Challenge URL: /dvwa/vulnerabilities/weak_id/
Objective: Work out how the ID is generated and then infer the IDs of other system users.
Tools needed: None

Did you remember to read this section's README?

The Guide

Here's what we start with:

Right away, the text tells us to look at our cookies, specifically one called "dvwaSession". And when I think cookies, I think the Firefox developer console. Let's pull that up via the keyboard with `Control+Shift+K`. Let's click the "Generate" button and enter the text `document.cookie` in the console. Here's what I see:

Note that I actually input `document.cookie.split(";")[0]` to hide my session ID. Just a privacy thing for me. You don't have to do that, and it impacts nothing besides what you see in my screenshots.

Oh no, **dvwaSession** is set to "1". I think you know exactly how this is going to go!

All the same, let's alternate between clicking the "Generate" button and viewing our cookie a few times:

dvwaSession becomes "2", then "3", then "4", *ad infinitum*.

So there's our answer. **dvwaSession** gets initialized as "1", then gets incremented by 1 each time you click "Generate". If there were other users, you'd keep following the above process, either manually or via a script of some sort. If you found a gap, something like **dvwaSession** going from "4" to "6", you could deduce another user has **dvwaSession=5** and plan further attacks from there (maybe use a cross-site scripting vulnerability to steal their cookie?).

It's nice to have a quick and easy one for once, isn't it? Challenge complete.