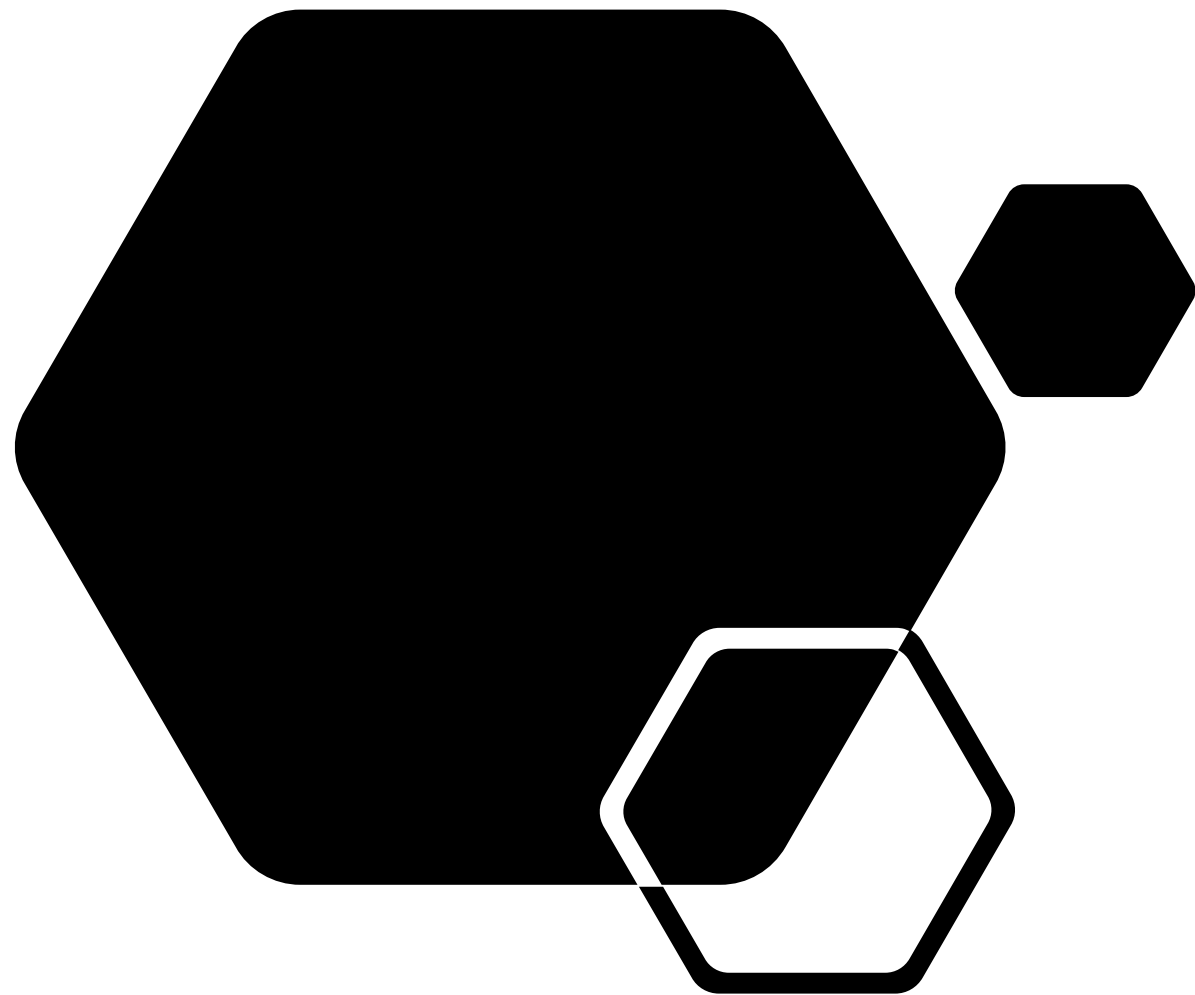


# 정보보안 분야

이지훈



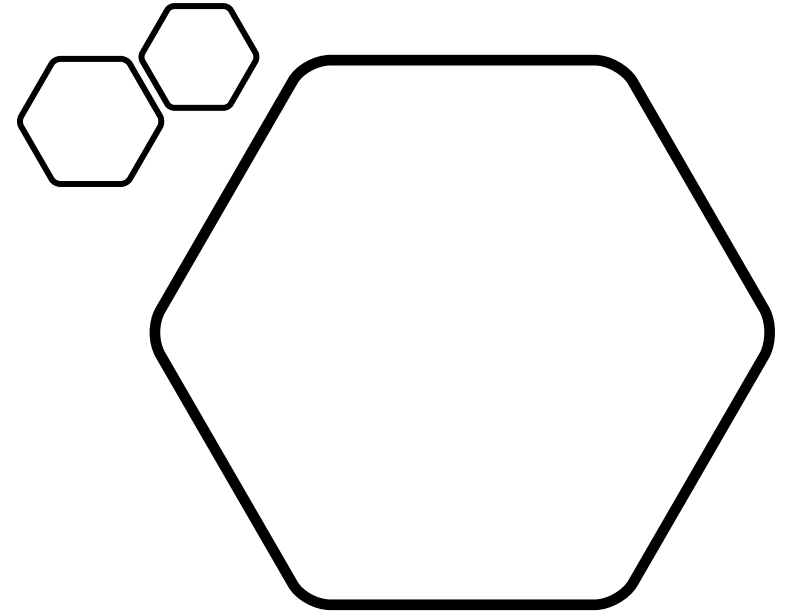
# 목차

- Pwnable
- Reversing
- Digital Forensic
- Web Hacking

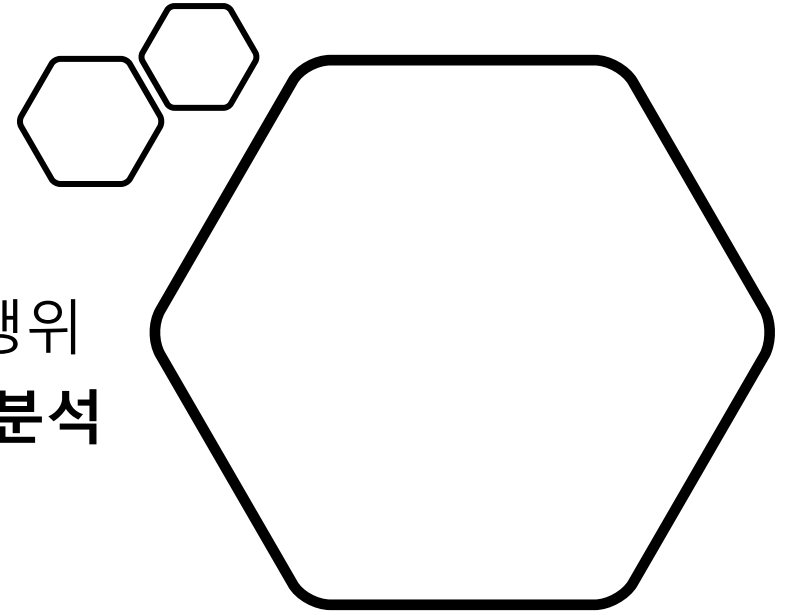


# Pwnable (시스템해킹)

- OS 또는 프로그램의 취약점을 찾아 공격
- 여러 공격 기법을 활용하여 관리자 권한을 빼앗는 행위
- Buffer Overflow (BOF)
  - Stack
  - Heap
- Format String Bug (FSB), Integer Overflow, Use After Free (UAF)
- OS, 컴퓨터/메모리구조, 네트워크기초, 코딩언어지식 ...



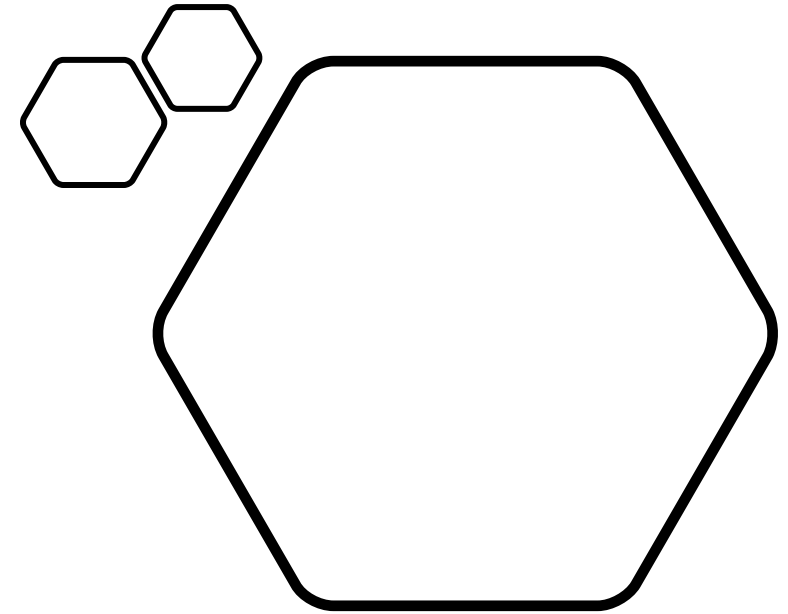
# Reversing (리버스 엔지니어링)



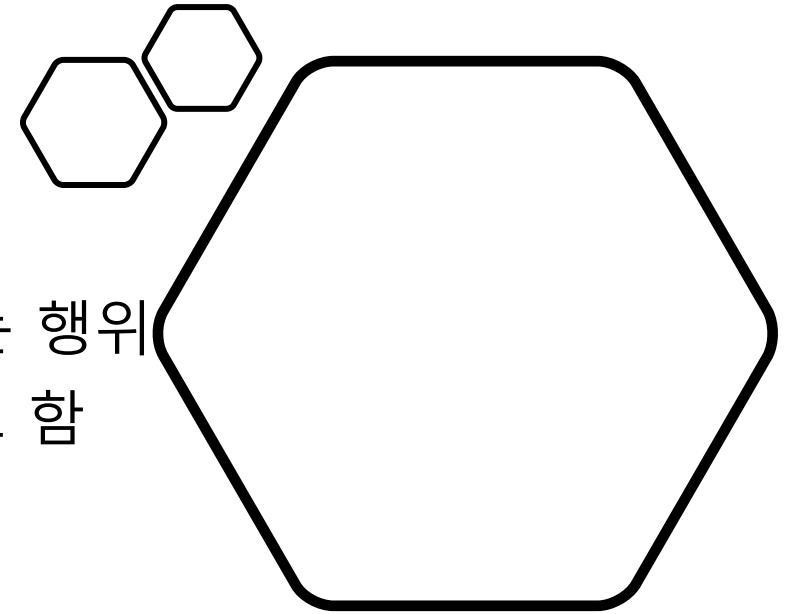
- 소스코드를 역추적, 재분석하여 프로그램을 파악하는 행위
- 프로그램을 실행시키지 않는 **정적분석**, 그 반대인 **동적분석**
- 긍정적 측면
  - 악성코드 분석
  - 모의해킹 및 보안검수
- 부정적 측면
  - 악성코드 개발
  - 해킹툴, 크랙, 우회

# Digital Forensic

- 디지털기기 내 데이터 수집/추출 등을 통해 범죄의 단서와 증거를 찾아내는 과학수사 기법
- 정보추출 포렌식
  - 범행 입증에 필요한 증거 발견 및 확보를 목적으로 함
- 사고대응 포렌식
  - 해킹과 같은 공격의 경로 및 공격자의 신원을 파악하는 것을 목적으로 함



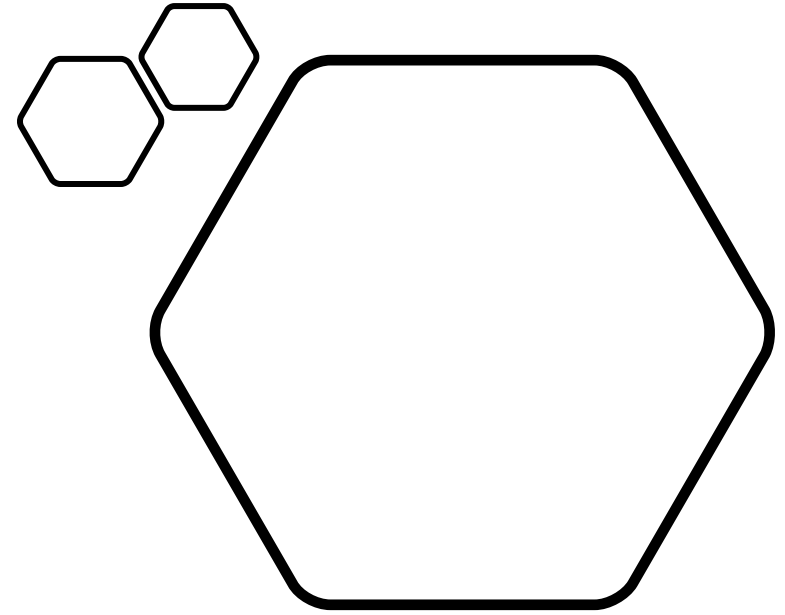
# Web Hacking

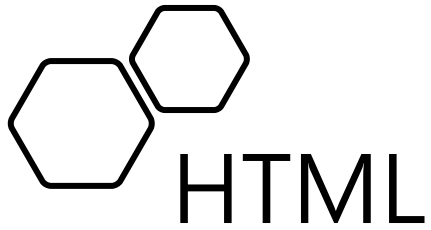


- 웹 서비스에서 발생하는 보안 허점을 파고들어 공격하는 행위
- 프레임워크, 웹 어플리케이션 서버 대상으로 공격하기도 함
- 대상지정, 정보수집, 취약점 분석, 공격 순으로 진행됨
  - 정보수집이 가장 중요하며 주기적으로 이뤄져야 함
- SQL Injection, Command Injection, Xpath Injection
- XXE, XSS, CSRF, File Up/Download 취약점 등 ...

# 무엇을 공부해야 하는가?

- 운영체제 기초, 네트워크 기초
  - Windows, Linux
- 프로그래밍 언어
  - C, java
- 웹 기술 기초
  - HTML (HyperText Markup Language)
  - CSS (Cascading Style Sheets)
  - Apache Server
  - SQL
  - PHP





- Html 문서는 메모장, 리눅스의 vi 로도 작성이 가능하다.
- <태그이름> // 시작태그  
</태그이름> // 종료 태그
- <!DOCTYPE html> : 어떤 버전의 html 언어로 작성되었는지 결정
- <html> : 문서의 루트 부분을 정의
- <head> : 문서의 메타데이터를 정의
- <title> : 툴바, 즐겨찾기, 검색결과에 표시되는 제목
- <body> : 웹 브라우저를 통해 보이는 내용

```
<!DOCTYPE html>
<html>
  <head>
    <title>HTML문서의 제목입니다.</title>
  </head>

  <body>
    <h1>제목 크기1입니다.</h1>

    <h2>제목 크기2입니다.</h2>

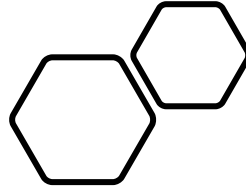
    <p>이 부분은 단락입니다.</p>
  </body>
</html>
```



```
1 <!DOCTYPE html>
2 <html lang="ko">
3
4 <head>
5     <meta charset="UTF-8">
6     <title>HTML Intro</title>
7 </head>
8
9 <body>
10
11     <h1>Hello, World!</h1>
12     <p>처음 해보는 html 프로그래밍입니다.<br></p>
13
14 </body>
15
16 </html>첫금없는 곳에 텍스트를 적으면?
```

# Hello, World!

처음 해보는 html 프로그래밍입니다.  
첫금없는 곳에 텍스트를 적으면?



- <http://www.tcpschool.com/html/intro>
- <https://www.slideshare.net/JinkyounKim8/pwnable-study-basic1>
- <https://hongpossible.tistory.com>
- <https://peemangit.tistory.com/312>
- <https://www.samsungsemiconstory.com/2300>