1 Authentication Bypass

2 Authorization(Forced Browsing, Privilege Escalation, IDOR etc)

3 Cross-Site Request Forgery (CSRF)

4 Injection (CSV injection, XPath Injection, Formula Injection, SQL Injection, Command Injection, XML Injection, Null byte injection etc)

5 LFI/RFI

6 XML Entity Expansion (Billion Laughs Attack)

7 Server-Side Request Forgery (SSRF)

8 Cross-Site Scripting (XSS)

9 Unrestricted File Upload

10 CORS

11 Session related issues, Session token in URL

12 SSL/TLS related issues

13 Directory Traversal

14 Functionality of Forgot Password

15 HTTP Smuggling/ Desync Attack

16 Idle session user timeout

17 Web Form Manipulation

18 Login CSRF Attack (In Oauth Authentication)

19 Version Disclosure (such as Web server, Framework, Javascript, Semanti UI..)