

# 网络安全实验室基础关 writeup

原创

4ct10n  于 2016-05-23 23:41:26 发布  21829  收藏 2

分类专栏: [WEB漏洞 write-up](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qq\\_31481187/article/details/51485783](https://blog.csdn.net/qq_31481187/article/details/51485783)

版权



[WEB漏洞 同时被 2 个专栏收录](#)

23 篇文章 2 订阅

订阅专栏



[write-up](#)

22 篇文章 2 订阅

订阅专栏

1. 寻找key, 这题比较简单直接上源代码。

□

2. 再加密一次你就得到key啦~分值: 150

加密之后的数据为xrlvf23xfqwsxsqf

题目中说再加密一次, 自然想到rot13加密

3. 猜猜这是经过了多少次加密? 分值: 200

加密后的字符串为:

看密码为base64加密, 则思路为使用解密直到不能解密为止

代码见附录:

密码为MD5码, 直接在线破解

5. 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!

观察http头发现能证明是中国人身份的只有accept-language:zh-CN, zh;

我们可以采用burp suite 修改http头改为en-us;

## 6. 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？

□

观察http头发现 user-agent:中有浏览器信息。将后面内容修改为HAHA即可。

## 7.

□ □

响应头中有key

## 8.

□

□

点开链接时发现存在一个search\_key.php文件无法访问，直接上burp suite抓包分析

## 9.

□

发现响应头中存在Login=0，Login一般是判断用户有没有用的，用burp suite将请求头修改为Login=1访问即可

## 10.

□

查看源码 输入数字最多三位，这是就想到修改请求头v=10000000000利用burp suite