网络安全实验室CTF—基础关 writeup

原创

今天也要美美哒 于 2020-04-14 20:52:05 发布 1353 收藏 5

分类专栏： CTF

本文链接：https://blog.csdn.net/weixin_45871855/article/details/105519140

CTF 专栏收录该内容

20 篇文章 1 订阅

订阅专栏

自己总结的解题方法，里面方法仅供查考

本文链接：https://blog.csdn.net/weixin_45871855/article/details/105519140

网络信息安全攻防学习平台--基础关

key在哪里？

安全攻防基础关1 key在哪里？

F12或Ctrl+U查看源码，得到flag

```
<html>
    <head>
        <meta http-equiv="content-type" content="text/html;charset=utf-8">
    </head>
    <body>
    key就在这里中，你能找到他吗？
        <!--key is jflsjklejflkdsjfklds-->
    </body>
```

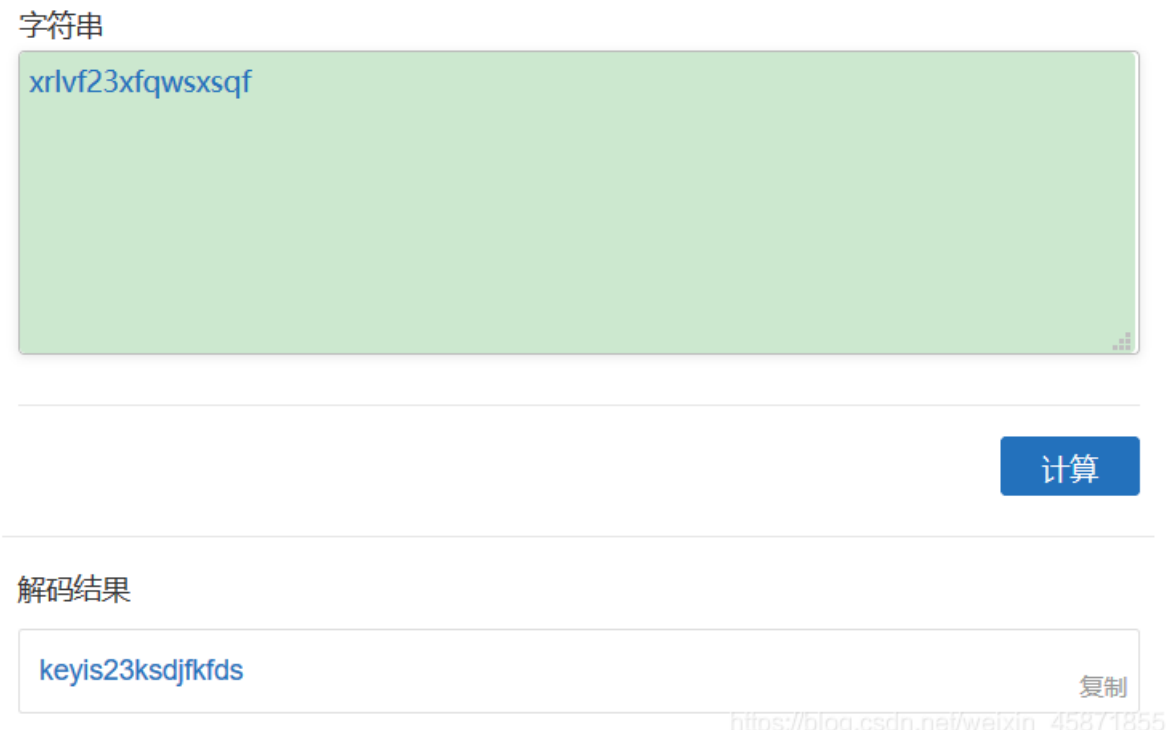
再加密一次你就得到key啦~

打开后得到

> 加密之后的数据为xrlvf23xfqwsxsqf

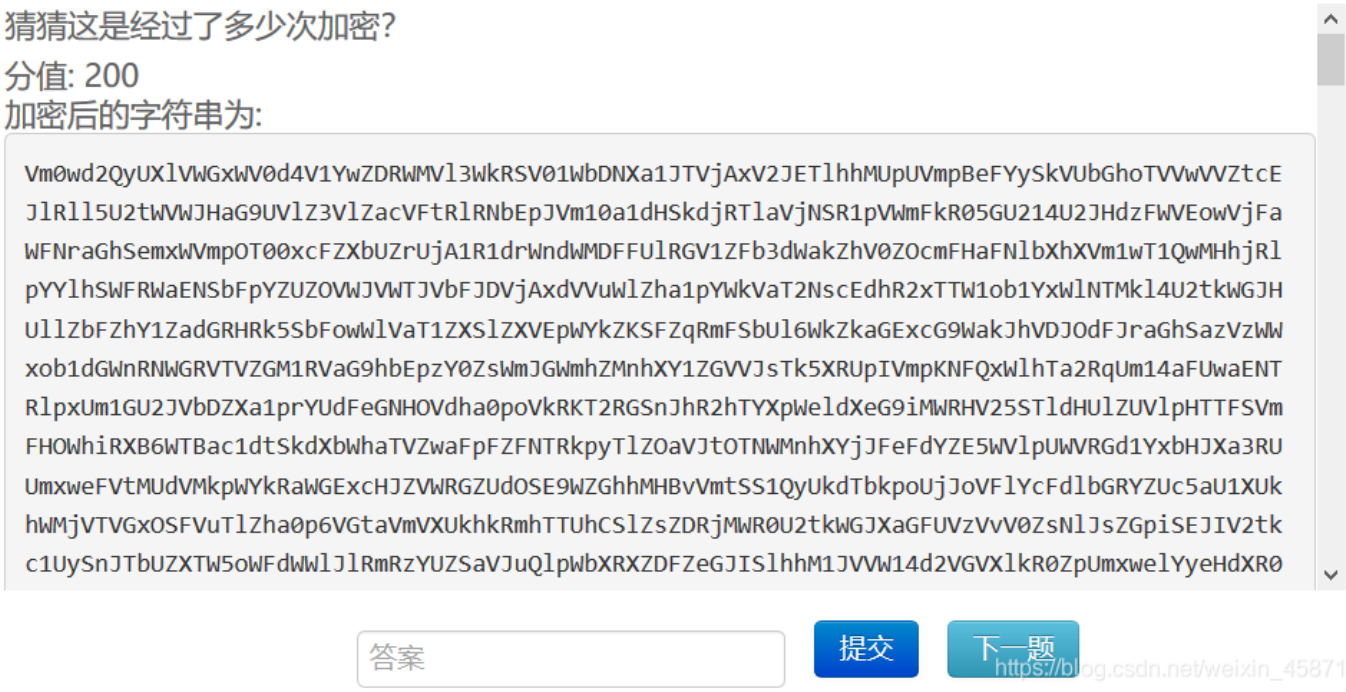
所以字符串解密一次就可得到flag
观察可能为MD5加密 或 ROT13加密
MD5解码得不到flag，使用 ROT3解码

ROT13在线解码工具



猜猜这是经过了多少次加密？

看到一堆字符串~~
看标题是加密多次的结果，所以我们得多次解密



字符串最后 “=” 应该是 BASE64编码

Base64在线加解密

多次解码得到 flag

据说MD5加密很安全，真的是么？

得到字符串 `e0960851294d7b2253978ba858e24633`

MD5在线解密工具

即可得到flag

种族歧视

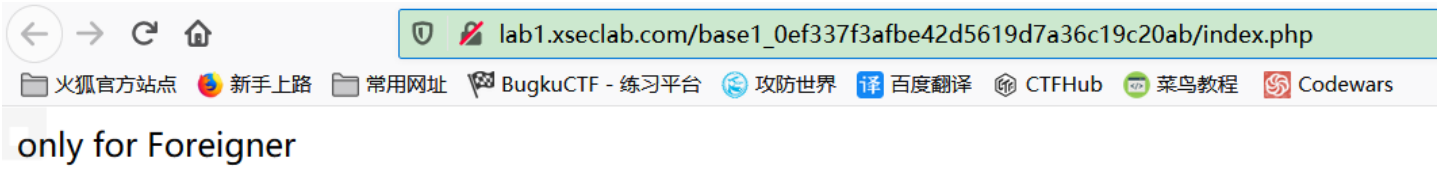
安全攻防基础关5 种族歧视

种族歧视

分值: 300

小明同学今天访问了一个网站，竟然不允许中国人访问！太坑了，于是小明同学决心一定要进去一探究竟！

通关地址

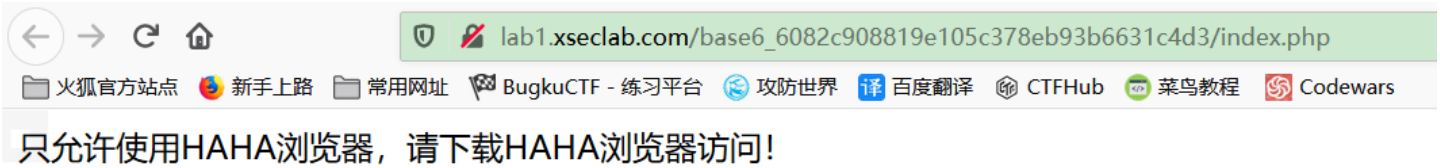



```
GET /base1_0ef337f3afbe42d5619d7a36c19c20ab/index.php HTTP/1.1
Host: lab1.xseclab.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://hackinglab.cn/ShowQues.php?type=bases
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```


将 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 中的 zh-CN,zh;zh-TW;zh-HK; 删除，得到 flag

HAHA浏览器

安全攻防基础关6 HAHA浏览器`




```
GET /base6_6082c908819e105c378eb93b6631c4d3/index.php HTTP/1.1
Host: lab1.xseclab.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://hackinglab.cn/ShowQues.php?type=bases
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```


将 User-Agent: Mozilla 改为 HAHA 得到 flag

key究竟在哪里呢？

安全攻防基础关7 key究竟在哪里呢？

使用抓包工具（burp）查看HTTP请求，在 Repeater 中查看响应头

key又找不到了

安全攻防基础关8 key又找不到了

点击 得到 “key is not here!” 抓包后 Response 依然是这个结果； 回到页面发现 url 显示： index_no_key.php，再用burp抓第一次跳转的页面得到

```
HTTP/1.1 302 Found
Server: nginx
Date: Thu, 19 Mar 2020 02:20:56 GMT
Content-Type: text/html
Connection: close
Location: http://hacklist.sinaapp.com/base8_0abd63aa54bef0464289d6a42465f354/index_no_key.php
Via: 10080
Content-Length: 224

<html>
    <head>
        <meta http-equiv="content-type" content="text/html;charset=utf-8">
    </head>
    <body>
        <a href="./key_is_here_now_.php">___</a><!--éƒ¼åʻŠè¯‰äº†åˆ°è¿™é‡Œæ‰¾keyçš„å•¦-->
    </body>
</html>
```

将Request 中的 search_key.php 改为 key_is_here_now_.php 得到 flag

冒充登录用户

安全攻防基础关9 冒充登录用户

使用抓包工具（burp）查看HTTP请求，在 Repeater 中查看响应头并改包

```
GET /base9_ab629d778e3a29540dfd60f2e548a5eb/index.php HTTP/1.1
Host: lab1.xseclab.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://hackinglab.cn/ShowQues.php?type=bases
Connection: close
Cookie: Login=0
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```


将 Cookie：login = 0 改为 1 得到 flag

比较数字大小

通过删除或修改代码或者本地代理改包进行js绕过

例：安全攻防基础关10 比较数字大小

可以看到 maxlength="3"，所以将 3 删除或者改为"null"，即可绕过，得到flag

本地的诱惑

安全攻防基础关11 本地的诱惑

本地的诱惑

分值: 200

小明扫描了他心爱的小红的电脑，发现开放了一个80端口，但是当小明去访问的时候却发现只允许从本地访问，可他心爱的小红不敢让这个诡异的小明触碰她的电脑，可小明真的想知道小红电脑的80端口到底隐藏着什么秘密(key)?

通关地址

查看源码

```
<html>
    <head>
        <meta charset="utf-8" />
    </head>
    <body>

<?php
//print_r($_SERVER);
$arr=explode(',',$_SERVER['HTTP_X_FORWARDED_FOR']);
if($arr[0]=='127.0.0.1'){
    //key
    echo "key is ^&*(UIHKJjkadshf";
}else{
    echo "必须从本地访问！";
}
?>    </body>
</html>
```

```
<?php
//SAE 服务调整,该题目无法继续...可尝试自行搭建环境测试.
echo file_get_contents(__FILE__);
```


必须本地访问，在 Request 中加入请求头 X-Forwarded-For:127.0.0.1 得到 flag

就不让你访问

就不让你访问

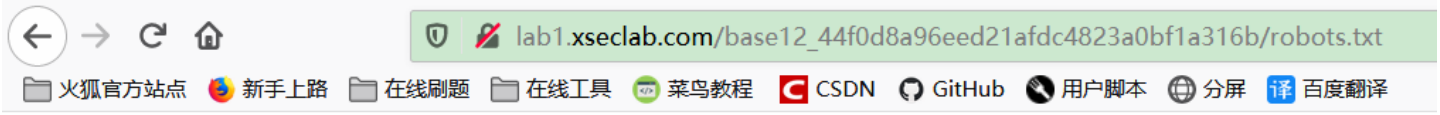
分值: 150

小明设计了一个网站，因为总是遭受黑客攻击后台，所以这次他把后台放到了一个无论是什么人都找不到的地方....可最后还是被黑客找到了，并被放置了一个黑页，写到:find you ,no more than 3 secs!

通关地址

安全攻防基础关12 就不让你访问

进入网页后显示：“I am index.php , I am not the admin page ,key is in admin page.”，尝试访问admin.php，但显示“Not Found”，查看网页是否存在robots.txt




```
User-agent: *
Disallow: /
Crawl-delay: 120
Disallow: /9fb97531fe95594603aff7e794ab2f5f/
Sitemap: http://www.hackinglab.sinaapp.com/sitemap.xml
```



```
User-agent: *
Disallow: /
Crawl-delay: 120
Disallow: /9fb97531fe95594603aff7e794ab2f5f/
Sitemap: http://www.hackinglab.sinaapp.com/sitemap.xml
```

显示有Disallow：不允许爬取的页面，将原网页index.php替换为9fb97531fe95594603aff7e794ab2f5f/访问该链接得到新的提示：“you find me,but I am not the login page. keep search.”
提示为login页面，在当前URL后添加login.php,即得到flag

最初的梦想绝对会到达，实现了真的渴望，才能够算到过了天堂。