Advanced Filter Evasion and Web Application Firewall Bypassing

Encoding and Filtering - understanding what kind of data encoding us being used and how it works is fundamental in ensuring that tests are performed as intended

- Data Encoding basics
  - Dissecting encoding types
    - URL Encoding
    - HTML Encoding
      - Document character encoding
      - Character references
    - Base (36|64) encoding
    - Unicode encoding
  - Multiple (De|En)codings
- Filtering basics
  - Regular Expressions
    - Metacharacters
    - Shorthand character classes
    - Non-printing characters
    - Unicode
  - Web Application Firewall
    - WAF Detection and Fingerprinting
  - Client-side Filters

Evasion Basic - advanced coverage of the most modern filter evasion techniques using different client side and server side languages. To have complete understanding of filters and encoding this section introduces the main Evasion Techniques that start from Base64 and lesser known URI obfuscation techniques and concludes with JavaScript and PHP Obfuscation techniques

- Base64 evasion
- URI Obfuscation techniques
  - URL shortening
  - URL Hostname obfuscation
- JavaScript Obfuscation Techniques
  - JavaScript Encoding
    - Non-alphanumeric
  - JavaScript Compressing
    - Minifying
    - Packing
- PHP Obfuscation Techniques
  - Basic Language Reference
    - Type Juggling
    - Numeric Data types
    - String Data types
    - Array Data types
    - Variable Variables
  - Non-alphanumeric Code
    - String generation

Cross-Site Scripting - advanced attack techniques and exotic XSS vectors, how to exploit any kind of XSS with the most advanced tools available

- Cross-Site Scripting
  - Reflected XSS
  - Persistent XSS
  - DOM XSS
  - Universal XSS
- XSS Attacks
  - Cookie Grabbing
    - Script Injection
    - Cookie Recording and Logging
    - Bypassing HTTPOnly flag
      - Cross-site Tracing(XST)
      - CVE: 2012-0053
      - BeEF's Tunnelling Proxy
  - Defacements
    - Virtual Defacement
    - Persistent Defacement
  - Phishing
  - Keylogging
    - Keylogging with Metasploit
    - Keylogging with BeEF
  - Network Attacks
    - IP detection
    - Subnet detection
    - Ping Sweeping
    - Port Scanning
      - Simple Port Scanner
      - HTML5 alternatives
  - Self-XSS
    - Browsers' security measures
      - Chromium based browser
      - Mozilla Firefox based browser
      - Internet Explorer
      - Safari
    - JavaScript console limitations
- Exotic XSS Vectors
  - Mutation-based XSS
    - mXSS Examples
    - mXSS Multiple Mutations

XSS Filter Evasion and WAF bypassing techniques - Starting from simple Blacklisting filters to different mechanisms to bypass common input sanitization techniques, browser filters and much more.

- Bypassing Blacklisting Filters
  - Injecting Script Code
    - Bypassing weak <script> tag banning
    - ModSecurity > Script tag based XSS
    - Beyond <script> tag - using HTML events
  - Keyword based filters
    - Character escaping
      - Unicode
      - Decimal, Octal, Hexadecimal
    - Constructor Strings

        - Execution Sinks
        - Pseudo-protocols
            - data
            - vbscript
- Bypassing Sanitization
    - String manipulations
        - Removing HTML Tags
        - Escaping Quotes
        - Escaping Parenthesis
- Bypassing Browser Filters
    - (Un)Filtered Scenarios
        - Injecting inside HTML Tag
        - Injecting inside HTML attributes
        - Injecting inside SCRIPT tag
        - Injecting inside event attributes
        - DOM Based
        - Other Scenarios

SQL Injection - Advanced Attack Techniques on different DBMS's

- SQL Injection
- Exploiting SQLi
    - Techniques Classification
    - Gathering Information from the environment
        - Identify the DBMS
            - Error Code Analysis > MySQL
            - Error Code Analysis > MSSQL
            - Error Code Analysis > Oracle
            - Banner Grabbing
            - Educated Guessing
            - String Concatenation
            - Numeric Functions
            - SQL Dialect
        - Enumerating the DBMS Content
            - MySQL
            - MSSQL
            - Oracle
            - Tables and Columns
            - Users and Privileges
- Advanced SQLi Exploitation
    - Out-of-Band Exploitation
        - Alternative OOB Channels
        - OOB via HTTP
            - Oracle URL_HTTP Package
            - Oracle HTTPURITYPE Package
        - OOB via DNS
            - DNS Exfiltration Flow
            - Provoking DNS requests
                - MySQL
                - MSSQL
                - Oracle
    - Exploiting Second-Order SQL Injection
        - First-order example
        - Security Considerations
        - Automation Considerations

SQLi Filter Evasion and WAF Bypassing - Advanced Attack Techniques on different DBMS's. Recognizing the presence of WAF's and filters and implement effective bypassing techniques.

- SQLi Filter Evasion and WAF Bypassing
  - DBMS gadgets
    - Functions
    - Constants and variables
    - System variables
    - Typecasting
  - Bypassing Keywords filters
    - Using comments
    - Case changing
    - Replaced keywords
    - Circumventing by Encoding
    - URL encode
    - Double URL encode
    - Characters encoding
    - Inline commnets
    - Allowed Whitespaces
  - Bypassing Functions Filters
  - Bypassing Regular Expression filters

Cross-Site Request Forgery - exploit Weak Anti-CSRF mechanisms concluding with Advanced Exploitation techniques

- XSRF
  - Vulnerable scenarios
- Attack Vectors
  - Force Browsing with GET
    - Example - change email address
  - Post Requests
    - Auto-submitting from > v1
    - Auto-submitting from > v2
- Exploiting Weak Anti-CSRF Measures
  - Using Post-only requests
  - Multi-Step Transactions
  - Checking Referer Header
  - Predictable Anti-CSRF token
  - Unverified Anti-CSRF token
  - Secret Cookies
- Advanced CSRF Exploitation
  - Bypassing CSRF defences with XSS
    - Bypassing Anti-CSRF Token
      - Request a valid form with a valid token
      - Extract the valid token from the source code
      - Forge the form with the stolen token

HTML5 - what are the most common security mechanisms developer use: these are critical to understand how to leverage even more sophisticated attacks. Analysis of UI rendering attacks and an overview of related new Attack Vectors introduced with HTML5

- HTML5

- Semantics
  - New attack vectors
    - Form Elements
    - Media Elements
    - Semantic/Structural Elements
    - Attributes
- Offline and Storage
  - Web Storage > Attack Scenario
    - Session Hijacking
  - Offline Web Application > Attack Scenatio
- Device Access
  - Geolocation > Attack Scenario
  - Fullscreen mode > Attack Scenario
    - Phishing
- Performance, Integrity and Connectivity
  - Attack Scenarios

• Exploiting HTML5
- CORS Attack Scenario
  - Universal Allow
    - Allow by wildcard value *
    - Allow by server-side
  - Weak Access Control
    - Check Origin Example
  - Intranet Scanning
    - JS-Recon
  - Remote Web Shell
    - The Shell of the Future
- Storage Attack Scenario
  - Web Storage
    - Session Hijacking
    - Cross-directory attacks
    - User Tracking and Confidential Data disclosure
  - IndexedDB
    - IndexedDB vs WebSQL Database
- Web Messaging Attack Scenarios
  - Web Messaging
    - DOM XSS
    - Origin Issue
- Web Sockets Attack Scenrios
  - Web Sockets
    - Data Validation
    - MiTM
    - Remore Shell
    - Network Reconnaissance
- Web Workers Attack Scenarios
  - WebWorkers
    - Broswer-Based Botnet
    - Distributed Password Cracking
    - DDoS Attacks

• HTML5 Security Measures
- Security Headers
  - X-XSS-Protection
  - X-Frame-Options
  - Strict-Transport-Security
  - X-Content-Type-Options
  - Content Security Policy

• UI Readressing: The x-Jacking Art
- ClickJacking
- LikeJacking
- StrokeJacking

- New Attack Vectors in HTML5
  - Drag-and-Drop
    - Text Field Injection
    - Content Extraction

XML Attacks - most modern related attacks such as XML Tag Injection, XXE, XEE, Path Injection. For each of them basic and advanced exploitation techniques are analysed

- XML Attacks
  - Entities block
    - XML Document with External DTD + Entities
- XML Tag Injection
  - Testing XML Injection
    - Single/Double Quotes
    - Ampersand
    - Angular parentheses
    - XSS with CDATA
- XML eXternal Entity
  - Taxonomy
    - External Entities: Private vs Publix
  - Resource Inclusion
  - Resource Inclusion - Improved
    - Invalid resource to extract
    - CDATA Escape using Parameter Entities
    - PHP://I/O Stream
  - Bypassing Access Control
  - Out-Of-Band Data Retrieval
    - OOB via HTTP
    - OOB via HTTP using XXEServe
- XML Entity Expansion
  - Recursive Entity Expansion
    - Billion Laugh Attack
  - Generic Entity Expansion
    - Quadratic Blowup Attack
  - Remote Entity Expansion
- XPath Injection
  - XPath 1.0 vs 2.0
    - New Operations and Expressions on Sequences
      - Functions on Strings
      - Function accessors
      - FOR Operator
      - Conditional Expression
      - Regular Expression
      - Assemble/Disassemble String
    - Data Types
  - Advanced XPath Exploitation
    - Blind Exploitation
      - Error Based Boolean Based
    - OOB Exploitaiton
      - HTTP Channel
      - DNS Channel