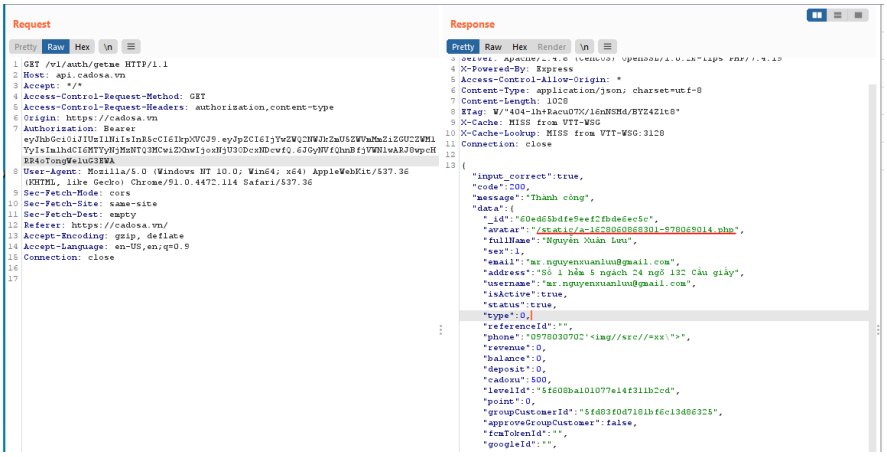
REPORT CADOSA

Tổng số lỗi: 3

1) Upload file tùy ý
   - Mức độ: Trung bình.
   - Phạm vi ảnh hưởng: chức năng upload avatar của khách hang.
   - 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:

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
```