深圳东风汽车有限公司

用友 U9 ERP 数据管理平台

数据泄露漏洞

1、漏洞详情

发现时间	2024 年 04 月 16 日
单位名称	深圳东风汽车有限公司
网站名称	DMP 数据工厂
漏洞类型	数据泄露漏洞
风险等级	低危
网站域名	无
IP 地址	http://183.63.182.228:8085/

2、漏洞分析

2.1 漏洞简述：

深圳东风汽车有限公司存在敏感数据泄露漏洞，攻击者可利用该漏洞构造不存在的路由页面，获取返回的报错包含环境参数、账户密码配置等敏感信息，用户可利用账户密码信息成功进入管理后台，拥有超级管理员权限，进行相应后门留置等机密性、完整性、可用性破坏。

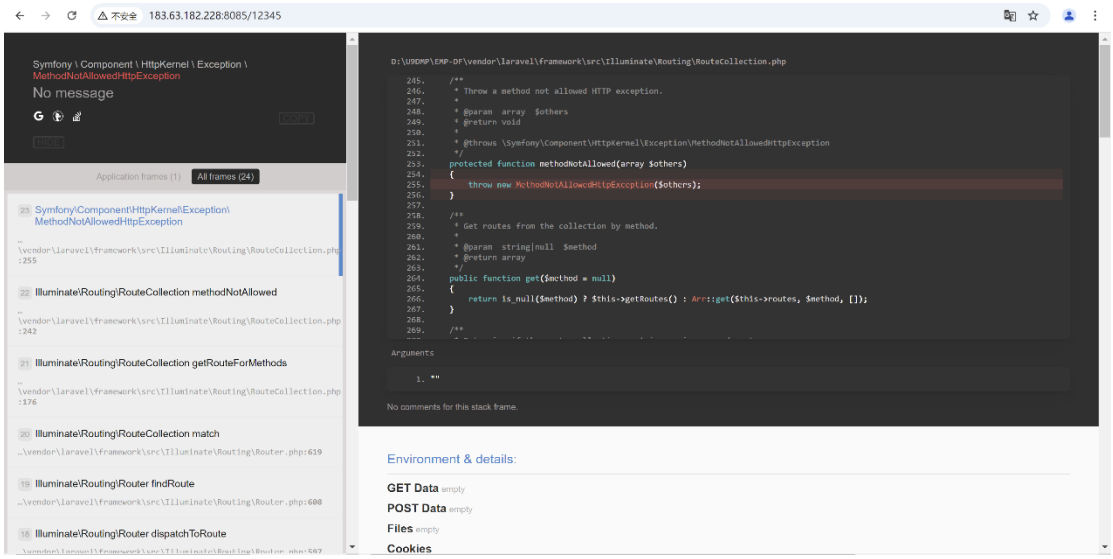
2.2 漏洞 URL

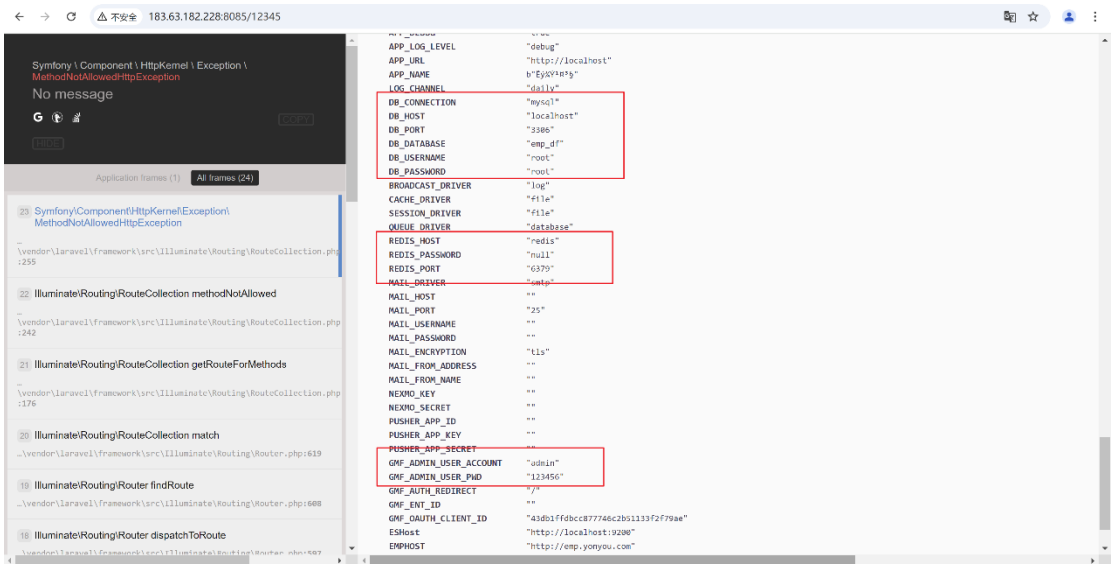
http://183.63.182.228:8085/

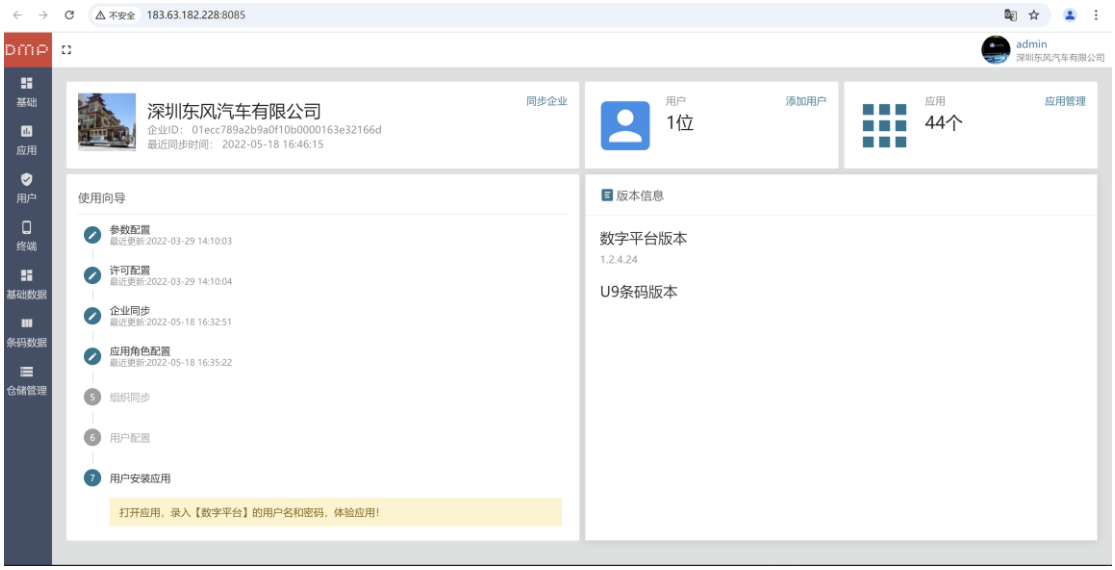
2.3 复现步骤

浏览器输入该平台网址 http://183.63.182.228:8085/xxx（构造任意不存在的路由页面），返回的报错包含环境参数、账户密码配置等敏感信息，如下图所示，即可以超级管理员身份进入该平台。此外，泄露的敏感信息中还包括数据库配置信息、redis 配置信息等。

超级管理员身份拥有最高权限，可对平台机密性、完整性、可用性进行破坏。


不安全 183.63.182.228:8085/12345
Symfony \ Component \ HttpKernel \ Exception \
MethodNotAllowedHttpException
No message
Application frames (1)
All frames (24)
Symfony\Component\HttpKernel\Exception\
MethodNotAllowedHttpException
Illuminate\Routing\RouteCollection methodNotAllowed
Illuminate\Routing\RouteCollection getRouteForMethods
Illuminate\Routing\RouteCollection match
Illuminate\Routing\Router findRoute
Illuminate\Routing\Router dispatchToRoute
D:\USDMP\EMP-DF\vendor\laravel\framework\src\Illuminate\Routing\RouteCollection.php
Arguments
No comments for this stack frame.
Environment & details:
GET Data
POST Data
Files
Cookies


不安全 183.63.182.228:8085/12345
APP_LOG_LEVEL "debug"
APP_URL "http://localhost"
APP_NAME
LOG_CHANNEL "daily"
DB_CONNECTION "mysql"
DB_HOST "localhost"
DB_PORT "3306"
DB_DATABASE "emp_df"
DB_USERNAME "root"
DB_PASSWORD "root"
BROADCAST_DRIVER "log"
CACHE_DRIVER "file"
SESSION_DRIVER "file"
QUEUE_DRIVER "database"
REDIS_HOST "redis"
REDIS_PASSWORD "null"
REDIS_PORT "6379"
MAIL_DRIVER "smtp"
MAIL_HOST ""
MAIL_PORT "25"
MAIL_USERNAME ""
MAIL_PASSWORD ""
MAIL_ENCRYPTION "tls"
MAIL_FROM_ADDRESS ""
MAIL_FROM_NAME ""
NEXMO_KEY ""
NEXMO_SECRET ""
PUSHER_APP_ID ""
PUSHER_APP_KEY ""
PUSHER_APP_SECRET ""
GMF_ADMIN_USER_ACCOUNT "admin"
GMF_ADMIN_USER_PWD "123456"
GMF_AUTH_REDIRECT "/"
GMF_ENT_ID ""
GMF_OAUTH_CLIENT_ID "43db1fdbcc877746c2b51133f2f79ae"
ESHost "http://localhost:9200"
EMPHOST "http://emp.yonyou.com"


不安全 183.63.182.228:8085
DMP
admin
深圳东风汽车有限公司
基础
应用
用户
终端
基础数据
条码数据
仓储管理
深圳东风汽车有限公司
企业ID: 01ecc789a2b9a0f10b0000163e32166d
最近同步时间: 2022-05-18 16:46:15
同步企业
用户
1位
添加用户
应用
44个
应用管理
使用向导
参数配置
最近更新:2022-03-29 14:10:03
许可配置
最近更新:2022-03-29 14:10:04
企业同步
最近更新:2022-05-18 16:32:51
应用角色配置
最近更新:2022-05-18 16:35:22
组织同步
用户配置
用户安装应用
打开应用，录入【数字平台】的用户名和密码，体验应用!
版本信息
数字平台版本
1.2.4.24
U9条码版本

3、漏洞总结

深圳东风汽车有限公司存在敏感数据泄露漏洞，攻击者可利用该漏洞构造不存在的路由页面，获取返回的报错包含环境参数、账户密码、数据库配置等敏感信息。

用户可利用账户密码信息成功进入管理后台，拥有超级管理员权限，进行相应后门留置等机密性、完整性、可用性破坏。

4、修复建议

（1）对非法路由进行拦截、重定向设置；

（2）敏感配置信息脱敏处理。