上海公共交通卡股份有限公司
ETC 拓展管理平台渗透测试报告

杭州安恒信息技术股份有限公司

2022 年 11 月 04 日

■ 文档信息

文档编号：	AH-SH-22101401
版本编号：	Ver 1.0
密　　级：	商业机密
日　　期：	2022-11-04

■ 适用性声明

本文档适用于杭州安恒信息技术股份有限公司（以下简称“安恒信息”）开展渗透测试服务。本次渗透测试结束之后，因内部环境或不可预知的国内国际政治、经济、法律等社会环境的变化，可能会影响评估结论的有效性。再者，任何应用系统控制都存在一定的局限性，违反应用系统控制的情况仍然有可能发生及不被发现。

■ 版权声明

■ 文档变更记录

版本	日期	变更人	变更内容
0.1	2022-10-14	韩亚豪	创建文档
1.0	2022-11-04	张嘉毅	审核文档

目录

1. 摘要

1.1. 报告摘要

应上海公共交通卡股份有限公司的委托，安恒信息对其下属 ETC 报表系统进行了一次渗透测试。本次测试有效时间从 2022 年 10 月 11 日开始至 2022 年 10 月 14 日结束。针对测试的结果本报告书进行了详细的说明，并提供了相应的修复建议等信息。

渗透测试作为检验目标系统安全性最有效的服务，需要服务人员通过智能工具探测、人工测试、分析的手段，以模拟黑客入侵的方式对服务目标系统进行模拟入侵测试，主要评估目标系统是否存在 SQL 注入、跨站脚本、跨站请求伪造、认证会话管理、弱口令、信息加密性、文件包含、目录浏览、不安全的跳转、溢出、上传、不安全的数据传输、未授权的访问等脆弱性问题，识别服务目标存在的安全风险。

渗透测试可以有效帮助上海公共交通卡股份有限公司对信息系统的安全性得到较深的认知，不仅有助于后续的安全建设，还能用于验证经过安全保护后的系统安全状况是否真实的达到了预定安全目标、遵循了安全策略。

1.2. 报告说明

本报告书中含有发现的漏洞信息及其恶意使用的方法，安恒信息建议谨慎使用。

对本系统的问题点的评估方法是根据过去的经验、当下可利用的攻击信息及已知的攻击方法，实施的一种非定性的检查，而信息系统的最终安全取决于系统的使用者。因此，通过此次检查能够判断出本系统存在的主要漏洞，但是，安恒信息并不能保证此为所有潜在的漏洞，也不能保证安恒信息提供的解决方案和建议包含了所有能够防止漏洞暴露或被恶意使用的防范措施。

另外，本报告书中关于漏洞的分析结果是基于本报告制作时所知晓的技术或已知的攻击手法，而攻击技术手段或风险会随着时间的迁移而改变。因此，本系统运维过程中发生的漏洞及防止该漏洞暴露的解决方法也在发生变化。除另行书面同意的情况下，安恒信息不会对本系统环境的变更或在本报告书记载的时间之后发现的问题进行实施以外的评估或分析。

本报告书中可能会推荐使用其他公司制造、维护的软件或硬件产品。安恒信息是根据该产品使用的实际情况而做出相关推荐的，但是安恒信息并不保证该产品一定能够达到其广告中宣传的功能或效果。

关于第三方使用本报告的情况，按照安恒信息与贵公司之间签订的服务合同及保密协议中的相关规定执行。

2. 漏洞概要

2.1. 漏洞信息统计

本次渗透测试发现的安全漏洞如下表所示：

信息系统	漏洞名称	安全等级
ETC 拓展管理平台（163.10.10.136）	垂直越权	高危
	业务重放	中危
	图形验证码可识别	中危
	jQuery 版本漏洞	低危
	敏感信息泄露	低危
	敏感信息明文传输	低危
	基于 HTTP 连接的登录请求	低危
	密码可设置为和旧密码一致	低危

漏

高危(High-Risk)

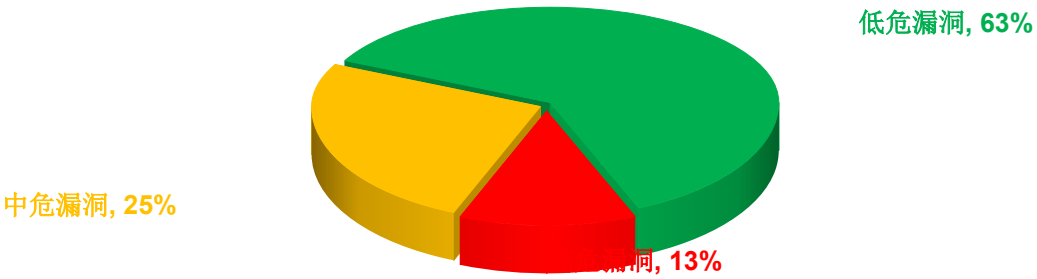
低危(Low-Risk)

中危(Mid-Risk)

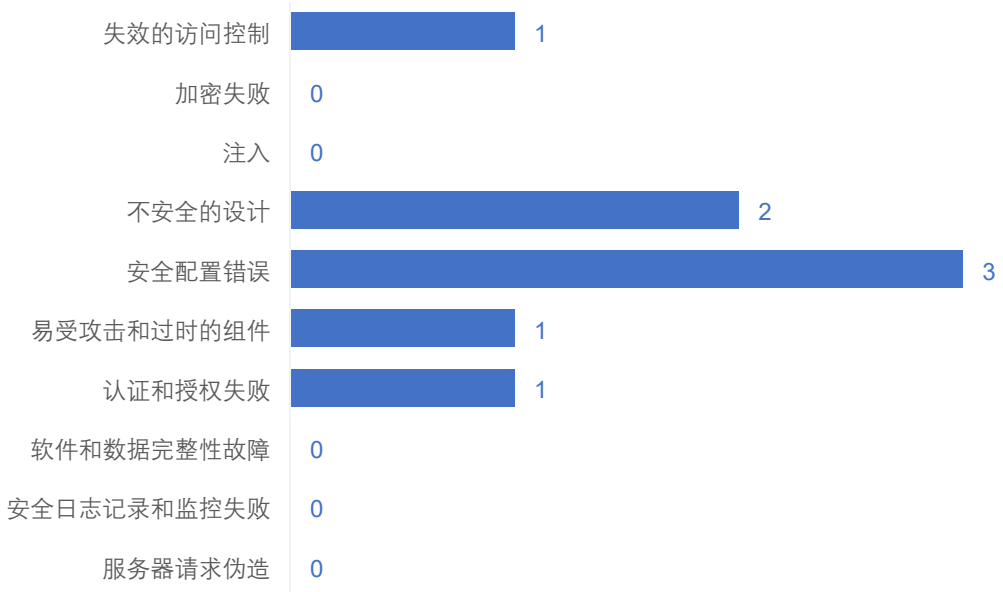
2.2. 漏洞风险分布

信息系统	高危	中危	低危	合计
ETC 拓展管理平台（163.10.10.136）	1	2	5	8

漏洞风险分布



2.3. OWASP TOP 10



2.4. 漏洞等级

漏洞等级	等级描述
高危	包括但不限于以下情况： 1.不需要登录直接获取设备 root 权限的漏洞，包括但不限于上传 Webshell，任意代码执行，远程命令执行等。 2.需要登录的重要业务逻辑漏洞，包括但不限于权限绕过等。 3.包含重要业务敏感信息的非授权访问，包括但不限于绕过认证直接访问管理后台、后台弱密码、可直接获取大量内网敏感信息的 SSRF 等。
中危	包括但不限于以下情况： 1.不需要交互对用户产生危害的安全漏洞，包括但不限于一般页面反射型 XSS 等。 2.普通信息泄露漏洞，包括但不限于少量的用户信息泄露和业务敏感信息泄露等。 3.其他操作中度影响的漏洞，例如：没有敏感信息的 SQL 注入、无法回显的 SSRF 等。
低危	包括但不限于以下情况： 1.不涉及安全问题的 bug，包括但不限于功能缺陷、网页乱码、样式混乱、静态文件遍历、应用兼容性等问题。 2.影响轻微的漏洞，包括但不限于 self-xss、无意义的异常堆栈、内网 IP 地址/域名泄露等。 3.不能对目标系统产生直接影响且利用条件较为苛刻的漏洞。

2.5. 参考标准

渗透测试参考的标准包括但不限于：

标准名称	标准类型
国际 OWASP 组织发布的最新版 OWASP TOP 10	国际标准
《信息系统审计标准》	国际标准

《信息安全技术 Web 应用安全扫描产品安全技术要求》	国家标准
《信息安全技术 网络安全漏洞标识与描述规范》	国家标准
《信息安全技术 网络安全漏洞分类分级指南》	国家标准
《信息安全技术 互联网信息服务安全通用要求》	国家标准
《信息技术 安全技术 信息技术安全性评估准则》	国家标准
《信息安全技术 安全技术 实体鉴别》	国家标准
《信息安全技术 网络安全等级保护安全设计技术要求》	国家标准
《信息安全技术 网络安全等级保护基本要求》	国家标准
《信息安全技术 网络安全漏洞管理规范》	国家标准
《信息安全技术 网络安全管理支撑系统技术要求》	国家标准
《信息技术 安全技术 网络安全 第 1 部分》	国家标准
《信息技术 安全技术 网络安全 第 2 部分》	国家标准
《信息技术 安全技术 IT 网络安全 第 3 部分》	国家标准
《信息技术 安全技术 IT 网络安全 第 4 部分》	国家标准
《信息技术 安全技术 网络安全 第 5 部分》	国家标准
《信息安全技术 信息系统密码应用基本要求》	国家标准

3. 渗透测试对象

3.1. 测试目标

本次测试目标如下表所示：

序号	信息系统	域名/IP 地址	协议	端口	根目录
1	ETC 拓展管理平台	163.10.10.136	http	80	etcwebmngr

3.2. 测试时间

- 2022 年 10 月 11 日至 10 月 14 日

3.3. 测试账号

序号	账号（用户名）	账号类型
1	test	低权限账号
2	testadmin	高权限账号

3.4. 测试人员

安恒信息组成专项安全风险深度评估小组，由安恒信息安全工程师主要参与，上海公共交通卡股份有限公司相关工作人员配合。

具体人员列表如下：

姓名	邮箱	负责事项
韩亚豪	tommy.han@dbappsecurity.com.cn	渗透测试、报告撰写

3.5. 测试方式

测试方式	描述
远程	整个测试过程中工具使用、人工分析、编写报告均为远程操作。

3.6. 测试地址

测试性质	测试时间	出口 IP 地址	归属地
初测	2022 年 10 月 11 日至 10 月 14 日	163.10.10.16	上海

3.7. 测试类型

测试类型	描述
黑盒测试	指测试小组在不知晓目标网络环境的情况下，模拟黑客对目标域名或 IP 地址进行无害安全测试，通过技术手段获取目标网站的控制权限或敏感数据。

3.8. 测试工具

本次测试工具使用包括但不限于：

工具名称	工具简介
Burpsuite	Burpsuite 是一款 Web 应用程序集成平台，通过拦截 http/https 的 web 数据包进行拦截、修改、重放数据包进行测试。
Nmap	Nmap 是一款网络端口开放状态检测软件，用来检测目标设备上开放的网络情况。同时，根据端口与指纹信息，确定相关端口版本、操作系统信息。
Sqlmap	Sqlmap 是一款用来检测与利用 SQL 注入漏洞的免费开源工具，它的特性是对数据库指纹、访问底层文件系统、执行命令进行自动化检测与利用。

冰蝎	冰蝎客户端基于 JAVA，可以跨平台使用，主要功能为：基本信息、命令执行、虚拟终端、文件管理、Socks 代理、反弹 shell、数据库管理、自定义代码等，功能非常强大。
Dirsearch	Dirsearch 是一个 python 开发的目录扫描工具，目的是扫描网站的敏感文件和目录从而找到突破口。
JSFinder	JSFinder 是一款快速扫描网站的 js 文件的工具，利用该工具可以从 js 中提取 URL、子域名。
Wappalyzer	Wappalyzer 是一款快速识别网站指纹信息的浏览器插件。可以快速识别网站的开发语言、框架等基本信息。
Packer-Fuzzer	Packer Fuzzer 是一款对 Webpack 等前端打包工具所构造的网站进行快速、高效安全检测的扫描工具。当我们在 Goby 中遇到前端打包器所生成的站点时，联动 Packer Fuzzer 可以自动解析全部 JS 文件并提取该站点所有 API 及 API 参数，从而进行高效漏洞模糊检测。
MAT	MAT 是一款非常强大的内存分析工具，在 Eclipse 中有相应的插件，同时也有单独的安装包。在进行内存分析时，只要获得了反映当前设备内存映像的 hprof 文件，通过 MAT 打开就可以直观地看到当前的内存信息。
Coding 编码转换工具	Coding 编码转换小工具集合了多种编码的转换，如 ANSI-Unicode-utf8 相互转换、URL 编码解码、MD5 加密、base64 加解密等。
Msfconsole	Msfconsole 简称 msf 是一款常用的渗透测试工具，包含了常见的漏洞利用模块和生成各种木马。

4. 渗透测试结果

4.1. ETC 拓展管理平台（163.10.10.136）

4.1.1. 垂直越权【高危】

垂直越权

漏洞描述

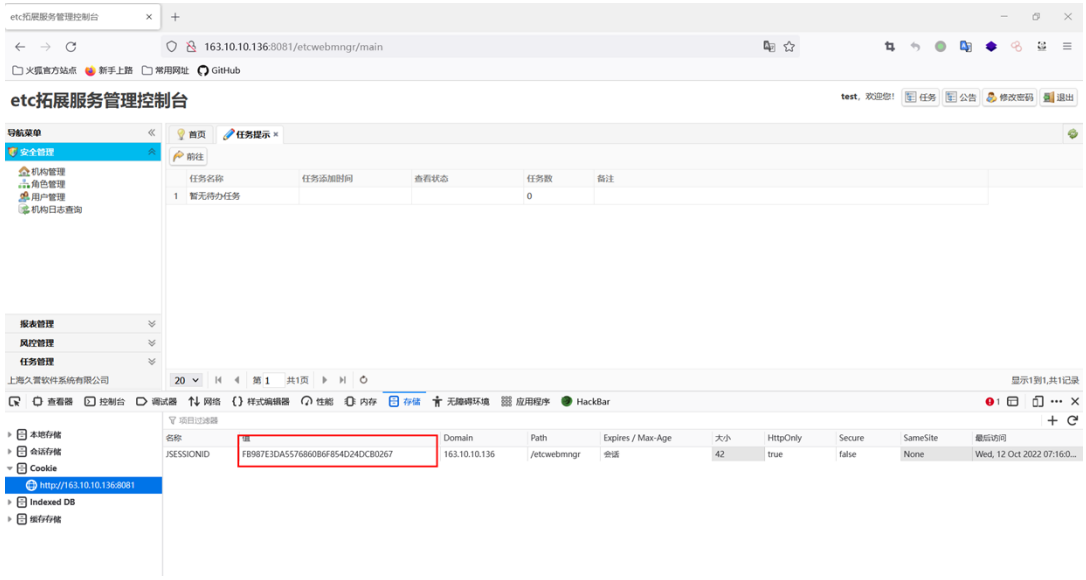
攻击者在获得低权限用户帐户后，可以利用一些方式绕过权限检查，访问或者操作到原本无权访问的高权限功能。

漏洞地址

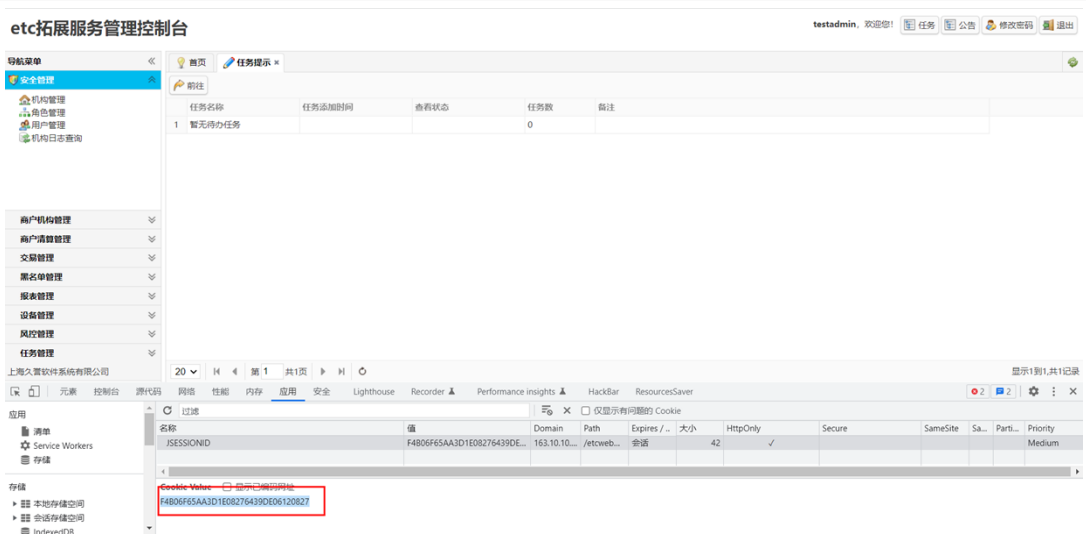
http://163.10.10.136:8081/etcwebmngr/

测试过程

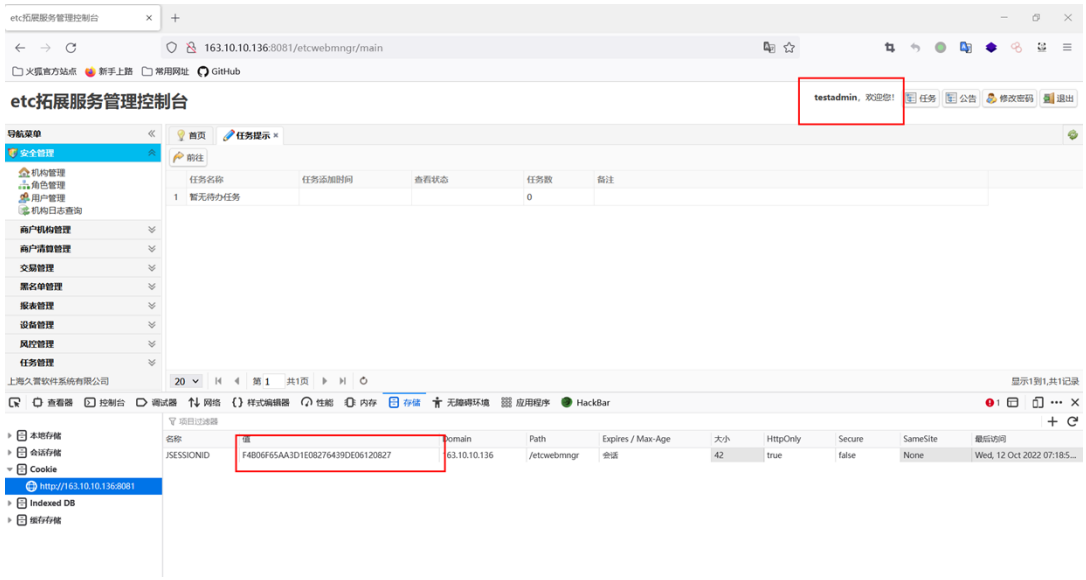
1.登录低权限账号，查看 cookie



2.登录高权限账号，复制下 cookie 值



3.回到低权限账号中，把高权限账户的 cookie 替换低权限的，然后刷新页面，页面变成高权限账号的主页。



修复建议

1、对用户操作进行权限校验，防止通过修改参数进入未授权页面及进行非法操作。

2、在服务端对请求的数据和当前用户身份做校验检查。

4.1.2. 业务重放【中危】

业务重放

漏洞描述

在系统某个功能点处存在重放漏洞的话，可以对提交数据进行重放。如：留言板处存在

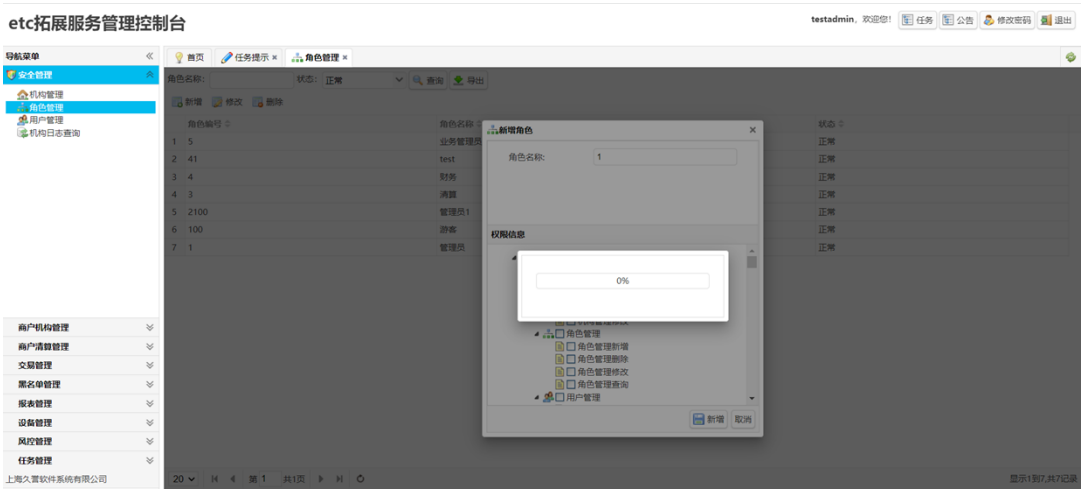
重放漏洞，攻击者可以提交留言并抓包，重放该数据包则可以重复发表留言，导致恶意刷留言等问题。

漏洞地址

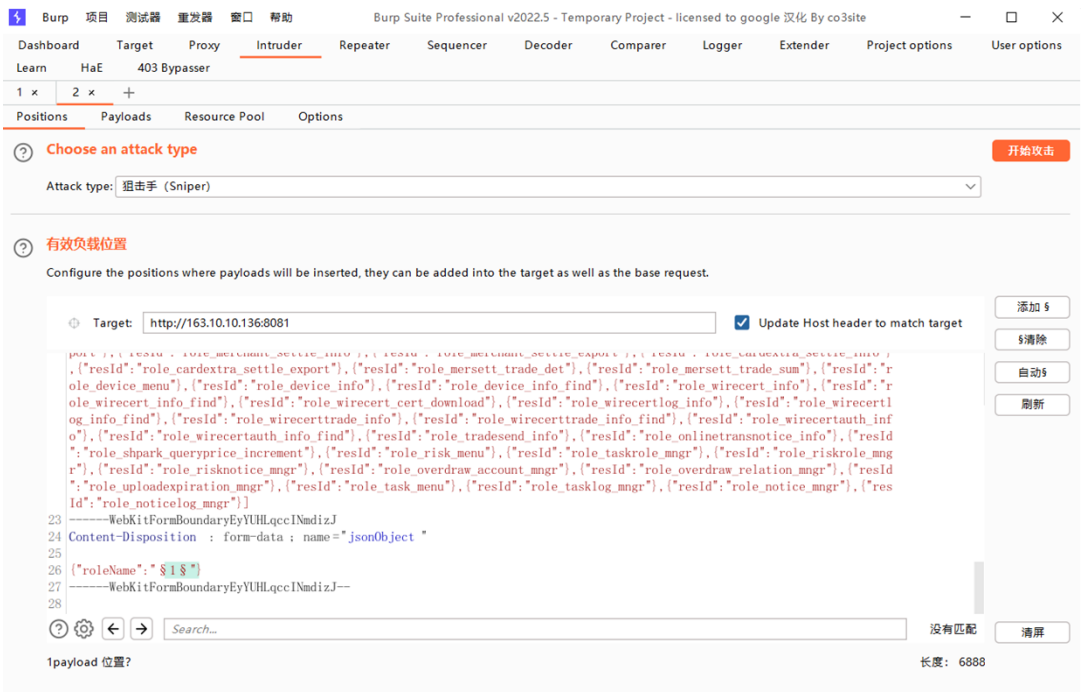
http://163.10.10.136:8081/etcwebmngr/

测试过程

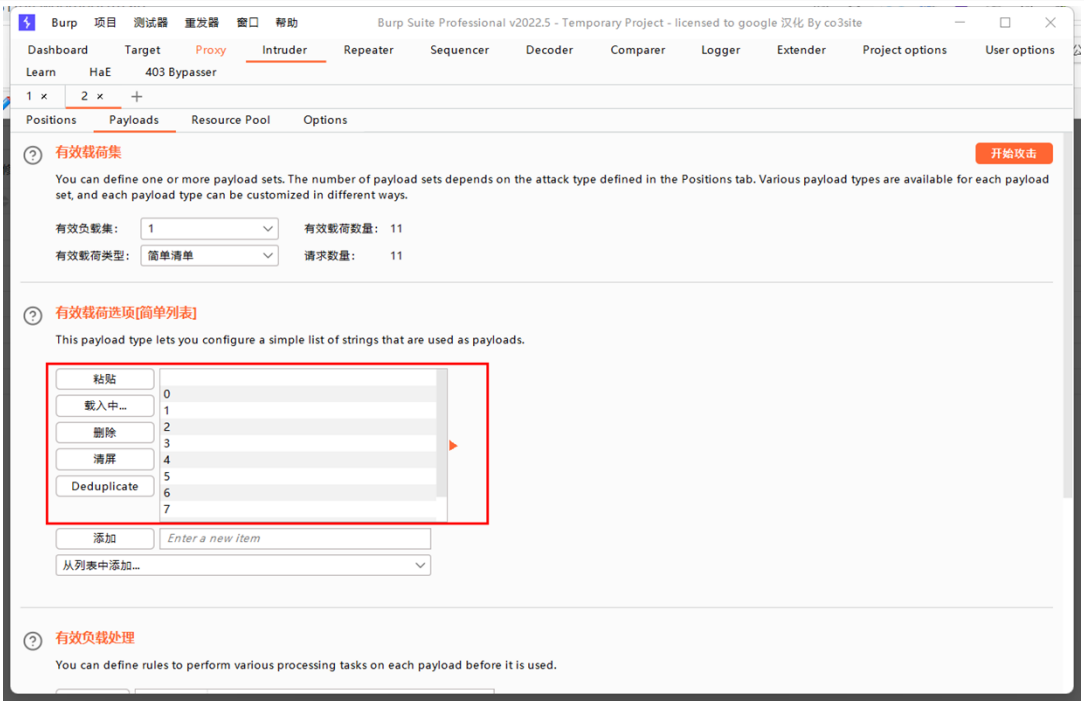
1、访问测试地址进入角色管理模块，选择添加角色，输入参数后点击新增后抓包：



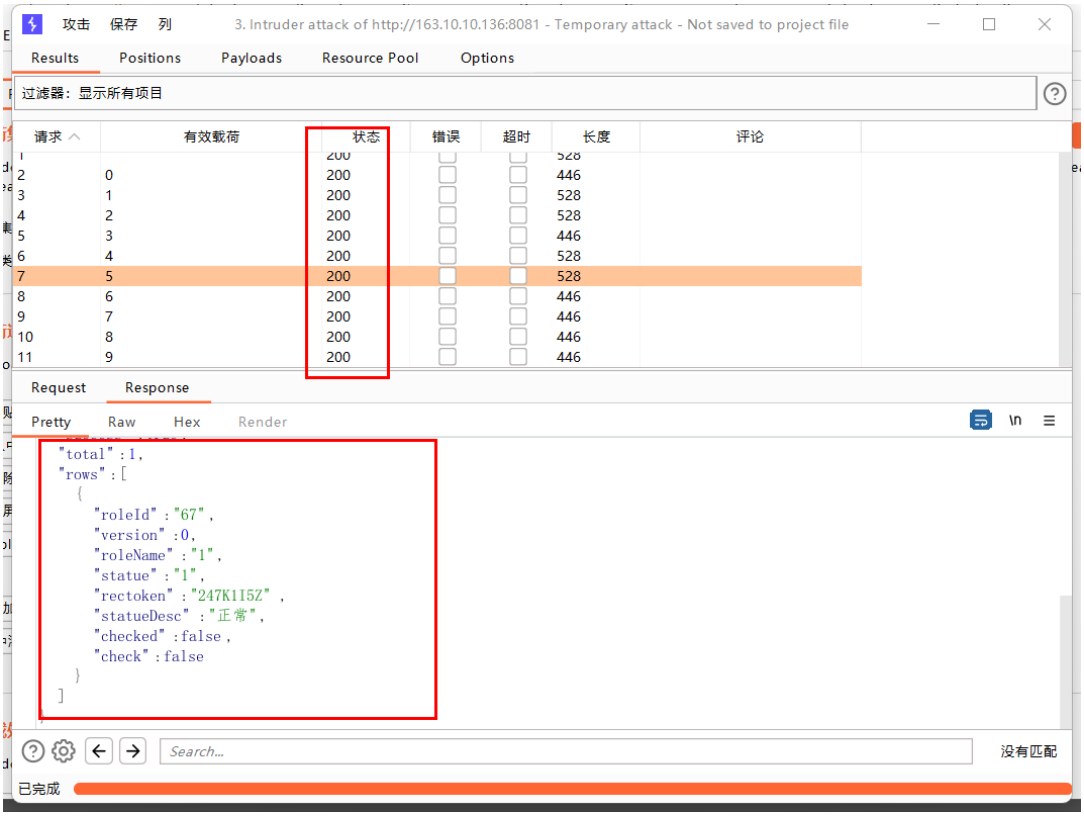
2、把包发到测试器模块，把角色名标记为参数：



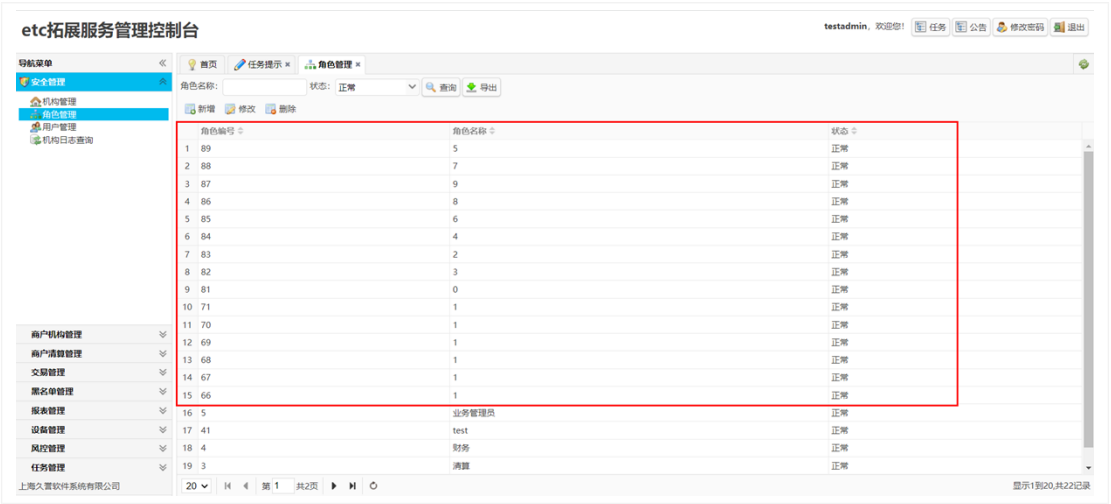
3、添加 payload 后开始攻击：



4、发现成功添加了 10 条角色名递增的角色信息：



5、回到测试地址发现数据添加成功。



修复建议

使用加时间戳、随机数、流水号来有效应对抗重放攻击。

4.1.3. 图形验证码识别【中危】

图形验证码识别

漏洞描述

在破解验证码中需要用到的知识一般是 像素，线，面等基本 2 维图形元素的处理和色差分析，简单的图形验证码可经过一些工具进行识别。

漏洞地址

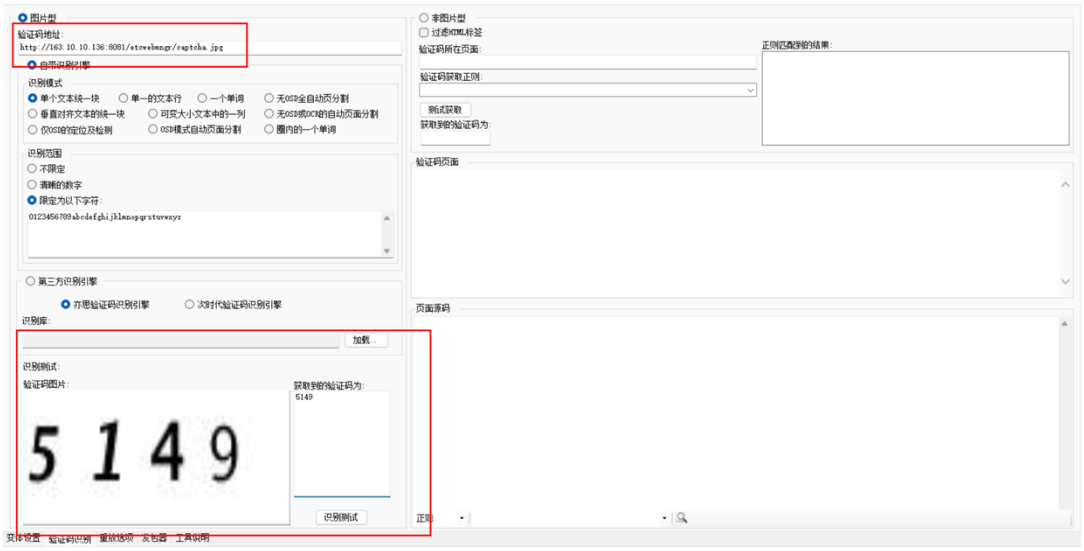
http://163.10.10.136:8081/etcwebmngr/login/

测试过程

1. 使用 Burp 抓包，找出图形验证码的请求包

2. 将包复制到 PKAV 工具,标记验证码。

3. 输入图片验证码地址后，点击多次识别验证码测试，都可以识别出验证码。



修复建议

采取一定的干扰措施且不可预测，如字体倾斜，加背景噪点、横线等。

4.1.4. jQuery 版本漏洞【低危】

jQuery 版本漏洞

漏洞描述

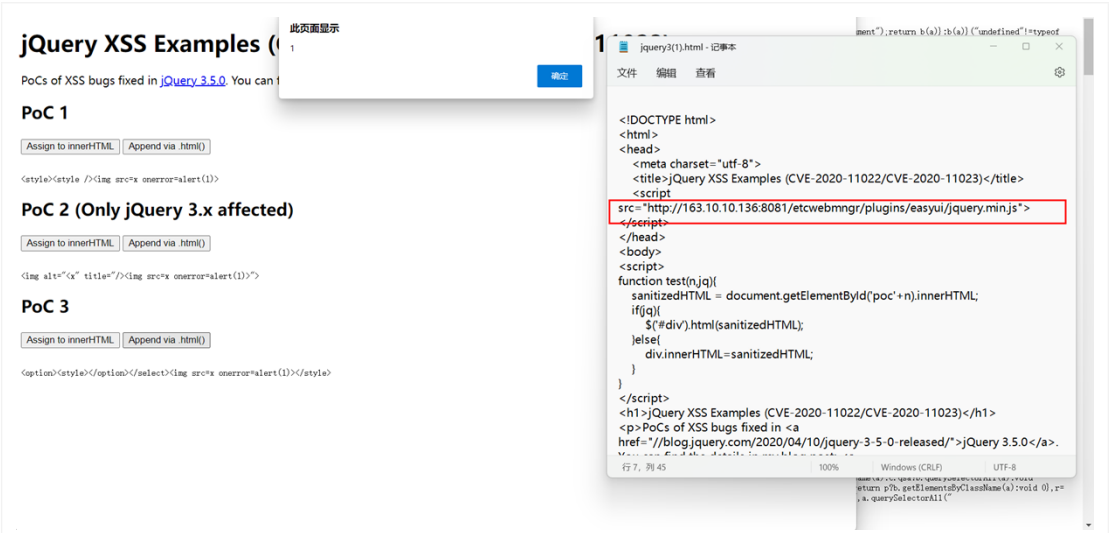
jQuery 是美国 John Resig 程序员的一套开源、跨浏览器的 JavaScript 库。该库简化了 HTML 与 JavaScript 之间的操作，并具有模块化、插件扩展等特点。jQuery 3.4.0 之前版本中存在跨站脚本漏洞，该漏洞源于 WEB 应用缺少对客户端数据的正确验证。攻击者可利用该漏洞执行客户端代码。

漏洞地址

http://163.10.10.136:8081/etcwebmngr/plugins/easyui/jquery.min.js

测试过程

访问漏洞地址可以发现系统所使用的 jQuery 版本过低。用 POC 文件对网址进行验证，发现成功弹窗。



修复建议

建议将 jQuery 版本升级到最新版本。

4.1.5. 敏感信息泄露【低危】

敏感信息泄露

漏洞描述

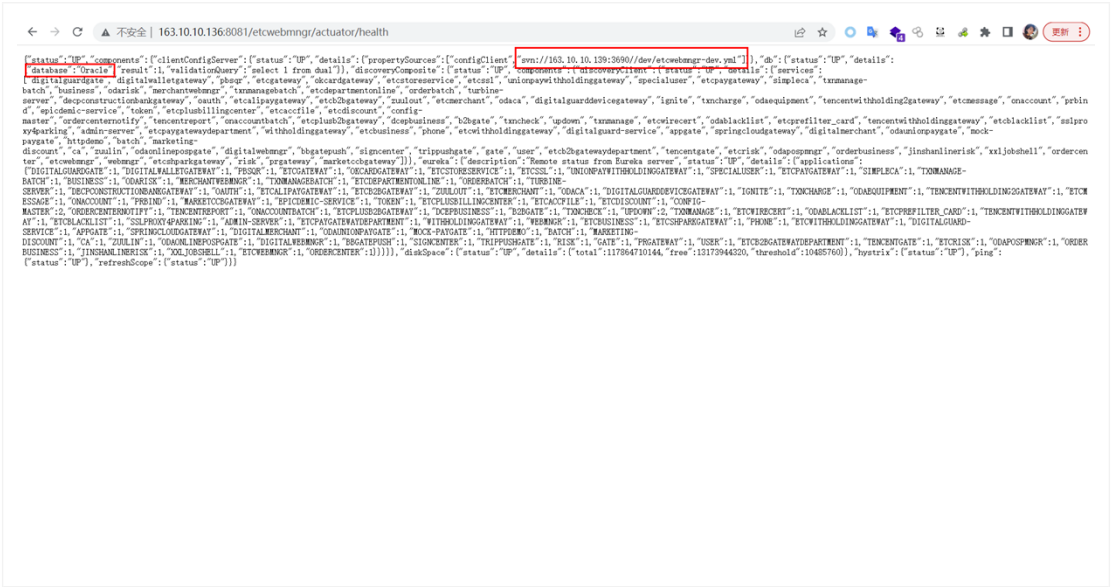
信息泄露指在网站页面或应用中泄露了敏感信息。通过这些信息，攻击者可进一步入侵服务器。（信息泄露包括不限于网站备份文件泄露、js 文件敏感信息泄露、物理路径泄露、中间件信息泄露、密钥泄露、Robots 文件存放敏感路径、内网 IP 泄露等）

漏洞地址

http://163.10.10.136:8081/etcwebmngr/actuator/health

测试过程

访问测试地址，发现网页数据中暴露出的内网 IP 和数据库名。



修复建议

如不必要建议及时将内网 IP 信息隐藏或使用域名进行替换。。

4.1.6. 敏感信息明文传输【低危】

敏感信息明文传输

漏洞描述

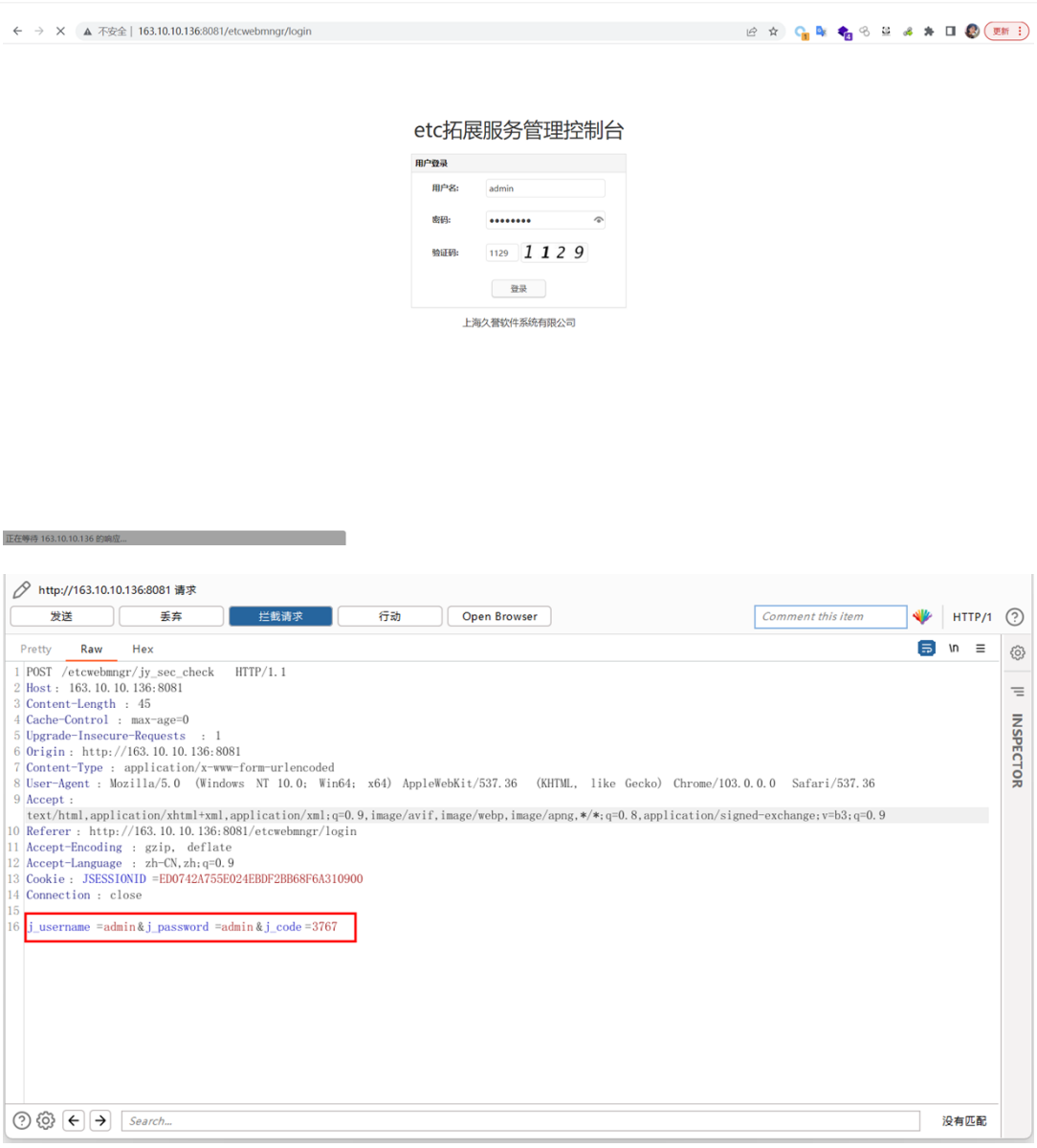
敏感信息使用明文传输的方式存在嗅探风险，如登录接口用户名和密码使用明文传输的方式，攻击者在局域网中嗅探网络流量，可轻易窃取账号信息。

漏洞地址

http://163.10.10.136:8081/etcwebmngr/login/

测试过程

访问测试地址，输入账号密码进行登录抓包，可以发现数据包里未加密的账号密码。



修复建议

1、建议系统使用安全加密协议，避免使用明文传输协议如 HTTP 等。

2、建议系统将敏感信息进行加密，防止在明文传输协议中被窃取。

4.1.7. 基于 HTTP 连接的登录请求【低危】

基于 HTTP 连接的登录请求

漏洞描述

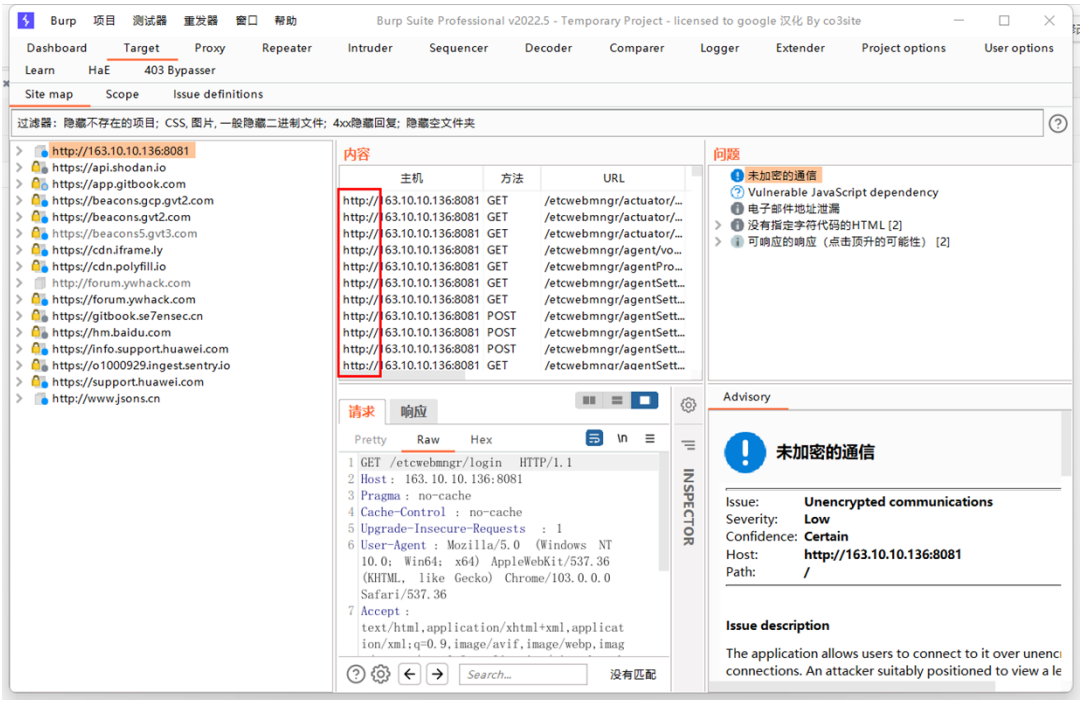
互联网传输的 CS/BS 架构应用使用了 http 协议进行数据传输。

漏洞地址

http://163.10.10.136:8081/etcwebmngr/

测试过程

使用 burp 工具对测试网址进行抓包，发现网址使用的服务协议为 http 协议。



修复建议

互联网传输的 CS/BS 架构应用应采用 VPN 链路加密或 HTTPS（应采用 TLS 加密）进行数据传输。

4.1.8. 密码可设置为和旧密码一致【低危】

密码可设置为和旧密码一致

漏洞描述

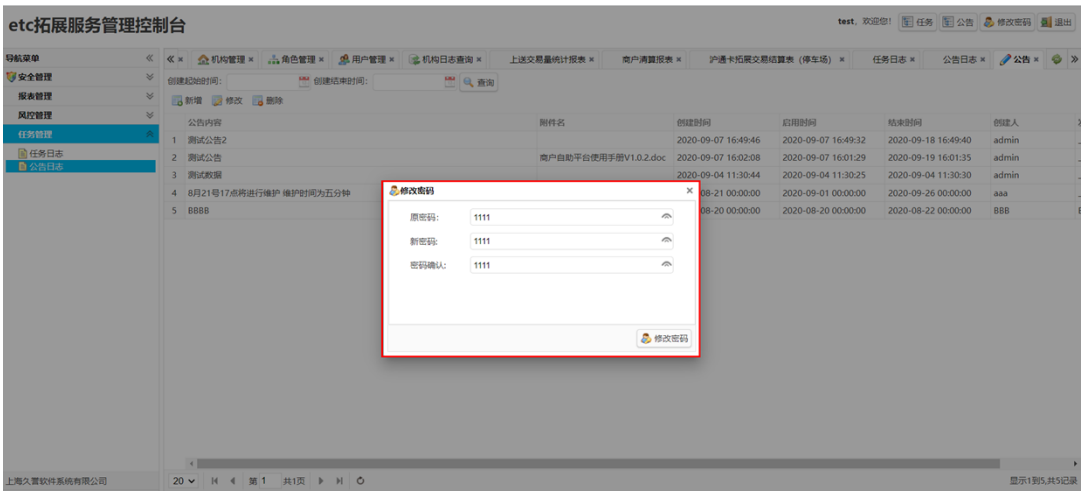
密码可修改为和旧密码一致的密码。

漏洞地址

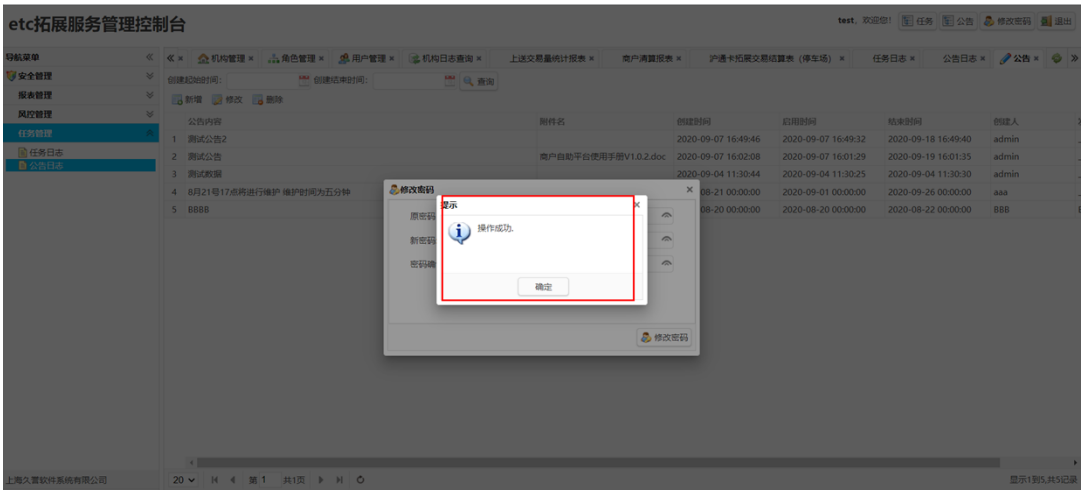
http://163.10.10.136:8081/etcwebmngr/

测试过程

1、在修改密码功能处填写和旧密码一致的密码，尝试修改：



2、发现修改成功：



修复建议

禁止新密码与最近两次密码相同。

5. 结论

5.1. 应用系统风险评级

此次渗透测试，安恒信息通过可利用性指标及影响指标对漏洞危害程度及信息系统进行了多维分析，并采用了国际评测标准对信息系统危害程度进行如下评级：

5.1.1. 可利用性分析

- 攻击矢量：此度量标准反映了可以利用漏洞的方式。可以是互联网上的，也可以是本地环境的。
- 攻击复杂度：此度量标准描述了利用漏洞的攻击复杂度。
- 权限需求：此度量标准描述了攻击者在成功利用此漏洞之前必须拥有的权限级别。
- 用户交互：此度量标准捕获除攻击者之外的用户是否需要交互触发该漏洞。
- 范围：此度量标准漏洞危害是否超出本身所赋予的资源或特权。

攻击矢量	攻击复杂度	权限需求	用户交互	范围
网络	低	低	无	不改变

5.1.2. 影响指标分析

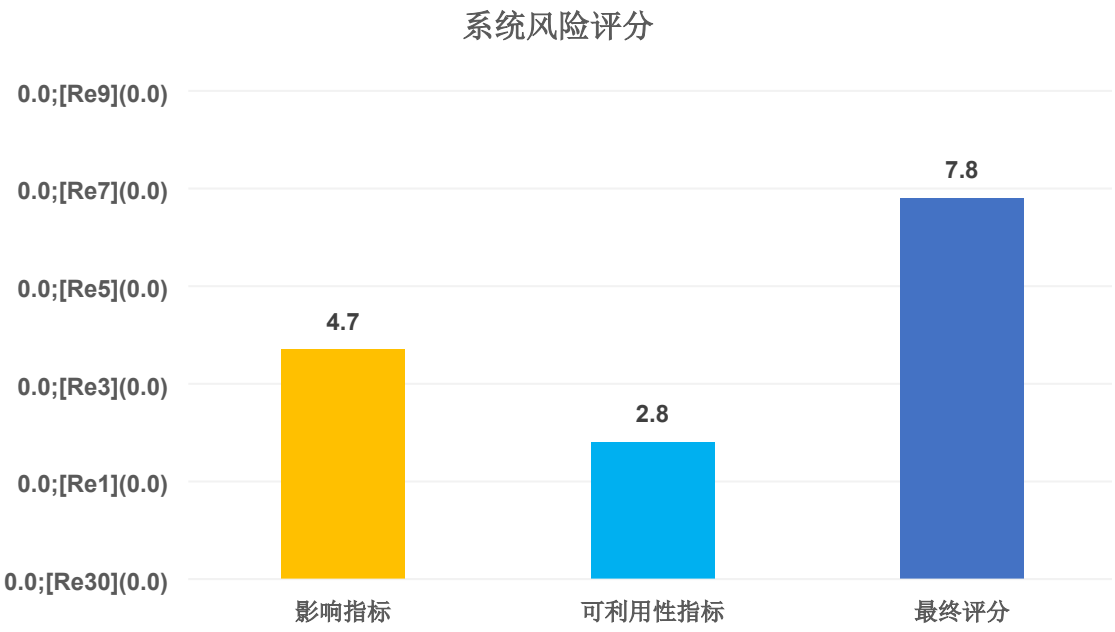
- 机密性影响：此度量标准衡量成功利用漏洞是否影响系统机密性。
- 完整性影响：此度量标准衡量成功利用漏洞是否影响系统完整性。
- 可用性影响：此度量标准衡量成功利用漏洞是否影响系统可用性。

机密性影响	完整性影响	可用性影响
高	低	低

5.1.3. 风险评级划分

等级	分值
紧急风险	9.0-10.0
高风险	7.0-8.9
中风险	4.0-6.9
低风险	0.1-3.9
安全	0.0

5.1.4. 系统风险评级



经评测，系统最终风险等级为：高风险

5.2. 安全建议

通过信息系统最终评级发现信息系统本身存在风险性，导致此风险存在的漏洞有：“垂直越权”等安全漏洞，漏洞最高级别为高。针对这些漏洞建议立即进行安全整改。同时，安恒信息作为一家致力于 Web 应用安全的专业产品和服务提供商，建议上海公共交通卡股份有限公司进行以下安全建设，以长期保证信息系统安全：

1、 定期进行专业的安全评估；

2、 针对安全评估结果协调开发团队或厂商进行有效的安全整改和修复；

3、 持续完善网络安全设备规划与部署，以应对日益增进的网络恶意攻击并进行安全防护；

4、 持续完善现有的安全管理制度、信息系统的日常维护和使用规范；

5、 持续完善应急响应预案和流程，并定期进行应急演练，一旦发现发生任何异常状况可及时进行处理和恢复，有效避免网站业务中断带来损失；

6、 定期对相关管理人员和技术人员进行安全培训，提高安全技术能力和实际操作能力。

5.3. 感谢

在本次渗透测试过程中，安恒信息感谢上海公共交通卡股份有限公司的领导及相关人员的大力支持，使得我们的工作顺利完成。