Category Name	Vulnerabilty Name	Tool Name
Recon and Information gathering	Discovering hidden and default content	Shodan, Censys, Wayback machine
	Identifying the technologies and frameworks being used	Wappalyzer extension
	Testing for Debug Parameters	Manual
	Subdomain Enumeration	Subfinder, Subbrute, Google Dorks
	Port Scan	Nmap
	Finding hidden endpoints	Wfuzz and Dirsearch
Server Security Misconfiguration	Using Default Credentials	During Recon
Authentication Based	No Password Policy	Manual
	Authentication Bypass	
	Username Enumeration	Manual/ Burp Intruder
	Test for Password Reset Functionality	
	If Login Credentials are being sent over HTTP	Wireshark
Session	Check for insecure transmission of tokens	
	Check session termination	
	CSRF(Application Wide)	Burpsuite
	Failure to Invalidate Session on Logout(Client And Server Side)	
	Failure to Invalidate Session on Password Reset or Change	
	Disclosure of tokens in logs and URL	
Input Validation	IDOR	Burp Repeater
	Privilege Escalation	
	Reflected XSS	Repeater/ Manually
	Stored XSS	Repeater/ Manually
	SQLi Injection	SQlmap
	XXE Injection	
	DOM XSS	
	XSS(IE11 Only)	Manual
	XSS Referer	Burp Repeater
	XSS Universal(UXSS)	Burp Repeater
	OAuth Misconfiguration (Missing/Broken State Parameter)	
	OAuth Misconfiguration (Insecure Redirect URI)	
	Subdomain takeover	Aquatone, can-i-take-over-xyz
	Local File Inclusion	
	Remote File Inclusion	
	Finding Private API keys	Recon
	Server Side Request Forgery(SSRF)	
	Command Injection	
	Mail Server Misconfiguration	

Miscellaneous	No rate limting on forms(Registration, Login, emails)	Burp Intruder
	Clickjacking	Burp Clickbandit
	Open Redirects	Manual
	Hardcoded Password	
	Application Level DoS	
	Usage of Components with Unknown Vulnerabilities(Rosetta Flash)	
	Unsafe Cross Origin Resource Sharing	Burp History
	Path Traversal	
	Directory Listing Enabled	
	SSL Attack(BREACH, POODLE etc.)	SSLtest, Tessl.sh
	Unnecessary Open Ports and Services	NMAP
	Remote Code Execution	
Sensitive Information Disclosure	Password Disclosure	
	EXIF Geolocation Data Not Stripped From Uploaded Images	
	Visible Detailed Error/Debug Page	Manual
	Token leakage via Referer(Over HTTP)	
	Sensitive Token in URL(User facing)	
	Weak Password Reset Implementation(Password reset token sent over HTTP)	
	Cross Site Script inclusion(XSSI)	
	Private API keys	Recon
Broken Cryptography	Cryptographic Flaw	
Server Security Misconfiguration	Missing SPF on Email Domain	
	Email Spoofable via Third-Party API Misconfiguration	
	DBMS misconfiguration(Excessively Privileged User / DBA)	
	Lack of Password Confirmation while Deleting Account	Manual
	Missing Secure or HttpOnly Cookie Flag	Burp Request-Response
	Captcha Bypass(Implementation Vulnerability)	
	Lock of Security Headers(Cache Control for a Sensitive page)	Burp Request-Response
	Misconfigured DNS(Zone Transfer)	
Server-Side Injection	HTTP Response manipulation(Response-Splitting CRLF)	
	Content-Spoofing(Iframe Injection)	
	External Authentication Injection	
	Email HTML Injection	
Insecure Data Storage	Server-Side credentials storage in Plaintext	
	Sensitive Application Data Stored Unencrypted on External Storage	
Insecure Data Transport	Executable Download(No Secure Integrity Check)	
Privacy Concerns	Unnecessary Data collection(Wifi SSiD+Password)	

[redacted]