CVE-2018-14574

环境搭建

vulhub docker-compose

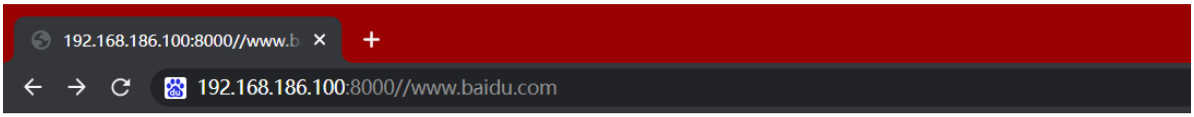
漏洞讲解

什么是任意url跳转漏洞：
服务端未对传入的跳转url变量进行检查和控制，可能导致可恶意构造任意一个恶意地址，诱导用户跳转到恶意网站。
由于是从可信的站点跳转出去的，用户会比较信任
假如http://www.aaa.com/acb?Url=http://www.zhapian.com
（只要将该链接发给用户诱导其点击，即可实现漏洞目的）

Django (<2.0.8)任意url跳转漏洞原因：
Django的配置下，如果匹配上的URL路由中最后一个是/，而用户访问的时候没加/，则Django的配置会转移到带/的请求中。（由配置项中的django.middleware.common.CommonMiddleware，APPEND_SLASH来决定）。

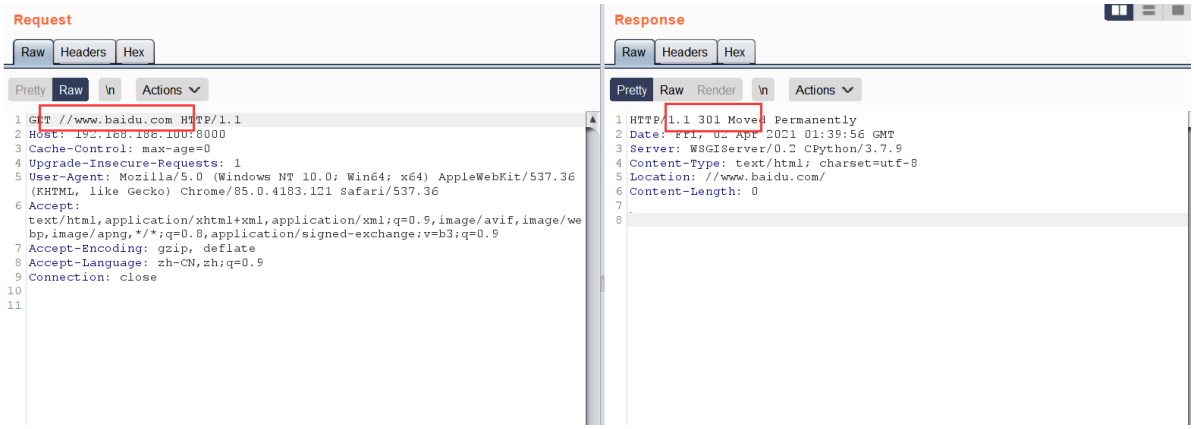
复现

只要在url后加上//想跳转的网页，即可实现跳转，比如百度



Hello, world.

抓包分析



末尾没加/的url自动填补/然后重新发起请求，以如果在末尾加上了/是不会跳转成功的