Penetration Testing Report for

Function Ekyc In APP

I. Tóm tắt

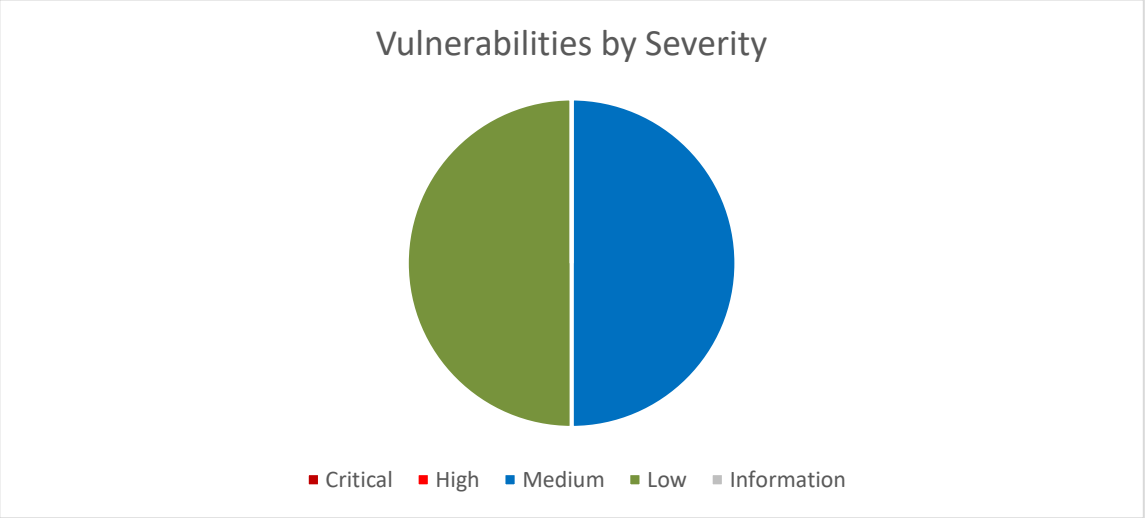
Scope	Security level	Grade
Web API perimeter	Good	B

Under Defense Grading Criteria:

Grade	Security	Criteria Description
A	Excellent	Bảo mật vượt tiêu chuẩn “Industry Best Practice”. Tổng thể được cho là xuất sắc chỉ với một số phát hiện rủi ro ***thấp*** được xác định.
B	Good	Bảo mật đáp ứng các tiêu chuẩn được chấp nhận cho “Industry Best Practice”. Tổng thể được cho là tốt chỉ có một số thiếu sót có rủi ro ***trung bình*** và ***thấp*** được xác định.
C	Fair	Các giải pháp hiện tại bảo vệ một số khu vực của doanh nghiệp khỏi các vấn đề bảo mật. Cần có những thay đổi vừa phải để nâng các lĩnh vực được thảo luận lên tiêu chuẩn “Industry Best Practice”
D	Poor	Tồn tại những thiếu sót bảo mật đáng kể. Cần chú ý ngay đến các vấn đề đã thảo luận để giải quyết các phơi nhiễm đã xác định. Cần có những thay đổi lớn để nâng cao tiêu chuẩn “Industry Best Practice”.
F	Inadequate	Tồn tại những thiếu sót bảo mật nghiêm trọng. Những thiếu sót đã được xác định trong hầu hết hoặc thậm chí tất cả các biện pháp kiểm soát bảo mật được kiểm tra. Cải thiện an ninh sẽ yêu cầu phân bổ nguồn lực lớn.

1. Đối tượng & Phạm vi

Organization	Vietcap
Method Type	White Box
Asset URL	www.vietcap.com.vn/mo-tai-khoan-qc/mbApp



Các chuyên gia bảo mật đã thực hiện kiểm tra bảo mật thủ công theo Phương pháp kiểm tra ứng dụng web ***OWASP***, cho thấy các kết quả sau.

Severity	**Critical**	**High**	**Medium**	**Low**	**Informational**
# of issues	0	0	4	3	0

Severity scoring:

- **Critical** - Mối đe dọa trực tiếp đối với các quy trình kinh doanh chính.
- **High** – Mối đe dọa trực tiếp đến các quy trình kinh doanh chính.
- **Medium** – Mối đe dọa gián tiếp đối với các quy trình kinh doanh chính hoặc mối đe dọa một phần đối với các quy trình kinh doanh.
- **Low** – Không có mối đe dọa trực tiếp tồn tại. Lỗ hổng có thể bị khai thác bằng các lỗ hổng khác.
- **Informational** – Phát hiện này không chỉ ra lỗ hổng, nhưng nêu một nhận xét thông báo về các lỗi thiết kế và triển khai không đúng cách có thể gây ra sự cố về lâu dài

2. Các thử nghiệm đã thực hiện:

- Tập hợp 10 mối đe dọa bảo mật hàng đầu của ***OWASP Top 10 2021***

Criteria Labels	Status
A01: Broken Access Control	Meet Criteria
A02: Cryptographic Failures	Meet Criteria
A03: Injection	Fail Criteria
A04: Insecure Design	Meet Criteria
A05: Security Misconfiguration	Fail Criteria
A06: Vulnerable and Outdated Components	Meet Criteria
A07: Identification and Authentication Failures	Fail Criteria
A08: Software and Data Integrity Failures	Meet Criteria
A09: Security Logging and Monitoring Failures	Meet Criteria
A10: Server-Side Request Forgery	Meet Criteria

3. Các công cụ được sử dụng

- Burp Suite Pro
- SQLmap
- Different Burp Suite plugins (JWT Edit, JSON Token Attack, Burp Bounty, etc.)

4. Phương pháp thực hiện

Phương pháp kiểm tra thâm nhập của chúng tôi dựa trên các hướng dẫn và tiêu chuẩn sau:

- OWASP Testing Guide
- OWASP Top 10 Web Application

II. Chi tiết lỗ hỏng tìm được

1. A07 Identification and Authentication Failures

1.1. Access Token hard code

SEVERITY: **Medium**

LOCATION:

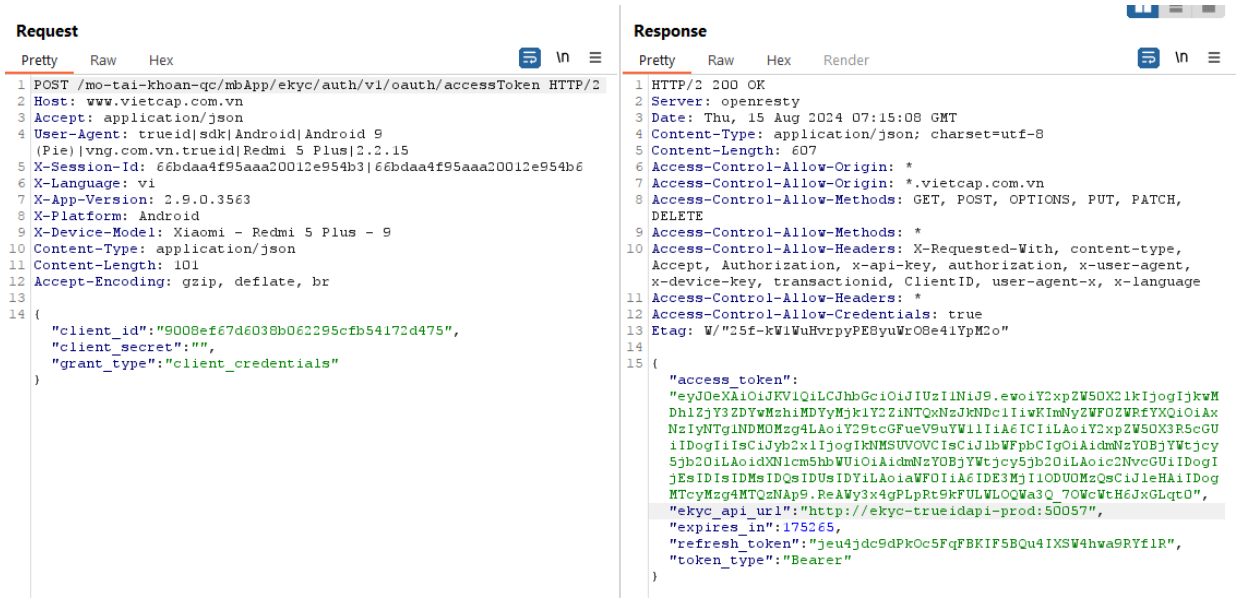
/mo-tai-khoan-qc/mbApp/ekyc/auth/v1/oauth/accessToken

ISSUE DESCRIPTION:

- Token được generate khi request không thay đổi. (token này được sử dụng để chứng thực với vendor - trueid)

PROOF OF VULNERABILITY:

/mo-tai-khoan-qc/mbApp/ekyc/auth/v1/oauth/accessToken



Request

Pretty Raw Hex

```
POST /mo-tai-khoan-qc/mbApp/ekyc/auth/v1/oauth/accessToken HTTP/2
Host: www.vietcap.com.vn
Accept: application/json
User-Agent: trueid|sdk|Android|Android 9 (Pie)|vng.com.vn.trueid|Redmi 5 Plus|2.2.15
X-Session-Id: 66bdaa4f95aaa20012e954b3|66bdaa4f95aaa20012e954b6
X-Language: vi
X-App-Version: 2.9.0.3563
X-Platform: Android
X-Device-Model: Xiaomi - Redmi 5 Plus - 9
Content-Type: application/json
Content-Length: 101
Accept-Encoding: gzip, deflate, br

{
  "client_id":"9008ef67d6038b062295cfb54172d475",
  "client_secret":"",
  "grant_type":"client_credentials"
}
```

Response

Pretty Raw Hex Render

```
HTTP/2 200 OK
Server: openresty
Date: Thu, 15 Aug 2024 07:15:08 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 607
Access-Control-Allow-Origin: *
Access-Control-Allow-Origin: *.vietcap.com.vn
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, PATCH, DELETE
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: X-Requested-With, content-type, Accept, Authorization, x-api-key, authorization, x-user-agent, x-device-key, transactionid, ClientID, user-agent-x, x-language
Access-Control-Allow-Headers: *
Access-Control-Allow-Credentials: true
Etag: W/"25f-kW1WuHvrpyPE8yuWrO8e41YpM2o"

{
  "access_token":
  "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.ewoiY2xpZW50X2lkIjogIjkwM
  Dh1ZjY3ZDYwMzhiMDYyMjk1Y2ZiNTQxNzJkNDc1IiwKImNyZWFOZWRfYXQiOiAx
  NzIyNTg1NDM0Mzg4LAoiY29tcGFueV9uYW1lIiA6ICIiLAoiY2xpZW50X3R5cGU
  iIDogIiIsCiJyb2xlIjogIkNMSUVOVCIsCiJlbWFpbCIgOiAidmNzYOBjYWtjcy
  5jb2OiLAoidXNlcm5hbWUiOiAidmNzYOBjYWtjcy5jb2OiLAoic2NvcGUiIDogI
  jEsIDIsIDMsIDQsIDUsIDYiLAoiaWFOIiA6IDE3MjI1ODUOMzQsCiJleHAiIDog
  MTcyMzg4MTQzNAp9.ReAWy3x4gPLpRt9kFULWLOQWa3Q_7OWcWtH6JxGLqtO",
  "ekyc_api_url":"http://ekyc-trueidapi-prod:50057",
  "expires_in":175265,
  "refresh_token":"jeu4jdc9dPkOc5FqFBKIF5BQu4IXSW4hwa9RYflR",
  "token_type":"Bearer"
}
```

RECOMMENDATIONS:

- Generate random token
- Ẩn token này, không trả response phía client

1.2. Access Token Not Timeout too long

SEVERITY: **Medium**

LOCATION:

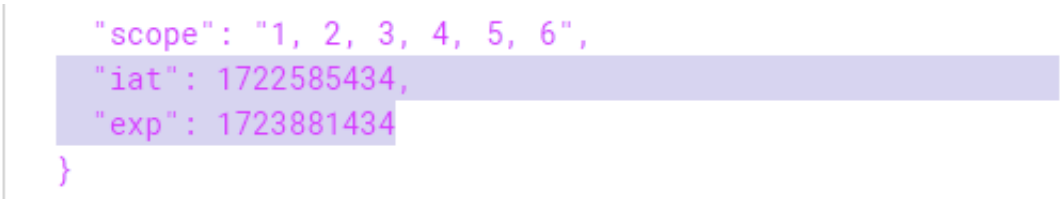
/mo-tai-khoan-qc/mbApp/ekyc/auth/v1/oauth/accessToken

ISSUE DESCRIPTION:

- Sau **15 ngày** access token sẽ được tự động expired và cấp mới. → quá lâu → Nhân viên có thể liên tục sử dụng trong nhiều giờ đồng hồ

PROOF OF VULNERABILITY:

Thời gian Expired của TOKEN quá lâu (15 NGÀY)



RECOMMENDATIONS:

- Terminate token sau 15 phút.

2. A03: Injection

2.1. Input Validation

SEVERITY: **Medium**

LOCATION:

/mo-tai-khoan-qc/mbApp/ekyc/request/create

/mo-tai-khoan-qc/mbApp/otp/resend

/mo-tai-khoan-qc/mbApp/otp/request

/mo-tai-khoan-qc/mbApp/ekyc/request/create

/mo-tai-khoan-qc/mbApp/otp/confirm

/mo-tai-khoan-qc/mbApp/personal/accounts/check

/mo-tai-khoan-qc/mbApp/personal/accounts/confirm

/mo-tai-khoan-qc/mbApp/personal/accounts/suggest

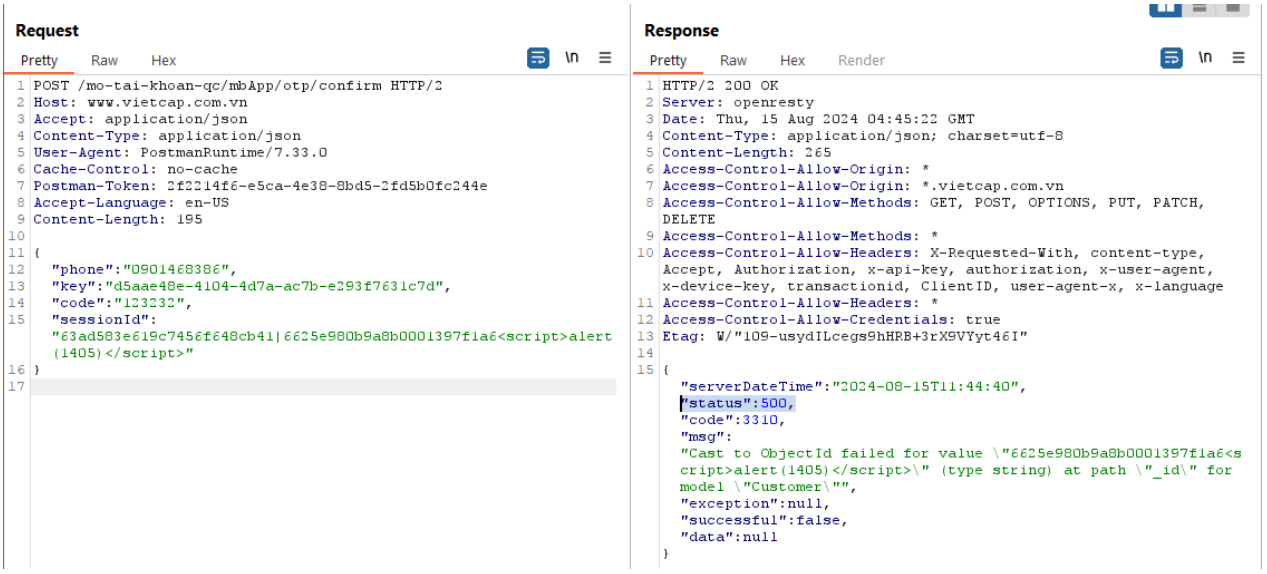
/mo-tai-khoan-qc/mbApp/personal/services

ISSUE DESCRIPTION:

Truyền các tham số ngẫu nhiên vào các Param trong Payload. Các tham số đầu vào không được ***validate*** có thể làm tiền đề cho các cuộc tấn công Injection.

PROOF OF VULNERABILITY:

/mbApp/personal/accounts/check



RECOMMENDATIONS:

- Lọc dữ liệu từ người dùng.

2.2. Script-Base Attack

SEVERITY: **Medium**

LOCATION:

/mo-tai-khoan-qc/mbApp/ekyc/id/verify/back
/mo-tai-khoan-qc/mbApp/ekyc/id/verify/front
/mo-tai-khoan-qc/mbApp/ekyc/selfie/verify

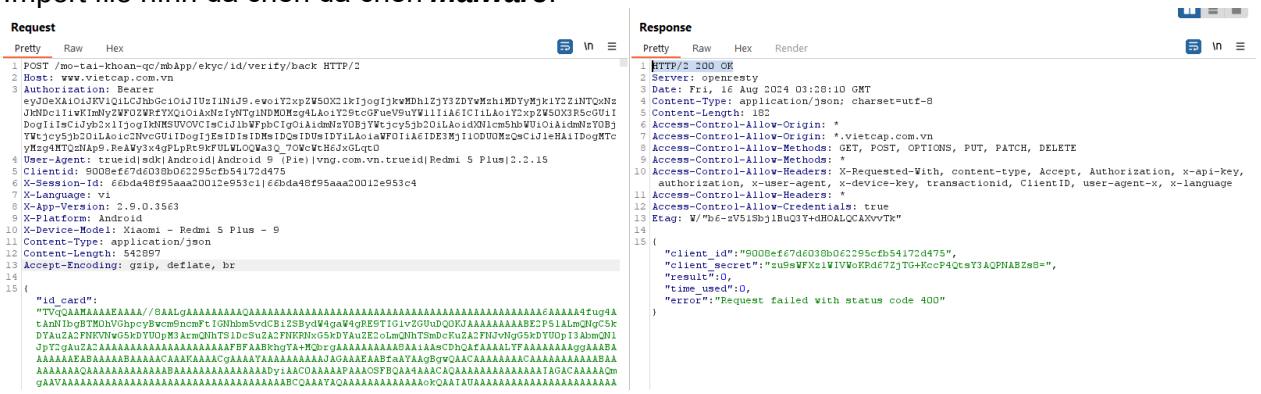
ISSUE DESCRIPTION:

Chưa kiểm tra based64 upload.

PROOF OF VULNERABILITY:

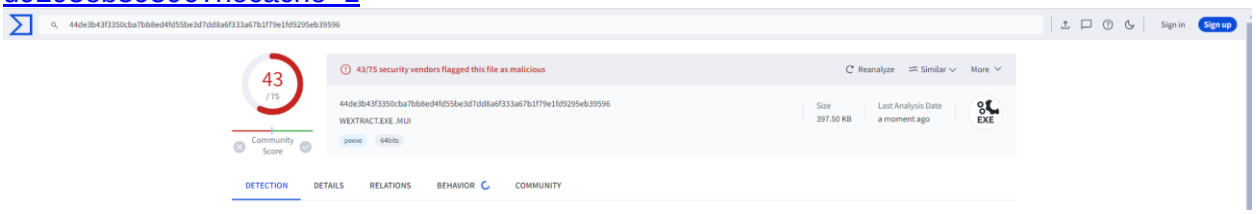
/mo-tai-khoan-qc/mbApp/ekyc/id/verify/back

Import file hình đã chèn đã chèn ***malware***.



*Check file with **virustotal:***

https://www.virustotal.com/gui/file/44de3b43f3350cba7bb8ed4fd55be3d7dd8a6f333a67b1f79e1fd9295eb39596?nocache=1



RECOMMENDATIONS:

- Kiểm tra kĩ loại file Upload (File Extension).

3. A05: Security Misconfiguration

3.1. Appliccation Error Message

SEVERITY: **Low**

LOCATION:

//mo-tai-khoan-qc/mbApp/banks

/mo-tai-khoan-qc/mbApp/banks/branches

/mo-tai-khoan-qc/mbApp/configs

/mo-tai-khoan-qc/mbApp/otp/confirm

/mo-tai-khoan-qc/mbApp/otp/request

/mo-tai-khoan-qc/mbApp/otp/resend

/mo-tai-khoan-qc/mbApp/ekyc/auth/v1/oauth/accessToken

ISSUE DESCRIPTION:

Tiêu đề "Access-Control-Allow-Origin" điều kiện quá dễ dàng

PROOF OF VULNERABILITY:

Request & Response
/mo-tai-khoan-qc/mbApp/otp/request

Request

Pretty Raw Hex

```
POST /mo-tai-khoan-qc/mbApp/otp/request HTTP/2
Host: www.vietcap.com.vn
Accept: application/json
X-Device-Model: Xiaomi - Redmi 5 Plus - 9
X-Platform: Android
X-App-Version: 2.9.0
X-Otp-Protection:
808c0e3fb981a742798159c478305292445c26b7e58f6d9a219510f2c06bd3488e0a3f4
ed4e8405aec553102a612e0ef6e26ac0e12c412a1ab60eeb4ebab4efc946e076831ce9d
7fe8be554829b6e78df2cd013db35100e28d6083941d000193a81ed63f70666d5d76955
712b3d15ecdac3bcc0217089cf0121b9972ea4188bd
Content-Type: application/json
Content-Length: 114
Accept-Encoding: gzip, deflate, br
User-Agent: okhttp/4.9.2

{
  "email":"">\"'><script>alert(16)</script>"","phone":"0955684588","
  region":"HOCHIMINH","serviceNoBroker":"ACTIVE"}
```

Response

Pretty Raw Hex Render

```
HTTP/2 400 Bad Request
Server: openresty
Date: Wed, 14 Aug 2024 10:18:09 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 836
Etag: W/"344-t7LE9aC7agsVqT8qncD9fcoPtB8"

{
  "success":false,
  "status":400,
  "message":"Unexpected token > in JSON at position 11",
  "path":"/mbApp/otp/request",
  "stack":
  "SyntaxError: Unexpected token > in JSON at position 11\n    at JSON.
  parse (<anonymous>)\n    at parse (/usr/src/app/node_modules/body-par
  ser/lib/types/json.js:92:19)\n    at /usr/src/app/node_modules/body-p
  arser/lib/read.js:128:18\n    at AsyncResource.runInAsyncScope (node:
  async_hooks:203:9)\n    at invokeCallback (/usr/src/app/node_modules/
  raw-body/index.js:238:16)\n    at done (/usr/src/app/node_modules/raw
  -body/index.js:227:7)\n    at IncomingMessage.onEnd (/usr/src/app/nod
  e_modules/raw-body/index.js:287:7)\n    at IncomingMessage.emit (node
  :events:517:28)\n    at endReadableNT (node:internal/streams/readable
  :1400:12)\n    at process.processTicksAndRejections (node:internal/pr
  ocess/task_queues:82:21)"
}
```

RECOMMENDATIONS:

Không hiển thị thông tin nhạy cảm của ứng dụng.

3.2. Overly Permissive CORS Access Policy

SEVERITY: **Low**

LOCATION:

/mo-tai-khoan-qc/mbApp/banks

/mo-tai-khoan-qc/mbApp/banks/branches

/mo-tai-khoan-qc/mbApp/configs

/mo-tai-khoan-qc/mbApp/otp/confirm

/mo-tai-khoan-qc/mbApp/otp/request

/mo-tai-khoan-qc/mbApp/otp/resend

/mo-tai-khoan-qc/mbApp/personal/accounts/check

/mo-tai-khoan-qc/mbApp/personal/accounts/confirm

/mo-tai-khoan-qc/mbApp/personal/accounts/suggest

/mo-tai-khoan-qc/mbApp/personal/services

/mo-tai-khoan-qc/mbApp/personal/signature

/mo-tai-khoan-qc/mbApp/referral

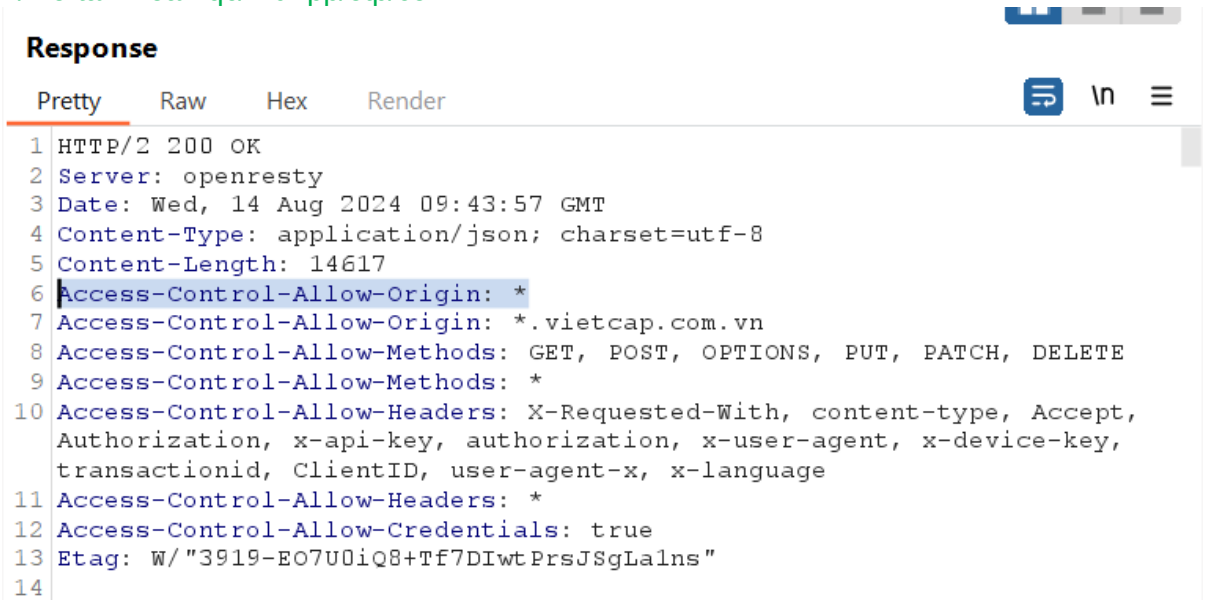
ISSUE DESCRIPTION:

Tiêu đề "Access-Control-Allow-Origin" điều kiện quá dễ dàng

PROOF OF VULNERABILITY:

Request & Response

/mo-tai-khoan-qc/mbApp/otp/confirm



RECOMMENDATIONS:

Access-Control-Allow-Origin: ***.vietcap.com.vn***

3.3. Missing or insecure "X-Content-Type-Options" Header

SEVERITY: **Low**

LOCATION:

/mo-tai-khoan-qc/mbApp/

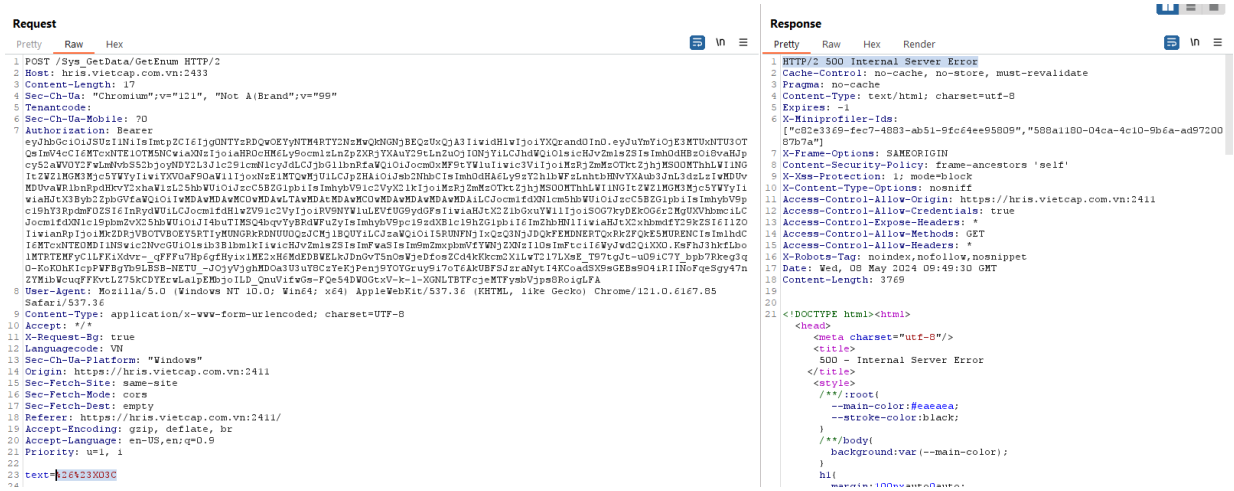
ISSUE DESCRIPTION:

Thiếu header X-Content-Type-Options có thể dẫn đến tấn công Clickjacking và Cross-Frame Scripting.

PROOF OF VULNERABILITY:

Request & Response

/mo-tai-khoan-qc/mbApp/



RECOMMENDATIONS:

Cấu hình lại header Strict-Transport-Security: max-age=<expire-time>; includeSubDomains.

3.4. Missing or insecure HTTP Strict-Transport-Security Header

SEVERITY: **Low**

LOCATION:

/mo-tai-khoan-qc/mbApp/banks

/mo-tai-khoan-qc/mbApp/banks/branches

/mo-tai-khoan-qc/mbApp/configs

/mo-tai-khoan-qc/mbApp/otp/confirm

/mo-tai-khoan-qc/mbApp/otp/request

/mo-tai-khoan-qc/mbApp/otp/resend

/mo-tai-khoan-qc/mbApp/personal/accounts/check

/mo-tai-khoan-qc/mbApp/personal/accounts/confirm

/mo-tai-khoan-qc/mbApp/personal/accounts/suggest

/mo-tai-khoan-qc/mbApp/personal/services

/mo-tai-khoan-qc/mbApp/personal/signature

/mo-tai-khoan-qc/mbApp/referral

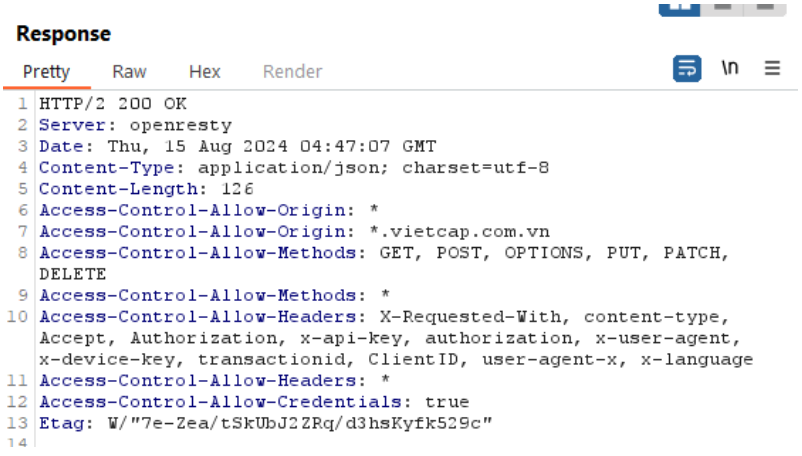
ISSUE DESCRIPTION:

Thiếu header Strict-Transport-Security, HSTS là một cơ chế buộc các trình duyệt sử dụng kết nối an toàn. Nếu được trang bị HSTS, sever sẽ buộc trình duyệt giao tiếp qua HTTPS (HTTP Secure). Điều này ngăn chặn chuyển hướng request từ HTTPS đến HTTP.

PROOF OF VULNERABILITY:

Request & Response

/Sys_GetData/GetEnum



RECOMMENDATIONS:

Cấu hình lại header Strict-Transport-Security: max-age=<expire-time>; includeSubDomains