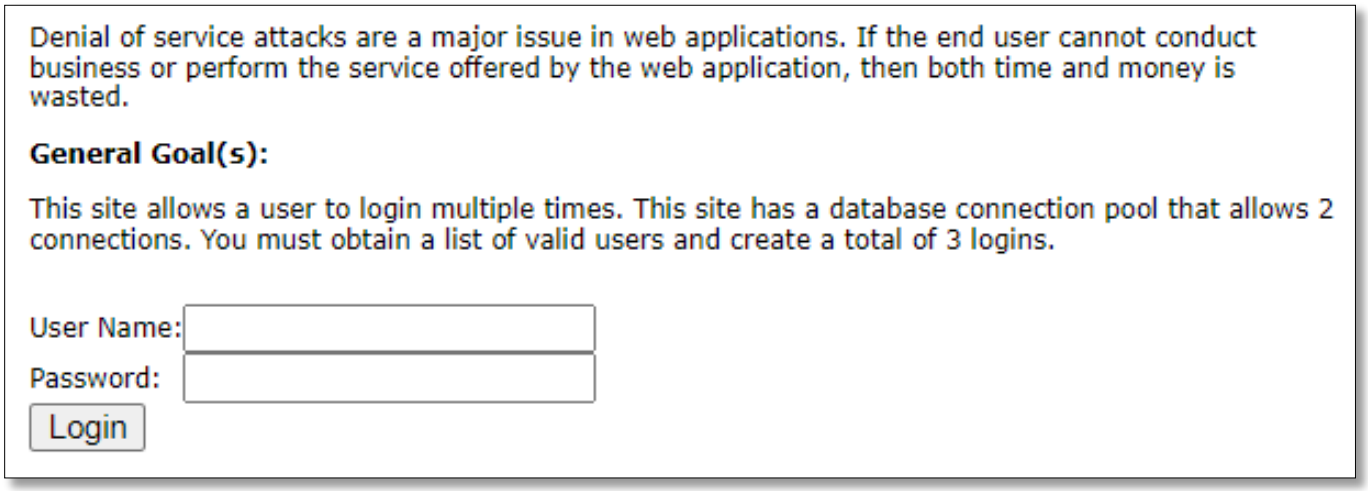
Denial of Service (DoS-DDoS)

Denial-of-Service (DoS) là một cuộc tấn công từ chối dịch vụ phân tán, một nỗ lực làm cho những người dùng không thể sử dụng tài nguyên của một máy tính. Các cuộc tấn công DoS thường hoạt động bằng cách cố tình làm quá tải mục tiêu với các request cho đến khi không thể xử lý, dẫn đến từ chối dịch vụ cho người dùng. Trong cả hai trường hợp, DoS đều tước quyền sử dụng dịch vụ hoặc tài nguyên hợp pháp của người dùng. Một cuộc tấn công DoS được đặc trưng bằng cách sử dụng một máy tính duy nhất để khởi động cuộc tấn công.

Vàoooooo bài nàoooooooooooooo!

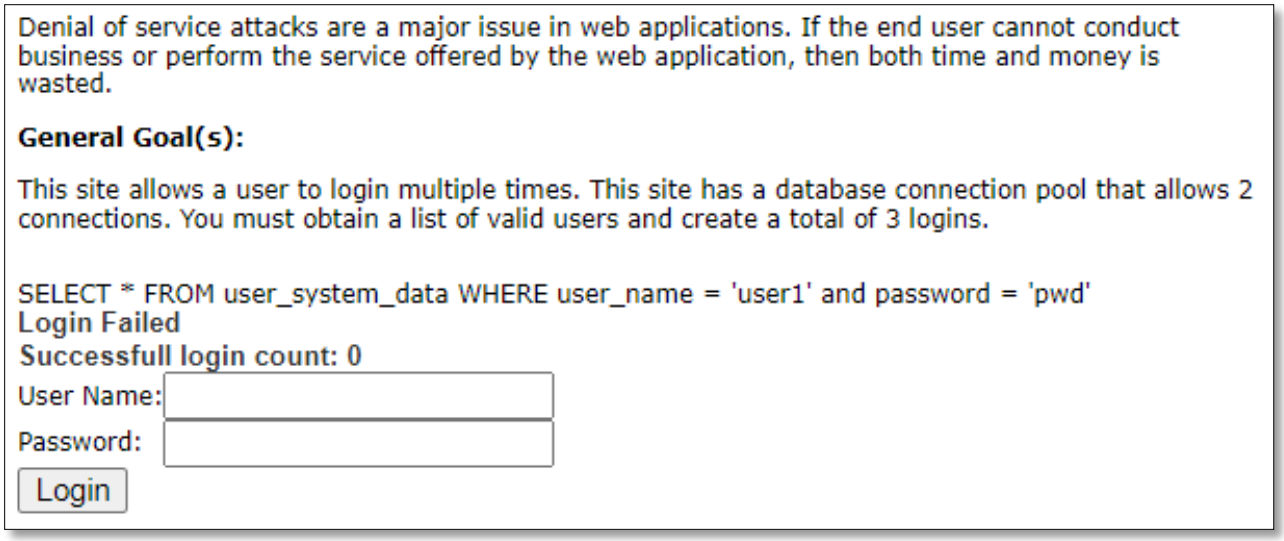


Okay, bài tập yêu cầu ta tấn công từ chối dịch vụ 1 máy chủ web. Máy chủ này chỉ chấp nhận 2 yêu cầu đăng nhập cùng 1 lúc tại 1 thời điểm. Nhìn là biết ta phải làm cách nào đó gửi 1 lúc 3 login request tại 1 thời điểm rồi.

Có nhiều cách làm nhé, bạn có thể mở 3 tab, thực hiện đăng nhập và bắt cả 3 gói tin login lại bằng proxy BurpSuite, rồi nhanh tay forward chúng. Hoặc có thể chỉ bắt 1 yêu cầu login và bruteforce login dựa trên gói tin đó cũng được.

```
1  POST /WebGoat/attack?Screen=63&menu=1200 HTTP/1.1
2  Host: 192.168.48.131
3  Content-Length: 40
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  Origin: http://192.168.48.131
7  Content-Type: application/x-www-form-urlencoded
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
    Safari/537.36
9  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9
   d-exchange;v=b3;q=0.9
10 Referer: http://192.168.48.131/WebGoat/attack?Screen=
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: JSESSIONID=0702E8A391ED290717959535A1275A0B
14 Connection: close
15
16 Username=user1&Password=pwd&SUBMIT=Login
```

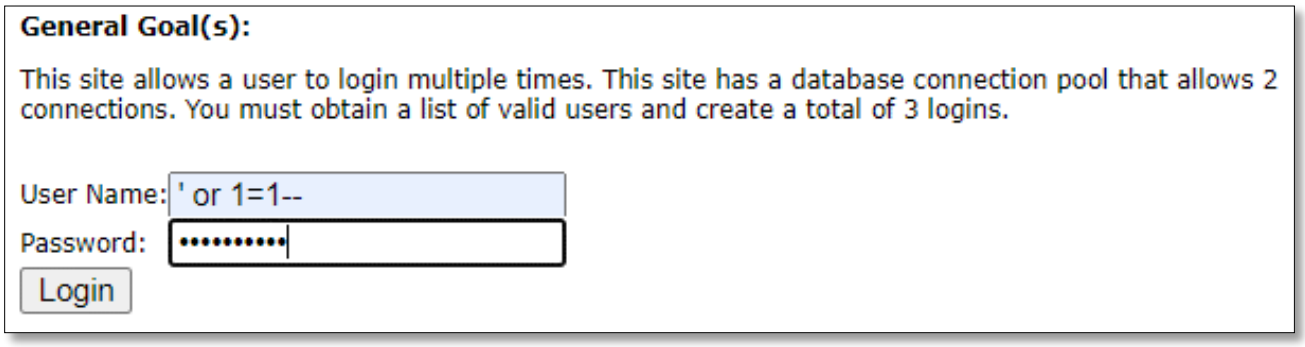
Okay, đây là yêu cầu login của người dùng, mình có tạo 3 request đó nhưng chỉ chụp 1 cái đại diện thôi (vì phải forward 1 cái mới nhìn thấy request thứ 2, mà làm vậy thì không thể nhanh chóng forward cả 3 được). Nhanh tay forward cả 3 tới Server để hoàn thành bài học.

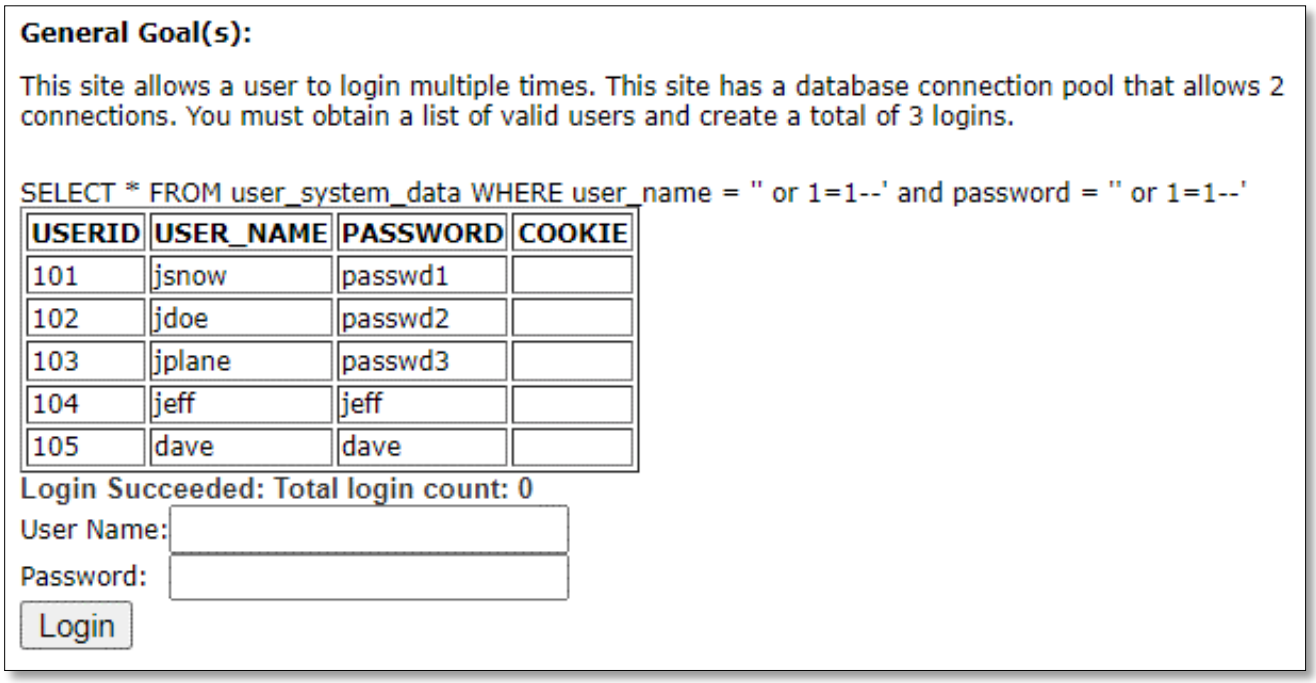


Ở đây thì phát sinh ra 1 vấn đề, vì bài tập không đưa ra chỉ dẫn nào về việc đăng nhập, nên thông tin đăng nhập là tự mình nghĩ ra.

Nhưng chỉ dẫn ở đây! Login lỗi thì nó thông báo lại 1 câu lệnh dùng để truy vấn thông tin của người dùng. Nhìn vào cấu trúc của câu lệnh là ta biết, có thể chèn SQLi vào để vét cạn toàn bộ thông tin trong câu lệnh rồi.

Về việc áp dụng SQLi, mình sẽ không hướng dẫn lại đâu nhé.





Giờ thì có đủ thông tin người dùng để làm bài rồi. Làm lại bước đầu, bắt 3 gói tin login và forward chúng tới server nhé.

```
1  POST /WebGoat/attack?Screen=63&menu=1200 HTTP/1.1
2  Host: 192.168.48.131
3  Content-Length: 44
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  Origin: http://192.168.48.131
7  Content-Type: application/x-www-form-urlencoded
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
    Safari/537.36
9  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9
   d-exchange;v=b3;q=0.9
10 Referer: http://192.168.48.131/WebGoat/attack?Screen=
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: JSESSIONID=0702E8A391ED290717959535A1275A0B
14 Connection: close
15
16 Username=jsnow&Password=passwd1&SUBMIT=Login
```

General Goal(s):

This site allows a user to login multiple times. This site has a database connection pool that allows 2 connections. You must obtain a list of valid users and create a total of 3 logins.

*** Congratulations. You have successfully completed this lesson.**

Congratulations! Lesson Completed