**InfoSec Learn Lab - Reconnaissance**

**13.03.2023**

**Grigoraș Ana-Maria**

**Application Security and Pentesting ILV mcr22**

**Dr. Gerald Emerick**

**Task 2:**

Google advanced commands:

1. site:cfrcalatori.ro intitle:login - <https://www.cfrcalatori.ro/cum-cumpar-online/capture-login/>
2. site:ratbv.ro inurl:16-dus.html - <https://www.ratbv.ro/afisaje/16-dus.html>
3. filetype:pdf intitle:train - <https://www.oebb.at/static/tarife/en/guide_for_travelling_with_the_oebb_night_train_in_germany/Resources/pdf/1834078859__en.pdf>
4. filetype:ppt intext:mama - <https://t1.daumcdn.net/cfile/tistory/153A5B4450179A6028?download>

**Task 3:**

**3.1:**

**3.1. a:**

312Ville 192.168.1.10/isihack/

Web server type: Microsoft-IIS/7.5

Web server version: 7.5

**3.1. b:**

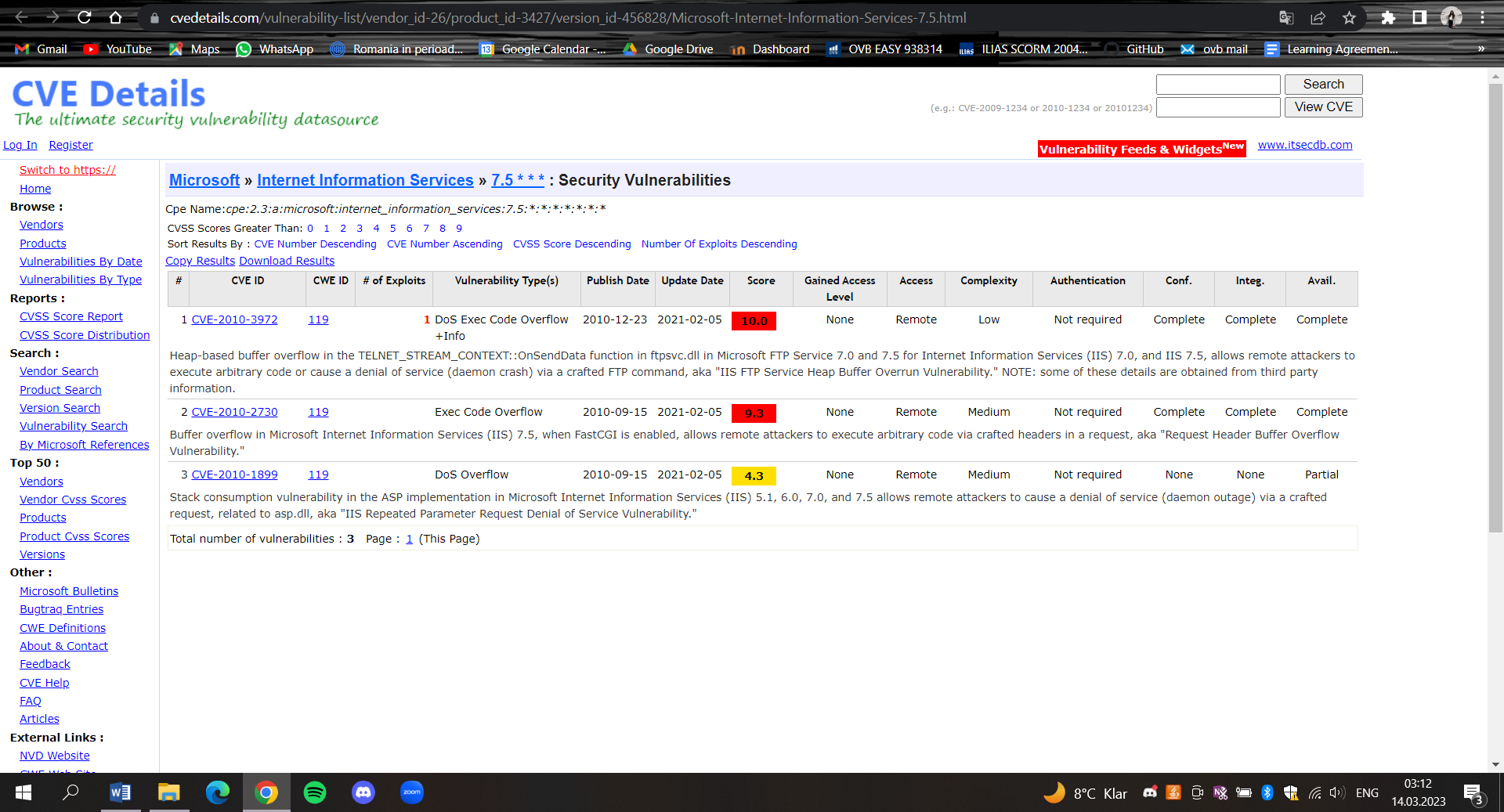
MSP2 192.168.1.40/dvwa

Web server type: Apache/2.2.8 (Ubuntu) DAV/2

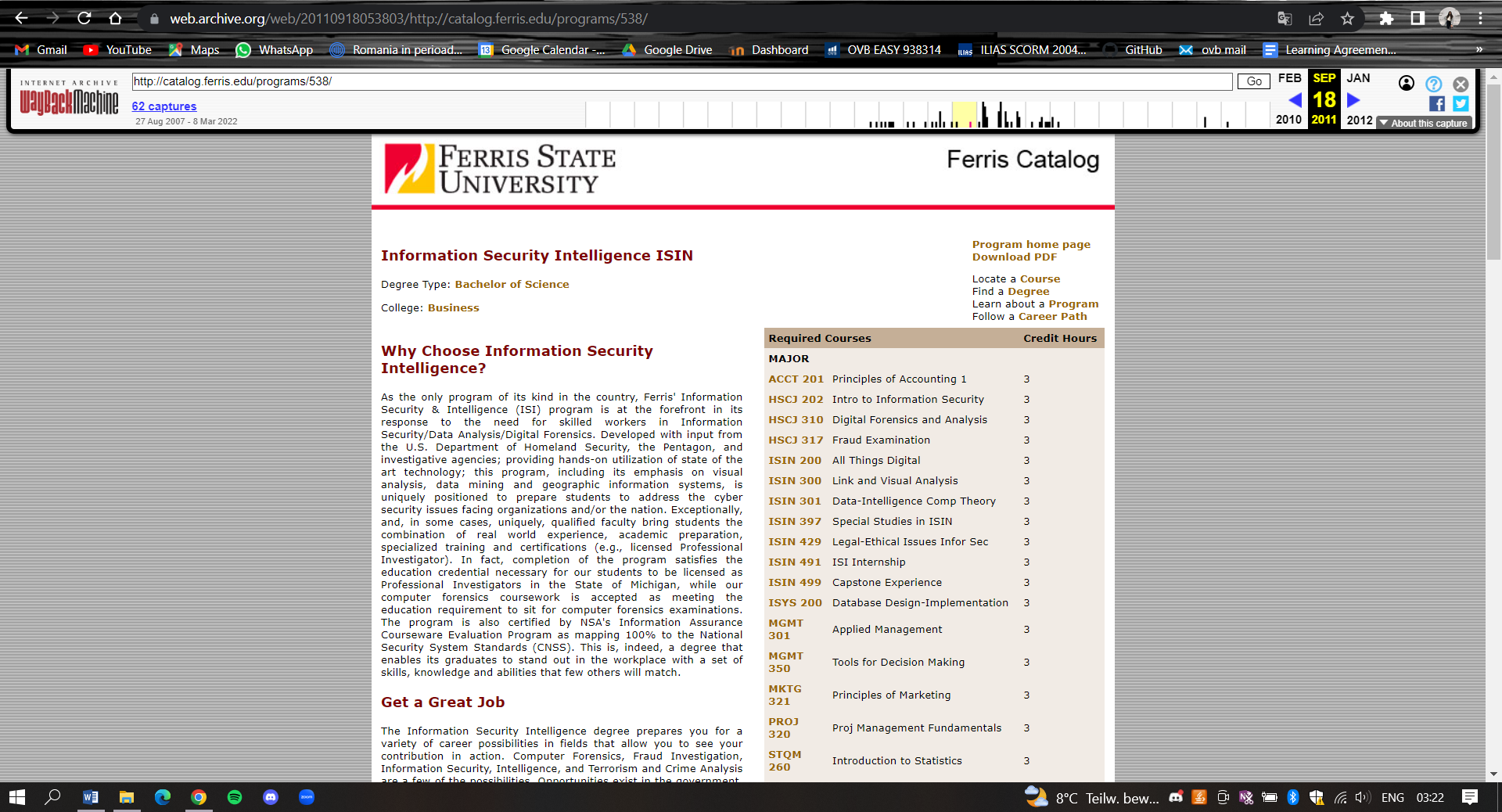
Web server version: 2.2.8

**3.2:**

By using the website provided, I have discovered a vulnerability that involves denial of service, code overflow, and unauthorized information access. Specifically, there is a heap-based buffer overflow in Microsoft-IIS/7.5 that allows hackers to execute malicious and oppressive code or cause a server disruption. This vulnerability is identified by the Common Weakness Enumeration (CWE) ID, 119, which relates to the operations performed on memory buffers and the lack of certainty in validating each location.



**Task 4:**

****

PREL 240 -> it appears until 25 Feb 2011. Since 18 Sept 2011, it does not appear anymore because it is not required anymore.

The GISC ones are the same, all present at 25 Feb 2011 and 18 Sept 2011. They appear in 2012 too.