**2024 HQ cyber security class**

**Individual project guideline**

**(modified version)**

1. **Topics : Cyber security coding using ML,DL Python library**
2. **Language : Python**
3. **Library : Scikit-learn, TensorFlow on python(choose one)**
4. **Format : guided format**
5. **Page volumes : 15pages at least**
6. **Submission address : class Google drive**
7. **Submission dead line : Sep 24, 25**
8. **Mission :**

* **Survey AI security Python source code example from ref. site**
* **Clone/download the code**
* **Execute the code, find the error and fix it as far as you do**
* **Explain the code**

1. **Reference site**

|  |
| --- |
| **AI chatbots: In Vietnam, various generative AI chatbots such as ChatGPT, Gemini AI and Bing Chat are popular.** |

* **Gemini AI**

Google's latest AI chatbot model, multimodal function

Understands and processes data in various formats.

* **Gemini official site**: [Gemini AI](https://gemini.google.com/?hl=ko) 1
* **DeepMind Gemini tech.page**: [DeepMind Gemini](https://deepmind.google/technologies/gemini/) 2
* **Gemini supporting**: [Gemini 지원](https://support.google.com/gemini/answer/13278668?hl=ko) 3
* **Google Cloud Gemini** : [Google Cloud Gemini](https://cloud.google.com/ai/gemini?hl=ko) 4

https://gemini.google.com/app/cae785ec9a0df194

* **Bing AI Chat**

<https://www.bing.com/?toWww=1&redig=A519D80C0451458E816B246AB9A14D8D>

Microsoft's conversational AI service Bing Chat is an AI-based chat tool that can be used for various purposesin Vietnam. When a user asks a question or makes a request, this tool provides answers or helps generate the necessary information.

* **WRTN**

Korean site, a platform that provides useful information and opportunities

for communication in Vietnam

<https://wrtn.io/en/overview/>

[https://wrtn.ai/](https://wrtn.ai/)%EC%97%90)

[https://wrtn.ai/chat/u/663397a3208f03982f4f7dae/c/66c9955571626b4b88890188?type=u](https://wrtn.ai/chat/u/663397a3208f03982f4f7dae/c/66c9955571626b4b88890188?type=u&fbclid=IwZXh0bgNhZW0CMTAAAR1dhuzIs2qZvgRYI-0TnskHW2bj_7YWLh0iJIDcsghMB10yRqL0mS47LOM_aem_XOShWVwdozpXILLR-pyYow)

* **Chatgpt**

[https://chatgpt.com/share/f63baf30-74c6-4dcb-8908-f8a1893da6ad](https://chatgpt.com/share/f63baf30-74c6-4dcb-8908-f8a1893da6ad?fbclid=IwZXh0bgNhZW0CMTAAAR10HFqoiOyV8WH4ZqBOwwPFDnCG5PY4JZMBBWMzhh8B6NImvOBD0mJOlsc_aem_iFWMrkL0ge5zwPIh5KsI6g)

* **git HUB**

Repository exploration: On the main page of GitHub, you can search for

topics or languages ​​of interest to explore related repositories. You can check the project overview and usage through the README file of each repository.

* **Process of source code exercise**

|  |
| --- |
| **Sign - up -> log-in -> search the topic code -> compile the code -> find error -> explain the error -> explain the code** |

**Individual project topic**

(Topic NO. 01) “ code example of detecting DoS IP Spoofing using Python Scikit-learn”

(Topic NO. 02) “code example of detecting malware file on my computer using Scikit-learn”

(Topic NO. 03) “code example of detecting DDoS attack using Python Scikit-learn”

(Topic NO. 04) “code example of detecting DoS attacks using TensorFlow”

(Topic NO. 05) “SQL injection Python code example using TensorFlow”:

example

(Topic NO. 06) “malware detection code example on my computer using TensorFlow”

(Topic NO. 07) “ code example of how to load other files(excel,html) on scikit learn program”

(Topic NO. 08) “ code example of basic process of sklearn.preprocessing using Python Scikit-learn”

**(Topic NO. 09) To perform an scanning test on a specific server IP (e.g., 111.111.111.111) using Scikit-Learn in Python**

**(Topic NO. 10) To perform an security risk analysis on a specific server IP (e.g., 111.111.111.111) using Scikit-Learn in Python**

**(Topic NO. 11) To perform a web system security check on a specific URL (e.g., https://test.com) using Scikit-Learn**

Report format

|  |  |
| --- | --- |
| class |  |
| Student id |  |
| Student name |  |
| Student email |  |
| Submitting date |  |

1. **Title :**

**2. Purpose of study(under five lines)**

(ex)

The purpose of this study is to establish the development direction about the system detecting and responding to the malicious codes. For this, we carried out a research on the domestic and foreign technologies that detect and deal with the spreading malicious codes.

**3. Scope of survey(list up the scope of the searching by items)**

**4. Results of exercise**

1. **Install Python Library**
2. **Clone the Code**
3. **Execute the program**
4. **Check error and modify the logics**
5. **Explain your code**

**5. Conclusion**

Feeling and opinion

Table 1. Comparative framework of Education VS. Training

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

\*Source:NIST Special Publication 800-16

Figure 1. Information security learning continuum

\*Source:NIST Special Publication 800-16

**7. Reference**

[1]

[2]