Malware Analysis (CS6038)

Week 12.1 Process Injection

Scott Nusbaum
nusbausa@ucmail.uc.edu

April 2, 2019

University of CINCINNATI

Overview

- Homework
- Final
- Process Injection

Homework

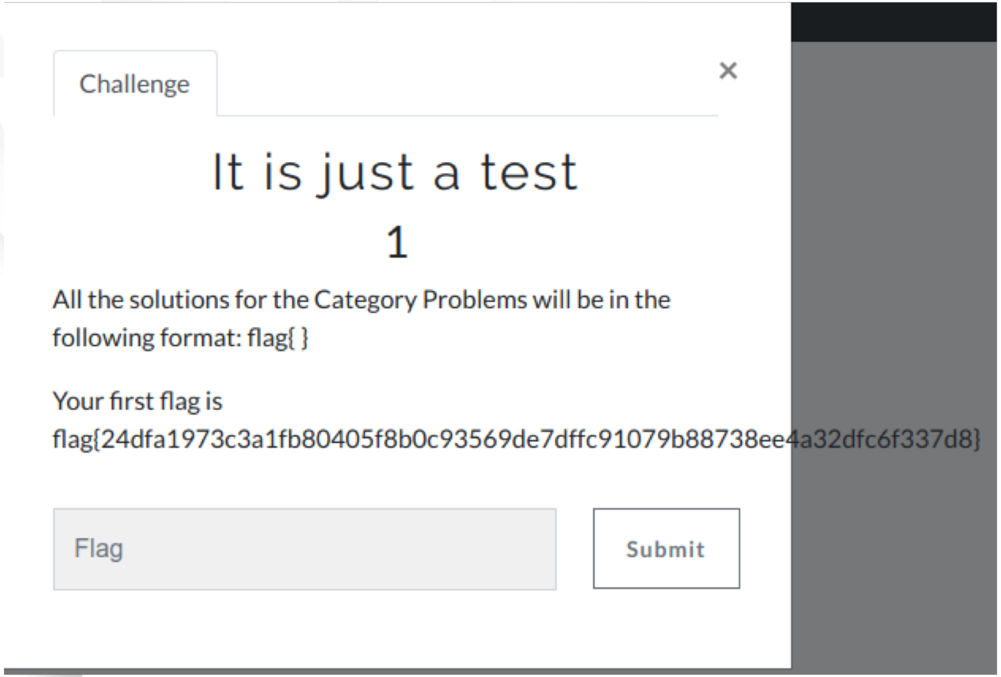
- Homework 5:
  - Due April 11, 2019
  - Reverse Engineering. 3 Problems Get Started!!!
- Homework 6:
  - Assign April 4, 2019
  - Due April 18, 2019
  - Process Injection -- Do it yourself!

Finals

- Starts April 11, 2019 at 23:59:59
  - 23 Challenges
    - 15 Multiple Choice
    - 1 Bonus
    - 2 GiveMe's (Solve First)
    - 5 Problems

University of CINCINNATI

2 Questions from your Final

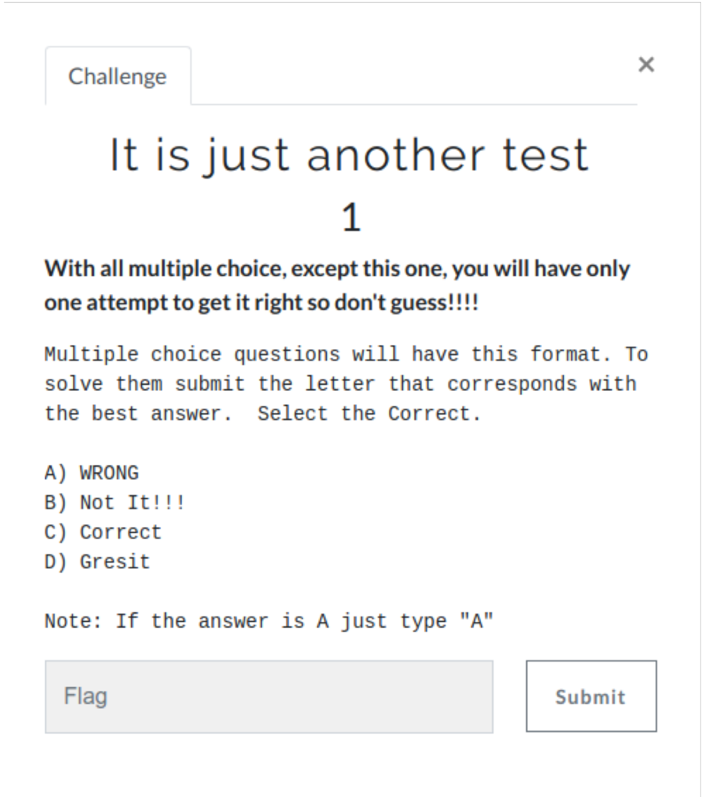


It is just a test

1

All the solutions for the Category Problems will be in the following format: flag{ }

Your first flag is flag{24dfa1973c3a1fb80405f8b0c93569de7dffc91079b88738ee4a32dfc6f337d8}



It is just another test

1

With all multiple choice, except this one, you will have only one attempt to get it right so don't guess!!!!

```
Multiple choice questions will have this format. To
solve them submit the letter that corresponds with
the best answer.  Select the Correct.

A) WRONG
B) Not It!!!
C) Correct
D) Gresit

Note: If the answer is A just type "A"
```

Process Injection

- The insertion of malicious code into otherwise benign software
- Multiple methods available
- Makes detection difficult
- Makes monitoring difficult
- Makes static analysis difficult

University of CINCINNATI

Process Injection

- Techniques
  - https://attack.mitre.org/techniques/T1055/
  - https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
  - https://github.com/secrary/InjectProc
  - https://github.com/hasherezade
  - https://www.darkreading.com/breaking-down-the-propagate-code-injection-attack/a/d-id/1332473