Web Penetration Testing

Unk9vvN

May
2022

Introduction

0x01 Web Frameworks

01x01 Content Management System

-- Joomla

-- Drupal

-- WordPress

-- CakePHP

-- Microsoft IIS

-- SharePoint

-- DotNetNuke

01x02 MS Exchange

01x03 Web Access Outlook

01x04 Web Architectures

-- Hypertext Preprocessor (PHP)

-- Common Gateway Interface (CGI)

-- Java Server Pages (JSP)

-- Active Server Pages (ASP)

-- Asynchronous JavaScript and XML (AJAX)

-- Microsoft Silverlight

-- JavaScript Object Notation (JSON)

-- Java Applets, JavaScript and VBScript

01x05 Web App Technologies

01x06 Languages and Frameworks

-- Node.js Express

-- Ruby on Rail

-- Python Django and Flask

-- PHP Laravel

-- Java Spring

-- JavaScript Angular and React

01x07 Web Design Patterns

01x08 Browser Extensions

-- ActiveX Controls

-- Silverlight

-- Flash Objects

-- Java Applets

01x09 Data Formats

-- JSON

-- CSV

-- XML

01x10 REST and SOAP

01x11 Java and Struts

01x12 Encoding Schemes

-- URL Encoding

-- HTML Encoding

-- UTF-8 Encoding

-- Unicode Encoding

-- Base64 Encoding

-- Hex Encoding

-- XOR

Information Gathering

0x01 Reconnaissance

- 01x01 Search Engine Discovery
- 01x02 Fingerprint Web Server
- 01x03 Review Webserver Metafiles
- 01x04 Enumerate Applications
- 01x05 Review Webpage Content
- 01x06 Identify Application Entry Points
- 01x07 Map Execution Paths
- 01x08 Fingerprint Web Application Framework
- 01x09 Map Application Architecture

0x02 Open Source Intelligence

- 02x01 People Investigation
  - -- Email Addresses
  - -- Usernames
  - -- Image Search
  - -- Phone Numbers
  - -- People Search Engines
  - -- Social Media
- 02x02 Infrastructure
  - -- Websites
  - -- Whois
  - -- DNS
  - -- IP Address

Web Vulnerabilities (One)

0x01 Misconfiguration
- 01x01 Network Configuration
- 01x02 App Platform Configuration
- 01x03 File Extensions Handling
- 01x04 Review Old Backup
- 01x05 Enumerate Admin Interfaces
- 01x06 HTTP Methods
- 01x07 HTTP Strict Transport Security
- 01x08 RIA Cross Domain Policy
- 01x09 File Permission
- 01x10 Subdomain Takeover
- 01x11 Cloud Storage
- 01x12 Content Security Policy

0x02 Identity Management
- 02x01 Role Definitions
- 02x02 User Registration
- 02x03 Account Provisioning
- 02x04 Account Enumeration
- 02x05 Weak Username Policy

0x03 Broken Authentication
- 03x01 Credentials Encrypted Channel
- 03x02 Default Credentials
- 03x03 Weak Lock Out Mechanism
- 03x04 Bypassing Authentication Schema
- 03x05 Vulnerable Remember Password
- 03x06 Browser Cache Weaknesses
- 03x07 Weak Password Policy
- 03x08 Weak Security Question Answer
- 03x09 Weak Password Reset Functionalities
- 03x10 Weaker Authentication in Alternative Channel

0x04 Broken Authorization
- 04x01 Directory Traversal File Include
- 04x02 Bypassing Authorization Schema
- 04x03 Privilege Escalation
- 04x04 Insecure Direct Object References
- 04x05 OAuth Weaknesses
- -- OAuth Authorization Server
- -- OAuth Client

0x05 Session Management
- 05x01 Session Management Schema
- 05x02 Cookies Attributes
- 05x03 Session Fixation
- 05x04 Exposed Session Variables
- 05x05 Cross Site Request Forgery
- 05x06 Logout Functionality

Web Vulnerabilities (Two)

05x07 Session Timeout
05x08 Session Puzzling
05x09 Session Hijacking
05x10 JSON Web Tokens
0x06 Input Validation
06x01 Reflected Cross Site Scripting
06x02 Stored Cross Site Scripting
-- Event Handlers
-- Consuming Tags
-- File Upload Attacks
-- Restricted Characters
-- Frameworks
-- Protocols
-- Other Useful Attributes
-- Special Tags
-- Encoding
-- Obfuscation
-- Dangling Markup
-- WAF Bypass Global Objects
-- Content Types
-- Response Content Types
-- Prototype Pollution
-- Classic Vectors (XSS Crypt)
-- XSS Blind
-- BeEF Framework
06x03 HTTP Verb Tampering
06x04 HTTP Parameter Pollution
06x05 SQL Injection
-- Oracle
-- MySQL
-- SQL Server
-- PostgreSQL
-- MS Access
-- NoSQL Injection
-- ORM Injection
-- Client-side
-- Out of Band
-- Second Order
-- Through Crypto
-- User Defined Functions
-- DNS Exfiltration
-- GBK Bypass
-- Truncation Bypass
-- SQLMap Tampers
06x06 LDAP Injection

Web Vulnerabilities (Three)

06x07 XML Injection
06x08 SSI Injection
06x09 XPath Injection
06x10 IMAP SMTP Injection
06x11 Code Injection
-- File Inclusion
06x12 Command Injection
06x13 Insecure Deserialization
06x14 Format String Injection
06x15 Incubated Vulnerability
06x16 HTTP Splitting Smuggling
06x17 HTTP Incoming Requests
06x18 Host Header Injection
06x19 Server Side Template Injection
06x20 Server Side Request Forgery
-- Blind SSRF
06x21 Mass Assignment
06x22 Regular Expression DoS
06x23 PHP Type Juggling

0x07 **Error Handling**

07x01 Improper Error Handling
07x02 Stack Traces

0x08 **Weak Cryptography**

08x01 Weak Transport Layer Security
08x02 Padding Oracle Attack
08x03 Information Unencrypted Channel
08x04 Weak Encryption
-- Hash Length Extension
-- Known Plaintext Attack
-- Cipher Block Chaining

0x09 **Business Logic**

09x01 Logic Data Validation
09x02 Ability to Forge Requests
09x03 Integrity Checks
09x04 Process Timing
09x05 Race Conditions
09x06 Circumvention of Work Flows
09x07 Defenses Against Application Misuse
09x08 Upload of Unexpected File Types
09x09 Upload of Malicious Files
09x10 Payment Functionality

0x10 **Client Side**

10x01 DOM-Based Cross Site Scripting
-- Self DOM Based
10x02 JavaScript Execution

Web Vulnerabilities (Four)

10x03 HTML Injection

10x04 Client Side URL Redirect

10x05 CSS Injection

10x06 Client Side Resource Manipulation

10x07 Cross Origin Resource Sharing

10x08 Client Side Template Injection

-- VueJS Reflected

-- AngularJS Sandbox Escapes Reflected

-- AngularJS Sandbox Escapes DOM

-- AngularJS CSP Bypasses

10x09 Cross Site Flashing

10x10 Clickjacking

10x11 WebSockets

10x12 Web Messaging

10x13 Browser Storage

10x14 Cross Site Script Inclusion

10x15 Reverse Tabnabbing

0x11 API Attacks

11x01 Broken Object Level Authorization

11x02 Broken Authentication

11x03 Excessive Data Exposure

11x04 Lack of Resources and Rate Limiting

11x05 Broken Function Level Authorization

11x06 Mass Assignment

11x07 Security Misconfiguration

11x08 Injection Attack

11x09 Improper Assets Management

11x10 Insufficient Logging and Monitoring

Unk9vvN

Phone:
026 368 06249

Email:
info@unk9vvn.com