Portswigger: Auth Bypass via Flawed State Machine

Sam Newman

April 2025

1 Website in Question

This section of the website contains a vulnerability with the control flow and state machine storing user authentication variables and states. The lab involves exploiting this vulnerability to access an administrator-privileged account, and using that to delete a user from the system.

2 Business Impact

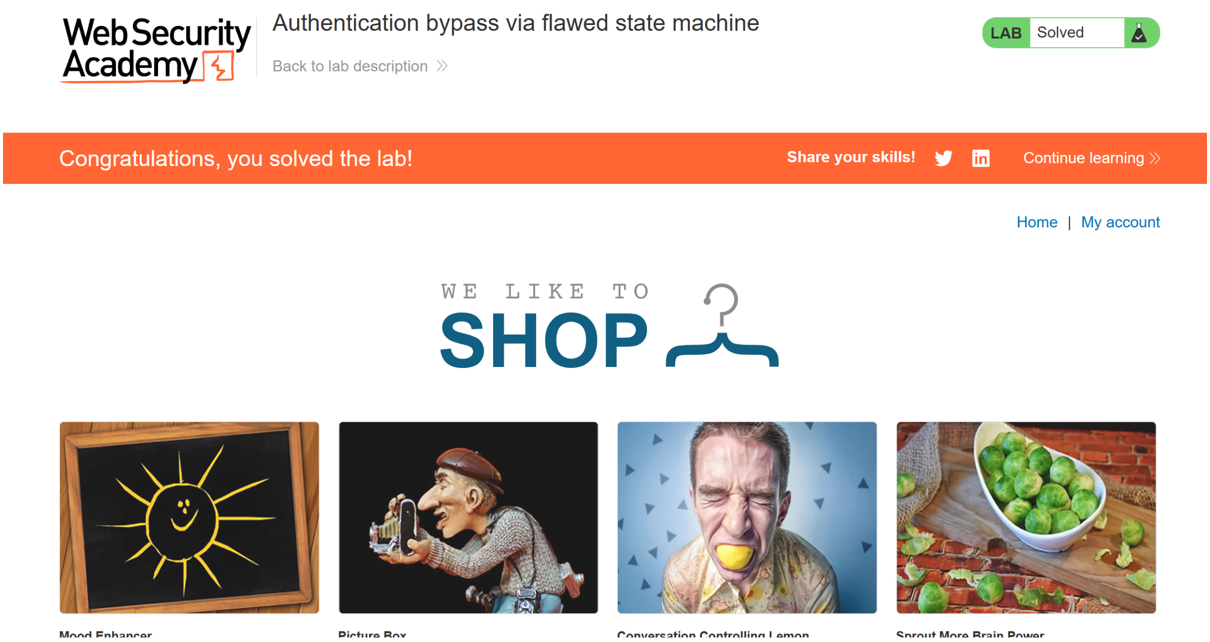
This is an extremely dangerous vulnerability. Using it, any user could gain administrator permissions over the system, wreaking havoc on customer data, orders, accounts, passwords, item prices, and anything else a website administrator could do. The impact from a vulnerability of this magnitude could be devastating to a company.

3 How It Works

- **Utilize** Portswigger to modify requests sent to the website
- **Login** through normal valid user credentials
- **Drop** the GET request directing the user to the /role-selector page
- **Navigate** back to the / directory by manually editing the URL
  You are now an Admin!

4 Why It Works

The website has a vulnerability in the control flow logic. It allows a user that exploits this method to enter states within the inner logic that a normal user should never be able to enter, like the state for *isAdmin* or something along those lines. By interrupting the control flow via dropping the role selection request, we have entered that state.



Authentication bypass via flawed state machine

Back to lab description »

Congratulations, you solved the lab!

Mood Enhancer

Picture Box

Conversation Controlling Lemon

Sprout More Brain Power

Figure 1: Solved Lab

5 How to Mitigate

Fix control flow in website to ensure login requests must complete all steps of the login procedure before they are assigned a valid session login cookie.