**CYB6004.2021.AC4 Off Campus Cyber Security**

**Assessment 4 CYB6004: Software Based Solution**

**Oluwaseun Abimibola BAKARE**

Student No: 10562938

Text

Description automatically generated

Campus: ECU/ Off Campus

Lecturer: Rob MCKNIGHT

Tutor: Shuchi DHIR

Table of Contents

[1. INTRODUCTION 3](#_Toc96506265)

[2. CODE FEATURES 3](#_Toc96506266)

[2.1 CODE QUALITY 3](#_Toc96506267)

[2 CODE TESTING 3](#_Toc96506268)

[3 LIMITATIONS & CHALLENGES 3](#_Toc96506269)

[4 FUTURE SCOPE OF IMPROVEMENT & CONCLUSION 4](#_Toc96506270)

[5 REFERENCES 4](#_Toc96506271)

# **INTRODUCTION**

The Australian Cyber Security Centre (ACSC) provides advice and information about how Australians can protect themselves. These advisories are usually in response to existing and emerging cyber threats.

This code scrapes the website and present the User with the following options:

Text

Description automatically generated

# **CODE FEATURES**

What Users Can Do:

1. Select a Security Alert subject they are interested in by entering a word or group of words
2. Further filter down this subject by entering some specific word or words to help.

Text

Description automatically generated

Based on these inputs, the code scrapes the website using the inputs that have been submitted and presents the user with the a dialog to make a selection.

## **CODE QUALITY**

To assure a high code quality, the code has:

1. A File Header comment.
2. All bash functions are appropriately commented to show what they do.
3. A TODO section is added to show the opportunity for future improvement

## **CODE RELIABILITY**

Various tests were carried out selecting different possible user input to check if the code breaks down. Based on the findings from this, the code was further strengthened .

# **CODE TESTING**

Code Testing was carried out by running the scripts against the web content on <https://www.cyber.gov.au/acsc/view-all-content/alerts&advisories> and checking the outcome of each choice made using Git Bash to capture error situations and address them.

# **LIMITATIONS & CHALLENGES**

The code plan is to be able to summarise treats by year and by criticality like the following table:

Table

Description automatically generated

A table like this will help to show the growing trends in sophistication of attack and number of threats over the years. Unfortunately, due to the limitation of time, I am unable to deliver on this. If this were done, a line graph could also be made to present a pictorial representation of the data.

# **FUTURE SCOPE OF IMPROVEMENT & CONCLUSION**

The opportunity is to expand the code to provide a trend analysis graph which can provide a pictorial of the perceived increase in threat level over time. Such a pictorial will be best depicted by a line or bar graph.

Additionally, the code can be expanded to allow user to click on the summarised date presented and this will open to show the detailed list of advisories based on their criticality levels of:

* High
* Medium
* Low or
* Not risked

Also, a filter can be added to sift the threats as to which Australian entities such as (a) Individuals (b) SME (c) Large Enterprises and (d) Government should pay particular attention to the threat reported.

# **REFERENCES**

1. Australian Cyber Security Centre. (n.d.). Alerts and Advisories.

<https://www.cyber.gov.au/acsc/view-all-content/alerts&advisories>

1. Sasikala (2010, March 10). AWK Arrays Explained with 5 Practical Examples. The Geek Stuff.<https://www.thegeekstuff.com/2010/03/awk-arrays-explained-with-5-practical-examples/>
2. psychocod3r (2021, March 22). Doing Statistics in awk.

<https://psychocod3r.wordpress.com/2021/03/22/doing-statistics-in-awk/>