实战CVE-2022-23131漏洞 | 身份认证绕过

前言：

Zabbix 是一个非常流行的开源监控平台，用于收集、集中和跟踪整个基础设施中的 CPU 负载和网络流量等指标。它与 Pandora FMS 和 Nagios 等解决方案非常相似。由于其受欢迎程度、功能和在大多数公司网络中的特权地位，Zabbix 是威胁参与者的高调目标。

Zabbix 对客户端提交的 Cookie 会话存在不安全的存储方式，导致在启动 SAML SSO 认证模式的前提下，恶意用户可通过构造特殊请求绕过认证，获取管理员权限，进而可实现 RCE。

Fofa 语句:

app="ZABBIX-监控系统" && body="saml"

适用版本：

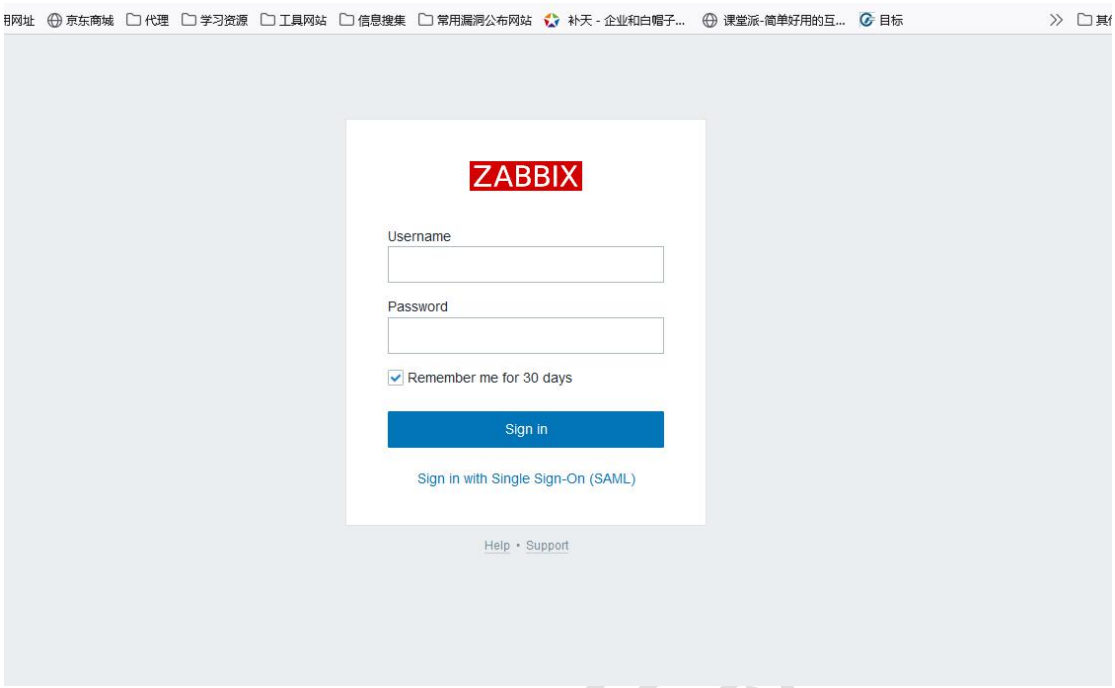
zabbix 5.4.0 - 5.4.8

zabbix 6.0.0alpha1

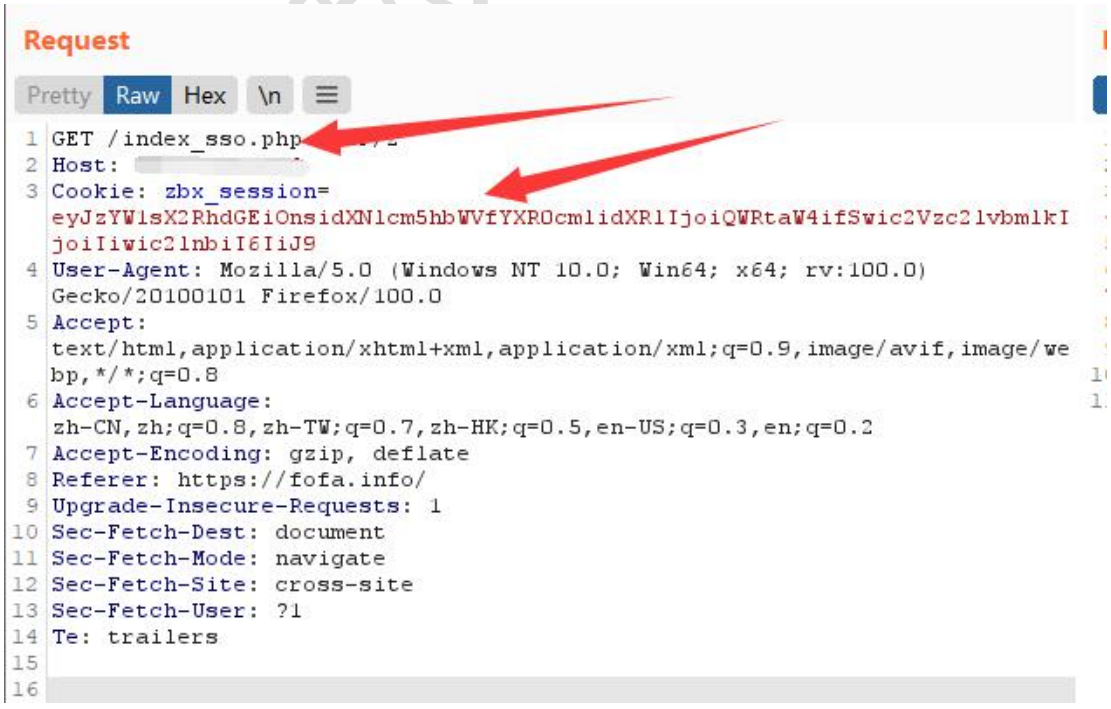
正文：

这次没有靶场搭建，因为临时看到一篇文章所以想尝试复现的，这里我直接搜索，用的什么大家懂得都懂，不懂得这个洞也没必要看，这个在国内能搜索到的很少，基本都是国外的，修复的比例也比较大，找了二十几条数据也就一个有这个漏洞。所以也没有提交的必要。

国内的基本都修复了大家就不用尝试了，多去 M 国那边搞搞就行了
Ok，复现开始
我这里直接实战上手，页面如下

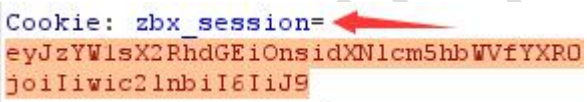


大致就是这个样子，原理我们不讲那么多，大致原理就是
该漏洞存在于 index_sso.php 文件中，由于 index_sso.php 文件未调用 CEncryptedCookieSession::checkSign()
方法对 cookie 进行校验，且客户端的 cookie 可被伪造。
具体的大家可以网上找，这里偏向小白向的复现
我们到了登录页面，打开 burp 进行抓包，开启拦截，我们刷新登录页面
对抓到的页面进行以下修改



一个是第一个箭头处那个位置改为 index_sso.php
第二个就是 cookie 处修改，是我们构造的 payload 加密 base64
Payload：
{"saml_data":{"username_attribute":"Admin"},"sessionid":"","sign":""}

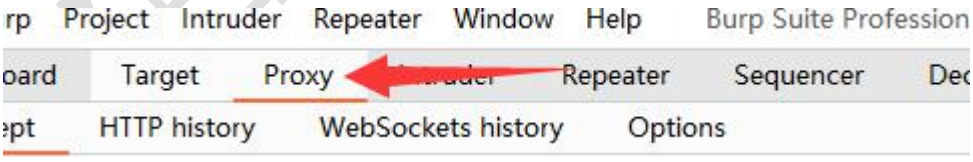
加密后：
eyJzYW1sX2RhdGEiOnsidXNlcm5hbWVfYXR0cmlidXRlIjoiQWRtaW4ifSwic2Vzc2lvbmlkIjoiIiwic2lnbiI6IiJ9

注，如果抓到的包 cookie 后面不是 

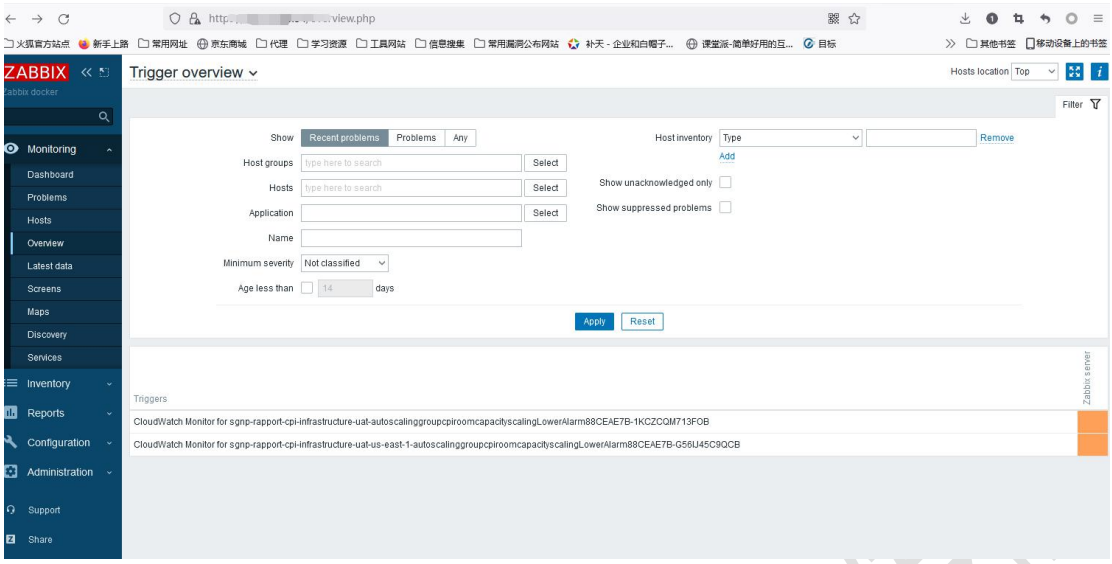
“zbx_session=”这个开头基本就是不能利用

我们修改后发送到重发器中发送

这里有这个回显即为可用，同时返回 302 状态码
我们直接到 proxy 中将修改后的包提交上去即可



然后我们就来到了登录页面



到这里就复现成功了。

交流群：70844080
公众号：白安全组
作者：【白】

参考文章：

https://jishuin.proginn.com/p/763bfbd747db
https://blog.csdn.net/weixin_46944519/article/details/123131257

Exp：
https://github.com/jweny/zabbix-saml-bypass-exp
https://github.com/Mr-xn/cve-2022-23131