

Authentication: Lab

Student worksheet · OWASP Juice Shop

You will get into accounts without stealing the password: guess it, then reset it.

Open **Juice Shop**: `http://localhost:3000`, and the **Score Board**: `http://localhost:3000/#/score-board`. Each solved challenge turns green there.

Rule: do this only on our own Juice Shop. Guessing passwords or resetting someone's account on a real system is an offence under the IT Act.

1. Password Strength (2 stars)

1. Go to **Account** → **Login**.
2. Log in as the admin: email `admin@juice-sh.op`, password `admin123`.
3. You are in as the admin. The Score Board shows **Password Strength** solved.

Why: the admin uses a weak, common password, and the login has no limit on guesses. A real attacker runs a wordlist of the most common passwords; `admin123` is on every such list. Two failures meet here: a weak password *and* no lockout.

If stuck: Login fails: type `admin123` exactly (lower case, digits at the end). The admin's email is on product reviews if you want to see where an attacker finds it.

2. Reset Jim's Password (3 stars)

Jim is a real user. His "security question" has a public answer.

1. On the login page, click *Forgot your password?*.
2. In the email box, type `jim@juice-sh.op`. His security question appears: *"Your eldest sibling's middle name?"*
3. Answer `Samuel` (Jim is a Star Trek reference; it is public trivia). Set any new password in both boxes, for example `Reset2026!`, and submit.
4. The Score Board shows **Reset Jim's Password** solved. You could now log in as Jim with that password.

Why: a security question is a second password that the user did not choose and cannot keep secret: the answer can be looked up. A safe reset sends a one-time link to the account's verified email instead.

If stuck: No question appears: the email must be exactly `jim@juice-sh.op`. "Wrong answer": it is `Samuel`, capital S. Password rejected: use something like `Reset2026!` with a letter, a digit and a symbol.

Stretch. Unsigned JWT (5 stars)

After you log in, the server gives you a token (a **JWT**) with three parts joined by dots: `header.payload.signature`. The signature proves the server made it.

1. Log in. In the developer tools, **Application** → **Local Storage**, copy the `token`.
2. Decode it (for example at `jwt.io`, offline). Read the header and payload.
3. Forge a new token: set the header algorithm to `none`, set the payload email to `jwtn3d@juice-sh.op`, and leave the signature **empty** (keep the trailing dot). Put it back in Local Storage and reload.

Why: a server that accepts `alg: none` trusts a token with *no* signature, so anyone can forge any identity. The fix is one check: accept only the exact algorithm you issue, and reject `none`.

If stuck: It is rejected: that is what a correct server does. Juice Shop accepts it only for the exact forged email. Do not spend long on this one.

What you did

Two ways into an account, neither using the real password: you guessed a weak one (Password Strength) and reset another through a public answer (Reset Jim). Authentication is the whole system around the password: strong passwords, a lockout, no security questions, and ideally a second factor.