EC-Council Licensed Penetration Tester

Methodology: Web Application Penetration Testing

Penetration Tester:			
Organization:			
Date:		**Location:**	

Test 1.1: Manually browse the target website

Target Organization	
URL	
Fingerprinting the Web Application Environment	1. 2. 3. 4. 5.
Targeted Website	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 1.2: Check the HTTP and HTML processing by the browser

Target Organization	
URL	
Analyzed HTTP and HTTPS Request Headers	1. 2. 3. 4. 5.
HTML Source Code	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 1.3: Perform web spidering

Target Organization	
URL	
Generated Site map by Using Spidering Tools	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 1.4: Perform search engine reconnaissance

Target Organization	
URL	
Techniques to Query Search Engines	
Information Collected	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 1.5: Perform server discovery

Target Organization		
URL		
Active Servers on the Internet		
Information Gathered from		
Whois Lookup	DNS Interrogation	Port Scanning
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 1.6: Perform banner grabbing to identify the target server

Target Organization	
URL	
Identified Make, Model, and Version of the Web Server Software	
Vulnerability Databases Used to Attack the Web Server and Applications	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 1.7: Perform service discovery

Target Organization	
URL	
Target Web Server	
Common Ports Used by Web Servers for Different Services	1. 2. 3. 4. 5.
Identified Services that Acts as Exploit Paths for Web Application Testing	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 1.8: Identify server-side technologies

Target Organization	
URL	
HTTP Headers and HTML Source Code	
Identified Server-Side Technologies	
Identification Information Gathered by Examining URLs and Error Page Messages	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 1.9: Identify server-side functionality

Target Organization	
URL	
Determined Internal Structure and Functionality of Web Applications	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 1.10: Investigate the output from HEAD and OPTIONS HTTP requests

Target Organization	
URL	
Output from HEAD and OPTIONS HTTP Requests	
Web Server Software Version	
Scripting Environment or Operating System in Use	
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____

Results Analysis:

____

____

____

____

____

____

Test 1.11: Investigate the format and wording of 404/other error pages

Target Organization	
URL	
Format and Wording of 404/Other Error Pages	
Software Versions of the Scripting Language in Use	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 1.12: Test for the recognized file types/extensions/directories

Target Organization	
URL	
Common File Extensions Requested	1. 2. 3.
Test Results for the Recognized File Types/Extensions /Directories	1. 2. 3. 4. 5.
Unusual Output or Error Codes	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 1.13: Examine source of the available pages

Target Organization	
URL	
Examined Source of the Available Pages	
Information about Application Environment	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 1.14: Manipulate inputs in order to elicit a scripting error

Target Organization	
URL	
Wildcard Strings or Long Strings Used to Manipulate User Inputs	
Scripting Error Generated with Input Manipulation	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 1.15: Test for hidden fields (Discover Hidden Content)

Target Organization	
URL	
Test Results for Hidden Fields	
Sensitive Data Collected from Hidden Fields	
Test Results for Input Parameters Manipulated to Exploit Logical Flow of Web Applications	1. 2. 3.
Non-Malicious Queries Sent to Manipulate Input Variables	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 1.16: Test for discover default content

Target Organization	
URL	
Sensitive Information Gathered from Default Content and Sample Scripts	1. 2. 3. 4. 5.
SQL Queries Used to Access Exploitable Content and Scripts in the Client's Web Server	1. 2. 3.
Vulnerabilities Detected in Default Content And Scripts	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 1.17: Test for directory traversal

Target Organization		
URL		
Accessed Restricted Directories		
Arbitrary Content Sent To File Directories		
Overwritten/ Exploited Source Code and Sensitive Data in the Server		
Non-Malicious Scripts Sent to File APIs		
Request Parameters Contain File Types or Directory Names that are Vulnerable	□ YES	□ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 1.18: Test for debug parameters

Target Organization		
URL		
Check for Hidden Debug Parameters in Application Pages	□ YES	□ NO
Test Results for Anomalies in Application's Responses with Parameters that Disrupt Application Processing	1. ____ 2. ____ 3. ____ 4. ____ 5. ____	
Tested to Send Non-Malicious Scripts to Overwrite or Manipulate Code and Debug Parameters	□ YES	□ NO
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 2.1: Test for default credentials

Target Organization	
URL	
Located Overtly Accessible Web Servers with Administrative Interfaces that Run on Different Ports	1. 2. 3. 4.

Default Credentials of Web Servers and Network Devices	
User Names	Passwords
1.	1.
2.	2.
3.	3.
4.	4.
5.	5.

Password Cracking Techniques	1. 2. 3. 4. 5.	
Application Mapping Techniques Used		
Checked and Exploited Administrative Interfaces that are Vulnerable	☐ YES	☐ NO
Performed Port Scanning of the Web Server	☐ YES	☐ NO
Found Administrative Interfaces Running Applications On Different Ports And Targets	1. 2. 3.	

Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 2.2: Test for dangerous HTTP methods

Target Organization		
URL		
List of Http Request or Dangerous Http Methods that Can Be Exploited	1. 2. 3. 4. 5. 6. 7.	
Enabled Web-Based Distributed Authoring and Versioning (WebDAV) Methods	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 2.3: Test for proxy functionality

Target Organization		
URL		
Target Host		
Checked HTTP Requests that Maneuver Web Servers	☐ YES	☐ NO
Information Retrieved From the Servers	1. 2. 3.	
Common Port Numbers to which HTTP Requests Connect	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 2.4: Test for virtual hosting misconfiguration

Target Organization	
URL	
Common Configuration Errors	1. 2. 3. 4. 5.
HTTP Requests that Connect to the Root Directory	
Identified Results	1. 2. 3. 4. 5.
Default Content and Directory Listings	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

All Rights Reserved. Reproduction is Strictly Prohibited.

Results Analysis:

Test 2.5: Test for web server software bugs

Target Organization	
URL	
Host Web Server	
Vulnerabilities Found in the Host Web Server	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 2.6: Test for server-side include injection attack

Target Organization		
URL		
Execute Non-malicious Scripts of a Web Application	□ Yes	□ No
Applications Properly Validating User Inputs	□ True	□ False
Special Characters Used in Data Fields to Verify Results	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 3.1: Test the inner workings of a web application

Target Organization	
URL	
Javascript and Other Client-Side Code Used to Gather Information on Inner Workings of a Web Application	1. 2. 3. 4. 5.
Maximum Value of a Tinyint Field in Database Systems	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3.2: Test the database connectivity

Target Organization		
URL		
Database Used		
Target Application		
Checked Security Vulnerabilities, Insecure Connections Between Database and Web Applications	□ YES	□ NO
Test Results for Manipulated User Input Variables	1. 2. 3. 4. 5.	
Checked for Vulnerable Connection Strings	□ YES	□ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 3.3: Test the application code

Target Organization		
URL		
Test Results for Exception Handling		
Test for Login IDs and Passwords	□ YES	□ NO
Information Gathered by Testing the Application Code	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 3.4: Test the use of GET and POST in the web application

Target Organization	
URL	
Use of GET Web Application	
Use of POST Web Application	
Information Gathered	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3.5: Test for improper error handling

Target Organization	
URL	
Test Results for Improper Error Handling	1. 2. 3.
Vulnerabilities Identified from Error Messages	1. 2. 3.
Information gathered about application condition	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3.6: Identify functionality

Target Organization		
URL		
Target Application		
Examined the Core Functionality	□ YES	□ NO
List of Functions it is Designed to Perform	1. 2. 3.	
Key Security Mechanisms in an Application	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 3.7: Identify entry points for user input

Target Organization	
URL	
Determined All User Input Fields	1. 2. 3. 4. 5.
Identified HTTP Header Parameters that can be Processed as User Inputs	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 3.8: Test for parameter/form tampering

Target Organization	
URL	
Manipulated Parameters Exchanged Between Client and Server	
Exploited Vulnerabilities in Integrity and Logic Validation Mechanisms	
Manipulated URL Strings	
Sensitive Information Retrieved	1. ____ 2. ____ 3. ____
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 3.9: Test for URL manipulation

Target Organization		
URL		
Host Web Server		
Modified a URL: Access to a Host Web Server Successful	□ YES	□ NO
Added Different Values and Manipulated Different Parts of the Website	□ YES	□ NO
Test Results for modified URL Parameters of the Website	1. 2. 3. 4. 5.	
Tested Directories and File Extensions	□ YES	□ NO
Identified Information from the above Test	1. 2. 3. 4. 5.	
Tested Using Different Strings or Characters	□ YES	□ NO
Access to Unauthorized Parts of a Site Successful	□ YES	□ NO
Scripts Sent to the URL	1. 2. 3. 4. 5.	

All Rights Reserved. Reproduction is Strictly Prohibited.

Hidden Files and Other Information Revealed on the Host Server	1. 2. 3. 4. 5.	
Used Path Traversal or Directory Traversal Attacks	□ YES	□ NO
Manipulated URL of the Host Website	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 3.10: Test for hidden field manipulation attack

Target Organization	
URL	
Field Values Stored as Hidden Fields in HTML	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 3.11: Map the attack surface

Target Organization	
URL	
Map the Attack Surface	
Information	Attack
1.	1.
2.	2.
3.	3.
4.	4.
5.	5.
6.	6.
7.	7.
8.	8.
9.	9.
10.	10.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3.12: Test for known vulnerabilities

Target Organization		
URL		
Tested for Known Vulnerabilities in the Third-Party Software Used in the Web Applications	□ YES	□ NO
List of Vulnerabilities Detected	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 3.13: Perform denial-of-service attack

Target Organization		
URL		
Performed Denial-of-Service Attack Successful	□ YES	□ NO
Various Techniques Used for Performing DoS Attack	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 3.14: Check for insufficient transport layer protection

Target Organization		
URL		
Checked for Insufficient Transport Layer Protection	□ YES	□ NO
Checked for Underprivileged SSL setup	□ YES	□ NO
Phishing and MITM Attacks Successful	□ True	□ False
Information Gathered	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 3.15: Check for weak SSL ciphers

Target Organization		
URL		
Host Application		
Performed SSL Scans and SSL Tests	□ YES	□ NO
Common Flaws Detected in SSL Service	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 3.16: Check for insecure cryptographic storage

Target Organization		
URL		
Target Application		
Check for Insecure Cryptographic Storage	□ YES	□ NO
Information Gathered		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 3.17: Check for unvalidated redirects and forwards

Target Organization	
URL	
Host Web Environment	
Social Engineering Techniques Used	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 4.1: Test for bad data

Target Organization	
URL	
Target Application	
Test Results for Bad Data	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 4.2: Test transmission of data via the client

Target Organization		
URL		
Target Application		
Various Tests Performed for Transmission of Data via the Client	1. 2. 3. 4. 5.	
Identified Application's Logic Used for the Input Fields	1. 2. 3. 4. 5.	
Areas where Fields are Exploited	1. 2. 3. 4. 5.	
Client Applications Transmit Opaque Data	□ YES	□ NO
Test Results for Transmission of Data	1. 2. 3. 4. 5. 6.	

All Rights Reserved. Reproduction is Strictly Prohibited.

Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 4.3: Test client-side controls over user input

Target Organization		
URL		
Target Application		
Type of Client-Side Controls Used by Applications		
Arbitrary Requests Sent to the Server Successful	□ YES	□ NO
Target Server Response	1. 2. 3.	
Exploitable Inputs in the Validation of Client-Side Controls	1. 2. 3.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Test 4.4: Identify client-side scripting

Target Organization	
URL	
Target Application	
Technologies Used on the Client's Side	1. 2. 3. 4. 5.
Identified Client-side Scripting	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 4.5: Test thick-client components

Target Organization		
URL		
Java Applets Supported by the Client Application	□ True	□ False
Identified .class and .jar file types and applet tags Used in HTML Code		
.class File Types	.jar File Types	Applet Tags
Validation Process of Thick-client Components		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 4.6: Test ActiveX controls

Target Organization	
URL	
Identified HTML Parameters for the ActiveX Controls	
Vulnerable ActiveX Controls	
Methods Executed by the Control and Test Validation Process with the Server	
Information Gathered about the Client Controls	
Tools/Services Used	1. __________ 2. __________ 3. __________ 4. __________ 5. __________

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 4.7: Test shockwave flash objects

Target Organization		
URL		
Flash Object Functions Employed by the Browser	1. 2. 3.	
Data Transmitted to the Server can be Exploited and Modified	□ True	□ False
Test Results for Shockwave Flash Objects	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 4.8: Check for frame injection

Target Organization		
URL		
Host Applications Support Editing of Frames and Frameset Tags in HTML Pages	□ YES	□ NO
Frameset Code on the HTML Page		
Vulnerable Host Site Tampered with URL Parameters		
Forged Site that Controls Contents of the Host Site		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 4.9: Test with user protection via browser settings

Target Organization	
URL	
Browser Settings	
Test Results for User Protection via Browser Settings	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 5.1: Understand the mechanism

Target Organization	
URL	
Host Environment	
Common Authentication Mechanisms Implemented in the Host Environment	1. 2. 3. 4. 5.
Key Areas where Authentication Process is Executed	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Test 5.2: Test password quality

Target Organization		
URL		
Host Environment		
Password Quality Rules are Implemented and Executed on the Host Environment	□ YES	□ NO
Password Validation Techniques	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 5.3: Test for username enumeration

Target Organization	
URL	
Username Enumeration	
Valid Username	Corresponding Password
1.	1.
2.	2.
3.	3.
4.	4.
Test Results for Username Enumeration	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 5.4: Test resilience to password guessing

Target Organization	
URL	
Techniques Used to Gather Password List	1. 2. 3. 4. 5.
dictionary of all possible passwords	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 5.5: Test any account recovery function, and remember me function

Target Organization		
URL		
Password Changing Functionality within the Application		
vulnerabilities in Password Change Functionality	1. 2. 3. 4. 5.	
Password Recovery Techniques Used	1. 2. 3.	
Bypass Authentication Mechanisms Successful	□ YES	□ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 5.6: Perform password brute-forcing

Target Organization		
URL		
Cracking the log-in Passwords Successful	☐ YES	☐ NO

Password Brute-forcing	
Valid Username	Password
1.	1.
2.	2.
3.	3.
4.	4.

Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 5.7: Perform session ID prediction/brute-forcing

Target Organization	
URL	
Captured Valid Session ID Values	1. 2. 3. 4. 5.

Session ID Generation Process in an Application		
Structure of Session ID	Information to Create the ID	Encryption Algorithm Used

Technique Used to Generate and Test Different Values of Session ID		
Access to the Application Successful	☐ YES	☐ NO
Vulnerable Session Generation Mechanisms		
Tools/Services Used	1. 2. 3. 4. 5.	

All Rights Reserved. Reproduction is Strictly Prohibited.

Results Analysis:

Test 5.8: Perform authorization attack

Target Organization		
Target Application		
Modifying Input Fields to Manipulate the HTTP Requests		
Techniques Used for Parameter Tampering		
☐ Cookies		☐ Query String
☐ URL		☐ POST Data
☐ Hidden Tags		☐ HTTP Headers
Tools/Services Used	1. ________ 2. ________ 3. ________ 4. ________ 5. ________	

Results Analysis:

____

____

____

____

____

____

Test 5.9: Perform HTTP request tampering

Target Organization		
URL		
Query String Tampering		
Access to Protected Application Functionalities Successful	□ YES	□ NO
Test Results for HTTP Request Tampering	1. ____ 2. ____ 3. ____ 4. ____ 5. ____	
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 5.10: Perform authorization attack - Cookie parameter tampering

Target Organization	
URL	
Target Application	
Cookie Generation Mechanism	
Test Results for Authorization Attack - Cookie Parameter Tampering	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 6.1: Understand the mechanism

Target Organization		
URL		
Mechanism Used for Managing Sessions and State		
Application Uses Session Tokens to Handle Requests from Users	□ YES	□ NO
Other Methods Used to Handle Requests from Users	1. 2. 3. 4.	
Data Used To Re-identify the Users	1. 2. 3. 4.	
Session-dependent Page or Function	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Template WAPT/16 Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Results Analysis:

Test 6.2: Test tokens for meaning

Target Organization	
URL	
Guessed Token Issued to the Application	
Recorded Tokens Received from the Server	
Tokens Related to the Username	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 6.3: Session token prediction (Test tokens for predictability)

Target Organization	
URL	
Guessed Token Issued to the Application	
Determined Valid Session Tokens from Requests Sent to Session-dependent Page	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 6.4: Check for insecure transmission of tokens

Target Organization		
URL		
Session Tokens are Transmitted Over an HTTP Connection	□ YES	□ NO
Test Results for Insecure Transmission of Tokens	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 6.5: Check for disclosure of tokens in logs

Target Organization	
URL	
Target Application	
Instances where Session Tokens are Transmitted within the URL	
Valid Session Tokens Issued to Users	
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____

Results Analysis:

____

____

____

____

____

____

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 6.6: Check mapping of tokens to sessions

Target Organization		
URL		
Target Application		
Modified User-related Components of the Token		
Resulting Token Accepted by the Application Successfully	□ YES	□ NO
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____	

Results Analysis:

____

____

____

____

____

____

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Test 6.7: Test session termination

Target Organization		
URL		
Target Application		
Session Expiration Implemented on the Server	□ True	□ False
Logout Function Exists	□ True	□ False
Logout Function Invalidates the User's Session on the Server	□ True	□ False
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 6.8: Test for session fixation attack

Target Organization	
URL	
Target Website	
Techniques Used to "Fix" the Session ID Value	1. 2. 3.
Test Results for Session Fixation Attack	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 6.9: Test for session hijacking

Target Organization	
URL	
Target User	
Hijacked Session	
Test Results for Session Hijacking	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 6.10: Check for XSRF

Target Organization		
URL		
Target Application		
Method Used for Transmitting Session Tokens		
Key Functionality of the Application		
Application Uses AJAX	□ YES	□ NO
Instances for JSON Hijacking Vulnerabilities	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 6.11: Check cookie scope

Target Organization	
URL	
Target Application	
Results from the Cookie Scope Test Performed	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 6.12: Test cookie attacks

Target Organization		
URL		
Target Application		
Unauthorized Access to Accounts Successful	□ YES	□ NO
Results from the Cookie Attacks Test Performed	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Test 7.1: Understand the access control requirements

Target Organization		
URL		
Target Application		
Checked the Areas of Functionality and Data Resources	□ YES	□ NO
Targets for Privilege Escalation Attacks	1. 2. 3.	

Accounts with Different Vertical and Horizontal Privileges	
Accounts with Vertical Privileges	**Accounts with Horizontal Privileges**
1.	1.
2.	2.
3.	3.
4.	4.
5.	5.

Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 7.2: Testing with multiple accounts

Target Organization		
URL		
Is the Attempt to Use One Account to Access Data Belonging to the Other Account Successful?	□ YES	□ NO
Results for Test with Multiple Accounts		
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____	

Results Analysis:

____

____

____

____

____

____

Test 7.3: Testing with limited access

Target Organization	
URL	
Identifiers Associated with Other Users' Data	
Broken Access Controls Test	
Application Mapping that Uses a Low-Privileged Account	
URLs for Privileged Functions	
Results for Test with Limited Access	
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____

Results Analysis:

____

____

____

____

____

____

Test 7.4: Test for insecure access control methods

Target Organization	
URL	
Target Application	
Modified Parameters in Key Requests	1. __________ 2. __________ 3. __________
Application's Base Access Control Decisions	
Tools/Services Used	1. __________ 2. __________ 3. __________ 4. __________ 5. __________

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 7.5: Test segregation in shared infrastructures

Target Organization		
URL		
Hosting Environment		
Remote Access Facility Uses a Secure Protocol	□ YES	□ NO
Customers are Able to Access Files, Data, and Other Resources	□ YES	□ NO
Customers are Able to Gain Information within the Hosting Environment	□ Yes	□ No
Test Results for Segregation in Shared Infrastructures	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 7.6: Test segregation between asp-hosted applications

Target Organization		
URL		
Application Belongs to an ASP-host Service	□ YES	□ NO
Identify Shared Components	1. 2. 3. 4.	
Common Database Uses a Shared Environment	□ True	□ False
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 8.1: Test for LDAP injection

Target Organization		
URL		
Target Application		
Query Sent to the Server that Generates an Invalid Input		
Error Returned from LDAP Server		
Is the Application vulnerable to LDAP Code Injection?	□ YES	□ NO
Information Gathered	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 9.1: Test for XML structure

Target Organization	
URL	
Malformed XML Message Sent to the Server	
List of Parameters being Validated	
1.	7.
2.	8.
3.	9.
4.	10.
5.	11.
6.	12.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 9.2: Test for XML content-level

Target Organization		
URL		
Web Services		
Can the Web Services be by Escalated Privileges	□ YES	□ NO
Test Results for XML Content-level	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Test 9.3: Test for WS HTTP GET parameters/REST attacks

Target Organization	
URL	
Query String Test for HTTP GET	1. 2. 3. 4. 5.
Result of Test Query String	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 9.4: Test for suspicious SOAP attachments

Target Organization		
URL		
WSDL which Accepts Attachment		
Bypassing Web Services Authentication Mechanisms Successful	□ YES	□ NO
Tools/Services Used	1. ________ 2. ________ 3. ________ 4. ________ 5. ________	

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 9.5: Test for XPath injection attack

Target Organization	
URL	
Syntax of XPath	
Test Results for XPath Injection Attack	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Test 9.6: Test for WS replay

Target Organization	
URL	
Captured HTTP Traffic	
Determined Session ID Patterns	
Valid Session ID Used for the Replay Attack	
Determined Host Server	
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 10.1: Identify the key attack surface

Target Organization	
URL	
Target Application	
Results of Application Mapping	
Identified Key Attack Surface	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 10.2: Test for logic flaws

Target Organization	
URL	
Target Application	
Identified Logic Flow	
Test Results for Logic Flaws	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 10.3: Test multistage processes

Target Organization		
URL		
Sequence of Stages that can be Accessed via a Series of GET or POST Requests for Distinct URLs	1. 2. 3. 4. 5.	
Multistage Process that Involves Different Users Performing Operations on the Same Set of Data	1. 2. 3. 4. 5.	
Are Multistage Functions Accessed Out of Sequence?	□ YES	□ NO
Test Results for Multistage Processes	1. 2. 3. 4. 5.	
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Test 10.4: Test handling of incomplete input

Target Organization	
URL	
Target Application	
Application Response Behavior	
Test Results for Handling of Incomplete Input	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 10.5: Test trust boundaries

Target Organization	
URL	
Target Application	
Test Results for Trust Boundaries	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

All Rights Reserved. Reproduction is Strictly Prohibited.

Test 10.6: Test transaction logic

Target Organization	
URL	
Checked Application Algorithms for Adjustments Made	
Methods of Manipulating the Application's Behavior	1. 2. 3. 4. 5.
Test Results for Transaction Logic	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.