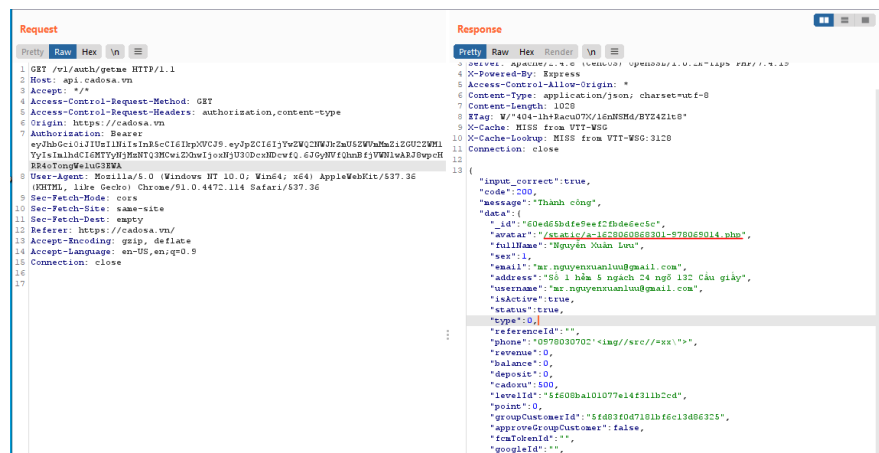


# REPORT CADOSA

Tổng số lỗi: 3

## 1) Upload file tùy ý

- **Mức độ:** Trung bình.
- **Phạm vi ảnh hưởng:** chức năng upload avatar của khách hàng.
- **Ảnh hưởng:** có xấu có thể xử dụng domain cadosa để phân tán các file độc hại tới người dùng.
- **Fix:** fix cứng extension file người dùng upload.
- **PoC:**



## 2) Debug mode on

- **Mức độ:** Trung bình.
- **Phạm vi ảnh hưởng:** toàn bộ trang web.
- **Ảnh hưởng:** từ những thông tin ở phần debug này, kẻ tấn công có thể thu thập thông tin về máy chủ.
- **Fix:** throw catch error message bằng những thông báo chung chung.
- **PoC:**

```

1 HTTP/1.1 400 Bad Request
2 Date: Wed, 04 Aug 2021 06:50:11 GMT
3 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.19
4 X-Powered-By: Express
5 Access-Control-Allow-Origin: *
6 Content-Security-Policy: default-src 'none'
7 X-Content-Type-Options: nosniff
8 Content-Type: text/html; charset=utf-8
9 Content-Length: 587
10 X-Cache: MISS from VTT-WSG
11 X-Cache-Lookup: MISS from VTT-WSG:3128
12 Connection: close
13
14 <!DOCTYPE html>
15 <html lang="en">
16   <head>
17     <meta charset="utf-8">
18     <title>
19       Error
20     </title>
21     </head>
22     <body>
23       SyntaxError: Unexpected string in JSON at position 166<br>
24       <pre>
25         anbsp; anbsp;at JSON.parse (lit:anonymous):<br>
26         anbsp; anbsp;at parse (/var/deployments/cadosa-production/node_modules/body-parser/lib/types/json.js:89:19)<br>
27         anbsp; anbsp;at /var/deployments/cadosa-production/node_modules/body-parser/lib/read.js:121:18<br>
28         anbsp; anbsp;at invokeCallback (/var/deployments/cadosa-production/node_modules/raw-body/index.js:224:16)<br>
29         anbsp; anbsp;at done (/var/deployments/cadosa-production/node_modules/raw-body/index.js:212:7)<br>
30         anbsp; anbsp;at IncomingMessage.onEnd (/var/deployments/cadosa-production/node_modules/raw-body/index.js:273:7)<br>
31         anbsp; anbsp;at IncomingMessage.emit (events.js:387:35)<br>
32         anbsp; anbsp;at endReadableNT (internal/streams/readable.js:1217:12)<br>
33         anbsp; anbsp;at processTicksAndRejections (internal/process/task_queues.js:82:21)
34       </pre>
35     </body>
36   </html>

```

### 3) Leak server information

- **Mức độ:** Trung bình.
- **Phạm vi ảnh hưởng:** toàn bộ response.
- **Ảnh hưởng:** Kẻ tấn công từ những thông tin về máy chủ có thể tìm các lỗ hổng đã biết nhằm tấn công máy chủ.
- **Fix:** không hiển thị thông tin về server trong response.
- **PoC:**

```

HTTP/1.1 200 OK
Date: Wed, 04 Aug 2021 07:07:48 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.19
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: application/json; charset=utf-8
Content-Length: 1041
ETag: W/"411-RgbX3xbGQhm3noX6qXN4tSeShGI"
X-Cache: MISS from VTT-WSG
X-Cache-Lookup: MISS from VTT-WSG:3128
Connection: close

```