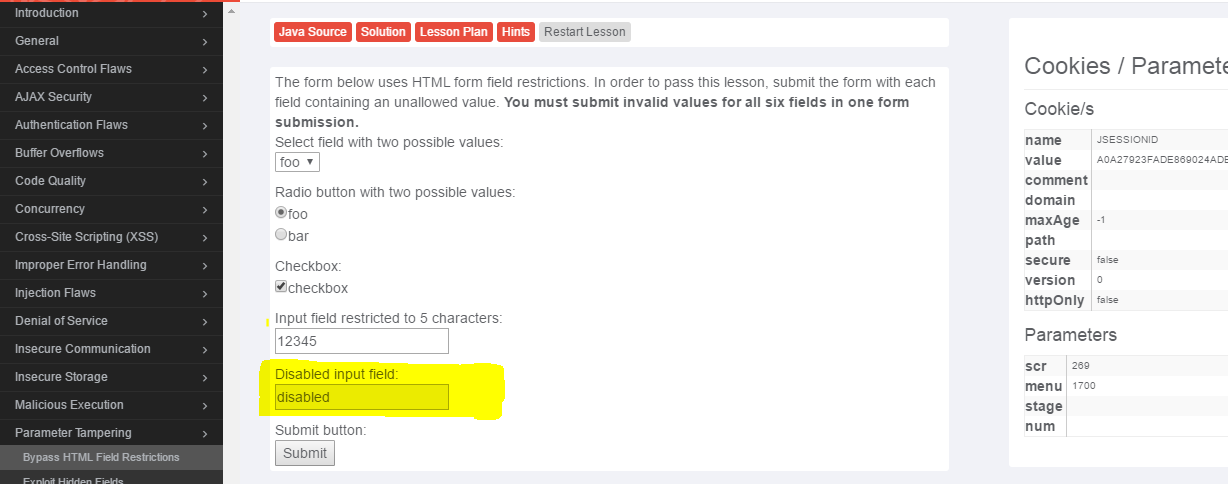
# WEBGOAT

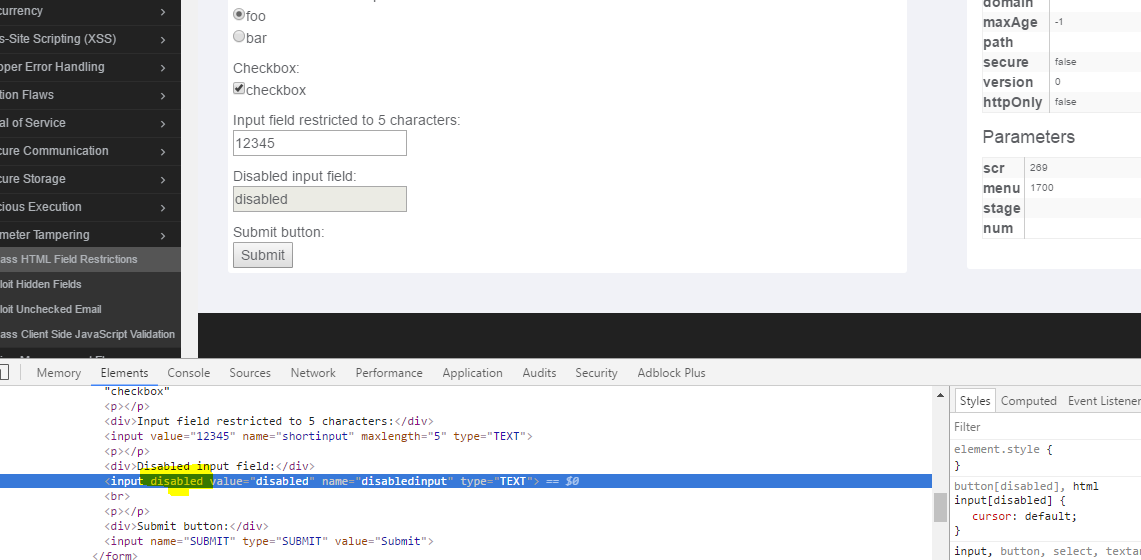
## Lầu Hôn Thìn 14110190

## Parameter Tampering

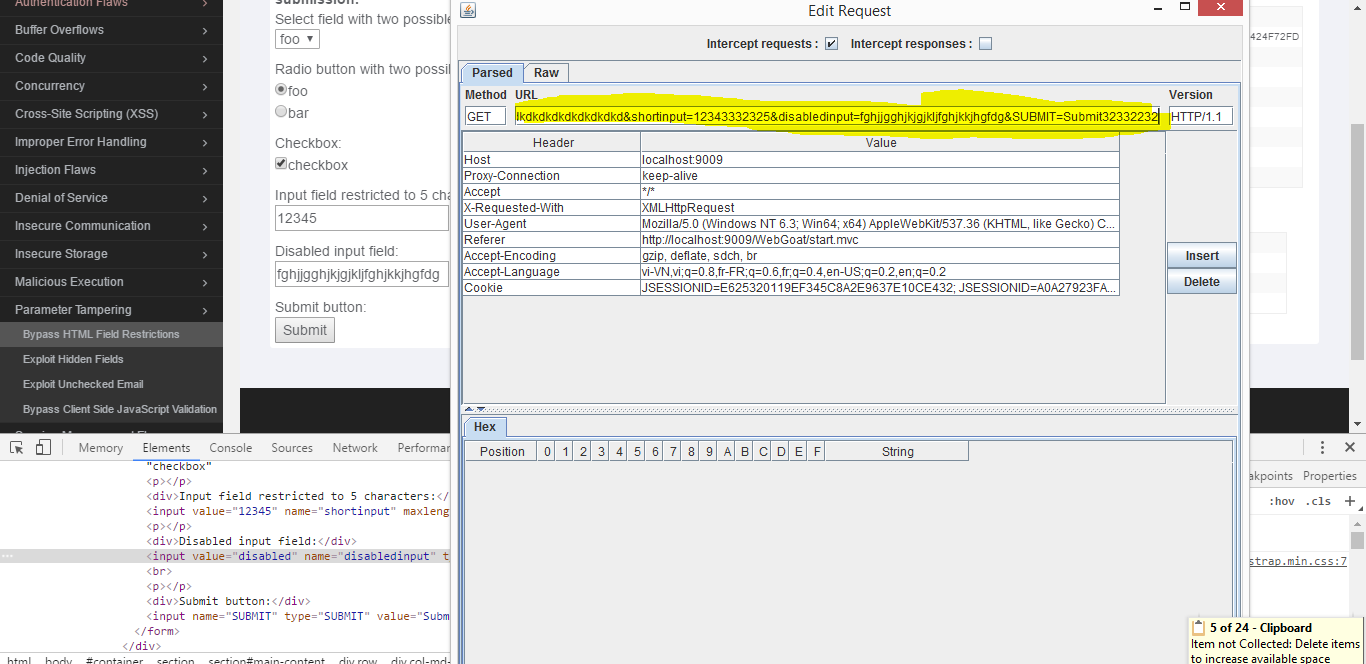
1. Bypass HTML Field Restrictions

Enable “Disabled input field:” nhấn F12 sau đó trỏ tới text input đó và xóa chữ disabled

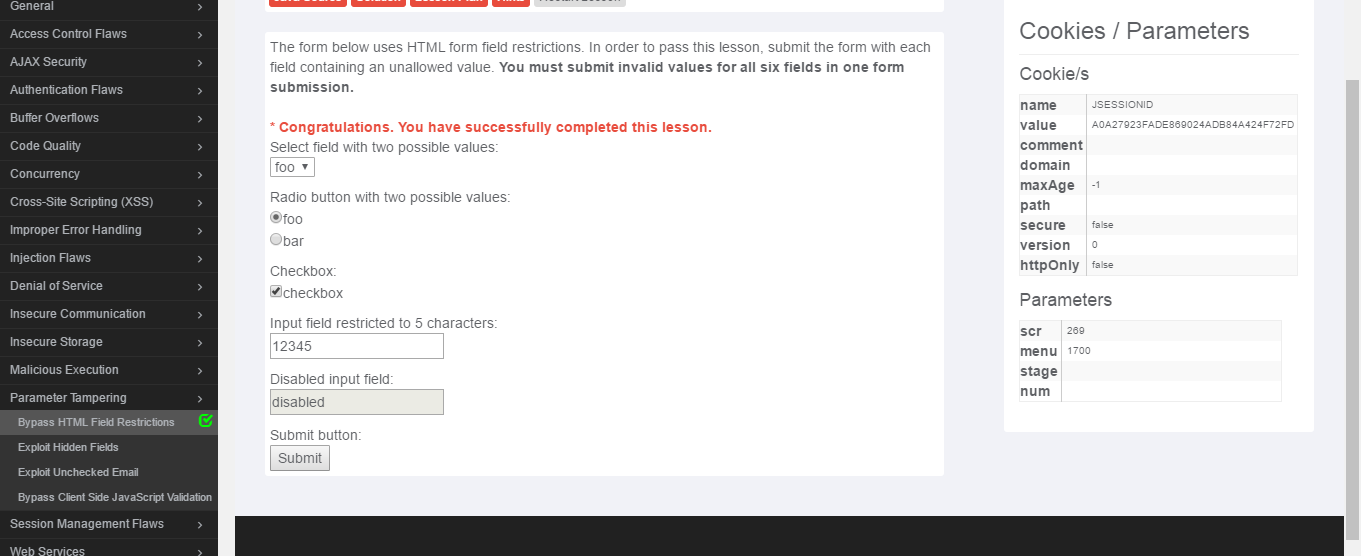


Xóa chữ “disabled” nhập dữ liệu bất kỳ vào ô đó

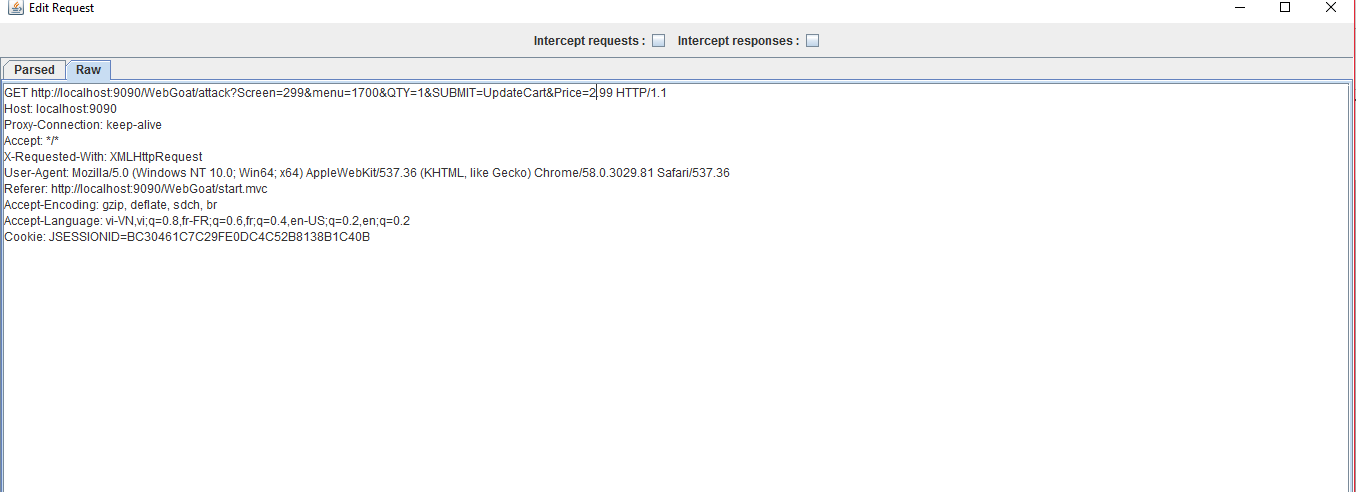
* dùng webscarab bắt gói tin sau khi nhấn submit, đổi giá trị(giá trị không hợp lệ cho mỗi trường) cho 6 ô truyền vào

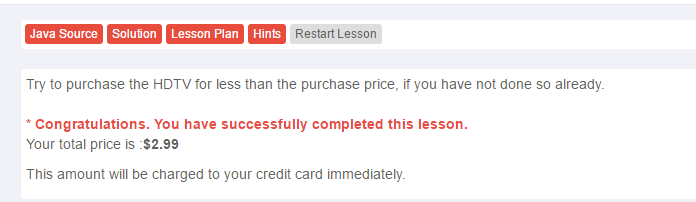


Nhấn Accept changes và được kết quả



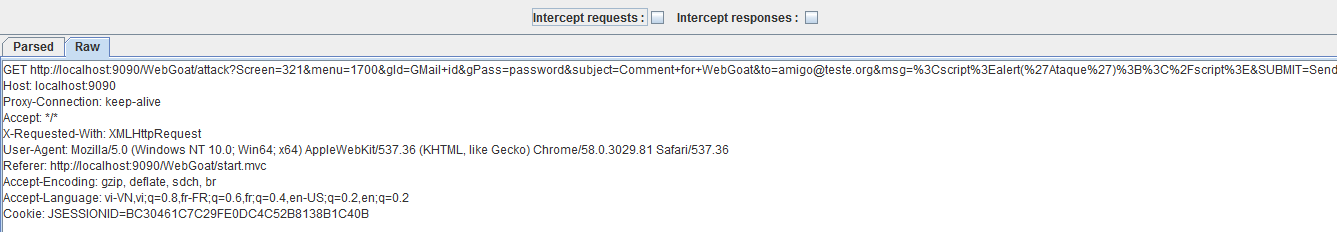
1. Exploit Hidden Fields

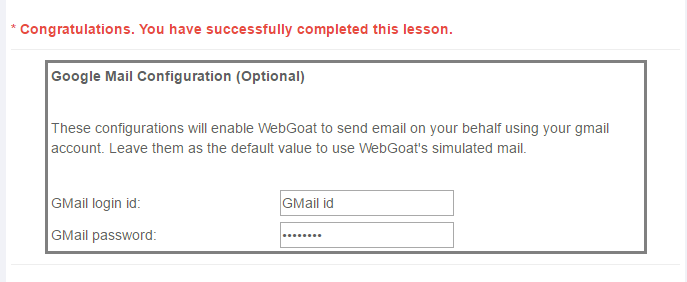
* Sửa UpdateCart&Price=2.99

Thành công

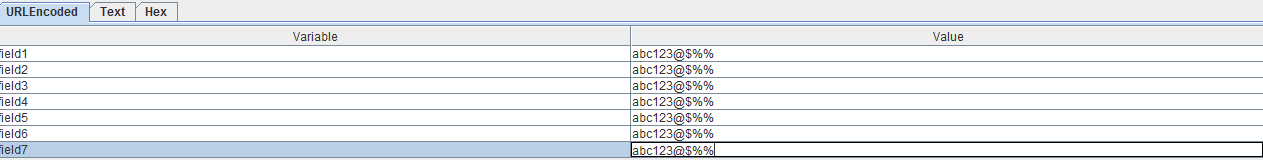
1. [Exploit Unchecked Email](http://localhost:9090/WebGoat/start.mvc#attack/321/1700)

Sửa to=amigo@teste.org



Thành công

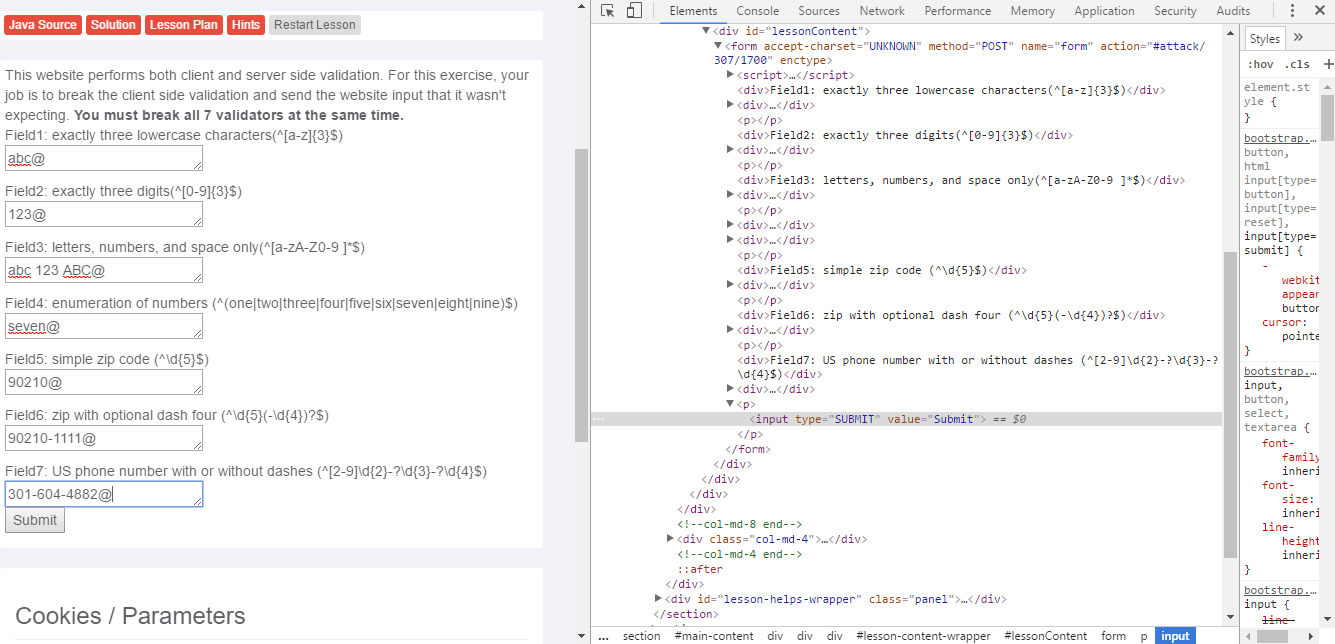
Sửa tất cả các field=abc123@$%%



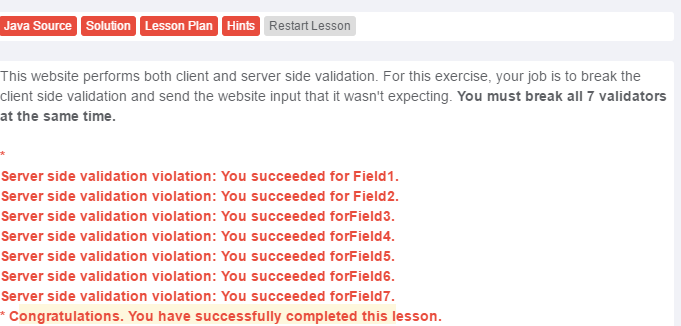
1. [Bypass Client Side JavaScript Validation](http://localhost:9090/WebGoat/start.mvc#attack/307/1700)

Xóa thẻ onclick và thay đổi input type= SUBMIT

Thay đổi tất cả các field



Thành công



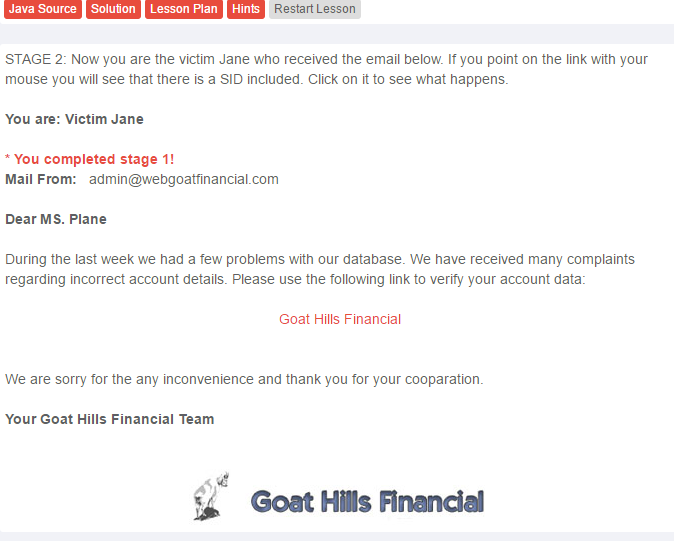
## Session Management Flaws

# Session Fixation

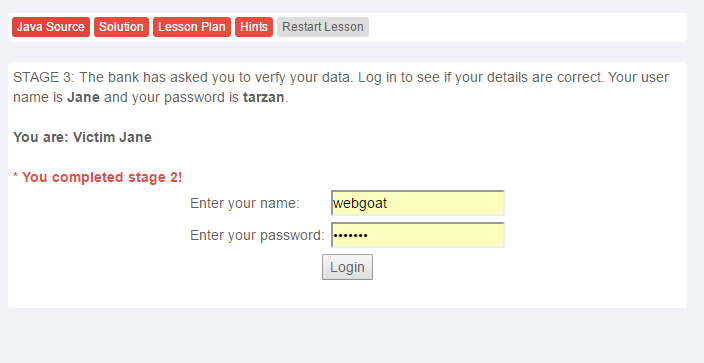
# Sửa thành <a href=#attack/310/1800&SID=Whatever> sau thẻ <center>

# 

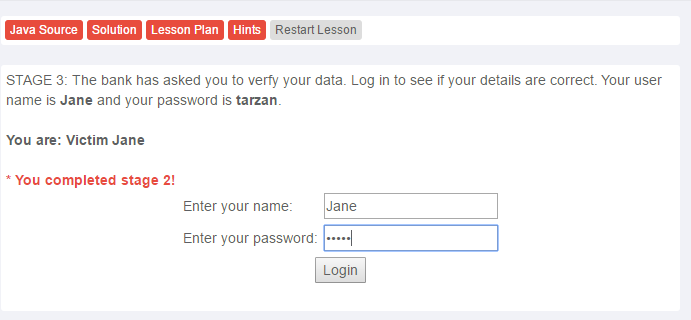
# Hoàn thánh stage1



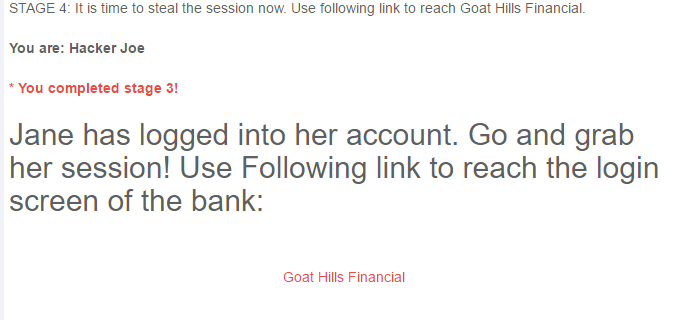
Click vào Goat Hills Financial hoàn thành stage 2



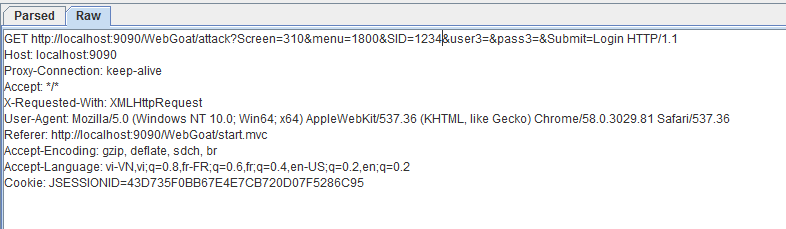
Điền mật khẩu như hình



Hoàn thành stage 3



Click vào Goat Hills Financial và sửa SID=1234



Thành công

