



Looting the Symphony Profiler with EOS



Pass The Salt 2020

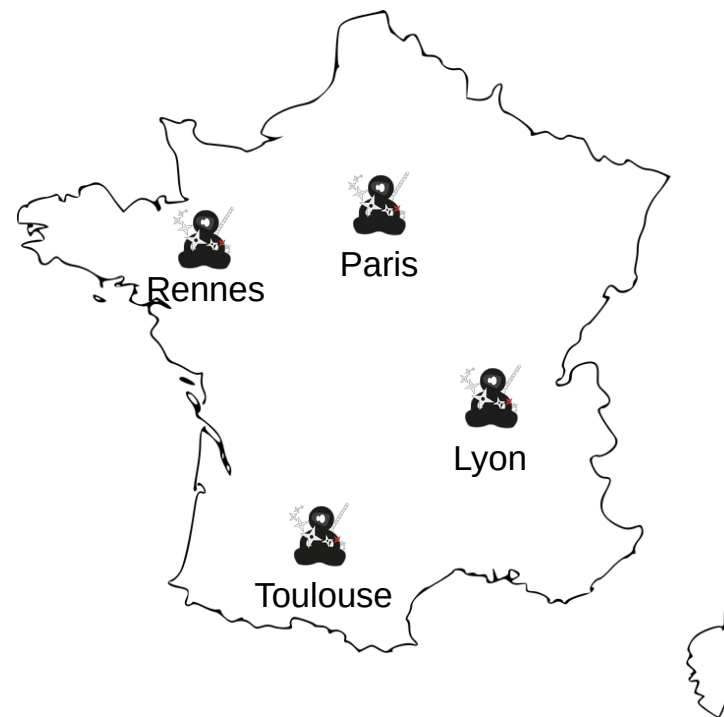
 Matthieu Barjole (@__aevy__)




Synacktiv

■ French IT security company

- Focus on offensive security
- 3 teams
 - Pentest
 - Reverse engineering
 - Development
- Remote friendly !
- ***apply@synacktiv.com***



Context

-  popular PHP framework for web applications
- Debug features exposed during assessments: web profiler
 - Wanna loot
 - Wanna automate

Context > Disclaimer

- **Not a Symfony vulnerability**

“ *The profiler is a powerful development tool that gives detailed information about the execution of any request. **Never enable the profiler in production environments** as it will lead to major security vulnerabilities in your project.* ”

Loot > Profiler

- Version dependent Kernel instantiation
 - `web/app.php + web/app_dev.php`
 - `public/index.php`

Loot > Profiler Toolbar

Welcome to the **Symfony Demo** application

Browse the **public section** of the demo application.

 Browse application

Browse the **admin backend** of

Profiler token [9cb45e](#)

Environment dev

Debug **enabled**

PHP version 7.3.11 [View phpinfo\(\)](#)

PHP Extensions **xdebug** **APCu** **OPcache** ✓

PHP SAPI cli-server

Resources [Read Symfony 5.0.1 Docs](#)

Help [Symfony Support Channels](#)

200

@ homepage

20 ms

2.0 MB



5



6



anon.



3 ms



Server



5.0.1



Loot > Phpinfo

PHP Variables

Variable	Value
<code>\$_SERVER['SYMFONY_DOTENV_VARS']</code>	SITE_URL,APP_ENV,APP_SECRET,MAILER_URL,DATABASE_URL,REDIS_HOST,MONGODB_URL,MONGODB_DB
<code>\$_ENV['SITE_URL']</code>	http://localhost
<code>\$_ENV['APP_ENV']</code>	dev
<code>\$_ENV['APP_SECRET']</code>	67d829bf61dc5f87a73fd814e2c9f629
<code>\$_ENV['MAILER_URL']</code>	smtp://:@172.16.0.12:25
<code>\$_ENV['DATABASE_URL']</code>	mysql://dbuser:s3cr3t@127.0.0.1/mock
<code>\$_ENV['REDIS_HOST']</code>	redis://172.16.0.11:6379
<code>\$_ENV['MONGODB_URL']</code>	mongodb://dbuser:m0ng0p@\$@\$@127.0.0.1:27017
<code>\$_ENV['MONGODB_DB']</code>	mockgo

Loot > Requests > Routes

http://localhost/a/x/e/f/o/e/g/s/o/s/w/i

Forwarded to: ErrorController (1f1075)

Method: GET HTTP Status: 404 IP: 172.17.0.1 Profiled on: Fri, 15 May 2020 13:33:05 +0000 Token: 81f68f

Last 10 Latest Search

Request / Response

Performance

Validator

Forms

Exception 1

Logs 1

Events

Routing

Cache

#	Route name	Path	Log
13	admin_index	/_{locale}/admin/post/	Path does not match
14	admin_post_index	/_{locale}/admin/post/	Path does not match
15	admin_post_new	/_{locale}/admin/post/new	Path does not match
16	admin_post_show	/_{locale}/admin/post/{id}	Path does not match
17	admin_post_edit	/_{locale}/admin/post/{id}/edit	Path does not match
18	admin_post_delete	/_{locale}/admin/post/{id}/delete	Path does not match
19	blog_index	/_{locale}/blog/	Path does not match
20	blog_rss	/_{locale}/blog/rss.xml	Path does not match
21	blog_index_paginated	/_{locale}/blog/page/{page}	Path does not match
22	blog_post	/_{locale}/blog/posts/{slug}	Path does not match

Loot > Requests > Credentials

http://localhost/en/login [Return to referer URL](#)

Method: POST HTTP Status: 302 IP: 172.17.0.1 Profiled on: Fri, 24 Apr 2020 00:43:21 +0000 Token: 6878fc

Last 10 Latest Search

Request / Response Performance Validator Forms Exception Logs Events Routing Cache Translation

Request Response Cookies Session Flashes Server Parameters

POST Parameters

Key	Value
_csrf_token	"wSoX3-RFRS0c0JnXnXFkWPWmuE0xmY1MnLabaqshSQ"
_password	"*****"
_target_path	" "
_username	"jane_admin"

Request Content

Raw

```
_username=jane_admin&_password=s3cr3t&_target_path=&_csrf_token=wSoX3-RFRS0c0JnXnXFkWPWmuE0xmY1MnLabaqshSQ
```

Loot > Requests > Remember Me Cookies

- Not enabled by default

```
protected function generateCookieHash(string $class, string $username,  
int $expires, string $password)  
{  
    return hash_hmac(  
        'sha256',  
        $class.self::COOKIE_DELIMITER.$username.self::COOKIE_DELIMITER.  
$expires.self::COOKIE_DELIMITER.$password,  
        $this->getSecret());  
}
```

Loot > Requests > Remember Me Cookies

`$_ENV['APP_SECRET']`

67d829bf61dc5f87a73fd814e2c9f629

http://localhost/en/login [Return to referer URL](#)

Method: POST HTTP Status: 302 IP: 172.17.0.1 Profiled on: Fri, 15 May 2020 15:18:13 +0000 Token: 3dc5b3

Last 10 Latest Search

Request Response Cookies Session Flashes Server Parameters

Request / Response Performance Validator Forms Exception

Session Attributes

Attribute	Value
<code>_csrf/authenticate</code>	<code>"kjGjxPKcpd711UkBALd6doa1qBomEBjYfqS5uf6rwVU"</code>
<code>_security_main</code>	<code>"C:74:"Symfony\Component\Security\Core\Authentication\Token\UsernamePasswordToken":271:{a:3:{i:0;N;i:1;s:4:"main";i:2;a:5:{i:0;C:15 "App\Entity\User" 145:{a:3:{i:0;i:1;i:1;s:10:"jane_admin";i:2;s:97:"\$argon2id\$v=19\$m=65536,t=4,p=1\$twoEeFEvfRnJ8T8UvjSDfg\$1i72DYn5RsUz6lpv3T082c7pJSkfrCobp0rpDIICE";}}i:1;b:1;i:2;N;i:3;a:0:{i:4;a:1:{i:0;s:10:"ROLE_ADMIN";}}}}"</code>

`base64(hmac("App\\Entity\\User:amFuZV9hZG1pbG==:1620664267:c05a2...e9b8b"))`

Loot > Files

src/Controller/Admin/BlogController.php line 57

```
55.      * @Route("/", methods={"GET"}, name="admin_post_index")
56.      */
57.      public function index(PostRepository $posts): Response
58.      {
59.          $authorPosts = $posts->findBy(['author' => $this->getUser()], ['publishedAt' => 'DESC']);
60.
61.          return $this->render('admin/blog/index.html.twig', ['posts' => $authorPosts]);
62.      }
63.
64.      /**
65.       * Creates a new Post entity.
66.       *
67.       * @Route("/new", methods={"GET", "POST"}, name="admin_post_new")
68.       *
```

Loot > Files > Config

config/services.yaml line 7

```
1. parameters:
2.     locale: 'en'
3.     app_locales: en|fr
4.     app.notifications.email_sender: no-reply@localhost
5.     images_upload_directory: '%kernel.project_dir%/public/uploads/images'
6.     images_upload_base_path: /uploads/images
7.     ldap:
8.         server: ldap.corp.local
9.         user: myapp
10.        password: s3cr3t!
11.        port: 389
```

Loot > Files > Source code

- No directory listing
- Only previously hit code paths appear on the Profiler

→ **Cache files**

Loot > Files > Source code

- `var/cache/%env%/filename.xml`
 - `env`: deployed environment, probably dev
 - `filename`: Kernel cache container file name

Loot > Files > Source code

- 2.0 – 4.1 : `srcDevDebugProjectContainer.xml`
- 4.2 – 4.4 : `srcApp_KernelDevDebugContainer.xml`
- 5.0 – 5.x : `App_KernelDevDebugContainer.xml`

Loot > Files > Source code

var/cache/dev/App_KernelDevDebugContainer.xml line 337

```
335.     <tag name="routing.route_loader"/>
336. </service>
337. <service id="App\Command\AddUserCommand" class="App\Command\AddUserCommand" autowire="true" autoconfigure="true">
338.     <tag name="console.command"/>
339.     <argument type="service" id="doctrine.orm.default_entity_manager"/>
340.     <argument type="service" id="security.user_password_encoder.generic"/>
341.     <argument type="service" id="App\Utils\Validator"/>
342.     <argument type="service" id="App\Repository\UserRepository"/>
343.     <call method="setName">
344.         <argument>app:add-user</argument>
345.     </call>
346. </service>
347. <service id="App\Command\DeleteUserCommand" class="App\Command\DeleteUserCommand" autowire="true" autoconfigure="true">
348.     <tag name="console.command"/>
349.     <argument type="service" id="doctrine.orm.default_entity_manager"/>
```

Automate

```
[+] Starting scan on http://localhost
[+] Info
[!] Symfony 5.0.1
[!] PHP 7.3.11-1~deb10u1
[!] Environment: dev
[...]
```

Request logs

```
[!] Found the following credentials with a valid session:
[!] bobadm: s3cr3t [ROLE_ADMIN]
[!] jane_admin: kitten [ROLE_ADMIN]
[...]
```

Phpinfo

```
[!] Found the following Symfony variables:
[!] APP_SECRET: 67d829bf61dc5f87a73fd814e2c9f629
[!] DATABASE_URL: mysql://dbuser:s3cr3t@127.0.0.1/mock
[!] MONGODB_URL: mongodb://dbuser:m0ng0p@$$@127.0.0.1:27017
[...]
```

Project files

```
[!] Found the following files:
[!] composer.lock
[!] config/routes.yaml
[!] config/services.yaml
[...]
```

Routes

```
[!] Found the following routes:
[!] /{_locale}/admin/post/
[!] /{_locale}/admin/post/
[!] /{_locale}/admin/post/new
[...]
```


Project sources

```
[!] Found the following source files:
[!] src/Command/AddUserCommand.php
[!] src/Command/DeleteUserCommand.php
[!] src/Command/ListUsersCommand.php
[...]
```

[+] Saved 92 files
[+] Scan completed in 0:00:21

```
output/
├── composer.lock
├── config
│   ├── routes.yaml
│   └── services.yaml
├── README.md
├── src
│   ├── Command
│   │   ├── AddUserCommand.php
│   │   ├── DeleteUserCommand.php
│   │   └── ListUsersCommand.php
│   ├── Controller
│   │   ├── Admin
│   │   │   └── BlogController.php
│   │   ├── BlogController.php
│   │   ├── SecurityController.php
│   │   └── UserController.php
│   ├── DataFixtures
│   │   └── AppFixtures.php
│   ├── Entity
│   │   ├── Comment.php
│   │   ├── Post.php
│   │   ├── Tag.php
│   │   └── User.php
│   ├── Events
│   │   └── CommentCreatedEvent.php
└── var
    ├── cache
    │   └── dev
    │       ├── App_KernelDevDebugContainer.xml
    │       ├── profiler
    │       └── index.csv
```

Automate

 **synacktiv** / **eos**

👁 Watch 2

★ Star 54

🍴 Fork 4

<> Code

! Issues 0

🔗 Pull requests 1

▶ Actions

📊 Projects 0

🛡 Security 0

📈 Insights

Enemies Of Symfony - Debug mode Symfony looter

🔑 4 commits

🌿 1 branch

📦 0 packages

🏷 0 releases

👤 1 contributor


📄 View license

Branch: master ▾

New pull request

Find file

Clone or download ▾

 aevy-syn	Clarifications and credits to Symfony		Latest commit d8393df 16 days ago
📁 eos	added cli switch -k to ignore ssl/tls cert validation		17 days ago
📄 Dockerfile	Release		18 days ago
📄 LICENSE	License		16 days ago
📄 README.md	Clarifications and credits to Symfony		16 days ago
📄 requirements.txt	Release		18 days ago
📄 setup.py	Release		18 days ago

Demo target

symfony / demo

Sponsor

Watch142

Star1.8k

Fork1.2k

<> Code

Issues14

Pull requests12

Actions

Security0

Insights

Symfony Demo Application <https://symfony.com/>

symfony

php

demo

symfony-application

1,580 commits

2 branches

0 packages

71 releases

116 contributors

MIT

Branch: master

New pull request

Find file

Clone or download

javiereguiluz

bug #1107 Updated jQuery to 3.5.1 (javiereguiluz) Latest commit b3b7d37 2 hours ago

assets	Use a more friendly message about hardcoding user details	4 months ago
bin	Updated the project to Symfony 5.0	6 months ago
config	Update markdown	2 months ago

Conclusion

- Basic tasks but now automated :)
- Do not expose debug features in prod :(



QUESTIONS ?



Thanks for your attention !

