

Phát triển và bảo mật ứng dụng web trên Laravel



Nội Dung

01.
Giới thiệu



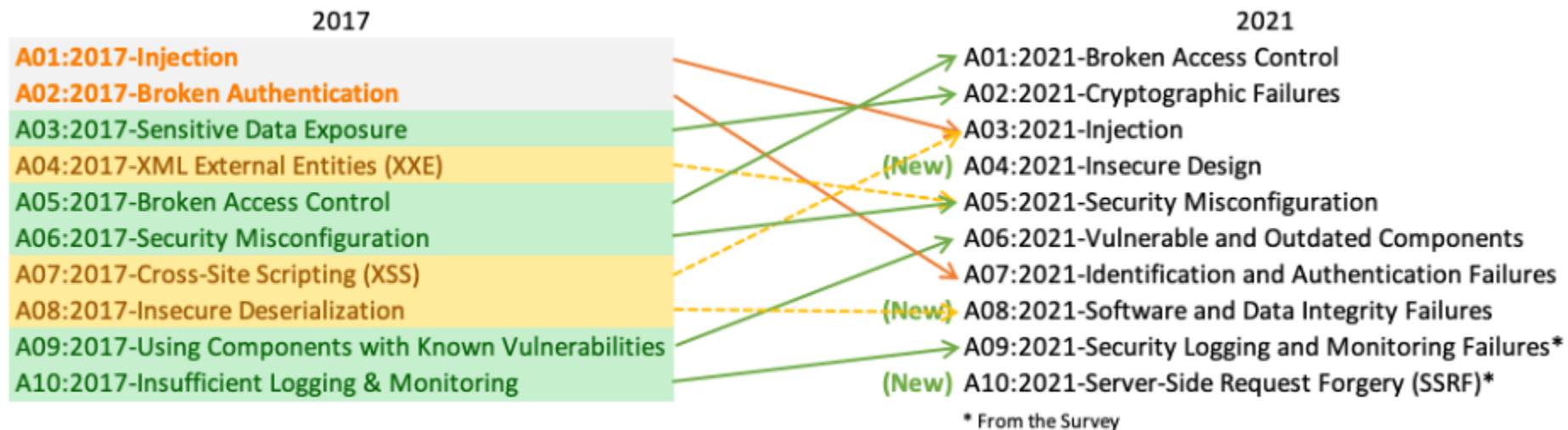
02.
**Xây dựng web và
bảo mật web**

03.
**Các lỗ hổng của
web và cách vá
các lỗ hổng**

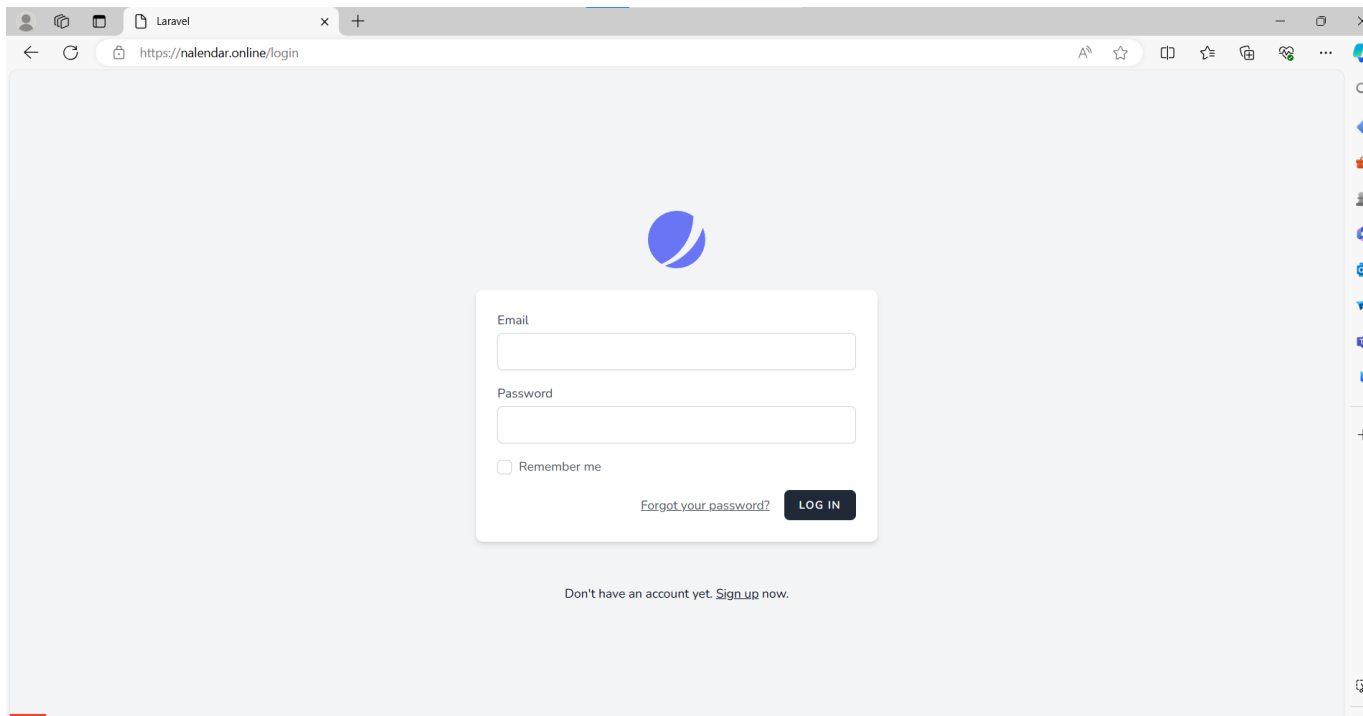
Giới thiệu

- Các cuộc tấn công web ngày càng phổ biến hơn.
- Nhu cầu về việc phát triển và bảo mật ứng dụng web cũng đang gia tăng.
- Nên đồ án này chúng ta sẽ xây dựng một trang mạng xã hội và bảo mật cho web để tránh các lỗ hổng phổ biến.

Giới thiệu



Giới thiệu



<https://nalendar.online>



Nội Dung

01.
Giới thiệu



02.
Xây dựng web và
bảo mật web

03.
Các lỗ hổng của
web và cách vá
các lỗ hổng

Xây dựng web: Laravel

- Laravel là **miễn phí và mã nguồn mở**(open-source)
- Laravel là một **framework** dựa trên **PHP** và được dùng để phát triển web theo mô hình **MVC**



Taylor Otwell

Xây dựng web: Livewire

- **Livewire** (Laravel livewire) là một **framework fullstack** dành cho Laravel.



Xây dựng web: Docker

- **Docker** giúp triển khai ứng dụng web
- Các **images** trong container web:
 - **PHP-fpm**: xử lý các yêu cầu PHP bằng cách tạo mới tiến trình hoặc luồng cho mỗi yêu cầu
 - **Nginx**: Web server
 - **MySQL**: Database
 - **PHPmyadmin**: cung cấp giao diện để quản trị MySQL

Bảo mật web: Cloudflare

- **CloudFlare** là dịch vụ hỗ trợ web
- **CloudFlare** dùng để TLS và DDos protection



Bảo mật web: Cloudflare

Edit rate limiting rule [About rate limiting rules](#)

Rule name (required)

Give your rule a descriptive name

If incoming requests match...

Field	Operator	Value	
<input type="text" value="URI Path"/>	<input type="text" value="equals"/>	<input type="text" value="^/.*"/> e.g. /content	<input type="button" value="And"/> <input type="button" value="X"/>
<input type="button" value="Or"/>			
<input type="text" value="URI Path"/>	<input type="text" value="equals"/>	<input type="text" value="/login"/> e.g. /content	<input type="button" value="And"/> <input type="button" value="Or"/> <input type="button" value="X"/>

Expression Preview

[Edit expression](#)

```
(http.request.uri.path eq "^/.*") or (http.request.uri.path eq "/login")
```

With the same characteristics...

Bảo mật web: Cloudflare

With the same characteristics...

When rate exceeds...

Requests (required) Period (required)

Then take action...

Choose action

Blocks matching requests and stops evaluating other rules

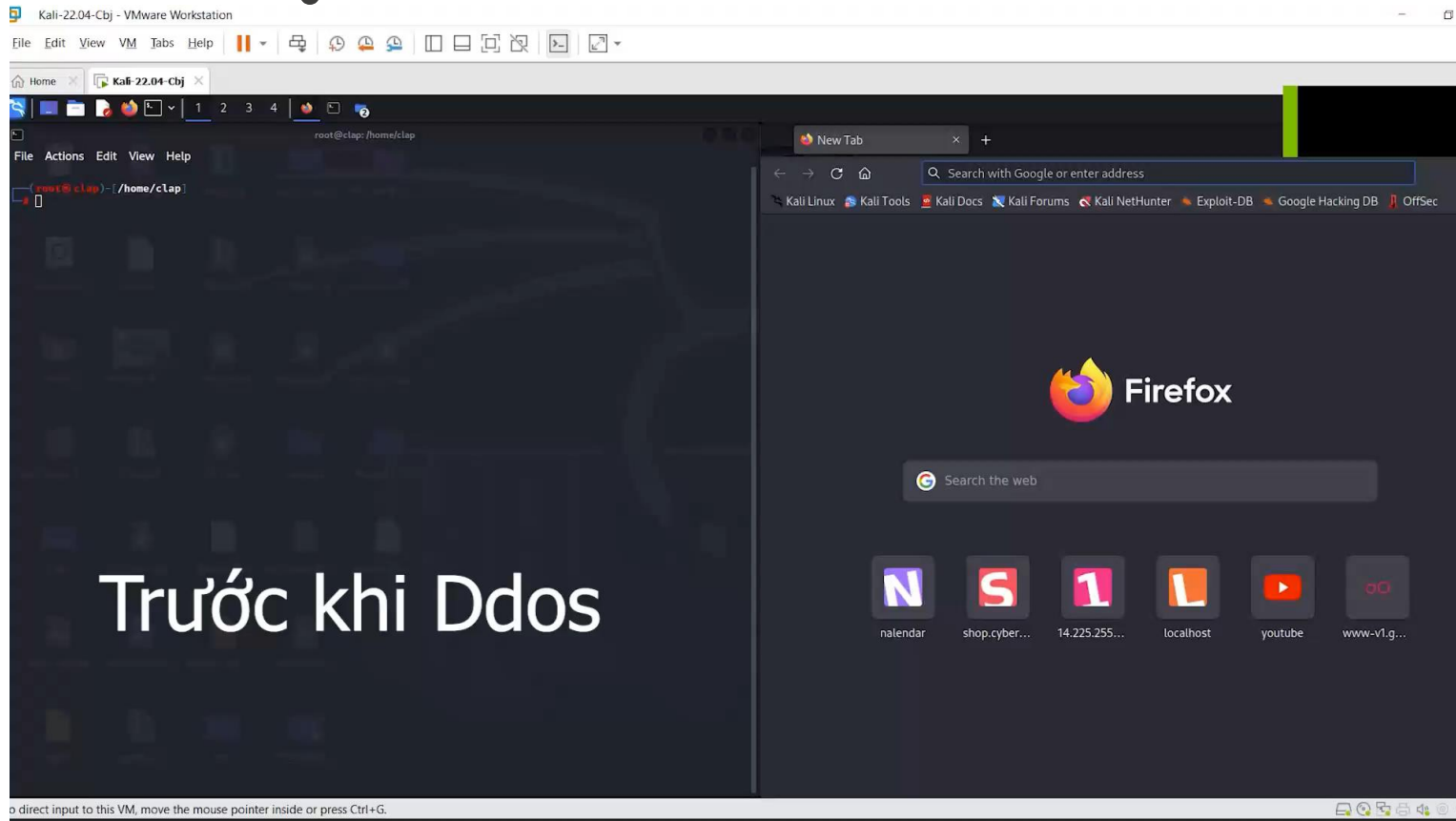
For duration...

Duration (required)

Cancel

Save

Bảo mật web: Cloudflare



Bảo mật web: Snyk

- **Snyk** là công cụ bảo mật cung cấp giải pháp tìm và sửa các lỗ hổng trong phần mềm



Bảo mật web: Snyk

- **Snyk** kiểm tra các lỗ hổng trong **mã nguồn**, **dependencies**, **image**, **container**, cơ sở hạ tầng dưới dạng cấu hình mã và môi trường cloud, đồng thời đưa ra cảnh báo, mức độ ưu tiên và biện pháp khắc phục
- **Snyk** hỗ trợ nhiều ngôn ngữ khác nhau như: **JavaScript**, **Python**, **PHP**, **Dockerfiles**, ...

Bảo mật web: Snyk

- **Snyk Code (SAST), Snyk Open Source(SCA):** kiểm tra code và các gói **3rd-party open source**
- **Snyk Container:** kiểm tra cấu hình file image và lỗ hổng trên nền tảng **Linux**
- **Snyk Infrastructure as Code:** cung cấp đánh giá cho các cấu hình **cơ sở hạ tầng cloud**

Bảo mật web: Snyk

Targets1

nguyen8amk1/UIT_NT230.N21.ATCL-Secure_Social_Network

2

C

17

H

35

M

83

L

Project

Imported

Tested

Issues ↓

docker/php/Dockerfile

3 minutes ago

3 minutes ago

1

C

1

H

0

M

79

L

composer.lock

3 minutes ago

3 minutes ago

1

C

0

H

0

M

0

L

docker/mysql/Dockerfile

3 minutes ago

3 minutes ago

0

C

16

H

28

M

0

L

docker/nginx/Dockerfile

3 minutes ago

3 minutes ago

0

C

0

H

4

M

2

L

Code analysis

2 minutes ago

2 minutes ago

0

C

0

H

3

M

2

L

package.json

3 minutes ago

3 minutes ago

0

C

0

H

0

M

0

L

docker/phpmyadmin/Dockerfile

3 minutes ago

3 minutes ago

0

C

0

H

0

M

0

L

Bảo mật web: Snyk

Clapboiz > [Projects](#) > [nguyen8amk1/UIT_NT230.N21.ATCL-Secure_Social_Network](#) main Open on GitHub

docker/mysql/Dockerfile

Overview History Settings

☐ Critical 0

☐ High 16

☐ Medium 28

☐ Low 0

▼ PRIORITY SCORE

Scored between 0 - 1000

▼ "FIXED IN" AVAILABLE

☐ Yes 44

☐ No 0

▼ COMPUTED FIXABILITY

☐ Fixable 0

☐ Partially fixable 0

☐ No supported fix 44

▼ EXPLOIT MATURITY

☐ Mature 0

H

openssl - Buffer Overflow [🔗](#)

VULNERABILITY

CWE-120 [#]

CVE-2022-3786 [#]

CVSS 7.5 [#]

HIGH

SNYK-ORACLE9-OPENSLL-3092709 [#]

SCORE

614

Introduced through

openssl@1:3.0.7-27.0.3.el9

Exploit maturity

NO KNOWN EXPLOIT

Fixed in

openssl@2:3.0.1-43.0.1.ksplice1.el9_0, @2:3.0.1-43.0.1.ksplice1.el9_0

Show less detail

^

Detailed paths

▪ Introduced through: mysql@8.0 > openssl@1:3.0.7-27.0.3.el9

Fix: Upgrade to openssl@2:3.0.1-43.0.1.ksplice1.el9_0 [?]

Security information

Factors contributing to the scoring:

▪ Snyk: CVSS 7.5 - High Severity

▪ NVD: CVSS 7.5 - High Severity

▪ Oracle Security Rating: IMPORTANT

[Why are the scores different? Learn how Snyk evaluates vulnerability scores](#)

Ignore

Bảo mật web: Snyk

- **Git hook pre-commit với Snyk CLI:** Tận dụng **Git hook pre-commit** của **Git** và **Snyk CLI** để có thể tự động kiểm tra mã nguồn của chúng ta trước khi commit để đảm bảo rằng không có lỗ hổng bảo mật nào trong code

Bảo mật web: Snyk

```
git> hooks > pre-commit
1  #!/bin/sh
2  # To enable this hook, rename this file to "pre-commit".
3  # Redirect output to stderr.
4  exec 1>&2
5
6  # Call Snyk CLI to scan the repository for dependencies vulnerabilities.
7  if ! snyk test; then
8    echo "Snyk dependencies vulnerabilities found. Commit aborted."
9    exit 1
10 fi
11
12 # Call Snyk CLI to scan the repository for code vulnerabilities.
13 if ! snyk code test; then
14   echo "Snyk code vulnerabilities found. Commit aborted."
15   exit 1
16 fi
17
18 # Commit can proceed if no vulnerabilities found.
19 exit 0
20
```

PROBLEMS OUTPUT DEBUG CONSOLE COMMENTS **TERMINAL** PORTS SQL CONSOLE push

```
LEGION3LAPTOP-EGHVE44L D:\Users\Desktop\UIT_NT230.N21.ATCL-Secure_Social_Network >main git add .
LEGION3LAPTOP-EGHVE44L D:\Users\Desktop\UIT_NT230.N21.ATCL-Secure_Social_Network >main git commit -m

Testing D:\Users\Desktop\UIT_NT230.N21.ATCL-Secure_Social_Network...

Organization:  clapboiz
Package manager:  yarn
Target file:  yarn.lock
Project name:  package.json
Open source:  no
Project path:  D:\Users\Desktop\UIT_NT230.N21.ATCL-Secure_Social_Network
Local Snyk policy:  found
Licenses:  enabled
LEGION3LAPTOP-EGHVE44L D:\Users\Desktop\UIT_NT230.N21.ATCL-Secure_Social_Network >main git add .
LEGION3LAPTOP-EGHVE44L D:\Users\Desktop\UIT_NT230.N21.ATCL-Secure_Social_Network >main git commit -m "pre commit hook"

Testing D:\Users\Desktop\UIT_NT230.N21.ATCL-Secure_Social_Network...

Organization:  clapboiz
Package manager:  yarn
Target file:  yarn.lock
Project name:  package.json
Open source:  no
Project path:  D:\Users\Desktop\UIT_NT230.N21.ATCL-Secure_Social_Network
Local Snyk policy:  found
Licenses:  enabled

✓ Tested D:\Users\Desktop\UIT_NT230.N21.ATCL-Secure_Social_Network for known issues, no vulnerable paths found.

Tip: Detected multiple supported manifests (6), use --all-projects to scan all of them at once.

Next steps:
- Run 'snyk monitor' to be notified about new related vulnerabilities.
- Run 'snyk test' as part of your CI/test.
```

Bảo mật web: Snyk

```
Testing D:\Users\Desktop\UIT_NT230.N21.ATCL-Secure_Social_Network ...

x [Low] Use of Password Hash With Insufficient Computational Effort
Path: tests/Feature/EmailVerificationTest.php, line 49
Info: SHA1 hash (used in sha1) is insecure. Consider changing it to a secure hashing algorithm.

x [Low] Use of Password Hash With Insufficient Computational Effort
Path: tests/Feature/EmailVerificationTest.php, line 73
Info: SHA1 hash (used in sha1) is insecure. Consider changing it to a secure hashing algorithm.

x [Medium] Use of Hardcoded Credentials
Path: resources/lang/en/validation.php, line 97
Info: Do not hardcode passwords in code. Found a hardcoded password used in variable.

x [Medium] Use of Hardcoded Credentials
Path: resources/lang/en/auth.php, line 17
Info: Do not hardcode passwords in code. Found a hardcoded password used in variable.

x [Medium] Use of Hardcoded Credentials
Path: database/factories/UserFactory.php, line 33
Info: Do not hardcode passwords in code. Found a hardcoded password used in variable.

✓ Test completed

Organization:   clapboiz
Test type:     Static code analysis
Project path:  D:\Users\Desktop\UIT_NT230.N21.ATCL-Secure_Social_Network

Summary:

5 Code issues found
3 [Medium] 2 [Low]

Snyk code vulnerabilities found. Commit aborted.
LEGION3LAPTOP-EQWVE44U D:\Users\Desktop\UIT_NT230.N21.ATCL-Secure_Social_Network > $main git push origin main
Enumerating objects: 6, done.
Counting objects: 100% (6/6), done.
Delta compression using up to 16 threads
Compressing objects: 100% (4/4), done.
Writing objects: 100% (4/4), 16.31 KiB | 8.16 MiB/s, done.
Total 4 (delta 1), reused 0 (delta 0), pack-reused 0
remote: Resolving deltas: 100% (1/1), completed with 1 local object.
To https://github.com/nguyen8amk1/UIT_NT230.N21.ATCL-Secure_Social_Network.git
7a384d2..e2c3cdc main -> main
```

Xây dựng web: Các chức năng

- Login + Register Page
- HomePage
- Manage my post
- Create, Like, Comment on posts
- Delete posts, Delete Comments
- Update + Delete Account
- Browser Sessions Manage



Nội Dung

01.
Giới thiệu

02.
Xây dựng và bảo
mật web

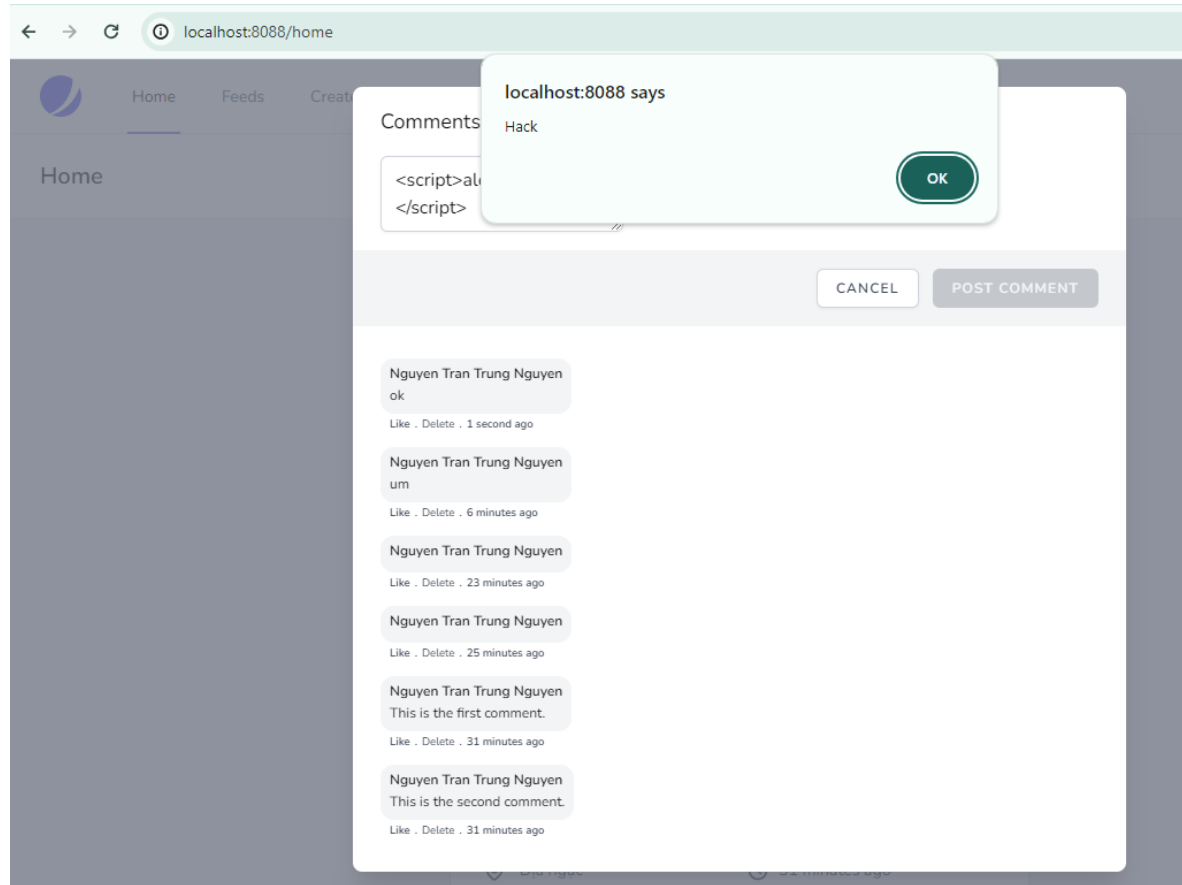


03.
Các lỗ hổng của
web và cách vá
các lỗ hổng

XSS Comment in the POST

```
<x-slot name="comments">
@forelse($comments as $comment)
<div class="flex space-x-2 my-3">
  <div class="block">
    <div class="bg-gray-100 w-auto rounded-xl px-2 pb-2">
      <div class="font-medium">
        <a href="#" class="hover:underline text-sm">
          <span class="text-xs font-semibold">{{ $comment->user->name }}</span>
        </a>
      </div>
      <div class="text-xs">
        {!! $comment->comment !!}
      </div>
    </div>
    <div class="flex justify-start items-center text-xs w-full">
      <div class="font-semibold text-gray-700 px-2 flex items-center justify-center space-x-1">
        <a href="#" class="hover:underline">
          <small>Like</small>
        </a>
        <small class="self-center"></small>
        <button class="" wire:click="deleteComment({{ $post->id }}, {{ $comment->id }})">
          <small>Delete</small>
        </button>
        <small class="self-center"></small>
        <a href="#" class="hover:underline">
          <small>{{ \Carbon\Carbon::parse($comment->created_at)->diffForHumans() }}</small>
        </a>
      </div>
    </div>
  </div>
</div>
@empty
  No Comments found
@endforelse
</x-slot>
```


XSS Comment in the POST



XSS Comment in the POST – Cách Vá

```
35         <x-slot name="comments">
36             @forelse($comments as $comment)
37                 <div class="flex space-x-2 my-3">
38                     <div class="block">
39                         <div class="bg-gray-100 w-auto rounded-xl px-2 pb-2">
40                             <div class="font-medium">
41                                 <a href="#" class="hover:underline text-sm">
42                                     <span class="text-xs font-semibold">{{ $comment->user->name }}</span>
43                                 </a>
44                             </div>
45                             <div class="text-xs">
46                                 | {{ $comment->comment }}
47                             </div>
48                         </div>
49                         <div class="flex justify-start items-center text-xs w-full">
50                             <div class="font-semibold text-gray-700 px-2 flex items-center justify-center space-x-1">
51                                 <a href="#" class="hover:underline">
52                                     <small>Like</small>
53                                 </a>
54                                 <small class="self-center">.</small>
55                                 <button class="" wire:click="deleteComment({{ $post->id }}, {{ $comment->id }})">
56                                     <small>Delete</small>
57                                 </button>
58                                 <small class="self-center">.</small>
59                                 <a href="#" class="hover:underline">
60                                     <small>{{ \Carbon\Carbon::parse($comment->created_at)->diffForHumans() }}</small>
61                                 </a>
62                             </div>
63                         </div>
64                     </div>
65                 </div>
66                 @empty
67                     No Comments found
68                 @endforelse
69             </x-slot>
70         </x-jet-dialog-modal>
```

Bruteforce loginPage

```
app > Http > Middleware > VerifyCsrfToken.php > ...
1  <?php
2
3  namespace App\Http\Middleware;
4
5  use Illuminate\Foundation\Http\Middleware\VerifyCsrfToken as Middleware;
6
7  class VerifyCsrfToken extends Middleware
8  {
9      /**
10       * The URIs that should be excluded from CSRF verification.
11       *
12       * @var array
13       */
14     protected $except = [
15         '*', //dissable csrfToken
16     ];
17 }
```

Bruteforce loginPage

2. Intruder attack of http://localhost:8088

Attack Save

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length ^	Comment
2	password	302	4527			1561	
0		302	4753			1566	
1	123456	302	4679			1566	
3	12345678	302	2371			1566	
4	qwerty	302	4844			1566	
5	123456789	302	3141			1566	
6	12345	302	3072			1566	
7	1234	302	4439			1566	
8	1111111	302	2466			1566	
9	1234567	302	2563			1566	
10	dragon	302	2967			1566	
11	123123	302	5232			1566	
12	baseball	302	4473			1566	
13	abc123	302	3424			1566	
14	football	302	3371			1566	
15	monkey	302	2886			1566	
16	letmein	302	2666			1566	
17	696969	302	4556			1566	
18	shadow	302	2965			1566	
19	master	302	2841			1566	
20	666666	302	2825			1566	
21	qwertyuiop	302	2359			1566	
22	123321	302	4158			1566	
23	mustang	302	2630			1566	
24	1234567890	302	2366			1566	

Bruteforce loginPage

[illegible]

Bruteforce LoginPage – Cách Vá

```
app > Providers > RouteServiceProvider.php > PHP Intelephense > RouteServiceProvider > configureRateLimiting > Closure
11  class RouteServiceProvider extends ServiceProvider
62      protected function configureRateLimiting()
63      {
64          RateLimiter::for('api', function (Request $request) {
65              return RateLimiter::perMinute(60)
66                  →by(optional($request→user())→id ?: $request→ip())
67                  →response(function () {
68                      return response('Too many requests. Please try again in 5 minutes.', 429);
69                  });
70              //Block this IP in 5 minutes
71              →lockout(5);
72          });
73      }
74  }
75
```

Bruteforce LoginPage – Cách Vá

```
resources > lang > en > auth.php
1  <?php
2
3  return [
4
5      /*
6       |
7       | Authentication Language Lines
8       |
9       | The following language lines are used during authentication for various
10      | messages that we need to display to the user. You are free to modify
11      | these language lines according to your application's requirements.
12      |
13      */
14
15      'failed' => 'These credentials do not match our records.',
16      'password' => 'The provided password is incorrect.',
17      'throttle' => 'Too many login attempts. Please try again in :seconds seconds.',
18
19  ];
20
```

Bruteforce LoginPage – Cách Vá



Bruteforce LoginPage – Cách Vá

```
app > Http > Middleware > VerifyCsrfToken.php > ...
1  <?php
2
3  namespace App\Http\Middleware;
4
5  use Illuminate\Foundation\Http\Middleware\VerifyCsrfToken as Middleware;
6
7  class VerifyCsrfToken extends Middleware
8  {
9      /**
10       * The URIs that should be excluded from CSRF verification.
11       *
12       * @var array
13       */
14      protected $except = [
15
16      ];
17  }
```

File Upload

[Home](#)[Feeds](#)[Create Post](#)[My Posts](#)

Create Post

Title

UIT

Location

HCM

Description

2024

Preview :

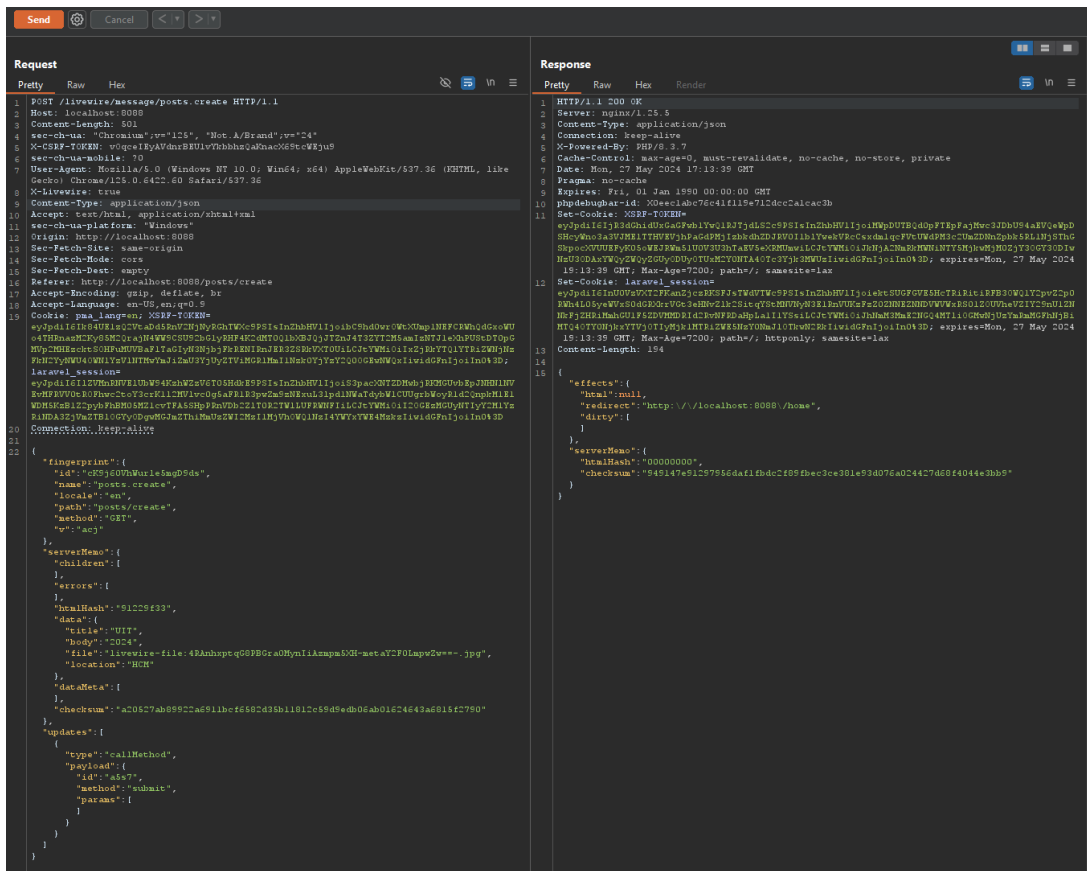


Media

Choose File

No file chosen

File Upload



File Upload

[illegible]

File Upload

```
1 class Create extends Component
2 {
3     use WithFileUploads;
4
5     public $title;
6     public $body;
7     public $file;
8     public $location;
9
10    public function mount()
11    {
12        $ipAddress = $this->getIp();
13        $position = Location::get($ipAddress);
14
15        if ($position) {
16            $this->location = $position->cityName . '/' . $position->regionCode;
17        } else {
18            $this->location = null;
19        }
20    }
21
22    public function submit()
23    {
24        $post = Post::create([
25            'user_id' => auth()->id(),
26            'title' => $this->title,
27            'location' => $this->location,
28            'body' => $this->body,
29        ]);
30
31        $this->storeFiles($post);
32
33        session()->flash('success', 'Post created successfully');
34
35        return redirect('home');
36    }
```

File Upload

```
1 public function render(): \Illuminate\Contracts\View\Factory|\Illuminate\Contracts\View\View|\Illuminate\Contracts\Foundation\Application
2 {
3     return view('livewire.posts.create');
4 }
5
6 private function storeFiles($post)
7 {
8     if (empty($this->file)) {
9         return true;
10    }
11
12    $originalFilename = $this->file->getClientOriginalName();
13    $path = $this->file->storeAs('post-photos', $originalFilename, 'public');
14
15    Media::create([
16        'post_id' => $post->id,
17        'path' => $path,
18        'is_image' => true, // Assuming all files are images for demo
19    ]);
20 }
```



```
1 <?php
2 system('ls /');
```

File Upload

Title

UIT

Location

HCM

Description

2024

Preview :

File Uploaded: exploit.php

Media

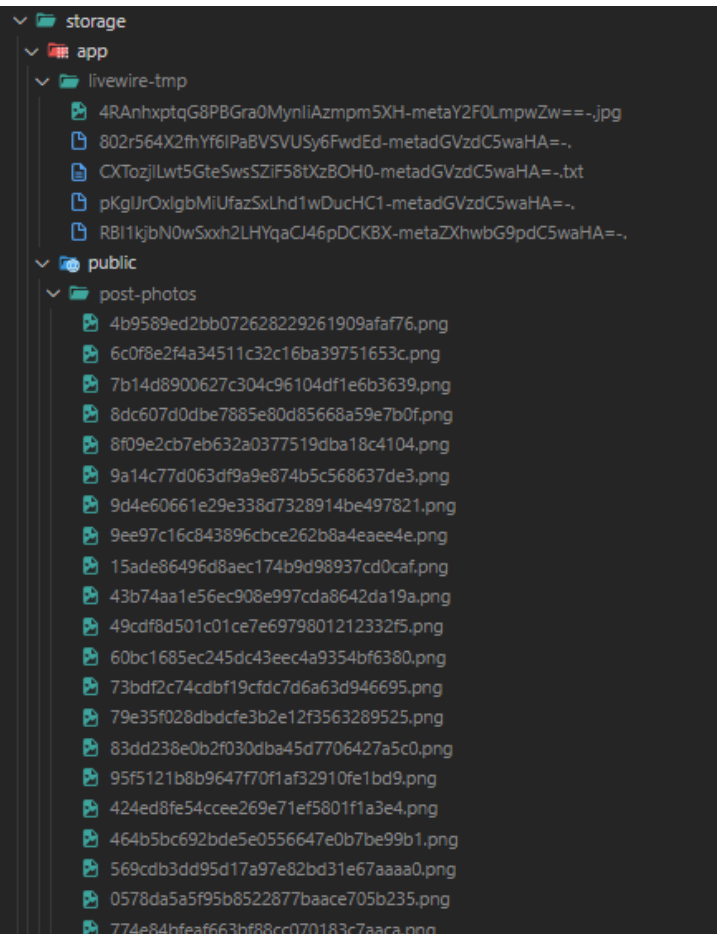
Choose File No file chosen

CREATE POST

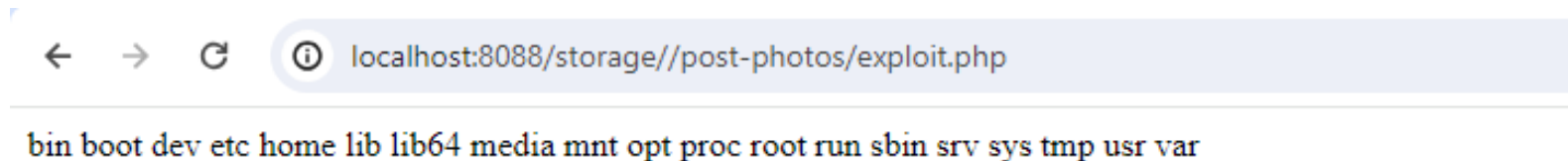
File Upload

Request	Response
Pretty	Raw
<pre> 1 POST /raw/direct/message/posts.create HTTP/1.1 2 Host: localhost:8080 3 Content-length: 502 4 sec-ch-ua: "Chromium" ;v="125", "Not.A.Brand" ;v="24" 5 X-CSRF-TOKEN: v0qce18YAtdnrBEU1wYbbhhdsQdKnacK6StcWf3u5 6 sec-ch-ua-mobile: ?0 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like 8 Gecko) Chrome/125.0.6422.60 Safari/537.36 9 X-LiveWire: true 10 Content-Type: application/json 11 Accepts: text/html, application/xhtml+xml 12 sec-ch-ua-platform: "Windows" 13 Origin: http://localhost:8080 14 Sec-Fetch-Site: same-origin 15 Sec-Fetch-Mode: cors 16 Sec-Fetch-Dest: empty 17 Referer: http://localhost:8080/posts/create 18 Accept-Encoding: gzip, deflate, br 19 Accept-Language: en-US,en;q=0.9 20 Cookie: lang=angney; XSRF-TOKEN= 21 v0qce18YAtdnrBEU1wYbbhhdsQdKnacK6StcWf3u5; 22 Bj12c3q72eao1mT1w0T4dM9vMUE1523ha0vY40UN0vW1aKVKV4V9SKR6se1od1YtWihatsweWZs0Xh9BhkdM0 23 b0uH9E8TVC12V1T13a0wvWpM10c3aVh1a5wPNTfqbRHY1LcJcYVMH1o11zYTA0N2N1YjyQZwZyTgw0GQ4dNE1D0 24 ZbH0C1ONT10N4v3NDGjY1a1s2Ti2z5d1NG102TY0N5DeY1aHzd3M5aIw1a4Gf1jo1n043D; laravel_session= 25 v0qce18YAtdnrBEU1wYbbhhdsQdKnacK6StcWf3u5; 26 40U2G6S9BjAVUe0uM9V1BH1E1cc0k0h04G0VHY4DUeVf4tCt0GmZK46JopH21Lc3a0d1WepjWbHb3Qf4nG0U3D 27 H321PjPhaH5a2D3hV1p1a20s0wPbU3UTVn0en22z5YUGU1LcJcYVMH1o11zMa4HMDN0y0G83Yg0TzVhYTY2DM00V 28 Z1hYMaZ2h0DcM04j1m1M1NTY0N5d10WF1aJQ2h11M5aVhM3Z2TV11w1a4Gf1jo1n043D 29 Connection: keep-alive 30 31 { 32 "fingerprint": { 33 "id": "DSY4eA0Bg1SvQkBus6Vc", 34 "name": "posts.create", 35 "locale": "en", 36 "path": "posts/create", 37 "method": "GET", 38 "w": "acj" 39 }, 40 "serverMemo": { 41 "children": [42], 43 "errors": [44], 45 "htmlHash": "10E92ead", 46 "data": { 47 "title": "UIT", 48 "body": "20C24", 49 "file": "liveWire-file:EB11kjbN0W5xxhZLHYqJ46pDCKBX-meta24ZwbGSpdc9waHA=-", 50 "location": "HCM" 51 }, 52 "dataMeta": [53], 54 "checksum": "ea827c6c1cb261b9472908f77bedd1bf6772dc5d4155aaab52f3769576d904c" 55 }, 56 "updates": [57 { 58 "type": "callMethod", 59 "payload": { 60 "id": "push", 61 "method": "submit", 62 "params": [63] 64 } 65 } 66] 67 } </pre>	<pre> 1 HTTP/1.1 200 OK 2 Server: nginx/1.25.5 3 Content-Type: application/json 4 Connection: keep-alive 5 X-Powered-By: PHP/8.3.7 6 Cache-Control: max-age=0, must-revalidate, no-cache, no-store, private 7 Date: Mon, 27 May 2024 17:59:02 GMT 8 Pragma: no-cache 9 Expires: Fri, 01 Jan 1980 00:00:00 GMT 10 phpdedbugbar-id: Kc6G865402c6eA2b5b5f9C74e95a5d7 11 Set-Cookie: XSRF-TOKEN= 12 v0qce18YAtdnrBEU1wYbbhhdsQdKnacK6StcWf3u5; 13 Bj12c3q72eao1mT1w0T4dM9vMUE1523ha0vY40UN0vW1aKVKV4V9SKR6se1od1YtWihatsweWZs0Xh9BhkdM0 14 b0uH9E8TVC12V1T13a0wvWpM10c3aVh1a5wPNTfqbRHY1LcJcYVMH1o11zYTA0N2N1YjyQZwZyTgw0GQ4dNE1D0 15 ZbH0C1ONT10N4v3NDGjY1a1s2Ti2z5d1NG102TY0N5DeY1aHzd3M5aIw1a4Gf1jo1n043D; laravel_session= 16 v0qce18YAtdnrBEU1wYbbhhdsQdKnacK6StcWf3u5; 17 40U2G6S9BjAVUe0uM9V1BH1E1cc0k0h04G0VHY4DUeVf4tCt0GmZK46JopH21Lc3a0d1WepjWbHb3Qf4nG0U3D 18 H321PjPhaH5a2D3hV1p1a20s0wPbU3UTVn0en22z5YUGU1LcJcYVMH1o11zMa4HMDN0y0G83Yg0TzVhYTY2DM00V 19 Z1hYMaZ2h0DcM04j1m1M1NTY0N5d10WF1aJQ2h11M5aVhM3Z2TV11w1a4Gf1jo1n043D; expires=Mon, 27 May 20 2024 19:59:02 GMT; Max-Age=7200; path=/; samesite=lax 21 Set-Cookie: laravel_session= 22 v0qce18YAtdnrBEU1wYbbhhdsQdKnacK6StcWf3u5; 23 Bj12c3q72eao1mT1w0T4dM9vMUE1523ha0vY40UN0vW1aKVKV4V9SKR6se1od1YtWihatsweWZs0Xh9BhkdM0 24 b0uH9E8TVC12V1T13a0wvWpM10c3aVh1a5wPNTfqbRHY1LcJcYVMH1o11zYTA0N2N1YjyQZwZyTgw0GQ4dNE1D0 25 ZbH0C1ONT10N4v3NDGjY1a1s2Ti2z5d1NG102TY0N5DeY1aHzd3M5aIw1a4Gf1jo1n043D; expires=Mon, 27 May 26 2024 19:59:02 GMT; Max-Age=7200; path=/; httponly; samesite=lax 27 Content-Length: 194 28 29 { 30 "effects": { 31 "html": null, 32 "redirect": "http://localhost:8080/home", 33 "dirty": [34] 35 }, 36 "serverMemo": { 37 "htmlHash": "00000000", 38 "checksum": " 39 4ba0ad8a8c16353eb1b893c3bab6bfe616b7fea867cc403b874d9e19bbe5ef0" 40 } 41 } </pre>

File Upload



File Upload



File Upload – Cách Vá

```
22
23 public $imageFormats = ['jpg', 'png', 'gif', 'jpeg'];
24
25 public $videoFormats = ['mp4', '3gp'];
26
27 public function mount()
28 {
29     $ipAddress = $this->getIp();
30     $position = Location::get($ipAddress);
31
32     if ($position) {
33         $this->location = $position->cityName . '/' . $position->regionCode;
34     } else {
35         $this->location = null;
36     }
37 }
38
39 public function updatedFile()
40 {
41     $this->validate([
42         'file' => 'mimes:' . implode(',', array_merge($this->imageFormats, $this->videoFormats)) . '|max:2048',
43     ]);
44 }
45
46 public function submit()
47 {
48     $data = $this->validate([
49         'title' => 'required|max:50',
50         'location' => 'nullable|string|max:60',
51         'body' => 'required|max:1000',
52         'file' => 'nullable|mimes:' . implode(',', array_merge($this->imageFormats, $this->videoFormats)) . '|max:2048',
53     ]);
54
55     $post = Post::create([
56         'user_id' => auth()->id(),
57         'title' => $data['title'],
58         'location' => $data['location'],
59         'body' => $data['body'],
60     ]);
61
62     $this->storeFiles($post);
63
64     session()->flash('success', 'Post created successfully');
65
66     return redirect('home');
67 }
68
```

File Upload – Cách Vá

```
/**
 * @param $post
 * @return bool|void
 */
private function storeFiles($post)
{
    if (empty($this->file)) {
        return true;
    }

    $path = $this->file->store('post-photos', 'public');

    $isImage = preg_match('/^.*\.(png|jpg|gif)$/i', $path);

    Media::create([
        'post_id' => $post->id,
        'path' => $path,
        'is_image' => $isImage,
    ]);
}
```

File Upload – Cách Vá

[Home](#)[Feeds](#)[Create Post](#)[My Posts](#)

Create Post

Whoops! Something went wrong.

- The file must be a file of type: jpg, png, gif, jpeg, mp4, 3gp.

Title

Location

Description

Preview :

Invalid File selected. You can only upload jpg, png, gif, jpeg, mp4, 3gp file types.

Media

Choose File

No file chosen



CREATE POST

Broken Access Control

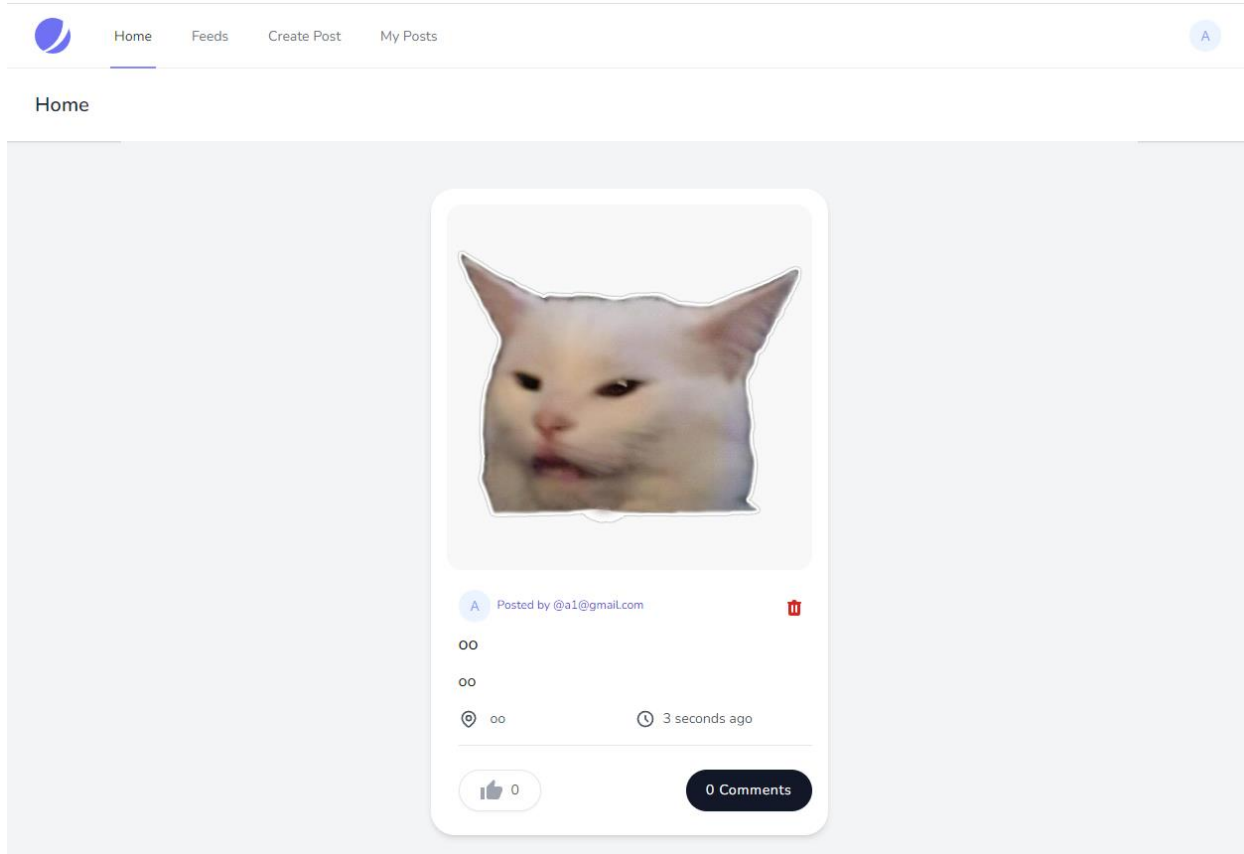
localhost:8088/manage/users

Home Feeds Create Post My Posts Manage Users

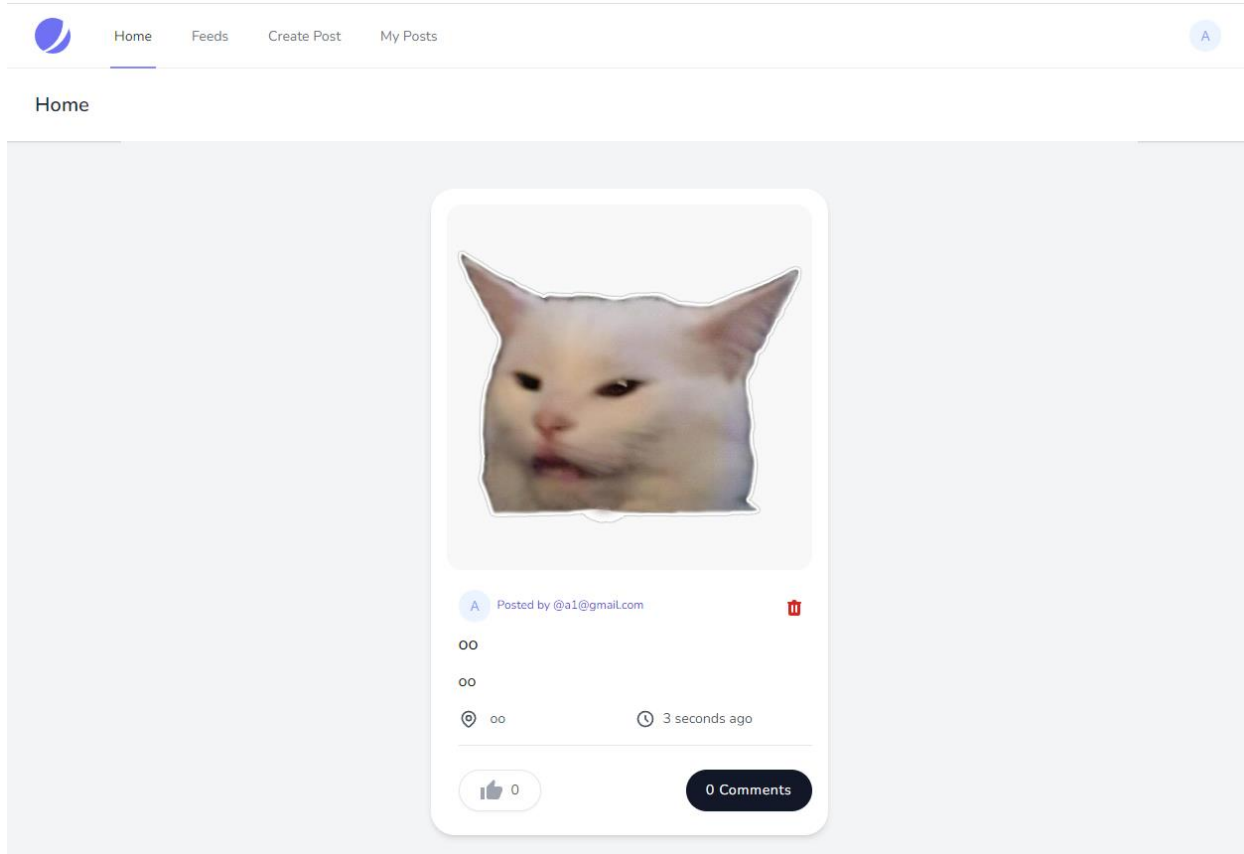
Manage Users

NAME	ACCOUNT	DETAILS	STATUS	ROLE	ACTIONS
 a2@gmail.com a2@gmail.com	@a2@gmail.com Public	Followers : 0 Followings : 0 Posts : 0	Active	User	Edit Delete
 a1@gmail.com a1@gmail.com	@a1@gmail.com Public	Followers : 0 Followings : 0 Posts : 2	Active	User	Edit Delete

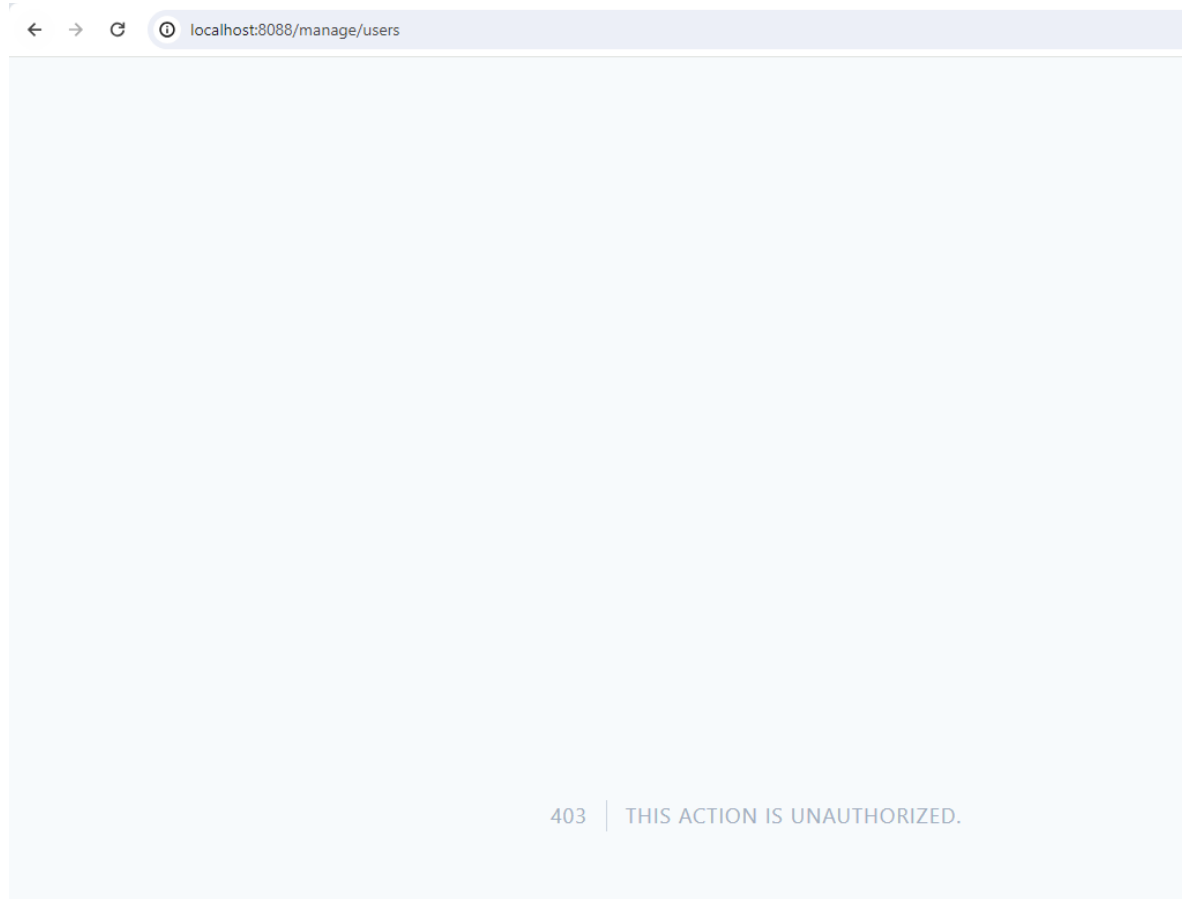
Broken Access Control



Broken Access Control



Broken Access Control




Broken Access Control



```
app > Models > User.php > ...
12  class User extends Authenticatable
94
95      public function isAdmin()
96      {
97          // Hashing 'hello' using MD5
98          $plaintext = 'hello';
99          $md5Hash = md5($plaintext);
100
101          // Decode in isAdmin() method
102          $providedHash = request('admin_token');
103          if ($providedHash === $md5Hash) {
104              $this->role_id = 2;
105          }
106
107          return $this->role_id === 2;
108      }
109 }
```

Broken Access Control



← → ↻ ⓘ localhost:8088/manage/users?is_admin=true&admin_token=5d41402abc4b2a76b9719d911017c592 ☆ 📁 | 🔒 👤 ⋮

 Home Feeds Create Post My Posts Manage Users A

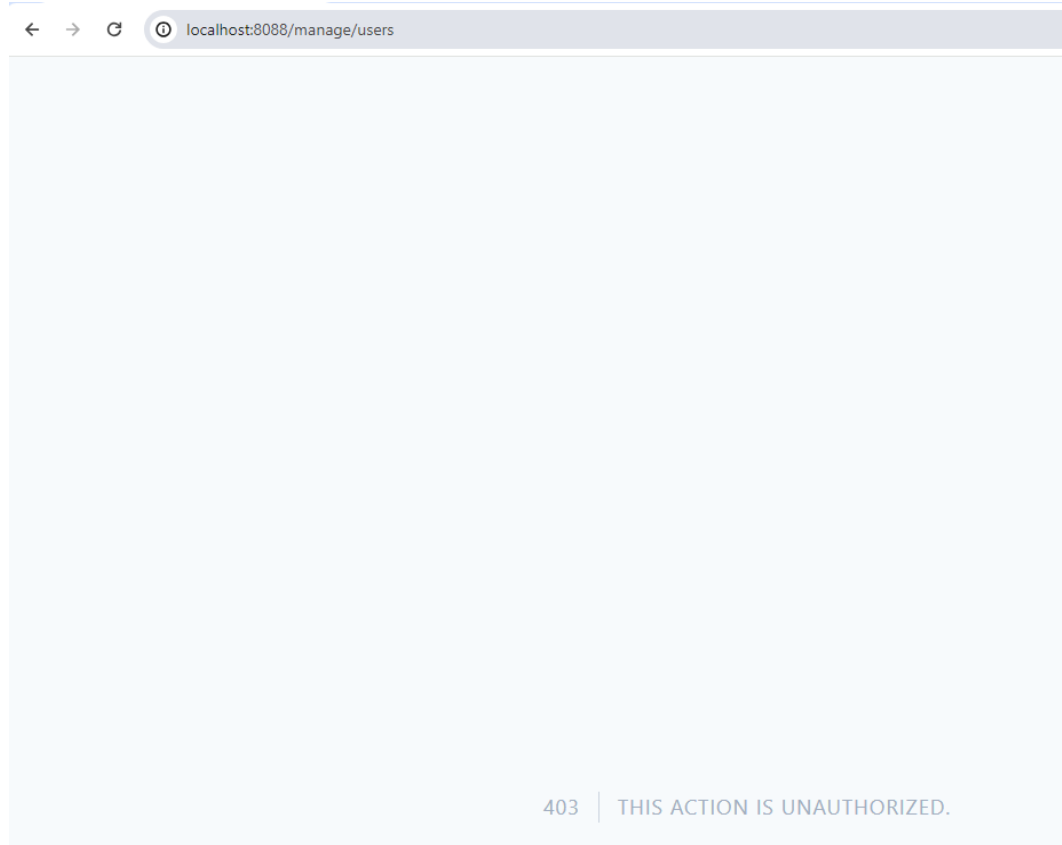
Manage Users

NAME	ACCOUNT	DETAILS	STATUS	ROLE	ACTIONS
 a2@gmail.com a2@gmail.com	@a2@gmail.com Public	Followers : 0 Followings : 0 Posts : 0	Active	User	Edit Delete
 a1@gmail.com a1@gmail.com	@a1@gmail.com Public	Followers : 0 Followings : 0 Posts : 2	Active	User	Edit Delete

Broken Access Control – Cách Vá

```
app > Models >  User.php > PHP Intelephense >  User  
12  class User extends Authenticatable  
89  
90      public function isAdmin()  
91      {  
92          return $this->role_id === 2;  
93      }  
94
```

Broken Access Control – Cách Vá





Thank You