ctf--网络信息安全攻防实验室之基础关writeup

原创

mbinary 于 2018-04-29 17:43:26 发布 2776 收藏 6

分类专栏： ctf 文章标签： ctf python browser requests http

本文链接：https://blog.csdn.net/marvellousbinary/article/details/80144329

> 此篇文章最先发表在个人博客上, 欢迎访问: smiley:
> 使用的工具
> * chrome
> * python3
> * md5 在线工具 (可搜索到))

第 1 题

Key 在哪里？

分值: 100

过关地址

http://lab1.xseclab.com/base1_4a4d993ed7bd7d467b27af52d2aaa800/index.php

key 就在这里中，你能找到他吗？

解答

ctrl+U 查看源码即得

key：jflsjklejflkdsjfklds

第 2 题

再加密一次你就得到 key 啦~

分值：150

加密之后的数据为 xrlvf23xfqwsxsqf

解答

最开始想到异或, 但是不对呀, 与谁异或, 后来想到 rot13, caser 密码的一种, 即 26 个字母移位即可

```
>>> s='xrlvf23xfqwsxsqf'
>>> li = list(s)
>>> for i,j in enumerate(li):
        if j.isalpha():
                li[i] = chr( ord('a')+(ord(j)-ord('a')+13)%26)


>>> li
['k', 'e', 'y', 'i', 's', '2', '3', 'k', 's', 'd', 'j', 'f', 'k', 'f', 'd',
 's']
>>> ''.join(li)
'keyis23ksdjfkfds'
```

key

`23ksdjfkfds`

第 3 题

猜猜这是经过了多少次加密？

分值：200

加密后的字符串为：Vm0wd2QyUXlVWGxWV0d4V1YwZ 太长省略一万字

解答

结尾有`=`, 猜测很可能是 base64 编码, 所以用 python 一直解码即可

```
s='....'.encode('utf8')
```

```
>>> while 1:
        try: s = base64.decodestring(s)
        except:
                print(s)
                break


b'key is jkljdkl232jkljkdl2389'
>>>
```

key

`jkljdkl232jkljkdl2389`

第 4 题

据说 MD5 加密很安全，真的是么？

分值: 200

e0960851294d7b2253978ba858e24633

解答

这题是 md5 解密
由于 MD5 是信息摘要, 不可逆的, 要想解密, 只有通过先生成明文与其 md5 的数据库, 来查找
搜索在线工具, md5,
地址：http://www.cmd5.com/

还要知道的是 MD5 有限对应无限的字符串, 存在不同的字符串有相同的 md5

key

`bighp`

第 5 题

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：

http://lab1.xseclab.com/base1_0ef337f3afbe42d5619d7a36c19c20ab/index.php

解答

这个猜测是限制了请求头的语言
所以用 python 的 requests 库构造请求头

注意到 requests 库的自身编码为: r.encoding = 'ISO-8859-1'
要转换为 utf8 才能显示中文, 下一题也是这样

```
>>> url = 'http://lab1.xseclab.com/base1_0ef337f3afbe42d5619d7a36c19c20ab/i
ndex.php'
>>> r = requests.get(url,headers = {'Accept-Language':'en'})
>>> r.encoding
'ISO-8859-1'
>>> r.encoding = 'utf8'
>>> r.text
'<html>\n\t <head>\n        <meta http-equiv="content-type" content="text/h
tml;charset=utf-8">\n    </head>\n    <body>\n    \tkey is: *(TU687jksf6&*'
>>>
```

key

`*(TU687jksf6&*`

第六题

HAHA 浏览器

分值: 200

据说信息安全小组最近出了一款新的浏览器，叫 HAHA 浏览器，有些题目必须通过 HAHA 浏览器才能答对。小明同学坚决不要装 HAHA 浏览器，怕有后门，但是如何才能过这个需要安装 HAHA 浏览器才能过的题目呢？ 通关地址：
http://lab1.xseclab.com/base6_6082c908819e105c378eb93b6631c4d3/index.php

只允许使用 HAHA 浏览器，请下载 HAHA 浏览器访问！

解答

同上, 构造 User-Agent

```
>>> r = requests.get(url,headers = {'User-Agent':'HAHA'})
r
>>> r.encoding='utf8'
>>> r.text
'<html>\n\t <head>\n        <meta http-equiv="content-type" content="text/h
tml;charset=utf-8">\n    </head>\n    <body>\n    \t恭喜您，成功安装HAHA浏览
器！key is: meiyouHAHAliulanqi'
>>>
```

key

`meiyouHAHAiiulanqi`

第七题

key 究竟在哪里呢？

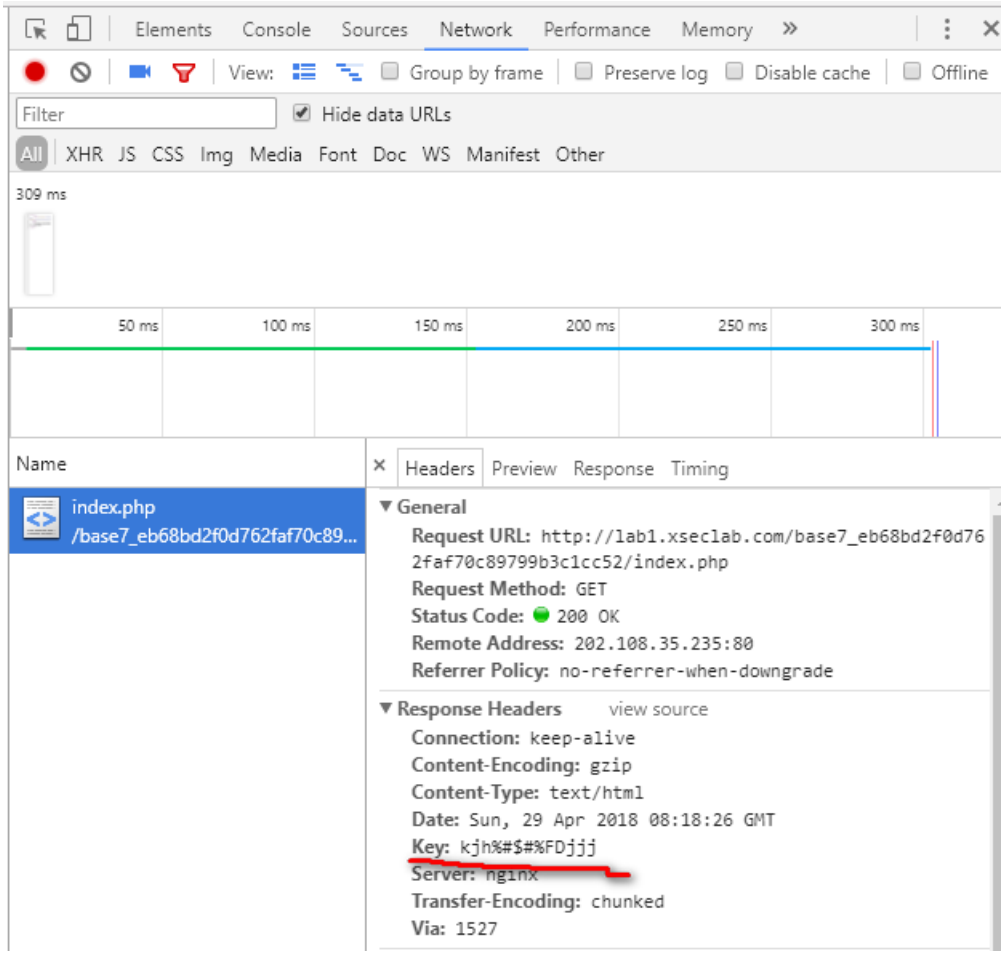
分值: 200

上一次小明同学轻松找到了 key，感觉这么简单的题目多无聊，于是有了找 key 的加强版，那么 key 这次会藏在哪里呢？ 通关地址： http://lab1.xseclab.com/base7_eb68bd2f0d762faf70c89799b3c1cc52/index.php

Key 就在这里，猜猜这里是哪里呢？(Web 找 key 加强版)

解答

源码没有信息, 很自然的想到请求返回的内容



key

`kjh%#$#%FDjjj`

第 8 题

key 又找不到了

分值: 350

小明这次可真找不到 key 去哪里了，你能帮他找到 key 吗？ 通关地址

解答

点击进入是一个链接

```
<html>
    <head>
        <meta http-equiv="content-type" content="text/html;charset=utf-8">
    </head>
    <body>
        <a href="./search_key.php">_到这里找key__</a>
    </body>
</html>
```

点击 search 那个链接, 显示

key is not here!

发现网址是 http://hacklist.sinaapp.com/base8_0abd63aa54bef0464289d6a42465f354/index_no_key.php

说明重定向了

所以防止重定向就可以了, 用 python requests 库, 在 get 时传递参数 `allow_redirects=False`

url 为 `http://lab1.xseclab.com/base8_0abd63aa54bef0464289d6a42465f354/search_key.php`

get 两次就发现了

```
>>> r = requests.get(url,allow_redirects=False)
>>> r.encoding='utf8'
>>> r.text
'<html>\n    <head>\n        <meta http-equiv="content-type" content="text/
html;charset=utf-8">\n    </head>\n    <body>\n        <a href="./key_is_he
re_now_.php">___</a><!--都告诉了到这里找key的啦-->\n    </body>\n</html>'
>>> url = 'http://lab1.xseclab.com/base8_0abd63aa54bef0464289d6a42465f354/k
ey_is_here_now_.php'
>>> r = requests.get(url,allow_redirects=False)
>>> r.encoding='utf8'
>>> r.text
'key: ohHTTP302dd'
>>>
```

key

`ohHTTP302dd`

第 9 题

冒充登陆用户

分值: 200

小明来到一个网站，还是想要 key，但是却怎么逗登陆不了，你能帮他登陆吗？ 通关地址：
http://lab1.xseclab.com/base9_ab629d778e3a29540dfd60f2e548a5eb/index.php

解答

网页中的内容为：您还没有登陆呢！

F12
发现 cookie 有一个键值是 Login=0, 猜测只要传递 Login=1 即可

```
>>> r = requests.post(url,cookies = {"Login":"1"})
>>> r.text
'<html>\n\t <head>\n        <meta http-equiv="content-type" content="text/h
tml;charset=utf-8">\n    </head>\n    <body>\n        key is: yescookieedit
7823789KJ'
>>>
                                                          Ln: 547  Col: 4
```

key

“

第 10 题

比较数字大小

分值: 100

只要比服务器上的数字大就可以了！ 通关地址：
http://lab1.xseclab.com/base10_0b4e4866096913ac9c3a2272dde27215/index.php

解答

进入网页, 查看源码, 有 maxlength 限制, 这是网页限制的, 用 python 就不用担心这些, 直接 post 一个很的数

```
>>> keywords = {
        'v':'999999999'
       }
>>> url = 'http://lab1.xseclab.com/base10_0b4e4866096913ac9c3a2272dde27215/
index.php'
>>> r = requests.post(url,data=keywords)
>>> r.text
'<html>\n    <head>\n        <meta http-equiv=Content-Type content="text/ht
ml;charset=utf-8">\n    </head>\n    <body>\n                <form action="
" method="post">\n            <input type="text" maxlength="3" name="v"/>\n
          <input type="submit" value="æ\x8f\x90äº¤"/>\n        </form>\n
 </body>\n</html>\nkey is 768HKyu678567&*&K'
>>>
```

key

`768HKyu678567&*&K`

第 11 题

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：http://lab1.xseclab.com/base11_0f8e35973f552d69a02047694c27a8c9/index.php

网页内容：必须从本地访问

解答

查看源码, emmmmmmmmmm

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

必须从本地访问!      </body>
</html>
```

```
<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__);
```

如果正常来做的话, 是在请求头传入'x-forwarded-for':'127.0.0.1' 来识别为本地 ip

key

`^&*(UIHKJjkadshf`

第 12 题

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：
http://lab1.xseclab.com/base12_44f0d8a96eed21afdc4823a0bf1a316b/index.php

网页内容：I am index.php , I am not the admin page ,key is in admin page.

解答

这里用到爬虫协议
这是介绍

> Robots 协议（也称为爬虫协议、机器人协议等）的全称是“网络爬虫排除标准”（Robots Exclusion Protocol），网站通过 Robots 协议告诉搜索引擎哪些页面可以抓取，哪些页面不能抓取。

进入
http://lab1.xseclab.com/base12_44f0d8a96eed21afdc4823a0bf1a316b/robots.txt

可以看到

```
User-agent: *

Disallow: /

Crawl-delay: 120

Disallow: /9fb97531fe95594603aff7e794ab2f5f/

Sitemap: http://www.hackinglab.sinaapp.com/sitemap.xml
```

disallow 就是爬虫不能搜索的

进入那个地址

提示不是 login 页面, 再进入 login.php 页面
http://lab1.xseclab.com/base12_44f0d8a96eed21afdc4823a0bf1a316b/9fb97531fe95594603aff7e794ab2f5/login.php
就找到了

key

`UIJ%%IOOqweqwsdf`

总结

哇, 用来整个下午的时间, 挺有趣的