**I. Information Gathering**

IP: 10.0.1.60

\* Fingerprint Web Server

A screen shot of a computer program

Description automatically generated

Type of Server and version: Apache/2.4.41

A screenshot of a computer error

Description automatically generated

\* Looking For Metafiles

\* Robots.txt

A screenshot of a computer

Description automatically generated

\* /application:

A screenshot of a computer

Description automatically generated

\* /composer.lock

A screenshot of a computer

Description automatically generated

\* composer.json

A screenshot of a computer program

Description automatically generated

\* Enumerating Web Server’s Applications:





\* Review the Web Contents

\* Identifying Applications’s Entry Point

\* Mapping Execution Paths:

Dirsearch:

A screen shot of a computer

Description automatically generated

\* Fingerprint Web Application Framework:

A screenshot of a computer

Description automatically generated

II. Configuration & Development Management Testing

\* Test Network Configuration

A screenshot of a computer program

Description automatically generated

\* Test Application Configuration

\* Test File Extension Handling

A screen shot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

A computer screen with white text

Description automatically generated

\* Review Backup & Unreferenced Files

\* Enumerate Infrastructure & Admin Interface

\* Testing HTTP methods



\* Test RIA Cross Domain Policy

\* Test File Permission

\* Test For Subdomain Takeover

\* Test Cloud Storage

III. Identify Management Testing

\* Test Role Definitions

\* Test User Registration Process

\* Test Account Provisioning Process

\* Testing For Account Enumeration



\* Test For Weak Username Policy

IV. Authentication Testing

\* Test For Un-Encrypted Channel

\* Test For Default Credentials

\* Test For Weak Lockout Mechanism

A screenshot of a computer

Description automatically generated

\* Test For Bypassing Authentication Schema

\* Test For Vulnerable Remember Password

\* Test For Browser Cache Weakness

+ Login Completed

A screenshot of a computer

Description automatically generated

+ Logout:

A screenshot of a computer

Description automatically generated

+ Nhấn quay lại trên browser:

A computer and a cup of coffee

Description automatically generated

=> Không đăng nhập lại

\* Test Weak password Policy

V. Authorization Testing

VI. Session Management Schema

VII. Input Validation Testing

VIII. Error Handling Testing

IX. Weak Cryptography testing

X. Business Logic Testing

XI. Malicious File Upload

A screenshot of a computer

Description automatically generated