@hackinarticles
https://github.com/Ignitetechnologies
https://in.linkedin.com/company/hackingarticles

OWASP Testing Checklist

www.hackingarticles.in

Authentication Testing

- **WSTG-ATHN-07**
  - Testing for Weak Password Policy
  - Determine the resistance of the application against brute force password guessing using available password dictionaries by evaluating the length, complexity, reuse, and aging requirements of passwords.
  - Tools
    - Burp Proxy
    - ZAP
    - Hydra
  - OWASP Top 10
    - A7
  - CWE
    - CWE-521
    - CWE-1391
- **WSTG-ATHN-08**
  - Testing for Weak Security Question Answer
  - Determine the complexity and how straight-forward the questions are. Assess possible user answers and brute force capabilities.
  - Tools
    - Browser
  - OWASP Top 10
    - A7
  - CWE
    - CWE-640
- **WSTG-ATHN-09**
  - Testing for Weak Password Change or Reset Functionalities
  - Determine whether the password change and reset functionality allows accounts to be compromised.
  - Tools
    - Browser
    - Burp Proxy
    - ZAP
  - OWASP Top 10
    - A7
  - CWE
    - CWE-620
    - CWE-640
- **WSTG-ATHN-10**
  - Testing for Weaker Authentication in Alternative Channel
  - Identify alternative authentication channels. Assess the security measures used and if any bypasses exists on the alternative channels.
  - Tools
    - Browser
  - OWASP Top 10
    - A7
  - CWE
    - CWE-288
- **WSTG-ATHN-11**
  - Testing Multi-Factor Authentication
  - Identify the type of MFA used by the application. Determine whether the MFA implementation is robust and secure. Attempt to bypass the MFA.
  - Tools
    - JMeter
  - OWASP Top 10
    - A7
  - CWE
    - CWE-288
    - CWE-304
    - CWE-308
- **WSTG-ATHN-01**
  - Testing for Credentials Transported over an Encrypted Channel
  - Check referrer whether its HTTP or HTTPs. Sending data through HTTP and HTTPS.
  - Tools
    - Burp Proxy
    - ZAP
  - OWASP Top 10 - NA
  - CWE - NA
- **WSTG-ATHN-02**
  - Testing for Default Credentials
  - Determine whether the application has any user accounts with default passwords.
  - Tools
    - Burp Intruder
    - THC Hydra
    - Nikto 2
  - OWASP Top 10
    - A7
  - CWE
    - CWE-1392
- **WSTG-ATHN-03**
  - Testing for Weak Lock Out Mechanism
  - Evaluate the account lockout mechanism's ability to mitigate brute force password guessing.
  - Tools
    - Browser
  - OWASP Top 10
    - A7
  - CWE
    - CWE-307
- **WSTG-ATHN-04**
  - Testing for Bypassing Authentication Schema
  - Ensure that authentication is applied across all services that require it.
  - Tools
    - WebGoat
    - OWASP Zed Attack
  - OWASP Top 10
    - A1
    - A7
  - CWE
    - CWE-287
    - CWE-288
    - CWE-290
    - CWE-294
    - CWE-302
    - CWE-304
    - CWE-306
    - CWE-425
    - CWE-804
- **WSTG-ATHN-05**
  - Testing for Vulnerable Remember Password
  - Validate that the generated session is managed securely and do not put the users credentials in danger.
  - Tools
    - Browser
  - OWASP Top 10
    - A4
    - A5
  - CWE
    - CWE-315
    - CWE-522
    - CWE-524
- **WSTG-ATHN-06**
  - Testing for Browser Cache Weaknesses
  - Review if the application stores sensitive information on the client-side. Review if access can occur without authorization.
  - Tools
    - OWASP Zed Attack Proxy
  - OWASP Top 10
    - A4
  - CWE
    - CWE-525

Information Gathering

- **WSTG-INFO-01**
  - Conduct Search Engine Discovery Reconnaissance for Information Leakage
  - Identify what sensitive design and configuration information of the application, system, or organization is exposed directly (on the organization's website) or indirectly (via third-party services)
  - Tools
    - Bing
    - Shodan
    - Google
    - Common Crawl
  - OWASP Top 10 - NA
  - CWE - NA
- **WSTG-INFO-02**
  - Fingerprint Web Server
  - Determine the version and type of a running web server to enable further discovery of any known vulnerabilities
  - Tools
    - Netcraft
    - Nikto2
    - Nmap
    - Zenmap
  - OWASP Top 10
    - A5
    - A6
  - CWE
    - CWE-756
    - CWE -1352
- **WSTG-INFO-03**
  - Review Webserver Metafiles for Information Leakage
  - Identify hidden or obfuscated paths and functionality through the analysis of metadata files
  - Tools
    - Browser
    - curl
    - wget
    - Burp Suite
    - ZAP
  - OWASP Top 10
    - A1
  - CWE
    - CWE-200
- **WSTG-INFO-04**
  - Enumerate Applications on Webserver
  - Enumerate the applications within the scope that exist on a web server
  - Tools
    - Nmap
    - Nessus Vulnerability Scanner
    - Nikto2
  - OWASP Top 10 - NA
  - CWE - NA
- **WSTG-INFO-05**
  - Review Webpage Content for Information Leakage
  - Review webpage comments, metadata, and redirect bodies to find any information leakage.
  - Tools
    - Eyeballs
    - Curl
    - Zaproxy
    - Burp Suite
    - Waybackurls
    - Google Maps API Scanner
  - OWASP Top 10
    - A1
  - CWE
    - CWE-200
    - CWE-540
- **WSTG-INFO-10**
  - Map Application Architecture
  - Understand the architecture of the application and the technologies in use.
  - Tools
    - Browser
    - curl
    - wget
  - OWASP Top 10 - NA
  - CWE - NA
- **WSTG-INFO-09**
  - Fingerprint Web Application
  - Identify the web application and version to determine known vulnerabilities and the appropriate exploits.
  - Tools
    - Whatweb
    - BlindElephant
    - Wappalyzer
    - CMSmap
  - OWASP Top 10 - NA
  - CWE - NA
- **WSTG-INFO-08**
  - Fingerprint Web Application Framework
  - Fingerprint the components being used by the web applications.
  - Tools
    - WhatWeb
    - Wappalyzer
  - OWASP Top 10
    - A5
    - A6
  - CWE
    - CWE-756
    - CWE -1104
- **WSTG-INFO-07**
  - Map Execution Paths Through Application
  - Map the target application and understand the principal workflows.
  - Tools
    - ZAP
    - List of spreadsheet software
    - Diagramming software
  - OWASP Top 10 - NA
  - CWE - NA
- **WSTG-INFO-06**
  - Identify Application Entry Points
  - Identify possible entry and injection points through request and response analysis.
  - Tools
    - OWASP Zed Attack Proxy (ZAP)
    - Burp Suite
    - Fiddler
  - OWASP Top 10 - NA
  - CWE - NA

Session Management Testing

- **WSTG-SESS-01**
  - Testing for Session Management Schema
  - Gather session tokens, for the same user and for different users where possible.Analyze and ensure that enough randomness exists to stop session forging attacks.
  - OWASP Zed Attack Proxy Project (ZAP) - features a session token analysis mechanism.
  - Tools
    - Burp Sequencer
    - YEHG's JHijack
  - OWASP Top 10
    - A2
    - A4
  - CWE
    - CWE-315
    - CWE-330
    - CWE-539
    - CWE-694
- **WSTG-SESS-02**
  - Testing for Cookies Attributes
  - Ensure that the proper security configuration is set for cookies.
  - Tools
    - Intercepting Proxy
      - OWASP Zed Attack Proxy Project
      - Web Proxy Burp Suite
    - Browser Plug-in
      - Tamper Data for FF Quantum
      - "FireSheep" for FireFox
      - "EditThisCookie" for Chrome
      - "Cookiebro - Cookie Manager" for FireFox
  - OWASP Top 10
    - A5
  - CWE
    - CWE-16
    - CWE-614
    - CWE-1004
    - CWE-1275
- **WSTG-SESS-03**
  - Testing for Session Fixation
  - Analyze the authentication mechanism and its flow. Force cookies and assess the impact.
  - Tools
    - OWASP ZAP
  - OWASP Top 10
    - A7
  - CWE
    - CWE-384
- **WSTG-SESS-04**
  - Testing for Exposed Session Variables
  - Ensure that proper encryption is implemented. Review the caching configuration. Assess the channel and methods' security.
  - Tools
    - OWASP ZAP
    - Burp Proxy
  - OWASP Top 10
    - A7
  - CWE
    - CWE-598
- **WSTG-SESS-05**
  - Testing for Cross Site Request Forgery
  - Determine whether it is possible to initiate requests on a user's behalf that are not initiated by the user.
  - Tools
    - OWASP ZAP
    - CSRF Tester
    - Pinata-csrf-tool
  - OWASP Top 10
    - A1
  - CWE
    - CWE-352
- **WSTG-SESS-10**
  - Testing JSON Web Tokens
  - Determine whether the JWTs expose sensitive information. Determine whether the JWTs can be tampered with or modified.
  - Tools
    - John the Ripper
    - jwt2john
    - jwt-cracker
    - JSON Web Tokens Burp Extension
    - ZAP JWT Add-on
  - OWASP Top 10
    - A7
  - CWE
    - CWE-345
    - CWE-757
    - CWE-798
- **WSTG-SESS-09**
  - Testing for Session Hijacking
  - Identify vulnerable session cookies. Hijack vulnerable cookies and assess the risk level.
  - Tools
    - Jhijack
    - ZAP
  - OWASP Top 10
    - A2
  - CWE
    - CWE-523
- **WSTG-SESS-08**
  - Testing for Session Puzzling
  - Identify all session variables. Break the logical flow of session generation.
  - Tools
    - Burp Proxy
    - ZAP
  - OWASP Top 10
    - A7
  - CWE
    - CWE-841
- **WSTG-SESS-07**
  - Testing Session Timeout
  - Validate that a hard session timeout exists, after the timeout has passed, all session tokens should be destroyed or be
  - Tools
    - Burp Proxy
    - ZAP
  - OWASP Top 10
    - A7
  - CWE
    - CWE-613
- **WSTG-SESS-06**
  - Testing for Logout Functionality
  - Assess the logout UI. Analyze the session timeout and if the session is properly killed after logout.
  - Tools
    - Burp Suite - Repeater
  - OWASP Top 10
    - A7
  - CWE
    - CWE-613

Configuration and Deployment Management Testing

- **WSTG-CONF-08**
  - Test RIA Cross Domain Policy
  - Analyse the permissions allowed from the policy files (crossdomain.xml/clientaccesspolicy.xml) and allow-access-from.
  - Tools
    - Burp Proxy
    - ZAP
    - Nikto2
  - OWASP Top 10
    - A5
  - CWE
    - CWE-942
- **WSTG-CONF-09**
  - Test File Permission
  - Review and identify any rogue file permissions.
  - Tools
    - Windows AccessEnum
    - Windows AccessChk
    - Linux namei
  - OWASP Top 10
    - A1
    - A5
  - CWE
    - CWE-552
    - CWE-732
- **WSTG-CONF-10**
  - Test for Subdomain Takeover
  - Enumerate all possible domains (previous and current). Identify forgotten or misconfigured domains.
  - Tools
    - dig
    - recon-ng
    - theHarvester
    - Sublist3r
    - dnsrecon
  - OWASP Top 10 - NA
  - CWE
    - CWE-673
- **WSTG-CONF-11**
  - Test Cloud Storage
  - Assess that the access control configuration for the storage services is properly in place.
  - Tools
    - AWS CLI
  - OWASP Top 10
    - A1
  - CWE
    - CWE-264
- **WSTG-CONF-12**
  - Test for Content Security Policy
  - Review the Content-Security-Policy header or meta element to identify misconfigurations.
  - Tools
    - Google CSP Evaluator
    - CSP Auditor
    - CSP Generator
  - OWASP Top 10
    - A5
  - CWE
    - CWE-1021
- **WSTG-CONF-13**
  - Test for Path Confusion
  - Make sure application paths are configured correctly.
  - Tools
    - OWASP Zed Attack Proxy
    - Burp Suite
  - OWASP Top 10
    - A5
  - CWE
    - CWE-436
- **WSTG-CONF-01**
  - Test Network Infrastructure Configuration
  - Review the applications' configurations set across the network and validate that they are not vulnerable.
  - Tools
    - Nessus
  - OWASP Top 10
    - A1
    - A5
    - A6
  - CWE
    - CWE-284
    - CWE-1349
    - CWE-1352
- **WSTG-CONF-02**
  - Test Application Platform Configuration
  - Ensure that defaults and known files have been removed. Validate that no debugging code or extensions are left in the production environments.
  - Tools
    - Browser
    - Nikto2
  - OWASP Top 10
    - A1
    - A5
    - A9
  - CWE
    - CWE-13
    - CWE-117
    - CWE-223
    - CWE-200
    - CWE-201
    - CWE-489
    - CWE-532
    - CWE-548
    - CWE-651
    - CWE-778
- **WSTG-CONF-03**
  - Test File Extensions Handling for Sensitive Information
  - Dirbust sensitive file extensions, or extensions that might contain raw data (e.g. scripts, raw data, credentials, etc.).
  - Tools
    - wget
    - curl
    - google for "web mirroring tools"
  - OWASP Top 10
    - A1
  - CWE
    - CWE-200
    - CWE-425
    - CWE-552
- **WSTG-CONF-04**
  - Review Old Backup and Unreferenced Files for Sensitive Information
  - Find and analyse unreferenced files that might contain sensitive information.
  - Tools
    - Nessus
    - Nikto2
    - wget
    - Wget for Windows
    - Sam Spade
    - Xenu
    - curl
  - OWASP Top 10
    - A1
  - CWE
    - CWE-200
    - CWE-531
    - CWE-538
- **WSTG-CONF-05**
  - Enumerate Infrastructure and Application Admin Interfaces
  - Identify hidden administrator interfaces and functionality.
  - Tools
    - OWASP ZAP - Forced Browse
    - THC-HYDRA
    - netsparker
  - OWASP Top 10
    - A1
    - A4
  - CWE
    - CWE-284
    - CWE-419
- **WSTG-CONF-06**
  - Test HTTP Methods
  - Enumerate supported HTTP methods. Test for access control bypass. Test HTTP method overriding techniques.
  - Tools
    - Ncat
    - cURL
    - Nmap http-methods NSE script
  - OWASP Top 10
    - A5
  - CWE
    - CWE-650
    - CWE-749
- **WSTG-CONF-07**
  - Test HTTP Strict Transport Security
  - Review the HSTS header and its validity.
  - Tools
    - Burp Proxy
    - ZAP
    - curl
  - OWASP Top 10
    - A5
  - CWE
    - CWE-523

Client-Side Testing

- **WSTG-CLNT-01**
  - Testing for DOM-Based Cross Site Scripting
  - Identify DOM sinks. Build payloads that pertain to every sink type.
  - Tools
    - Burp Proxy
    - DOMinator
  - Testing for Self DOM Based Cross Site Scripting
  - OWASP Top 10
    - A3
  - CWE
    - CWE-79
- **WSTG-CLNT-02**
  - Testing for JavaScript Execution
  - Identify sinks and possible JavaScript injection points.
  - Tools
    - Burp Proxy
    - ZAP
  - OWASP Top 10
    - A3
  - CWE
    - CWE-79
- **WSTG-CLNT-03**
  - Testing for HTML Injection
  - Identify HTML injection points and assess the severity of the injected content.
  - Tools
    - Burp Proxy
    - ZAP
  - OWASP Top 10
    - A3
  - CWE
    - CWE-80
- **WSTG-CLNT-04**
  - Testing for Client-side URL Redirect
  - Identify injection points that handle URLs or paths.
  - Tools
    - Burp Proxy
    - ZAP
  - OWASP Top 10
    - A4
  - CWE
    - CWE-601
- **WSTG-CLNT-05**
  - Testing for CSS Injection
  - Identify CSS injection points.
  - Tools
    - Burp Proxy
    - ZAP
  - OWASP Top 10
    - A3
  - CWE
    - CWE-20
- **WSTG-CLNT-06**
  - Testing for Client-side Resource Manipulation
  - Identify sinks with weak input validation.
  - Tools
    - Burp Proxy
    - ZAP
  - OWASP Top 10
    - A3
  - CWE
    - CWE-20
- **WSTG-CLNT-07**
  - Testing Cross Origin Resource Sharing
  - Ensure that the CORS configuration is secure or harmless.
  - Tools
    - Burp Proxy
    - ZAP
  - OWASP Top 10
    - A5
  - CWE
    - CWE-942
- **WSTG-CLNT-14**
  - Testing for Reverse Tabnabbing
  - An Attack which can be used to redirect users to phishing pages.
  - OWASP Top 10
    - A3
  - CWE
    - CWE - 1022
- **WSTG-CLNT-13**
  - Testing for Cross Site Script Inclusion
  - Locate sensitive data across the system. Assess the leakage of sensitive data through various techniques
  - OWASP Top 10
    - A3
  - CWE
    - CWE - 79
- **WSTG-CLNT-12**
  - Testing Browser Storage
  - Determine whether the website is storing sensitive data in client-side storage.
  - OWASP Top 10
    - A1
    - A4
  - CWE
    - CWE-312
    - CWE-313
    - CWE-315
    - CWE-922
- **WSTG-CLNT-11**
  - Testing Web Messaging
  - Assess the security of the messages origin.
  - Tools
    - Burp Proxy
    - ZAP
  - OWASP Top 10
    - A5
  - CWE
    - CWE-1020
- **WSTG-CLNT-10**
  - Testing WebSockets
  - Assess its implementation by using the same tests on normal HTTP channels.
  - Tools
    - ZAP
  - OWASP Top 10
    - A2
    - A3
  - CWE
    - CWE-319
    - CWE-1347
- **WSTG-CLNT-09**
  - Testing for Clickjacking
  - Assess how strict the security measures are and if they are bypassable.
  - Tools
    - Burp Proxy
    - ClickjackingTool
  - OWASP Top 10
    - A5
  - CWE
    - CWE - 1021
- **WSTG-CLNT-08**
  - Testing for Cross Site Flashing
  - Decompile and analyze the application's code. Assess sinks inputs and unsafe method usages.
  - Tools
    - OWASP SWFIntruder
    - Decompiler – Flare
    - Disassembler – Flasm
    - Swfmill – Convert Swf to XML and vice versa
  - OWASP Top 10
    - A3
  - CWE
    - CWE - 79

Authorization Testing

- **WSTG-ATHZ-01**
  - Testing Directory Traversal File Include
  - Identify injection points that pertain to path traversal.Assess bypassing techniques and identify the extent of path traversal.
  - Tools
    - DotDotPwn
    - Path Traversal Fuz
    - OWASP ZAP
    - Burp Suite
    - Encoding/Decoding tools
    - String searcher "grep"
    - DirBuster
  - OWASP Top 10
    - A1
  - CWE
    - CWE-22
    - CWE-23
    - CWE-35
    - CWE-829
- **WSTG-ATHZ-02**
  - Testing for Bypassing Authorization Schema
  - Assess if horizontal or vertical access is possible.
  - Tools
    - OWASP Zed Attack Proxy (ZAP)
      - ZAP add-on: Access Control Testing
    - Port Swigger Burp Suite
      - Burp extension: AuthMatrix
      - Burp extension: Autorize
  - OWASP Top 10
    - A1
  - CWE
    - CWE-285
    - CWE-732
    - CWE-862
    - CWE-863
- **WSTG-ATHZ-03**
  - Testing for Privilege Escalation
  - Identify injection points related to privilege manipulation. Fuzz or otherwise attempt to bypass security measures.
  - Tools
    - OWASP Zed Attack Proxy (ZAP)
  - OWASP Top 10
    - A1
  - CWE
    - CWE-269
    - CWE-639
- **WSTG-ATHZ-04**
  - Testing for Insecure Direct Object References
  - Identify points where object references may occur. Assess the access control measures and if they're vulnerable to IDOR.
  - Tools
    - Burp Proxy (Autorize)
    - ZAP
  - OWASP Top 10
    - A1
  - CWE
    - CWE-639
- **WSTG-ATHZ-NA**
  - Testing for OAuth Client Weaknesses
  - Identify weaknesses in the OAuth client.
  - Tools
    - BurpSuite
    - EsPReSSO
    - OWASP ZAP
  - OWASP Top 10
    - A1
  - CWE-NA
- **WSTG-ATHZ-NA**
  - Testing for OAuth Authorization Server Weaknesses
  - Identify weaknesses in the Authorization Server.
  - Tools
    - BurpSuite
    - EsPReSSO
    - OWASP ZAP
  - OWASP Top 10
    - A1
  - CWE-NA
- **WSTG-ATHZ-05**
  - Testing for OAuth Weaknesses
  - Determine if OAuth2 implementation is vulnerable or using a deprecated or custom implementation.
  - Tools
    - BurpSuite
    - EsPReSSO
    - OWASP ZAP
  - OWASP Top 10
    - A1
  - CWE
    - CWE-290
    - CWE-345
    - CWE-798

Input Validation Testing

- **WSTG-INPV-11**
  - Testing for Code Injection
  - Identify injection points where you can inject code into the application.
  - Tools
    - Burp Proxy
    - ZAP
    - Liffy
    - Panoptic
  - Testing for File Inclusion
    - Tools
      - kadimus
      - LFI Suite
  - OWASP Top 10
    - A3
  - CWE
    - CWE-22
    - CWE-94
    - CWE-95
    - CWE-98
    - CWE-829
- **WSTG-INPV-12**
  - Testing for Command Injection
  - Identify and assess the command injection points.
  - Tools
    - OWASP WebGoat
    - Commix
  - OWASP Top 10
    - A3
  - CWE
    - CWE-77
    - CWE-78
- **WSTG-INPV-13**
  - Testing for Format String Injection
  - Assess whether injecting format string conversion specifiers into user-controlled fields causes undesired behavior from the application.
  - OWASP Top 10
    - A3
  - CWE
    - CWE-134
- **WSTG-INPV-14**
  - Testing for Incubated Vulnerability
  - Identify injections that are stored and require a recall step to the stored injection.
  - Tools
    - XSS-proxy
    - OWASP Zed Attack Proxy (ZAP)
    - Burp Suite
    - Metasploit
  - OWASP Top 10
    - A3
  - CWE
    - CWE-79
    - CWE-434
    - CWE-1236
- **WSTG-INPV-15**
  - Testing for HTTP Splitting Smuggling
  - Assess if the application is vulnerable to splitting, identifying what possible attacks are achievable.
  - Tools
    - Burp Proxy
    - ZAP
    - netcat
  - OWASP Top 10
    - A3
    - A4
  - CWE
    - CWE-93
    - CWE-113
    - CWE-444
- **WSTG-INPV-16**
  - Testing for HTTP Incoming Requests
  - Monitor all incoming and outgoing HTTP requests to the Web Server to inspect any suspicious requests.
  - Tools
    - Fiddler
    - TCPProxy
    - Charles Web Debugging Proxy
    - WireShark
    - PowerEdit-Pcap
    - pcapteller
    - replayproxy
    - Ostinato
  - OWASP Top 10 - NA
  - CWE - NA
- **WSTG-INPV-17**
  - Testing for Host Header Injection
  - Assess if the Host header is being parsed dynamically in the application. Bypass security controls that rely on the header.
  - OWASP Top 10
    - A4
  - CWE
    - CWE-74
    - CWE-116
- **WSTG-INPV-18**
  - Testing for Server-side Template Injection
  - Detect template injection vulnerability points. Identify the templating engine.
  - Tools
    - Tplmap
    - Backslash Powered Scanner Burp Suite extension
    - Template expression test strings/payloads list
  - OWASP Top 10
    - A4
  - CWE
    - CWE-1336
- **WSTG-INPV-19**
  - Testing for Server-Side Request Forgery
  - Identify SSRF injection points. Test if the injection points are exploitable.
  - OWASP Top 10
    - A10
  - CWE
    - CWE-918
- **WSTG-INPV-20**
  - Testing for Mass Assignment
  - Identify requests that modify objects. Assess if it is possible to modify fields never intended to be modified from outside
  - OWASP Top 10
    - A4
  - CWE
    - CWE-915
- **WSTG-INPV-01**
  - Testing for Reflected Cross Site Scripting
  - Identify variables that are reflected in responses. Assess the input they accept and the encoding that gets applied on return (if any).
  - Tools
    - PCE
    - Hackvertor
    - Burp Proxy
  - OWASP Top 10
    - A3
  - CWE
    - CWE-79
- **WSTG-INPV-02**
  - Testing for Stored Cross Site Scripting
  - Identify stored input that is reflected on the client-side. Assess the input they accept and the encoding that gets applied on return (if any).
  - Tools
    - PCE
    - Hackvertor
    - BeEF
    - XSS-Proxy
    - Burp-Proxy
  - OWASP Top 10
    - A3
  - CWE
    - CWE-79
- **WSTG-INPV-03**
  - Testing for HTTP Verb Tampering
  - Craft custom HTTP requests to test the other methods to bypass URL authentication and authorization.
  - Tools
    - netcat
  - OWASP Top 10 - NA
  - CWE - NA
- **WSTG-INPV-04**
  - Testing for HTTP Parameter Pollution
  - Identify the backend and the parsing method used. Assess injection points and try bypassing input filters using HPP.
  - Tools
    - OWASP ZAP Passive/Active Sc
  - OWASP Top 10
    - A3
  - CWE
    - CWE-235
- **WSTG-INPV-05**
  - Testing for SQL Injection
  - Identify SQL injection points. Assess the severity of the injection and the level of access that can be achieved through it.
  - Tools
    - Fuzzdb
    - sqlbftools
    - Bernardo Damele A. G.: sqlmap, automatic SQL injection tool
    - Muhaimin Dzulfakar: MySqloit, MySql Injection takeover tool
  - OWASP Top 10
    - A3
  - CWE
    - CWE-89
  - Testing for Oracle
    - Tools
      - Orascan
      - NGS SQuirreL
  - Testing for MySQL
    - Tools
      - Francois Larouche: Multiple DBMS SQL Injection tool
      - Reversing.org - sqlbftools
      - Bernardo Damele A. G.: sqlmap, automatic SQL injection tool
      - Muhaimin Dzulfakar: MySqloit, MySql Injection takeover tool
  - Testing for SQL Server
    - Tools
      - Bernardo Damele A. G.: sqlmap, automatic SQL injection tool
  - Testing PostgreSQL
    - Tools
      - SQLMap
  - Testing for MS Access
    - Tools
      - SQLMap
  - Testing for NoSQL Injection
    - Tools
      - NoSQLMap
  - Testing for ORM Injection
    - Tools
      - SQLMap
  - Testing for Client-side
    - Tools
      - SQLMap
- **WSTG-INPV-06**
  - Testing for LDAP Injection
  - Identify LDAP injection points. Assess the severity of the injection.
  - Tools
    - Softerra LDAP Browser
  - OWASP Top 10
    - A3
  - CWE
    - CWE-90
- **WSTG-INPV-07**
  - Testing for XML Injection
  - Identify XML injection points. Assess the types of exploits that can be attained and their severities.
  - Tools
    - XML Injection Fuzz Strings (from wfuzz tool)
  - OWASP Top 10
    - A5
  - CWE
    - CWE-91
    - CWE-611
    - CWE-652
- **WSTG-INPV-08**
  - Testing for SSI Injection
  - Identify SSI injection points. Assess the severity of the injection.
  - Tools
    - Web Proxy Burp Suite
    - OWASP ZAP
    - String searcher: grep
  - OWASP Top 10
    - A3
  - CWE
    - CWE - 97
- **WSTG-INPV-09**
  - Testing for XPath Injection
  - Identify XPATH injection points.
  - Tools
    - Burp Proxy
    - ZAP
  - OWASP Top 10
    - A3
  - CWE
    - CWE-91
    - CWE-643
- **WSTG-INPV-10**
  - Testing for IMAP SMTP Injection
  - Identify IMAP/SMTP injection points. Understand the data flow and deployment structure of the system. Assess the injection impacts.
  - Tools
    - Burp Proxy
    - ZAP
  - OWASP Top 10
    - A3
  - CWE
    - CWE - 147

Identity Management Testing

- **WSTG-IDNT-04**
  - Testing for Account Enumeration and Guessable User Account
  - Review processes that pertain to user identification (e.g. registration, login, etc.). Enumerate users where possible through response analysis.
  - Tools
    - OWASP Zed Attack Proxy (ZAP)
    - curl
    - PERL
  - OWASP Top 10
    - A7
  - CWE
    - CWE-204
- **WSTG-IDNT-05**
  - Testing for Weak or Unenforced Username Policy
  - Determine whether a consistent account name structure renders the application vulnerable to account enumeration.
  - Tools
    - Browser
    - Burp Proxy
    - ZAP
  - OWASP Top 10
    - A7
  - CWE
    - CWE-204
- **WSTG-IDNT-01**
  - Test Role Definitions
  - Identify and document roles used by the application.Attempt to switch, change, or access another role.
  - Tools
    - Burp's Autorize extension
    - ZAPs Access Control Testing add-on
  - OWASP Top 10
    - A4
  - CWE
    - CWE-266
    - CWE-269
- **WSTG-IDNT-02**
  - Test User Registration Process
  - Verify that the identity requirements for user registration are aligned with business and security requirements. Validate the registration process.
  - Tools
    - HTTP proxy tools
  - OWASP Top 10
    - A4
  - CWE
    - CWE-419
- **WSTG-IDNT-03**
  - Test Account Provisioning Process
  - Verify which accounts may provision other accounts and of what type.
    - Burp Proxy
    - ZAP
    - HTTP proxy tools
  - OWASP Top 10
    - A4
  - CWE
    - CWE-269
    - CWE-280

Testing for Error Handling

- **WSTG-ERRH-01**
  - Testing for Improper Error Handling
  - Identify existing error output. Analyze the different output returned.
  - Tools
    - Burp Proxy, ZAP
  - OWASP Top 10
    - A5
  - CWE
    - CWE-209
    - CWE-210
    - CWE-431
    - CWE-497
    - CWE-544
    - CWE-550
    - CWE-728
- **WSTG-ERRH-02**
  - Testing for Stack Traces
  - Analyze the different output returned.
  - Tools
    - Burp Proxy
    - ZAP
  - OWASP Top 10 - NA
  - CWE - NA

Testing for Weak Cryptography

- **WSTG-CRYP-03**
  - Testing for Sensitive Information Sent via Unencrypted Channels
  - Identify sensitive information transmitted through the various channels. Assess the privacy and security of the channels used.
  - Tools
    - curl
    - grep
    - Wireshark
    - TCPDUMP
  - OWASP Top 10
    - A2
  - CWE
    - CWE-311
    - CWE-319
    - CWE-523
- **WSTG-CRYP-04**
  - Testing for Weak Encryption
  - Provide a guideline for the identification weak encryption or hashing uses and implementations.
  - Tools
    - Vulnerability scanners
      - Nessus
      - NMAP (scripts)
    - static code analysis tool
      - Fortify
      - klocwork
  - OWASP Top 10
    - A2
  - CWE
    - CWE-261
    - CWE-320
    - CWE-321
    - CWE-322
    - CWE-323
    - CWE-324
    - CWE-325
    - CWE-326
    - CWE-327
    - CWE-328
    - CWE-329
    - CWE-330
    - CWE-331
    - CWE-335
    - CWE-336
    - CWE-337
    - CWE-338
    - CWE-340
    - CWE-347
    - CWE-354
    - CWE-759
    - CWE-760
    - CWE-780
    - CWE-798
    - CWE-916
- **WSTG-CRYP-01**
  - Testing for Weak Transport Layer Security
  - Review the digital certificate's cryptographic strength and validity. Ensure that the TLS security is not bypassable and is properly implemented across the application.
  - Tools
    - Nmap (various scripts)
    - OWASP O-Saft
    - sslscan
    - sslyze
    - SSL Labs
    - testssl.sh
  - OWASP Top 10
    - A2
    - A7
  - CWE
    - CWE-295
    - CWE-296
    - CWE-297
    - CWE-298
    - CWE-319
    - CWE-326
    - CWE-327
    - CWE-310
    - CWE-757
- **WSTG-CRYP-02**
  - Testing for Padding Oracle
  - Identify encrypted messages that rely on padding. Attempt to break the padding of the encrypted messages and analyze the returned error messages for further analysis.
  - Tools
    - Bletchley
    - PadBuster
    - Padding Oracle Exploitation Tool (POET)
    - Poracle
    - python-paddingoracle
  - OWASP Top 10
    - A2
  - CWE
    - CWE-326
    - CWE-649

Business Logic Testing

- **WSTG-BUSL-06**
  - Testing for the Circumvention of Work Flows
  - Review the project documentation for methods to skip or go through steps in the application process in a different order from the intended business logic flow.
  - Tools
    - Burp Proxy
    - ZAP
  - OWASP Top 10
    - A4
  - CWE
    - CWE-841
- **WSTG-BUSL-07**
  - Test Defenses Against Application Misuse
  - Understand the defenses in place and verify if they are enough to protect the system against bypassing techniques.
  - Tools
    - Burp Proxy
    - ZAP
  - OWASP Top 10
    - A4
  - CWE
    - CWE-693
- **WSTG-BUSL-08**
  - Test Upload of Unexpected File Types
  - Verify that file batch uploads are secure and do not allow any bypass against the set security measures.
  - Tools
    - Burp Proxy
    - ZAP
  - OWASP Top 10
    - A4
  - CWE
    - CWE-434
    - CWE-602
- **WSTG-BUSL-09**
  - Test Upload of Malicious Files
  - Review the project documentation to identify what file types are considered acceptable, and what types would be considered dangerous or malicious.If documentation is not available then consider what would be appropriate based on the purpose of the application.
  - Tools
    - Metasploit's payload generation functionality
    - Intercepting proxy
  - OWASP Top 10
    - A4
  - CWE
    - CWE-434
- **WSTG-BUSL-10**
  - Test Payment Functionality
  - Determine whether the business logic for the e-commerce functionality is robust.
  - Tools
    - Burp Proxy
    - ZAP
  - OWASP Top 10
    - A4
  - CWE
    - CWE-472
    - CWE-602
    - CWE-807
- **WSTG-BUSL-01**
  - Test Business Logic Data Validation
  - Validate that all checks are occurring on the back end and can't be bypassed.
  - Tools
    - ZAP
    - Burp Suite
  - OWASP Top 10
    - A4
  - CWE
    - CWE-840
- **WSTG-BUSL-02**
  - Test Ability to Forge Requests
  - Review the project documentation looking for guessable, predictable, or hidden functionality of fields.
  - Tools
    - ZAP
    - Burp Suite
  - OWASP Top 10
    - A4
  - CWE
    - CWE-840
- **WSTG-BUSL-03**
  - Test Integrity Checks
  - Determine what type of data is logically acceptable by the component and what types the system should guard against.
  - Tools
    - Burp Proxy
    - ZAP
  - OWASP Top 10
    - A4
  - CWE
    - CWE-840
    - CWE-472
- **WSTG-BUSL-04**
  - Test for Process Timing
  - Review the project documentation for system functionality that may be impacted by time.
  - Tools
    - Burp Proxy
    - ZAP
  - OWASP Top 10
    - A4
  - CWE
    - CWE-840
    - CWE-362
- **WSTG-BUSL-05**
  - Test Number of Times a Function Can Be Used Limits
  - Assess if there is a logical limit set on the functions and if it is properly validated.
  - Tools
    - Burp Proxy
    - ZAP
  - OWASP Top 10
    - A4
    - A7
  - CWE
    - CWE-799

API Testing

- **WSTG-APIT-01**
  - Testing GraphQL
  - Assess that a secure and production-ready configuration is deployed.
  - Tools
    - GraphQL Playground
    - GraphQL Voyager
    - sqlmap
    - InQL (Burp Extension)
    - GraphQL Raider (Burp Extension)
    - GraphQL (Add-on for OWASP ZAP)
  - OWASP Top 10
    - A3
  - CWE
    - CWE - 1347