Unknown Title

OWASP Based Checklist 🌟🌟
500+ Test Cases 🚀🚀

▲

INFORMATION GATHERING

Open Source Reconnaissance

☐

Perform Google Dorks search

☐

Perform OSINT

Fingerprinting Web Server

☐

Find the type of Web Server

☐

Find the version details of the Web Server

Looking For Metafiles

☐

View the Robots.txt file

☐

View the Sitemap.xml file

☐

View the Humans.txt file

☐

View the Security.txt file

Enumerating Web Server's Applications

☐

Enumerating with Nmap

☐

Enumerating with Netcat

☐

Perform a DNS lookup

☐

Perform a Reverse DNS lookup

Review The Web Contents

☐

Inspect the page source for sensitive info

☐

Try to find Sensitive Javascript codes

☐

Try to find any keys

☐

Make sure the autocomplete is disabled

Identifying Application's Entry Points

☐

Identify what the methods used are?

☐

Identify where the methods used are?

☐

Identify the Injection point

Mapping Execution Paths

☐

Use Burp Suite

☐

Use Dirsearch

☐

Use Gobuster

Fingerprint Web Application Framework

☐

Use the Wappalyzer browser extension

☐

Use Whatweb

☐

View URL extensions

☐

View HTML source code

☐

View the cookie parameter

☐

View the HTTP headers

Map Application Architecture

☐

Map the overall site structure

▲

CONFIGURATION & DEPLOYMENT MANAGEMENT TESTING

▲

IDENTITY MANAGEMENT TESTING

▲

AUTHENTICATION TESTING

▲

AUTHORIZATION TESTING

▲

SESSION MANAGEMENT TESTING

▲

INPUT VALIDATION TESTING

▲

ERROR HANDLING TESTING

▲

WEAK CRYPTOGRAPHY TESTING

▲

BUSINESS LOGIC TESTING

▲

CLIENT SIDE TESTING

▲

OTHER COMMON ISSUES

Shaped by: Hariprasaanth R

Reach Me: LinkedIn Portfolio Github