IDATT2503 - Solution Exercise 1

WebGoat

1. A1
2. A3
    - 2: Intercept the profile save request, modify "fullName" in the multipart/formdata to be: `../test`
    - 3: Same as above, but `....//test` (the fix was a non-global regex replace of the string `"../" -> ""`)
    - 4: Now the fullName parameter is fixed, but the user-supplied filename is used, and a path traversal is possible here using: `filename="../myfile.png"`
    - 5: Notice the Location: header in the response, and force browse to this to specify an image. After some fiddling, you may see pathnames in the response. Special chars like `../` are disallowed, so URL encode them and path traverse up until you find the secret file:
        - `%2f%2e%2e%2f%2e%2e%2fpath-traversal-secret`
    - 7: Use "slipit" (install via pip) to craft a Zipslip archive. Ensure that you have an image in your current folder with your WebGoat username. Create a Zipslip path traversal archive using:
        - `slipit --overwrite --separator '/' --prefix /home/webgoat/.webgoat-2023.4/PathTraversal/<username>/ zipslip.zip <username>.**jpg`
        - Note, the pathname may vary, check the WebGoat assignment text for the correct pathname. Next, select this file by clicking on the profile image and upload by clicking on the "Update" button.

Micro-CMS v1:

1. Flag 0: `/page/edit/6` (authorisation bypass via edit)
2. Flag 1: `/page/edit/6'` (apostrophy -> possible start to a SQL injection)
3. Flag 2: XSS in title of new page: `<script>alert(1)</script>`
4. Flag 3: XSS in page content via `<button>` or `<img>` tag: `<button onclick=alert(1)><img src=x onerror=alert(1)>`