https://github.com/viekko/Cybersecurity-and-Data-Privacy-Autumn-2025_Viekko/blob/main/part2.md

- It allows you to create birthdate for the same day → not 15 years old.
- Password has been hashed
- Absence of Anti-CSRF Tokens

  - No Anti-CSRF tokens were found in a HTML submission form.
    A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.

    CSRF attacks are effective in a number of situations, including:
    * The victim has an active session on the target site.
    * The victim is authenticated via HTTP auth on the target site.
    * The victim is on the same local network as the target site.

    CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.

- User Agent Fuzzer

  - Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

Discussion Post: Reporting Findings and Fixes

Introduction

Tester: Veikko

Testausvaihe: Docker & ZAP Security Testing

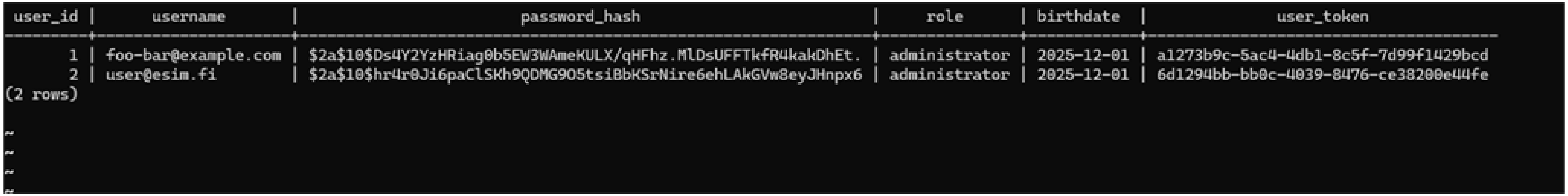
Top 5 Findings:

1. Salaamattomat salasanat
2. SQL Injection
3. Path Traversal
4. Puuttuvat CSRF-tokenit
5. Puuttuva CSP

Finding 1: Salaamattomat salasanat

Status: Fixed ✅

- Alkuperäinen: Salasanat tallennettiin selkokielisinä.
- Verifiointi: Rekisteröin testikäyttäjän, tarkistin tietokannan – salasanat hashattu.
- Evidence:



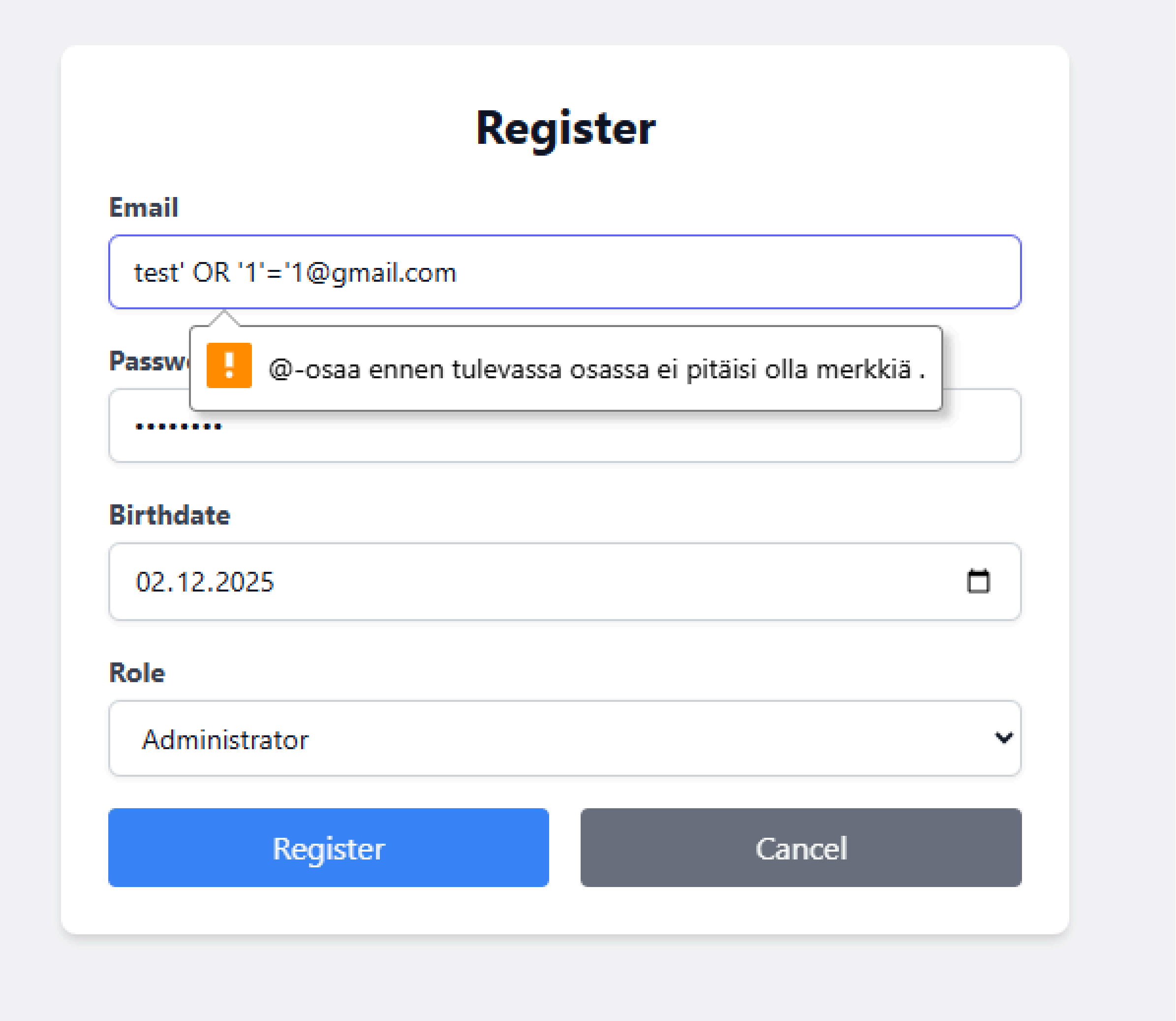
```
 user_id |      username       |                        password_hash                         |     role      | birthdate  |              user_token
---------+---------------------+--------------------------------------------------------------+---------------+------------+--------------------------------------
       1 | foo-bar@example.com | $2a$10$Ds4Y2YzHRiag0b5EW3WAmeKULX/qHFhz.MlDsUFFTkfR4kakDhEt. | administrator | 2025-12-01 | a1273b9c-5ac4-4db1-8c5f-7d99f1429bcd
       2 | user@esim.fi        | $2a$10$hr4r0Ji6paClSKh9QDMG9O5tsiBbKSrNire6ehLAkGVw8eyJHnpx6 | administrator | 2025-12-01 | 6d1294bb-bb0c-4039-8476-ce38200e44fe
(2 rows)

~
~
~
~
```

Finding 2: SQL Injection

Status: Fixed ✅

- Alkuperäinen: Parametrien manipulointi palautti piilotettua dataa.
- Verifiointi: Testasin samoilla syötteillä, ei datavuotoa.
- Evidence:
-



Register

Email

test' OR '1'='1@gmail.com

@-osaa ennen tulevassa osassa ei pitäisi olla merkkiä .

Passw

••••••••

Birthdate

02.12.2025

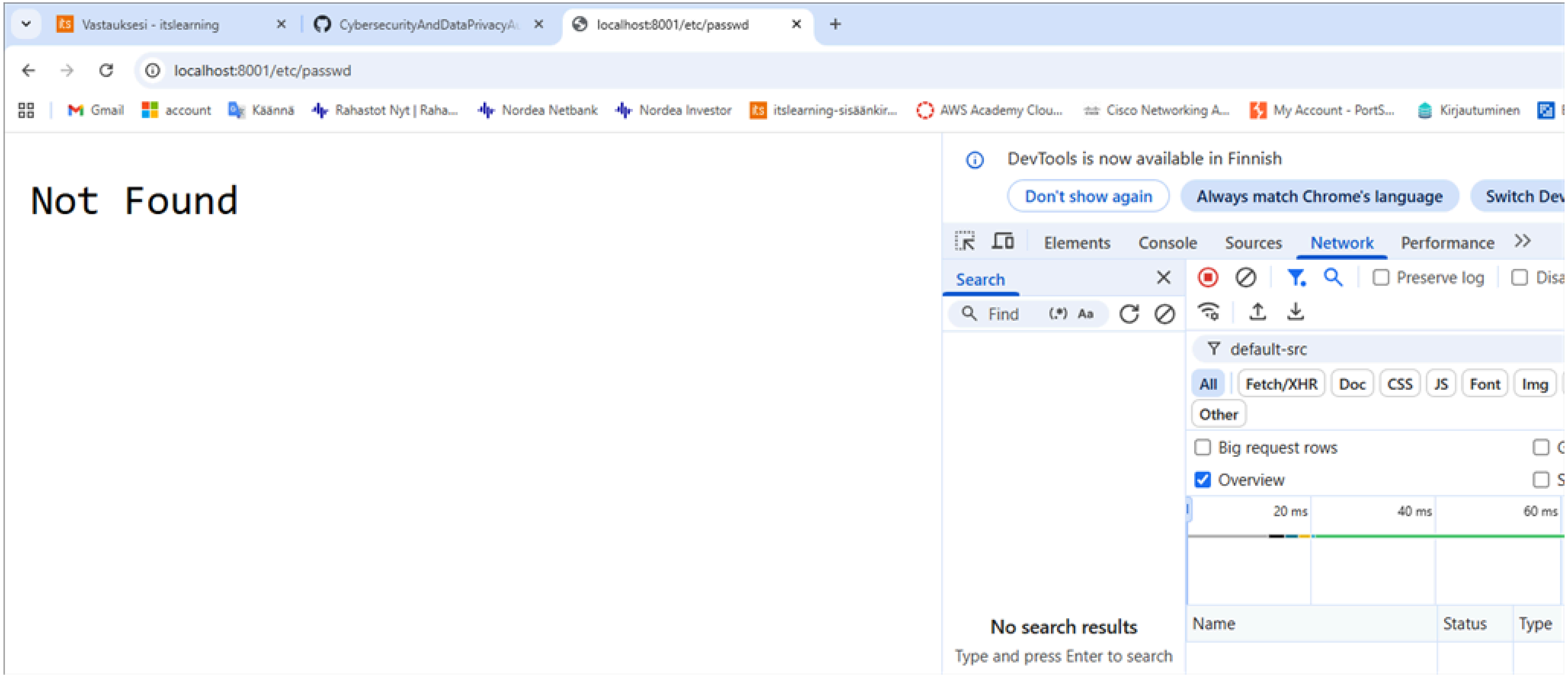
Role

Administrator

Finding 3: Path Traversal

Status: Fixed ✅

- Alkuperäinen: URL-manipulaatio (../) mahdollisti tiedostojen luvun.
- Verifiointi: Testasin ../-polkuja, palvelin esti pyynnöt.
- Evidence:



localhost:8001/etc/passwd

Not Found

DevTools is now available in Finnish

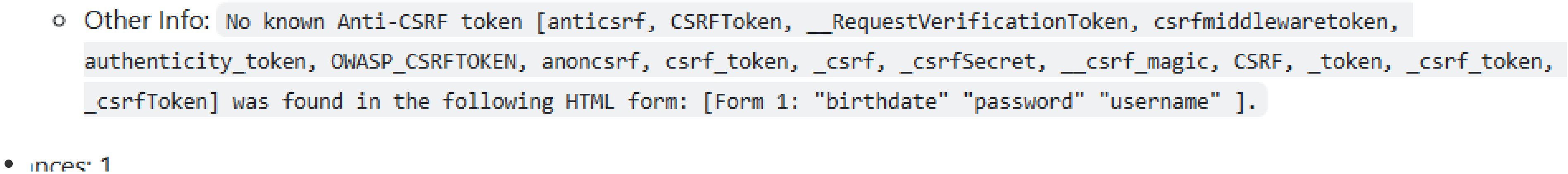
No search results

Type and press Enter to search

Finding 4: Puuttuvat CSRF-tokenit

Status: Not Fixed ⚠️

- Alkuperäinen: Lomakkeissa ei ollut anti-CSRF-suojausta.
- Verifiointi: ZAP-skannaus havaitsi edelleen puuttuvan tokenin rekisteröintilomakkeessa.
- Evidence:



- Other Info: `No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "birthdate" "password" "username"].`

- inces: 1

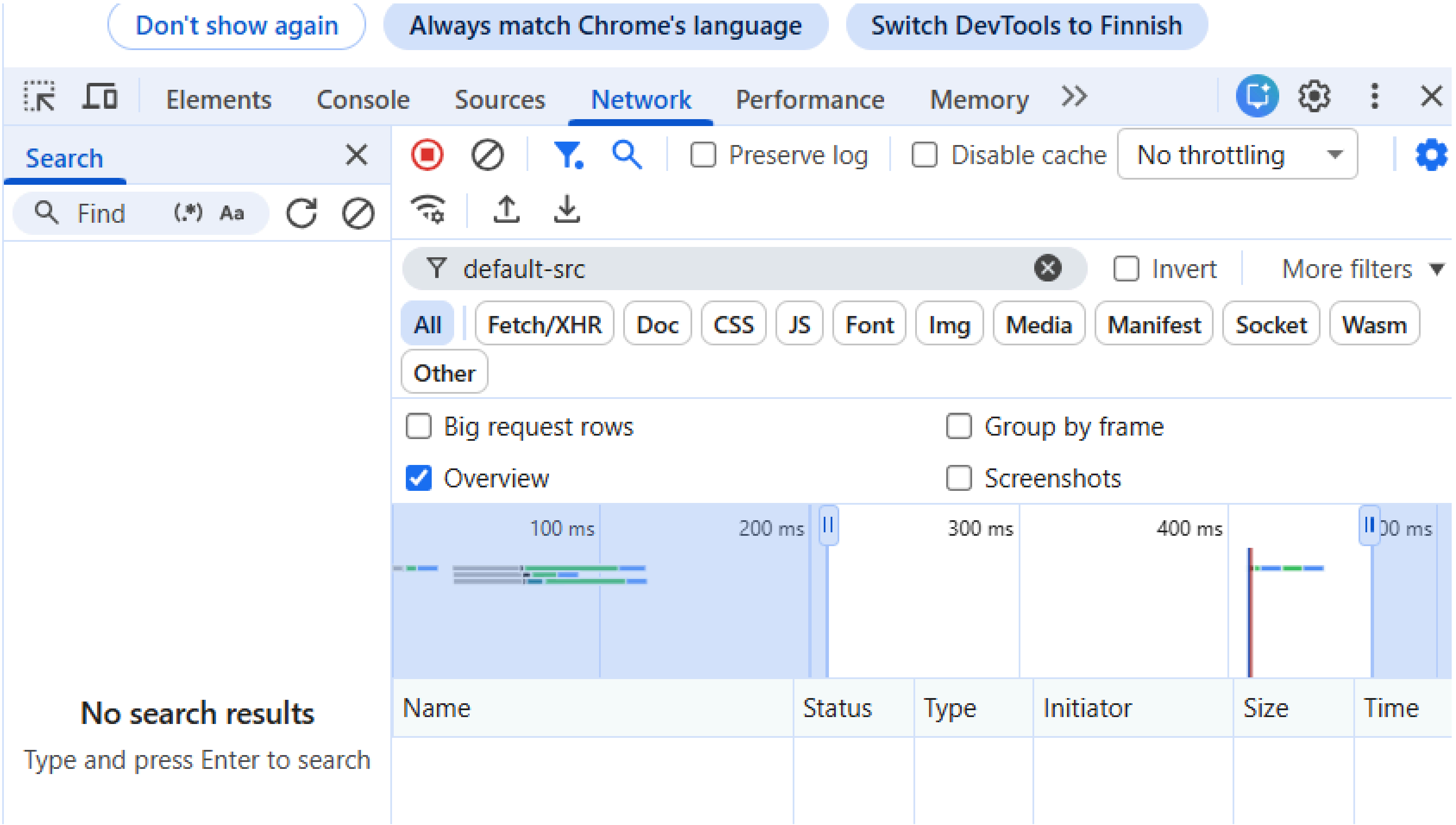
Finding 5: Puuttuva CSP

Status: Not Fixed ⚠️

- Alkuperäinen: Sivulla ei ollut Content Security Policy -asetuksia.
- Verifiointi: Tarkistin HTTP-headerit, CSP lisätty / puuttuu.
- ## 4️⃣ Content Security Policy (CSP)
- **Manuaalinen testaus:**

  1. Avaa sivu selaimessa ja tarkista HTTP-headerit (Chrome DevTools → Network → Response Headers).
  2. Etsi header `Content-Security-Policy`.
  3. **Jos CSP puuttuu tai on liian löysä (esim. `default-src *`), XSS on mahdollinen.**
  4. Voit testata myös manuaalisesti XSS-skripteillä (esim. `<script>alert(1)</script>`), ja jos ne suoritetaan, CSP ei suojaa.

- **Vinkki:** CSP voi myös olla osa HTML `<meta>`-tagia, tarkista sekin.
- Evidence:



□ Preserve log □ Disable cache

Filter: default-src □ Invert

□ Big request rows □ Group by frame

☑ Overview □ Screenshots

Name	Status	Type	Initiator	Size	Time

No search results

Type and press Enter to search

-

Summary Table

Finding	Status	Verified By
Salaamattomat salasanat	Fixed ✅	Tietokannan tarkistus
SQL Injection	Fixed ✅	Parametrisoidut testit
Path Traversal	Fixed ✅	URL-manipulaatiotestit
Puuttuvat CSRF-tokenit	Not Fixed ⚠️	ZAP-skannaus
Puuttuva CSP	Not Fixed ⚠️	Header-tarkistus