

Introduction to Software Security

3rd Quiz

Computer Security & OS Lab
Dept. of Software Science, DKU

Cho, Seong-je (조성제)

Spring, 2020

Answer the following five questions

1. Explain three properties (or features) of **cryptographic hash functions**?
 - Examples of cryptographic hash functions: MD5, SHA-256, ...
2. What is **Content Delivery Networks** (CDNs) and how it works?
3. Which attack is generally hard to be detected between passive and active attack? Why?

Answer the following five questions

4. What is the problem in the C program below? How can you fix it?

```
typedef unsigned int uint;
int getmin(int *arr, uint len) {
    int min;
    for (int i=0; i<len; i++)
        min = (min < arr[i]) ? min : arr[i];
    return min;
}
```

5. Show the output of the *printf()* in the C program below?

Explain how the *cresult* and *c3* variables are assigned to the printed value.

```
char cresult, c1, c2, c3;

c1 = 100; c2 = 90; c3 = -120;
cresult = c1 + c2 + c3;
printf("%c, %d, %c, %d\n", cresult, cresult, c3, c3);
```

Solving & Writing

- Solve the question individually (by yourself).
 - You must write a report including the answers to the quizzes by yourself.
 - No cheating
- The **cover page** of the report must include
 - Title (제목): “**The 3rd Quiz of Intro. to SW Security**”
 - 분반 (2분반 또는 3분반)
 - Student name, Student number
 - Date of submission
- Deadline
 - Submit your report by **5th April**.

Submission

- **File** naming of the answer report for the 3rd Quiz
 - ISS(분반)_Qz3_이름_학번_mmdd
 - If you are in the 2nd class, name = “전우치”, student number = 32171234, submission date = 3rd April, then the filename for this Quiz is
ISS(2)_Qz3_전우치_32171234_0403

- **Submit your report to TA by email.**
 - **Email** title: “SW보안개론(분반) 3번 Quiz 답안 제출”
 - The title for the 2nd class: “SW보안개론(2) 3번 Quiz 답안 제출”
 - The title for the 3rd class: “SW보안개론(3) 3번 Quiz 답안 제출”
 - TA: 한승재 (Seungjae Han) googgstmdwo@naver.com