实验5：会话标识固定漏洞

我个人对本漏洞的理解是，Session会话机制是一种服务端机制，它使用类似于哈希表的结构来保存信息，也就是服务器给用户发一个身份证，如果在程序交互过程中，用户拥有这个身份证，那么就证明客户之前和服务器有一个会话。

而产生漏洞的原因有：

- 会话预测：身份证号被人猜出来了
- 会话劫持：身份证被人抢走了
- 会话重用：你觉得这个身份证挂失了，但是公安局后台没销毁
- 会话固定：在用户进入登陆页面但还未登陆时，就已经产生了一个Session，用户输入信息登陆以后，Session的ID不会改变，也就是说没有建立新Session，原来的Session也没有被销毁。攻击者事先访问系统并建立一个会话，诱使受害者使用此会话登陆系统，然后攻击者再使用该会话访问系统即可登陆受害者的账户。。说白了就是公安局没验证你的信息，进屋就给你发证明，现在有个人搭了一个假公安局套你话。

实操

由于在网络上搜索资源，比较匮乏，环境迟迟搭建不起来，因此我们选择利用dvwa靶场，查看其两次的会话ID`session`是否相同，如果相同,Session的ID不会改变，也就是说没有建立新Session，原来的Session也没有被销毁。

起初的SessionID为：`29etqqb8jsocaqedtv52be81bg`

```
POST /dvwa/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 88
Cache-Control: max-age=0
sec-ch-ua: "Not?A_Brand";v="8", "Chromium";v="108"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/dvwa/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: security=impossible; PHPSESSID=29etqqb8jsocaqedtv52be81bg
Connection: close

username=admin&password=password&Login=Login&user_token=8c6d36cf151424d5615ca79080633629
```

登陆后重新退出的SessionID为：`29etqqb8jsocaqedtv52be81bg`

```
POST /dvwa/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 88
Cache-Control: max-age=0
sec-ch-ua: "Not?A_Brand";v="8", "Chromium";v="108"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/dvwa/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: security=impossible; PHPSESSID=29etqqb8jsocaqedtv52be81bg
Connection: close

username=admin&password=password&Login=Login&user_token=4928993a2e99d95b38e38cc130ac923c
```

PHPSESSID=29etqqb8jsocaqedtv52be81bg