PICUS RED TEAM (WEB) CHALLENGE QUESTIONS

- *This challenge includes 3 questions with different difficulty levels.*
- *You will get points for each question and partial points for your progress.*
- *You are expected to send your answers within a week.*
- *You can send emails to the address below for your inquiries.*
- *The unauthorized copying, sharing or distribution of these materials is strictly prohibited.*

Good luck and best wishes.
Red Team

Question - 1

What is the critical bug(s) in the following code and how do you exploit it/them? Please provide necessary technical details, exploit code(s) and possible fixes or mitigation suggestions.

The answer should include:

- Details and root causes of the vulnerabilities
- Working exploit written in a language of your choice
- Fix or mitigation suggestions

You can run the code using gunicorn if you like to

```
gunicorn -w 5 -b 0.0.0.0:8080 deserialize:app
```

```python
import pickle
import base64


def app(environ, start_response):

    data = "Nope"
    try:
        token =
pickle.loads(base64.b64decode(environ['HTTP_AUTH_CODE']))
        if token.sign and token.token:
            data = b"Login Success\n"

            status = '200 OK'
            response_headers = [
                ('Content-type', 'text/plain'),
                ('Content-Length', str(len(data)))
            ]
        else:
            status = '401 Unauthorized'
            response_headers = []

        start_response(status, response_headers)
    except:
        status = '401 Unauthorized'
        response_headers = []
        start_response(status, response_headers)

    return [data]
```

Question - 2

Explain Apache Log4j (CVE-2021-44228) vulnerability. Your solution should answer the following questions as detailed as possible.

- What is the root cause of the vulnerability?
- Which types of software weaknesses (CWE) caused the vulnerability?
- What are the possible exploitation methods and their impacts?
- What middle or long term impacts do you expect in terms of enterprise security?

Question - 3

There is a system that has users, permissions and assets. Permissions can be assignable to both users and assets. System has two types of permissions:

P1: can access to an asset

P2: can impersonate permissions of an asset after accessing it

Write an algorithm solving the following problems for any assets, users and permissions mapping. Then implement it in a language of your choice.

- Does a user have access to an asset?
- What is the optimum way for a user to access an asset?

A sample instance of the system with users, assets and mapping to test your algorithm:ß

- **Users**: U1, U2, U3
- **Assets**: A1, A2, A3, A4
- **Permission mapping**:
  - U1 has P1(A1), P1(A3) and P2
  - U2 has P1(A2)
  - U3 has P1(A1) and P2
  - A1 has P1(A2)
  - A2 has P1(A3), P1(A4)
  - A3 has P1(A2), P1(A5)
  - A4 has P1(A1)
  - A5 has none

Your program should get two inputs, a user and target asset. Then output should answer if the given user has access to the given asset. If so, what is the optimum path for the user to reach that asset?

Test your program with the mapping above for two inputs:

- User : U1, target asset: A5
- User: U2, target asset: A4
- User: U3, target asset: A5

The answer should include:

- Brief explanation of your solution like what is your approach to the problem, how did you model it and possible improvements of your solution.

- A working implementation of your solution for the sample system. The solution should work for any other instance of the system (different users, assets and permission mappings).
- Output of the test inputs for the sample system.