.
10	Avoid user accessing the file directly (even after login accessing others data directly should be avoided) - Files with random name
11	Use the Get method without side effects. If not, then validate.
12	Avoid Window Event Listener. If required then only to the specific domain name.
13	No mixed content
14	Control providing access of database for the remote machines
15	Do not Store the credentials in plain text. Hash it. Also use the salt.
16	Check whether bash history is accessible or not
17	Restrict permission to bashrc file
18	Change the default error reporting (Customize)
19	Restrict sending the server signature in http response
20	Enable user access logs (http and https) without sensitive data
21	Add Content Security Policy
22	Avoid Tabnabbing [supported by browser]
23	Sanitize and store log data [developer log]
24	Apache or other can have restricted access
25	Avoid using self-signed certificate
26	Sanitize all get and post content
27	Updated versions of the software
28	Forcing Strong Passwords
29	Session Age and unique session id
30	Cookie - httponly, own site and secure in all pages
31	Avoid hidden attributes
32	Session Id generation - Random and unguessable
33	No default credentials
34	Regular Backup on different machine
35	Limited Error Reporting
36	Fix OS command injection vulnerability
37	Buffer overflow restriction
38	Avoid HTML injection
39	No hardcoding of credentials except for automated
40	No sniff header for uploaded content

41	Session destroy at logout
42	Use non-persistent cookie
43	Access Control Validation
44	Disable Caching
45	Avoid insecure serialization
46	Use strong cryptographic algorithms
47	Database checksum
48	Upgrade insecure requests
49	Ensure Logout exit not only navigate
50	Avoid XXE injection
51	Use Captcha/re-Captcha to avoid bots bruteforce
52	Use robots.txt for performance and stop genuine crawlers