I.

1.1 Open Source Reconnaissance

A screenshot of a web page

Description automatically generated

A screenshot of a computer

Description automatically generated

1.2 Fingerprint Web Server

A screenshot of a computer

Description automatically generated

Server: Apache/ 2.4.41 (Ubuntu)

\* Details:

+ Using Netcraft:

A white background with colorful text

Description automatically generated

A screenshot of a computer

Description automatically generated

A white background with black text

Description automatically generated

A white background with black text

Description automatically generated

A screenshot of a computer

Description automatically generated

A close-up of a text

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1.3 Look for Metafiles

\* Robots.txt

A screenshot of a computer

Description automatically generated

\* Sitemap.xml

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

\* Humans.txt:

A screenshot of a computer

Description automatically generated

\* Security.txt:

A screenshot of a computer

Description automatically generated

+ With web Juice-shop.herokuapp.com

A screenshot of a computer

Description automatically generated

1.4: Enumerating Web Server’s Applications

\* DNS lookup:

A screen shot of a computer

Description automatically generated

A screenshot of a white line

Description automatically generated

\* Reverse DNS lookup:

\* Enumerating with Nmap:

+ Service running and version of each service

A screenshot of a computer

Description automatically generated

+ 9530

A screenshot of a computer

Description automatically generated

\*\* Topology:

A diagram of a diagram

Description automatically generated

1.5 Review the Web Contents

\* tag <!--



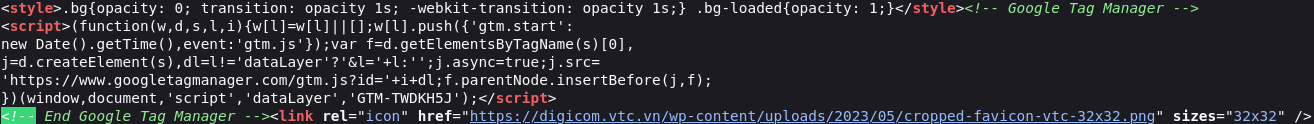


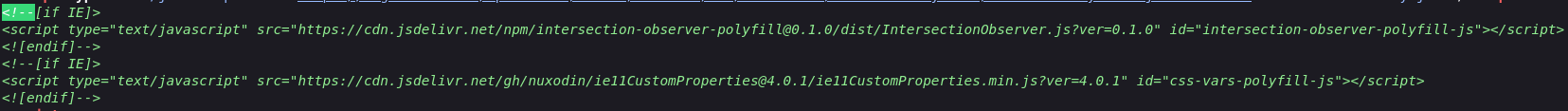
<!-- <link rel='stylesheet' id='contact-form-7-css' href='https://digicom.vtc.vn/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.9.3' type='text/css' media='all' /> -->

<!-- <link rel='stylesheet' id='flatsome-main-css' href='https://digicom.vtc.vn/wp-content/themes/flatsome/assets/css/flatsome.css?ver=3.17.0' type='text/css' media='all' /> -->

<!-- <script type="text/javascript" src="https://digicom.vtc.vn/wp-includes/js/jquery/jquery.min.js?ver=3.7.1" id="jquery-core-js"></script> -->

<!-- <script type="text/javascript" src="https://digicom.vtc.vn/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.4.1" id="jquery-migrate-js"></script> -->





A computer screen with white and green text

Description automatically generated

\* .DTD: Not found

\* META tag:





A screen shot of a computer

Description automatically generated

<meta name="generator" content="WordPress 6.5.2" />

<meta name="msapplication-TileImage" content="https://digicom.vtc.vn/wp-content/uploads/2023/05/cropped-favicon-vtc-270x270.png" />

\* <script></script>

<script>(function(html){html.className = html.className.replace(/\bno-js\b/,'js')})(document.documentElement);</script>

<script>(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':

new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],

j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src=

'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);

})(window,document,'script','dataLayer','GTM-TWDKH5J');</script>

A computer screen shot of a computer code

Description automatically generated

A black screen with white lines

Description automatically generated

A computer screen with white text

Description automatically generated

A screenshot of a computer program

Description automatically generated

A computer screen with white text

Description automatically generated

A black screen with white text

Description automatically generated

1.6 Identifying Application’s Entry Points

- Request

\* ZAP:

A screenshot of a computer

Description automatically generated

=> Method Using: GET, POST

+ Tham số sử dụng trong POST:

A screenshot of a computer program

Description automatically generated

Host, user-agent, cache-control, content-type, content-length

=> Where:   
=> Injection Point:

- Respond:

Với POST request:

+ Mã trạng thái: Hầu hết là 302

A white background with black text

Description automatically generated

+ có 200 ở:





1.7 Mapping Execution Paths

\* Using ZAP for Spidering:

A screenshot of a computer

Description automatically generated

1.8 Fingerprint Web Application Framework

\* Wappalyzer:

A screenshot of a phone

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

\* Whatweb:

A screen shot of a computer code

Description automatically generated

\*HTTP Header:

Xác định khung web:

Header X-Powered-By: Không có

\*\* Với 1 web khác: testphp.vulnweb.com

A screenshot of a computer

Description automatically generated

\*Cookie:

A screenshot of a computer

Description automatically generated

\* HTML Source Code:

A computer screen shot of a program code

Description automatically generated

II. **CONFIGURATION & DEPLOYMENT MANAGEMENT TESTING**

2.1 Test Network Configuration

2.2 Test Application Configuration

2.3 Test File Extension Handling for Sensitive Information

\* Curl

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

A computer screen shot of a computer program

Description automatically generated

\* Wget:

A computer screen shot of text

Description automatically generated

2.4 Review Old Backup and Unreferenced Files for Sensitive Information

2.5 Enumerate Infrastructure and Application Admin Interface

<https://digicom.vtc.vn/wp-login.php?redirect_to=https%3A%2F%2Fdigicom.vtc.vn%2Fwp-admin%2F&reauth=1>

A screenshot of a computer

Description automatically generated

2.6 Test HTTP Methods

A screen shot of a computer

Description automatically generated

2.7 Test HTTP Strict Transport Security

A computer code with white text

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

\*\* max-age=0 ⬄ Hủy HSTS: trình duyệt sẽ ngay lập tức ngừng việc yêu cầu kết nối HTTPS cho tên miền đó ⬄Vô hiệu hóa chính sách HSTS cho tên miền

2.8 Test RIA Cross Domain Policy

A screenshot of a computer

Description automatically generated

A screenshot of a browser

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

2.9 Test File Permission

2.10 Test for Subdomain Takeover

2.11 Test Cloud Storage

### III. [Identity Management Testing](https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/03-Identity_Management_Testing/README)

### 3.1 Test Role Definitions

### 3.2 Test User Registration Process

### VD: Portswigger Signup:

### + Chỉ bắt buộc email đăng nhập

### A screenshot of a computer Description automatically generated

### + Cùng một tài khoản đã đăng nhập trước đó

### A screenshot of a computer Description automatically generated

### A screenshot of a computer Description automatically generated

### A screenshot of a computer Description automatically generated

### => Không thể đăng ký nhiều lần cùng 1 danh tính

### + Đăng ký được xác minh thành công:

### A screenshot of a web security academy Description automatically generated

### 3.3 Test Account Provisioning Process

#### 3.4 [Testing for Account Enumeration and Guessable User Account](https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/03-Identity_Management_Testing/04-Testing_for_Account_Enumeration_and_Guessable_User_Account)

\* Người dùng hợp lệ với mật khẩu sai:

Trong Burp:

A screenshot of a computer program

Description automatically generated

Ở Portswigger:

A screenshot of a computer

Description automatically generated

\* Người dùng không tồn tại:

A screenshot of a computer

Description automatically generated

=> Vẫn là Login Fail

#### 3.5 [Testing for Weak or Unenforced Username Policy](https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/03-Identity_Management_Testing/05-Testing_for_Weak_or_Unenforced_Username_Policy)

**IV. Authentication Testing**

4.1 Test for Un-Encrypted Channel

+ HTTP Login page (http://testphp.vulnweb.com/login)

A screenshot of a computer

Description automatically generated

+ HTTP register or sign-in page:

A screenshot of a computer

Description automatically generated

### 4.2 Test for Default Credentials

### 4.3 Test For Weak Lockout Mechanism

### A screenshot of a computer Description automatically generated

### 4.4 Test For Bypassing Authentication Schema

### 4.5 Test For Vulnerable Remember Password

### 4.6 Test For Browser Cache Weakness

### 4.7 Test For Weak Password Policy

### 4.8 Test For Weak Security Questions

### 4.9 Test For Weak Password Reset Function

### 4.10 Test For Weak Password Change Function

### 4.11 Test For Weak Authentication In Alternative Channel

### VII. Input Validation Testing:

### 1. Test Reflected Cross Site Scripting

### A screenshot of a computer Description automatically generated

### Có XSS

### Payloads:

### \* Các ký tự đặc biệt được lọc (‘ <> “”&’)

### A screenshot of a computer Description automatically generated

### \* Kiểm tra với chuỗi thoát ký tự:

### A screenshot of a computer Description automatically generated

### \* Kiểm tra bằng cách thay thế < và > bằng các thực thể HTML < và >

### &lt;script&gt;alert('XSS')&lt;/script&gt;

### A screenshot of a computer Description automatically generated

### \* Kiểm tra tải trọng bằng cả chữ thường và chữ hoa

### A screenshot of a computer Description automatically generated

### \* Kiểm tra để phá vỡ biểu thức tường lửa bằng dòng mới /r/n

### <script>alert('XSS')\r\n</script>

### A screenshot of a computer Description automatically generated

### \* Kiểm tra bằng mã hóa kép

### %253Cscript%253Ealert('XSS')%253C/script%253E

### A screenshot of a computer Description automatically generated

### \* Thử nghiệm với bộ lọc đệ quy

### <<script>alert('XSS');//<</script>

### A screenshot of a computer Description automatically generated

### \* Kiểm tra việc chèn thẻ anchor không có khoảng trắng

### <a href=javascript:alert('XSS')>Click me</a>

### A screenshot of a computer Description automatically generated

### \* Kiểm tra bằng cách thay thế khoảng trắng bằng dấu đầu dòng

### <script•alert('XSS')•</script>

### A screen shot of a computer Description automatically generated

### \* Kiểm tra bằng cách thay đổi phương thức HTTP

### + POST:

### A screen shot of a computer screen Description automatically generated

### 2. Testing for Stored Cross Site Scripting

### + Chèn vào search <script>alert(“1”)</script>

### A screenshot of a computer Description automatically generated

### - Reload lại page:

### A screenshot of a computer Description automatically generated

### \* Hoặc trong biểu mẫu được upload lên hệ thống

3. Testing for HTTP Verb Tampering (Tương tự Test HTTP Methods ở 2.6)

4. Testing HTTP Parameter Pollution

5. Testing SQL Injection:

VIII. Test for Error Handling

**IX. Test for Weak Cryptography**

1. Testing for Weak Transport Layer Security

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Version TLS: v1.2

Thuật toán sử dụng: ECDHE-RSA-AES128-GCM-SHA256

Key strength: 2048 bit (Server public key – 2048 bit)

Cơ quan cấp: AMAZON

SAN (Subject Alternate Name): Không có

2. Testing for Padding Oracle:

3. Testing for Sensitive Information Sent via Unencrypted Channels

4. Testing for Weak Encryption