**一、靶场搭建**

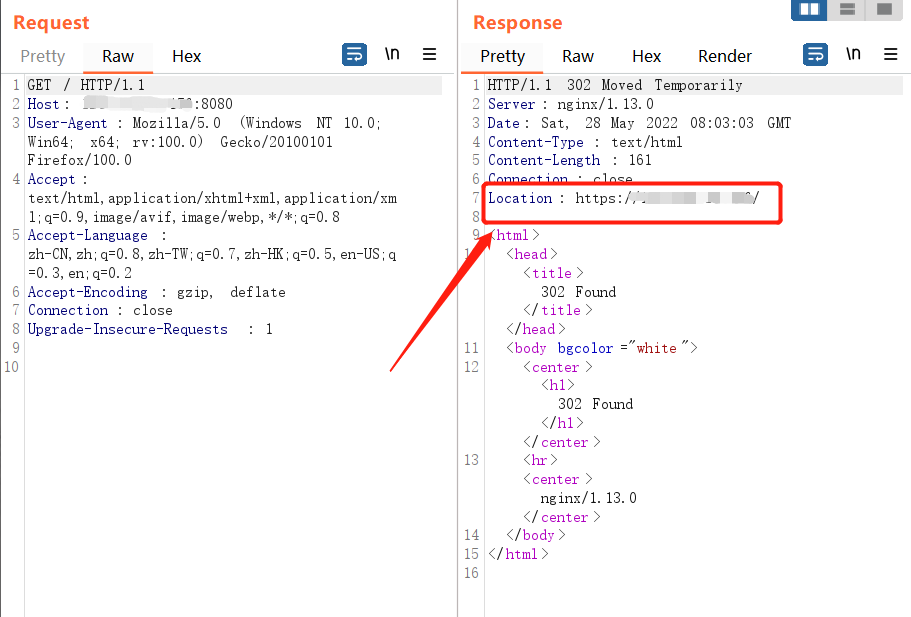
1、Vulhub启动

docker-compose up -d

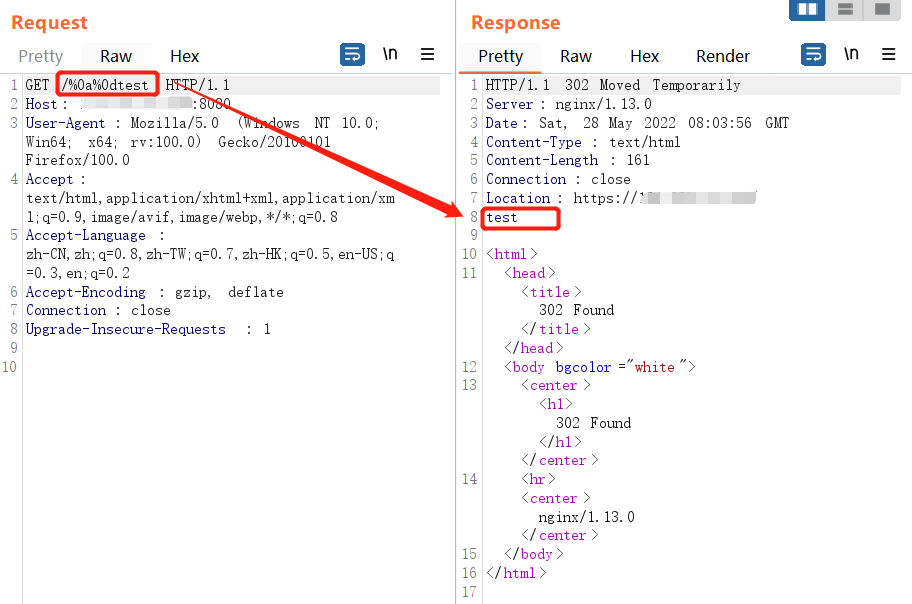
2、运行成功后，Nginx会监听8080/8081/8082三个端口，分别对应三个漏洞

**二、漏洞复现（CRLF注入）**

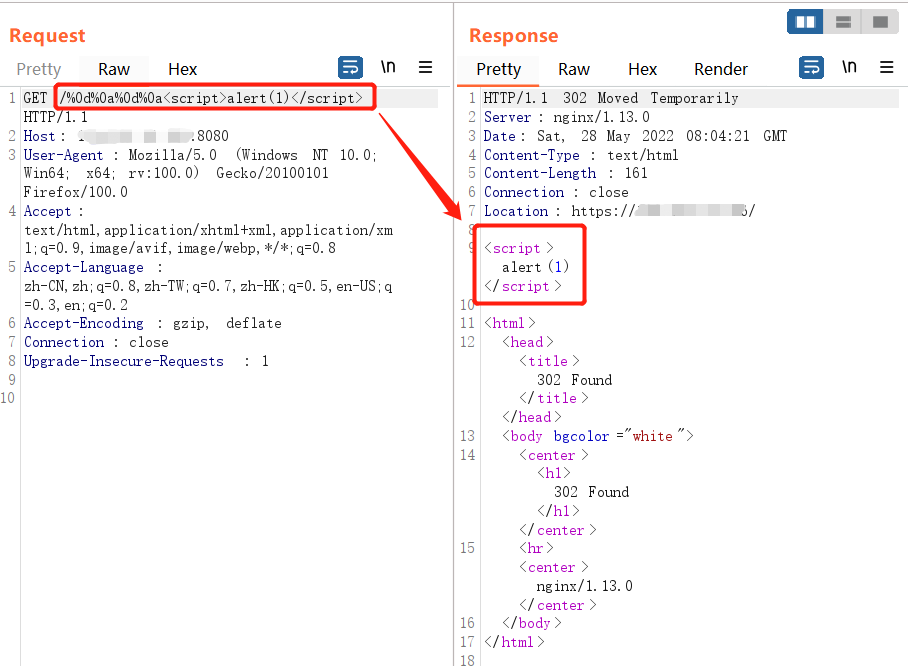
1、当访问8080端口时，Nginx重定向后，会在http响应头中出现Location字段



2、当我们访问<http://x.x.x.x:8080/%0a%0dtest>时，%0a%0d即\r\n，也就是换行符，所以在%0a%0d后可注入恶意数据

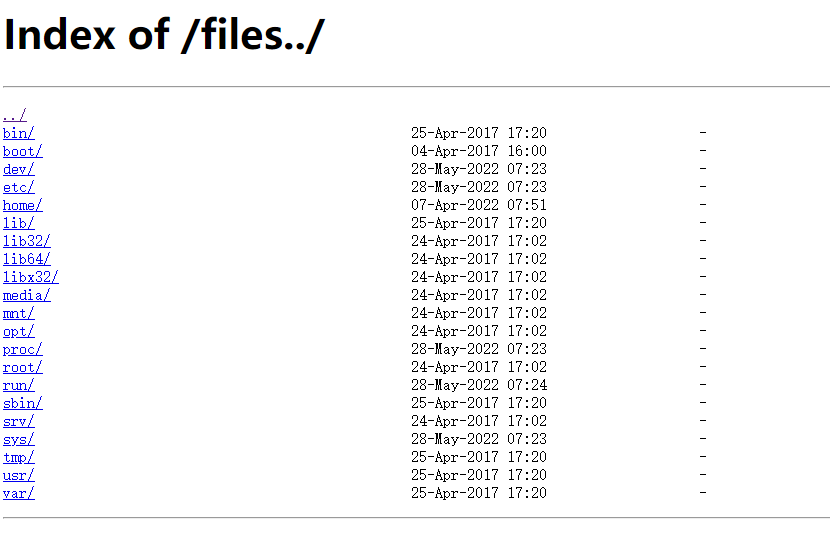


3、添加XSS代码，如[http://x.x.x.x:8080/%0d%0a%0d%0a<script>alert(1)</script](http://x.x.x.x:8080/%0d%0a%0d%0a%3cscript%3ealert(1)%3c/script)>，可以实现XSS攻击，由于浏览器filter限制了XSS，此处未成功弹窗



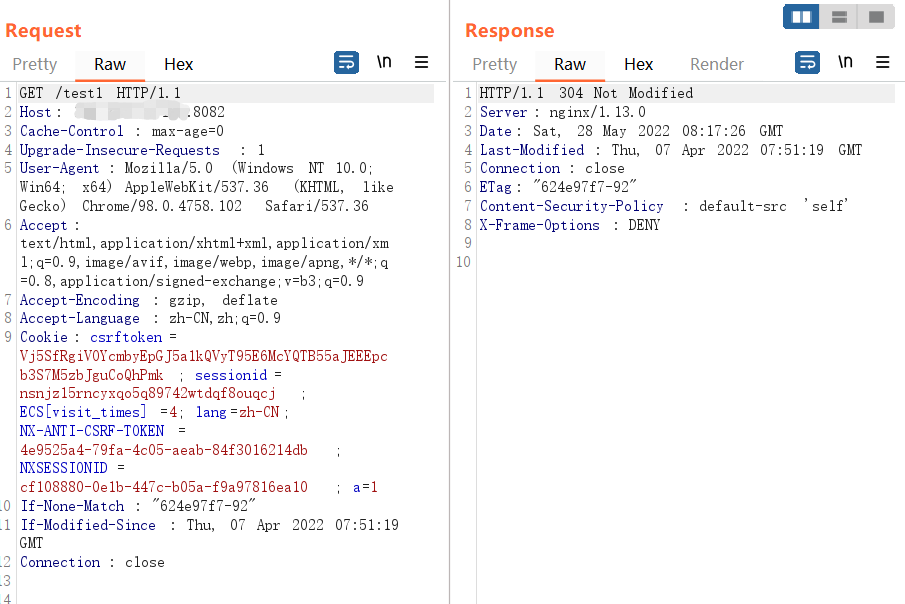
**三、漏洞复现（目录穿越）**

1、访问<http://x.x.x.x:8081/files../>，成功穿越到根目录



**四、漏洞复现（add\_header被覆盖）**

1、访问8082端口的/test1，再访问/test2时数据包中add\_header全部失效





2、构造xss，/test2#<img src=1 onerror=javascript:alert(‘x’)>，暂未成功

