# Damian Krawczyk

*Release 0.0.1*

**Damian Krawczyk**

**Jan 13, 2023**

# CONTENTS

**LimberDuck.org**

Tools for Cybersecurity engineers and managers to automate their work.

**PROJECTS**

Click here to check my projects.

**NOTES**

Click here to check my notes.

**BOOKMARKS**

Click here to check some interesting bookmarks.

**SHORTCUTS**

Click here to check useful shortcuts.

CHAPTER

ONE

# ABOUT

I'm an enthusiast of **automation** in both my private and professional life. The main reason for that is TIME - one of the most precious thing we have. Contemporary technology lets us design and implement user-friendly solutions that can significantly enhance the way we live or work. At the base of these solutions is DATA - a subsequent treasure that requires appropriate protection. This leads to my other biggest interest - **Information Security**[1] which should be a native part of every product at the early stage of its development, and properly maintained throughout its whole life cycle. I have a pleasure to do both working as a **Security Engineer** and **DevOps Engineer** being responsible for maintenance and improvement of **Vulnerability Assessment**[2] process through majority of my career.

I'm a promoter of open way of working. From coding point of view it means that whenever possible I'm trying to release my solutions as **Open Source**[3] or **Inner Source**[4]. I hope that projects posted here will prove to be handy for you as well.

### projects

Read more about my *projects*.

### contact

Feel free to *contact* with me.

---

[1] *Information Security*
[2] *Vulnerability Assessment*
[3] *Open Source*
[4] *Inner Source*

CHAPTER

TWO

# PROJECTS

## GPI - GOV PL Info


**GPI - GOV PL Info** is a project initiated on April 1, 2021. The main goal of this project is to provide information being sent by Polish Government in a form of mobile notifications, by using Telegram Channels , in both Polish and English.

*read more*

---

## LimberDuck.org

**LimberDuck** (pronounced lm.b dk) is a project initiated on November 26, 2018. The main goal of this project is to create an array of free and Open Source[1] tools dedicated for Security Engineers who wants to automate their work, decrease their workload and focus on data analysis.

*read more*

---

[1] read more about *Open Source* in glossary

## 2.1 GPI - GOV PL Info


**GPI - GOV PL Info** is a project initiated on April 1, 2021. The main goal of this project is to provide information being sent by the Polish Government in the form of mobile notifications. This has been easily achieved by using Telegram Channels. Since the source of information is provided in Polish, all notifications are being sent in Polish. However in addition they are automatically translated into English by the Google Translate service which should make life a bit easier for foreigners in Poland.

### 2.1.1 Target audience

This solution is dedicated **to everyone who cares about their health** and wants to receive information such as the following:

- **warnings about food products and everyday products recall** from sale in Poland due to varying health and safety related reasons published by Main Sanitary Inspectorate in Poland (MSI (Main Sanitary Inspectorate) pl. GIS (Główny Inspektorat Sanitarny)),
- **messages about medicines recall** from sale in Poland due to varying health and safety reasons published by Main Pharmaceutical Inspectorate in Poland (MPI (Main Pharmaceutical Inspectorate) pl. GIF (Główny Inspektorat Farmaceutyczny))
- Polish Government announcements and **actions regarding the coronavirus /** COVID-19.

This solution is dedicated **to everyone who cares about their time** and wants to conveniently receive:

- notifications directly to your smartphone, tablet or computer,
- notifications in English and Polish,
- easy-to-forward notifications,
- information directly from the source (gov.pl),
- information without distracting advertisements,
- an instant search of the message you're looking for, even among millions, e.g. gluten, Salmonella, Pfizer, Janssen, AstraZeneca, Anti-crisis shield, etc.

Finally, this solution is dedicated to everyone who wants to give themselves a break from Facebook, Twitter, TV or the radio.

### 2.1.2 How it works

Current implementation of the solution works as follows:

1. Every day after midnight, content is being downloaded from gov.pl websites.
2. If any articles were published on them on the previous day, you will receive a notification in the Telegram application on your smartphone, tablet or computer.

### 2.1.3 How to subscribe

1. If you don't have Telegram yet, download it from here https://telegram.org/dl/.

   Supported Operating Systems: Android, iOS, iPadOS, Windows, macOS, Linux.
2. Register by following the on-screen instructions.
3. Subscribe to the GPI (GOV PL Info) Telegram Channels.

---

**Note:**

**Your phone number is not visible to the rest of subscribers!**
By default, your number is only visible to people who you've added to your address book as contacts.
Read more here https://telegram.org/faq#q-who-can-see-my-phone-number

---

### 2.1.4 Channel list

**See also:**

Check *THE LIST OF AVAILABLE GPI TELEGRAM CHANNELS* and subscribe to the most interesting ones for you.

### 2.1.5 Technology stack

#### python


Python has been used here to write the code to download the data from the selected gov.pl subpages, parse it, extract articles lately released, translate them using Google Translate service and finally prepare them to be sent to the created Telegram Channels.

| | |
|---|---|
| GPI source code | https://github.com/damian-krawczyk/gov-pl-info |

### GitHub Actions

GitHub Actions have been used to define workflows for selected gov.pl threads and dedicated Telegram Channels. Each workflow starts after midnight CET (Central European Time) or CEST (Central European Summer Time) to get articles released on the previous day.

| GPI workflows | https://github.com/damian-krawczyk/gov-pl-info/actions |
|---|---|

### Telegram

Here, Telegram is the main medium to provide notifications about articles extracted from selected gov.pl subpages. Thanks to an unlimited amount of subscribers, it should be possible to provide notifications to everyone living in Poland (38 137 795 - GUS (Główny Urząd Statystyczny) CSO (Central Statistical Office) in Poland 2020 - source). Telegram supports the following Operating Systems: Android, iOS, iPadOS, Windows, macOS, Linux.

### Google Translate

Google Translate is used to translate notifications from Polish to English. Notifications containing information in both languages are being sent to dedicated Telegram Channels.

## 2.1.6 Contact

---

**Important:** Have you ever faced any problem with this solution?

Have you noticed any errors?

Would you like me to create similar solution suited to your exact needs?

**Let me know about it!**

*CONTACT DETAILS*

---

### GPI Channels

**Attention:** Telegram Channels listed below are not provided nor supported by Polish Government.

### Main Sanitary Inspectorate

MSI - Main Sanitary Inspectorate in Poland (pl. GIS - Główny Inspektorat Sanitarny w Polsce) provides information on its main website https://www.gov.pl/web/gis via threads:

- Messages (*pl. Wiadomości*)
- Warnings (*pl. Ostrzeżenia*)

Information from Warnings (*pl. Ostrzeżenia*) thread are being sent to the Telegram Channel listed below.

CLICK TO SUBSCRIBE GPI GIS Telegram Channel

**Tip:** Click Preview Channel to see the Channel content.

### Main Pharmaceutical Inspectorate

MPI - Main Pharmaceutical Inspectorate in Poland (pl. GIF - Główny Inspektorat Farmaceutyczny w Polsce) provides decisions on RDG website https://rdg.ezdrowie.gov.pl and on its main website https://www.gov.pl/web/gif via threads:

- Messages (*pl. Wiadomości*)
- Interpretations (*pl. Interpretacje*)
- Notifications (*pl. Komunikaty*)

Decisions and information from Messages (*pl. Wiadomości*) thread are being sent to the Telegram Channel listed below.

CLICK TO SUBSCRIBE GPI GIF Telegram Channel

**Tip:** Click Preview Channel to see the Channel content.

### Coronavirus

Polish Government provides information about coronavirus on dedicated website https://www.gov.pl/web/koronawirus via threads:

- Government actions (*pl. Działania rządu*)
- Notifications (*pl. Komunikaty*)

Information from these threads are being sent to the Telegram Channel listed below.

CLICK TO SUBSCRIBE GPI Coronavirus Telegram Channel

**Tip:** Click Preview Channel to see the Channel content.

### GPI Health Check Channel

This Telegram Channel provides information on the lack of articles for a given day. I encourage you to subscribe to this Channel and mute it because notifications will appear there every day in the absence of articles.

CLICK TO SUBSCRIBE GPI Health Check Telegram Channel

**Tip:** Click Preview Channel to see the Channel content.

**Tip:** Check how to mute Telegram Channel here.

## 2.2 LimberDuck.org

**LimberDuck** (pronounced lm.b dk) is a project initiated on November 26, 2018. The main goal of this project is to create an array of free and Open Source[1] tools dedicated for Security Engineers who wants to automate their work, decrease their workload and focus on data analysis.

Table 1: LimberDuck project details

| | |
|---|---|
| main page | https://limberduck.org |
| GitHub page | https://github.com/limberduck |

### Tools

#### nessus file analyzer

This is a GUI (Graphical User Interface) tool that allows you to analyze nessus files containing the results of scans performed by using *Nessus* or *Tenable.sc* by © Tenable, Inc. used for VA (Vulnerability Assessment)[2] process.

*read more*

---

#### nessus file reader

This is a python module that allows you to quickly parse nessus files containing the results of scans performed by using *Nessus* or *Tenable.sc* by © Tenable, Inc. used for VA[2] process.

*read more*

---

#### converter csv

This is a GUI tool that allows you to convert multiple large CSV (comma-separated value) files to XLSX (Microsoft Excel Open XML Spreadsheet) files keeping your operational memory usage at a low level.

[1] read more about *Open Source* in glossary
[2] read more about *Vulnerability Assessment* in glossary

*read more*

### 2.2.1 nessus file analyzer

This is a GUI tool which enables you to parse multiple nessus files containing the results of scans performed by using *Nessus* or *Tenable.sc* by © Tenable, Inc. used for VA[1] process. Parsed scan results are exported to a Microsoft Excel Workbook for effortless analysis.

Operational memory usage will be kept low while parsing even the largest of files. You can run it on your favorite operating system, whether it is Windows, macOS or GNU Linux. As a parsing result, you will receive spreadsheets with a summary view of the whole scan and/or all reported hosts. You will also be able to generate spreadsheets with a detailed view of all reported vulnerabilities[2] and/or noncompliance. It's free and Open Source[3] tool.

Table 2: nessus file analyzer project details

| | |
|---|---|
| main page | https://limberduck.org/en/latest/nessus-file-analyzer |

#### technology stack

[1] read more about *Vulnerability Assessment* in glossary
[2] read more about *vulnerability* in glossary
[3] read more about *Open Source* in glossary

### 2.2.2 nessus file reader

This is a python module which enables you to quickly parse nessus files containing the results of scans performed by using *Nessus* or *Tenable.sc* by © Tenable, Inc. used for VA[1] process. This module will let you get data through functions grouped into categories like file, scan, host, and plugin to get specific information from the provided nessus scan files e.g. file size, report name, report hosts names, the number of target hosts, the number of hosts scanned with credentialed checks, the number of reported plugins per Risk Factor, exact host scan times, outputs of particular plugins and a lot more. It's free and Open Source[2] tool.

Table 3: nessus file reader project details

| | |
|---|---|
| main page | https://limberduck.org/en/latest/nessus-file-reader |

#### technology stack

### 2.2.3 converter csv

This is a GUI tool which lets you convert multiple large CSV files to XLSX files keeping your operational memory usage at a low level. You can run it on your operating system no matter if it is Windows, MacOS or GNU Linux. It's free and Open Source[1] tool.

Table 4: converter csv project details

| | |
|---|---|
| main page | https://limberduck.org/en/latest/converter-csv |

[1] read more about *Vulnerability Assessment* in glossary
[2] read more about *Open Source* in glossary
[1] read more about *Open Source* in glossary

### technology stack



CHAPTER

THREE

# NOTES

## 3.1 Apple Automator

dakr.link/n2

dakr.link/n2

### 3.1.1 Quick Actions

#### Open in

#### Open in Visual Studio Code

1. Open *Automator*
2. Go to *File* > *New*.
3. Choose *Quick Action*.
4. Change *Workflow Receives current* to *files or folders* in *Finder.app*.
5. Add a *Run Shell Script* action by drag and drop.
6. Change *Pass input* to *as arguments*
7. Copy and paste the following in the shell script box:

```
open -n -b "com.microsoft.VSCode" --args "$*"
```

8. Go to *File* > *Save* and save it as e.g. *Open in Visual Studio Code*.
9. Go to Finder.
10. Click RMB (right mouse button) on folder or file.
11. Choose from menu *Quick Actions* > *Open in Visual Studio Code*

**Note:** If you have *Path Bar* enabled in Finder (`alt-cmd P`) and you want to use this *Quick Action* also from *Path Bar*, click RMB on folder or file in *Path Bar* and choose from menu *Services* > *Open in Visual Studio Code*.

Open in Visual Studio Code, based on jnovack post @ stackoverflow.com
CC BY-SA 4.0

### Open in pyCharm

1. Open *Automator*
2. Go to *File* > *New*.
3. Choose *Quick Action*.
4. Change *Workflow Receives current* to *files or folders* in *Finder.app*.
5. Add a *Run Shell Script* action by drag and drop.
6. Change *Pass input* to *as arguments*
7. Copy and paste the following in the shell script box:

```
open -n -b "com.jetbrains.pycharm" --args "$*"
```

8. Go to *File* > *Save* and save it as e.g. *Open in PyCharm*.
9. Go to Finder.
10. Click RMB on folder or file.
11. Choose from menu *Quick Actions* > *Open in PyCharm*

**Note:** If you have *Path Bar* enabled in Finder (`alt-cmd P`) and you want to use this *Quick Action* from *Path Bar*, click RMB on folder or file in *Path Bar* and choose from menu *Services* > *Open in PyCharm*

## 3.2 Insert current date and time


dakr.link/n1

### 3.2.1 Visual Studio Code

1. Install Insert Date String extension created by Jakub Synowiec.
2. Insert date and time:
   - `Shift-cmd I` (macOS)
   - `Ctrl-Shift I` (Windows/Linux)
3. Go to extension settings if you want to change format of inserted date and time and change setting named *Insert Date String: Format*:
   - `YYYY-MM-DD hh:mm:ss` (default value) e.g. `2021-12-30 09:07:11`
   - `YYYY-MM-DD hh:mm:ss ZZZZ` (UTC Time offset value included) e.g. `2021-12-30 09:07:52 +0100`
4. Read more in Usage instructions.

## 3.3 Test note

dakr.link/test-note

Test note body

CHAPTER

FOUR

# BOOKMARKS

dakr.link/bookmarks

Here you can find some interesting links. See **source file** and **changelog** on GitHub.

## 4.1 documentation

### 4.1.1 changelog

- keep a changelog - example how to maintain changelog `[en]` `[pl]` `[more]`

### 4.1.2 Sphinx

- **my list** of Sphinx related GitHub repositories `[en]`
- list of Sphinx extensions `[en]`

### 4.1.3 versioning

- Semantic Versioning 2.0.0 - set of rules and requirements that dictate how version numbers are assigned and incremented. `[en]` `[pl]` `[more]`

## 4.2 programming languages

### 4.2.1 python

- strftime.org - Python strftime cheatsheet `[en]`

## 4.3 version control systems

- starchart.cc - plot your repository stars over time [en]
- Shields.io - quality metadata badges for open source projects [en]

CHAPTER

FIVE

# SHORTCUTS


dakr.link/shortcuts

Here you can find some useful shortcuts. See source file and changelog on GitHub.

| shortcut | description | product name | OS (Operating System) |
|---|---|---|---|
| `CapsLock-alt LMB` | vertical marking | Visual Studio Code | macOS |
| `Shift-cmd-P` | command palette | Visual Studio Code | macOS |
| `Shift-alt Up` | copy selected lines | Visual Studio Code | macOS |
| `Shift-alt Down` | copy selected lines | Visual Studio Code | macOS |
| `alt Up` | move up selected lines | Visual Studio Code | macOS |
| `alt Down` | move down selected lines | Visual Studio Code | macOS |
| `cmd-D` | add this page to bookmarks | Safari, Chrome, Firefox | macOS |

CHAPTER

SIX

# CONTACT

linkedin.com/in/damian-krawczyk-in

github.com/damian-krawczyk

damian@damiankrawczyk.com

Katowice, Poland / remote

CHAPTER

SEVEN

# GLOSSARY

**Open Source**
: Generally, Open Source software is software that can be freely accessed, used, changed, and shared (in modified or unmodified form) by anyone. Open source software is made by many people, and distributed under licenses that comply with the Open Source Definition.

  *Source:* https://opensource.org/faq#osd

**Information Security**
: Information Security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.

  *Source:* https://www.sans.org/information-security

**Inner Source**
: InnerSource takes the lessons learned from developing open source software and applies them to the way companies develop software internally. As developers have become accustomed to working on world class open source software, there is a strong desire to bring those practices back inside the firewall and apply them to software that companies may be reluctant to release. For companies building mostly closed source software, InnerSource can be a great tool to help break down silos, encourage internal collaboration, accelerate new engineer on-boarding, and identify opportunities to contribute software back to the open source world.

  *Source:* https://innersourcecommons.org

**vulnerability**
: A vulnerability /vlnrblti/ is a weakness in a system that allows a threat source to compromise its security. It can be a software, hardware, procedural, or human weakness that can be exploited. A vulnerability may be a service running on a server, unpatched applications or operating systems, an unrestricted wireless access point, an open port on a firewall, lax physical security that allows anyone to enter a server room, or unenforced password management on servers and workstations.

  *Source: CISSP All-in-One Exam Guide, 8th Edition, 2018, by Shon Harris, Fernando Maymi, page 6*

**VA**

**Vulnerability Assessment**
: A vulnerability assessment identifies a wide range of vulnerabilities in the environment. This is commonly carried out through a scanning tool. The idea is to identify any vulnerabilities that potentially could be used to compromise the security of our systems. By contrast, in a penetration test, the security professional exploits one or more vulnerabilities to prove to the customer (or your boss) that a hacker can actually gain access to company resources.

  *Source: CISSP All-in-One Exam Guide, 8th Edition, 2018, by Shon Harris, Fernando Maymi, page 878*

# INDEX