

CYBERSECURITY LAB

Alessandro Renda

Dipartimento di Ingegneria e Architettura, Università degli Studi di Trieste

EPSS – LAB

Academic Year 2025/2026

Exam

Folder name for material submission **01_EPSS**

EPSS Lab

- *Can you predict which recent CVEs will achieve high EPSS scores in the coming months?*



... aka “**Fanta CVE**”

Tasks and delivery

Overview – Step I – Individual lab activity

Deadline: 17/10/2025

- Data gathering
 - NVD Data (published within the last month **01/09/2025 – 30/09/2025**)
 - EPSS Data (latest available as of today, **01/10/2025**)
- Data exploration
- CVE selection
 - Filter the CVEs with low EPSS (<1%)
 - Select 10 CVEs with low EPSS that you think will reach high EPSS by the end of the course
 - Share the selected CVE ids with the instructor (by the deadline, i.e., two weeks)
 - Track the EPSS of your CVEs over time

- See `template_submission.csv` as an example for submission
- Update your file in the Submissions folder in Teams as `[fancy-name].csv`

Overview – Step 2 – Class activity

- Discussion of takeaways
- Leaderboard reveal

On last course lecture



🏆 Leaderboard

	Gruppo	Most improved EPSS(CVE-i)	Sum of area under EPSS curves	Days above threshold (0.5)	CVEs above threshold
1	E.P.S.S. Express (Everyone P	0.0203	0.002	0	0
4	Hackstreet Boys	0.0209	0.0014	0	0
2	EPSScially Dangerous	0.0005	0.0001	0	0
7	Score & Exploit	0.0004	0.0001	0	0
3	Exploit This!	0.0004	0.00008	0	0
0	404NotFounders	0.0004	0.00007	0	0
6	Predictable Payloads	0.0002	0.00006	0	0
8	Segfault Syndicate	0.0004	0.00006	0	0
9	The Zero-Dayers	0.0004	0.00006	0	0
5	NullPointerZ	0.0001	0.00005	0	0

Exam: codebase and report required

- Codebase
- Technical report with the description and discussion of each step
 - Data gathering
 - NVD Data (published within the last month 01/09/2025 – 30/09/2025)
 - EPSS Data (as of today, 25/09/2025)
 - Data exploration
 - CVE selection
 - Filter the CVEs with low EPSS (<1%)
 - Select 10 CVEs with low EPSS that you think will reach high EPSS by the end of the course
 - Share the selected CVE ids with the instructor (by the deadline, i.e., two weeks)
 - Track the EPSS of your CVEs over time
 - Include takeaways at the end of the monitoring period

- Suggested tools for the required material in a later slide

Tools

Data Gathering

- CVEs metadata
- NVD API
<https://nvd.nist.gov/developers/vulnerabilities>
- JSON format

```
▼ root [] 3283 items
▼ 0
▼ cve
  id "CVE-2025-6935"
  sourceIdentifier "cna@vuldb.com"
  published "2025-07-01T00:15:26.503"
  lastModified "2025-07-07T14:46:10.930"
  vulnStatus "Analyzed"
  cveTags [] 0 items
▼ descriptions [] 2 items
  ▼ 0
    lang "en"
    value "A vulnerability was found in Campcodes Sales and Inventory System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /pages/payme
nt_add.php. The manipulation of the argument cid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used."
  ► 1
▼ metrics
  ► cvssMetricV40 [] 1 item
  ▼ cvssMetricV31 [] 2 items
    ► 0
    ▼ 1
      source "nvd@nist.gov"
      type "Primary"
      ▼ cvssData
        version "3.1"
        vectorString "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H"
        baseScore 9.8
        baseSeverity "CRITICAL"
        attackVector "NETWORK"
        attackComplexity "LOW"
        privilegesRequired "NONE"
        userInteraction "NONE"
        scope "UNCHANGED"
        confidentialityImpact "HIGH"
        integrityImpact "HIGH"
        availabilityImpact "HIGH"
        exploitabilityScore 3.9
        impactScore 5.9
      ► cvssMetricV2 [] 1 item
      ▼ weaknesses [] 1 item
        ► 0
      ▼ configurations [] 1 item
        ▼ 0
          ▼ nodes [] 1 item
            ▼ 0
              operator "OR"
              negate false
              ▼ cpeMatch [] 1 item
                ▼ 0
                  vulnerable true
                  criteria "cpe:2.3:a:campcodes:sales_and_inventory_system:1.0:*:*:*:*:*:*"
                  matchCriteriaId "B0012671-CC91-49D0-A3C8-152ADAB98F4B"
          ► references [] 6 items
```


Data Gathering

- EPSS data
https://www.first.org/epss/data_stats
- CSV format
 - CVE ID
 - EPSS
 - Percentile
 - CVE-1999-0005: EPSS = 0.17478 and percentile = 0.94767
 - It is more likely to be exploited than 94.767% of all CVEs

	cve	epss	percentile
0	CVE-1999-0001	0.01269	0.78596
1	CVE-1999-0002	0.16835	0.94646
2	CVE-1999-0003	0.90339	0.99569
3	CVE-1999-0004	0.04164	0.88205
4	CVE-1999-0005	0.17478	0.94767
...
287670	CVE-2025-8225	0.00013	0.01366
287671	CVE-2025-8226	0.00025	0.05121
287672	CVE-2025-8227	0.00051	0.15837
287673	CVE-2025-8228	0.00036	0.08912
287674	CVE-2025-8229	0.00028	0.06076
287675 rows x 3 columns			

(Suggested) tools

- Programming language: Python
- Environment: Jupyter notebooks (or [Google Colab](#))
 - Interactive web-based environment
 - New to jupyter? See [LAB_01_Environment.ipynb](#) for an introduction
- MISC (other tools and libraries)
 - Pandas
 - *"designed to make **data pre-processing** and **data analysis** fast and easy in Python"*
 - New to Pandas? See [LAB_02_Pandas.ipynb](#) for an introduction
 - You may want to also look at
 - [LAB_03_Plotting.ipynb](#) for an introduction to the plotting landscape in Python
 - [Streamlit](#): open-source Python framework to deliver dynamic data apps

(Suggested) tools for the technical report

1. Start from the template [LAB_EPSS.ipynb](#)
 - It contains code cells for initial data gathering
 - It contains some code cells for data exploration and text cells for comments
2. Modify the template
 - Update and add *code cells* at your need
 - Include *text cells* to explain and discuss each step
3. Produce the report
 - An html export of a well documented notebook is enough
 - ... include takeaways at the end of the monitoring period
4. Share codebase and report with the instructor

In particular:

- Discuss insights from exploratory analysis
- Describe CVE selection

Asynchronous project development

- ... *that is: you develop the project after the first deadline*
- Use the **same dataset**
 - NVD Data (published within **01/09/2025 – 30/09/2025**)
 - EPSS Data (as of **01/10/2025**)
- Exact same steps but **no need to share the selection**
 - Filter the CVEs with low EPSS (<1%)
 - Select 10 CVEs with low EPSS that you think will reach high EPSS by the end of the course
 - ~~• Share the selected CVE ids with the instructor (by the deadline, i.e., two weeks)~~
 - Track the EPSS of your CVEs over time