hackinglab 基础关 writeup

转载

weixin_30249203 于 2016-06-26 22:36:00 发布 87 收藏 1
原文链接：http://www.cnblogs.com/renzongxian/p/5618087.html

地址：http://hackinglab.cn/

基础关

key在哪里？
很简单，点击过关地址，在新打开的网页中查看网页源代码就能在 HTML 注释中发现 key

```
<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~
明文加密一次得到密文，密文再加密一次得到明文，这样的加密方式是“ROT13”，将“xrlvf23xfqwsxsqf”在加密一次得到`keyis23ksdjfkfds`

3. 猜猜这是经过了多少次加密？
给了个很长的字符串，看到结尾是等号，猜测是 Base64 加密，试了试解密一次没有出错，然后写程序循环解密就行，直到不能再用 Base64 解密就输出

```
#!/usr/bin/env python3
# Author: renzongxian
import base64

s = '$给出的字符串'
s = s.encode('utf-8')
count = 0
try:
    while True:
        s = base64.decodestring(s)
        count += 1
except Exception:
    print("密文加密了%d次，解密后结果为:\n\n%s" % (count, s))
```

运行后结果是

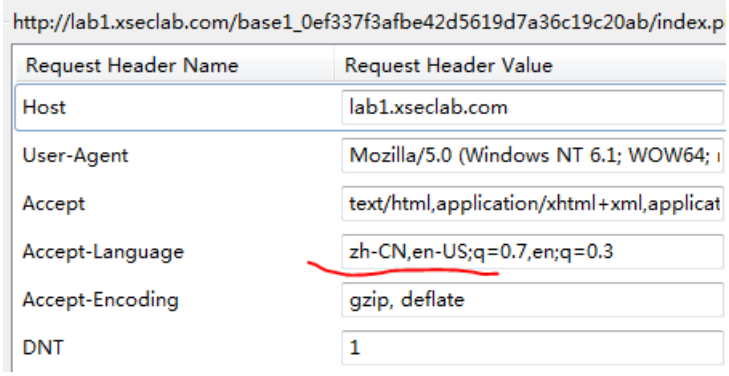
```
C:\Users\ \Desktop>python base64decode.py
密文加密了20次，解密后结果为:

b'key is jkljdkl232jkljkdl2389'
```

据说MD5加密很安全，真的是么？
md5 加密，直接扔到http://cmd5.org/里解密，结果是`bighp`

种族歧视

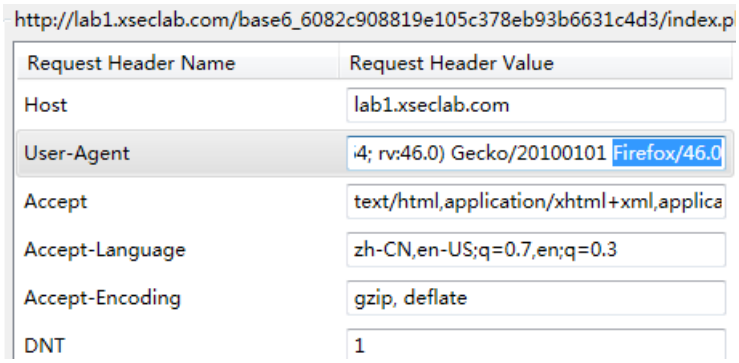
直接访问出现“only for Foreigner”，使用 Firefox 的 Tamper Data 拦截请求



Accept-Language 字段很可能就是用来限制访问的，把里面的“zh-CN,”删除，提交请求，得到`key is: *(TU687jksf6&*`

HAHA浏览器

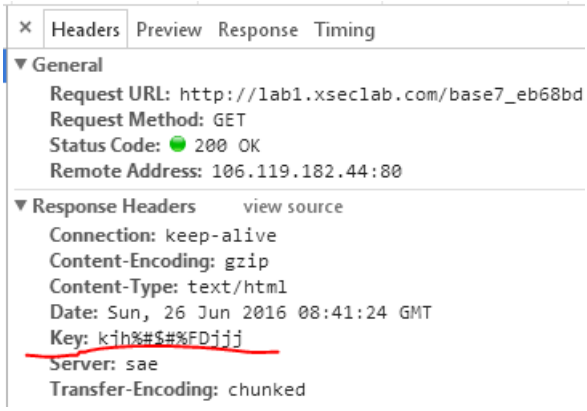
直接访问提示“只允许使用HAHA浏览器，请下载HAHA浏览器访问！”，看来是限制了 User-Agent 字段，使用 Tamper Data 拦截请求



将上图中的“Firefox/46.0”替换为“HAHA”，提交请求，得到恭喜您，成功安装HAHA浏览器！`key is: meiyouHAHAliulanqi`

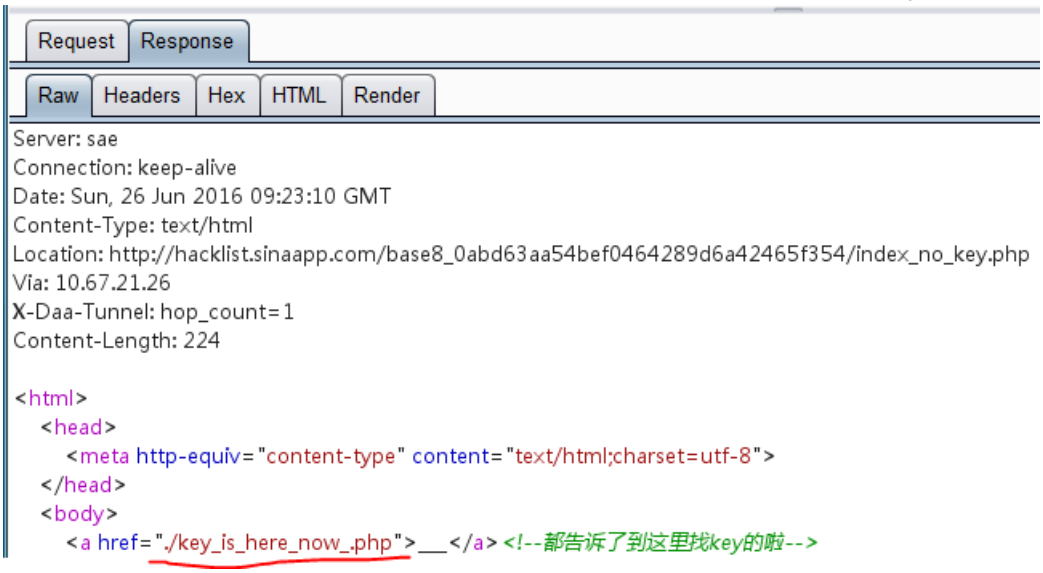
key究竟在哪里呢？

跟第1题类似，只不过这次 key 不是藏在注释里，而是藏在 Response Headers 里，使用浏览器的开发者工具可以抓到



key又找不到了

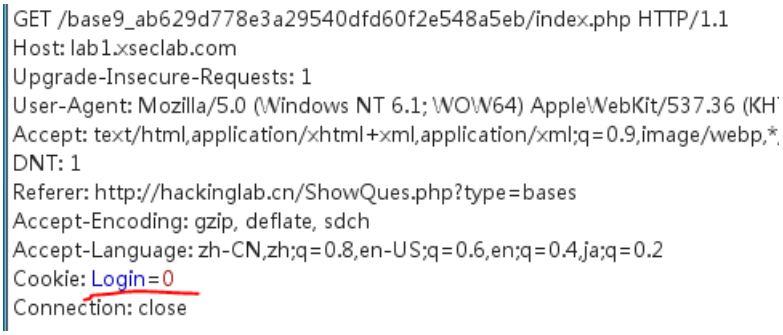
使用 Burp Suite 代理请求，发现有两个 Response，其中一个就含有 key 的地址



拼接 URL 访问得到`key： ohHTTP302dd`

冒充登陆用户

要求登陆，应该跟 Cookie 有关，使用 Burp Suite 拦截请求



发现 Cookie 的内容为“Login=0”，改为 1 后提交，即可得到`key is： yescookieedit7823789KJ`

比较数字大小

要输入一个大数字，但是却限制了数字最大长度为3

那么使用 Burp Suite 拦截请求，直接修改 POST 数据为一个大数字再提交就可以了，得到`key is 768HKyu678567&*&K`

本地的诱惑

应该是对请求头的 X-Forwarded-For 做了限制，因此拦截请求后在请求头添加该字段即可

Name	Value
Cache-Control	max-age=0
Upgrade-Insecure-Req...	1
User-Agent	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,ima
DNT	1
Referer	http://hackinglab.cn/ShowQues.php?type=bases
Accept-Encoding	gzip, deflate, sdch
Accept-Language	zh-CN,zh;q=0.8,en-US;q=0.6,en;q=0.4,ja;q=0.2
Connection	close
X-Forwarded-For	127.0.0.1

但是貌似现在不能这么做了，见下图

```
    <meta charset="utf-8">
    <!--?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！";
    }
    ?-->
    <!--?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__);--> == $0
</body>
```

网页源码给出了 key，以及题目不能做的原因。

就不让你访问

访问通关地址得到“I am index.php , I am not the admin page ,key is in admin page.”，尝试用“admin.php”、“manage.php”访问，结果 404，试了试“robots.txt”得到以下结果

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

在原来 URL 路径上拼接“9fb97531fe95594603aff7e794ab2f5f”，访问得到“you find me,but I am not the login page. keep search.”在上面 URL 的基础上拼接“login.php”访问得到`right! key is UIJ%%IOOqweqwsdf`

转载于:https://www.cnblogs.com/renzongxian/p/5618087.html