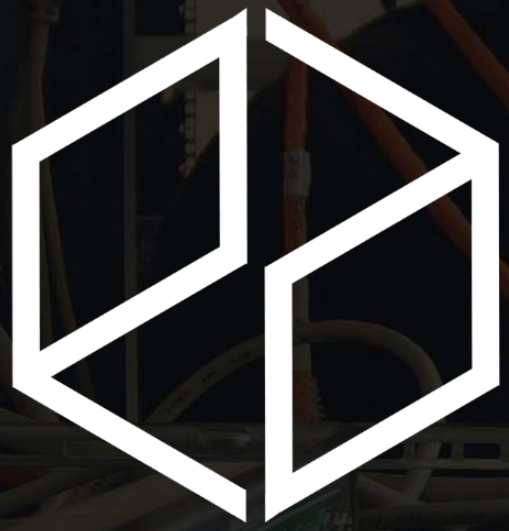
www.pandoralabs.net

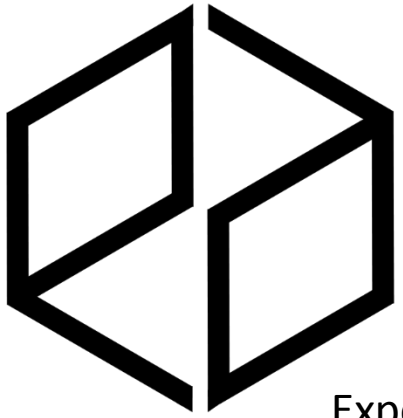


PANDORA
SECURITY LABS

Expert Advice. Experience Advantage.
Proactive Security Solutions Through Cutting-Edge Research.

Web App Testing: Pen-Testing Methodology

By @isaacsabas



PANDORA
SECURITY LABS

Expert Advice. Experience Advantage.
Proactive Security Solutions Through Cutting-Edge Research.
www.pandoralabs.net

We are a Security-as-a-Service company

Providing businesses with on-demand threat detection & intelligence capabilities to secure their IT infrastructure, 24x7.

We Make IT Secure

WEB APPLICATION TESTING

PENETRATION TESTING METHODOLOGY

OWASP Pen-Testing

Pen-Testers

- A structured approach to the testing activities
- A checklist to be followed

Clients

- A tool to understand web vulnerabilities and their impact
- A way to check the quality of the penetration tests they get

This aims to provide a pen-testing standard that creates a 'common ground' between the pen-testing industry and it’s clients.

This will raise the overall quality and understanding of this kind of activity and therefore the general level of security in our infrastructures.

Testing Model

The test is divided into 2 phases:

Passive mode: in the passive mode the tester tries to understand the application's logic and feature by observing the web app’s requests & responses.

Active mode: in this phase the tester begins to test using 6 distinct sub-phases of security assessment.

A. Passive Mode: Example

- Use an HTTP proxy to observe all the HTTP requests and responses.
- It's a tool can be used for observing all the HTTP requests and responses, through and from the web application.
  - OWASP ZAP (Zed Attack Proxy)
  - TamperData (Firefox Extension)
- At the end of this phase the tester should understand all the access points (gates) of the application (e.g. Header HTTP, parameters, cookies).

B. Active Mode

OWASP split the set of tests in 6:

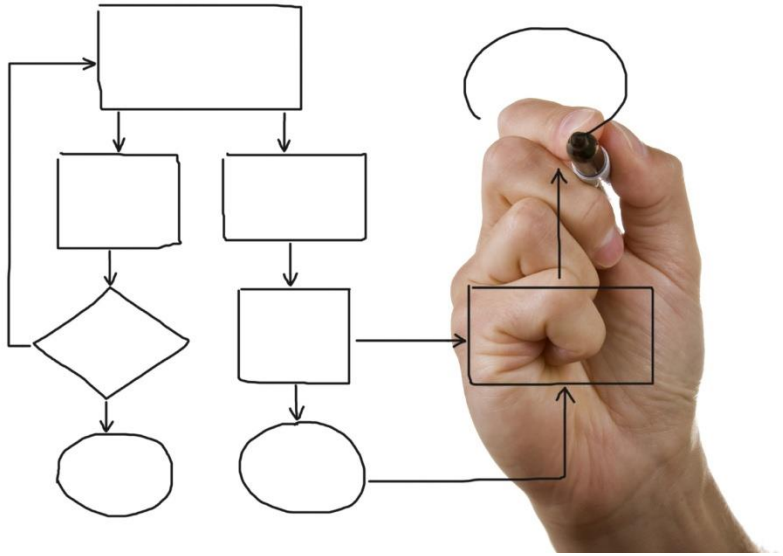
- Business logic testing
- Authentication Testing
- Session Management Testing
- Data Validation Testing
- Denial of Service Testing
- AJAX Testing

1. Business Logic Testing

In this phase, we look for flaws in the application business logic rather than in the technical implementation. Areas of testing include:

- Rules that express the business policy (such as channels, location, logistics, prices, and products)
- Workflows that are the ordered tasks of passing documents or data from one participant (a person or a software system) to another

- One of the most common results in this step of the analysis are flaws in the order of actions that a user has to follow.
- This step is the most difficult to perform with automated tools, as it requires the penetration tester to perfectly understand the business logic that is (or should be) implemented by the application

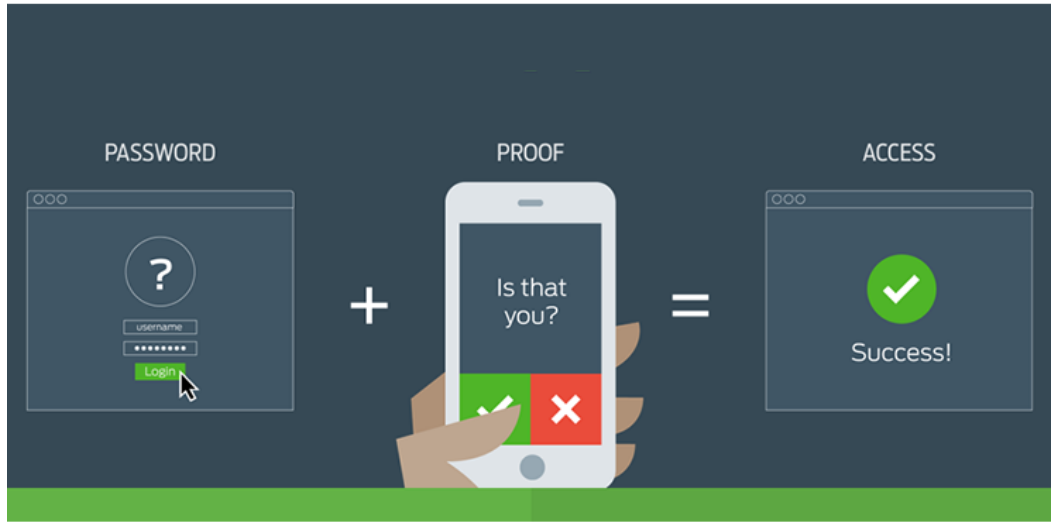


2. Authentication Testing

Testing the authentication scheme means understanding how the application checks for users' identities and using that information to circumvent that mechanism and access the application without having the proper credentials

Tests include the following areas:

- Default or Guessable Accounts
- Brute-force
- Bypassing Authentication
- Directory Traversal / File Include
- Vulnerable Password Reset/Forgot Password
- Logout and Browser Cache Management



3. Session Management Testing

Session management is a critical part of a security test, as every application has to deal with the fact that HTTP is by it's nature a stateless protocol. Session Management broadly covers all controls on a user from authentication to leaving the application.

Tests include the following areas:

- Analysis of the session management scheme
- Cookie and session token manipulation
- Exposed session variables
- Cross Site Request Forgery (CSRF)
- HTTP Exploiting

4. Data Validation Testing

In this phase we test that all input is properly sanitized before being processed by the application, in order to avoid several classes of attacks. This is the most common web application security weakness.

Cross site scripting (XSS)

- Test that the application filters JavaScript code that might be executed by the victim in order to steal his/her cookies

SQL Injection

- Test that the application properly filters SQL code embedded in the user input

Other attacks based of faulty input validation

- LDAP/XML/SMTP/OS injection
- Buffer overflows

5. Denial of Service Testing

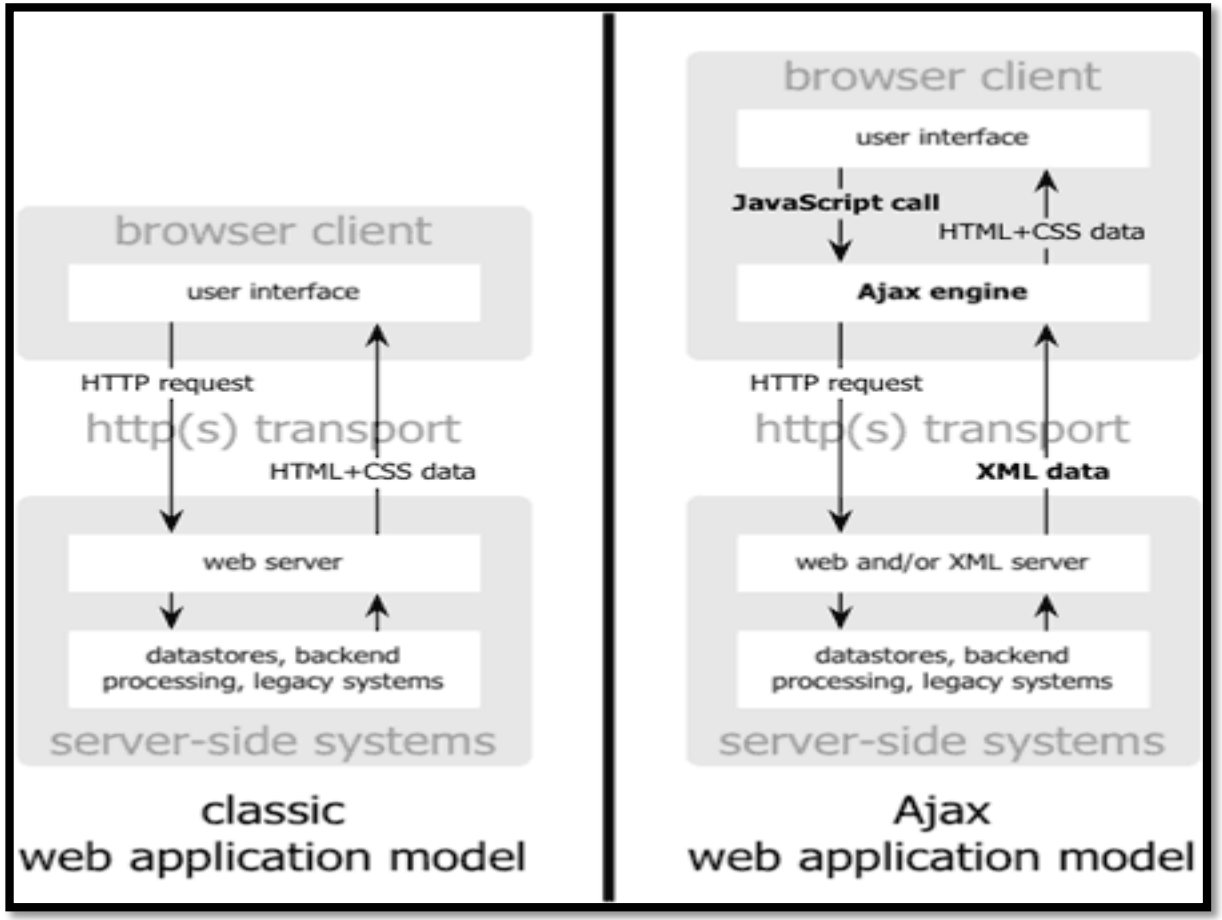
DoS are types of vulnerabilities within applications that can allow a malicious user to make certain functionality or sometimes the entire website unavailable. These problems are caused by bugs in the application, often resulting from malicious or unexpected user input.

- Locking Customer Accounts
- User Specified Object Allocation
- User Input as a Loop Counter
- Writing User Provided Data to Disk
- Failure to Release Resources
- Storing too Much Data in Session

Usually not performed in performed on production environments

6. AJAX Testing

- AJAX (Asynchronous JavaScript and XML) is a web development technique used to create more interactive web applications.
- Main security issues:
  - AJAX applications have a greater attack surface because a big share of the application logic is moved on the client side
  - AJAX programmers seldom keep an eye on what is executed by the client and what is executed by the server
  - Exposed internal functions of the application
  - Client access to third-party resources with no built-in security and encoding mechanisms
  - Failure to protect authentication information and sessions



AJAX Testing

While in traditional web applications it is very easy to enumerate the points of interaction between clients and servers, when testing AJAX pages things get a little bit more complicated, as server-side AJAX endpoints are not as easy or consistent to discover

To enumerate endpoints, two approaches must be combined:

- Look through HTML and Javascript (e.g: look for XmlHttpRequest objects)
- Use a proxy to monitor traffic
- Tools: OWASP Sprajax or Firebug add-on for Firefox
- Then you can test it as described before (SQL Injection, etc.)

TIME FOR

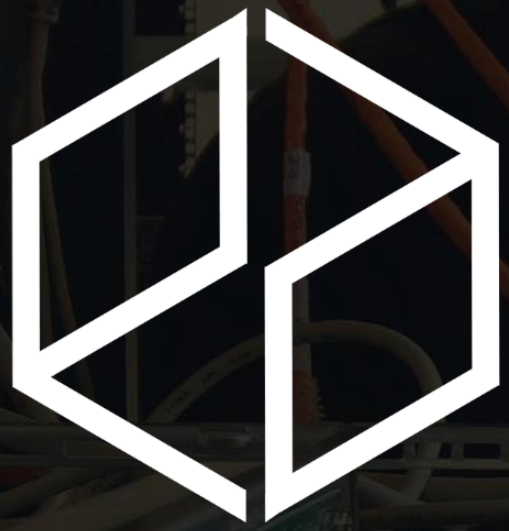
Q&A

WEB APP PEN-TESTING METHODOLOGY

WEB APPLICATION TESTING

PENETRATION TESTING METHODOLOGY

www.pandoralabs.net



PANDORA
SECURITY LABS

Expert Advice. Experience Advantage.
Proactive Security Solutions Through Cutting-Edge Research.

Web App Testing: Pen-Testing Methodology

By @isaacsabas