

보안 분야 조사

92113528 정보보호학전공 김민기

목차

- 보안이란?
- 리버싱(Reversing)
- 시스템(Pwnable)
- 웹(Web)

```
// ... imports from 'passport';
import LocalStrategy from 'passport-local';
import { Strategy as JwtStrategy, ExtractJwt } from 'passport-jwt';
import request from 'supertest';

import User from '../models/user.model';
import constants from '../config/constants';
import { createToken } from '../helpers/auth.helper';

// ... imports from 'passport';
const localOpts = { usernameField: 'username' };
const localLogin = new LocalStrategy(
  localOpts,
  (username, password, done) => {
    // ... logic to find user by username
    const user = User.findOne({ username });
    if (user.length === 0) {
      return done(null, false);
    }
    const userData = {
      username: user[0].username,
      password: user[0].password,
    };
    if (password === userData.password) {
      return done(null, user[0]);
    } else {
      return done(null, false);
    }
  }
);

// ... imports from 'passport';
const jwtOpts = {
  // Telling Passport to check authorization headers for JWT
  jwtFromRequest: ExtractJwt.fromAuthHeaderWithScheme('JWT'),
  // Telling Passport where to find the secret
  secretOrKey: constants.JWT_SECRET,
};
const jwtLogin = new JwtStrategy(jwtOpts, async (payload, done) => {
  try {
    console.log(payload);
    const user = await User.findOne({ user_uuid: payload.user_uuid });
    console.log(user[0].toJSON());

    if (user.length === 0 || !user) {
      return done(null, false);
    }

    return done(null, user[0]);
  } catch (e) {
    console.log(e);
    return done(e, false);
  }
});
```



보안이란?

리버싱(Reverse Engineering)

- 리버싱 엔지니어링
- 정적분석, 동적분석





시스템(Pwnable)

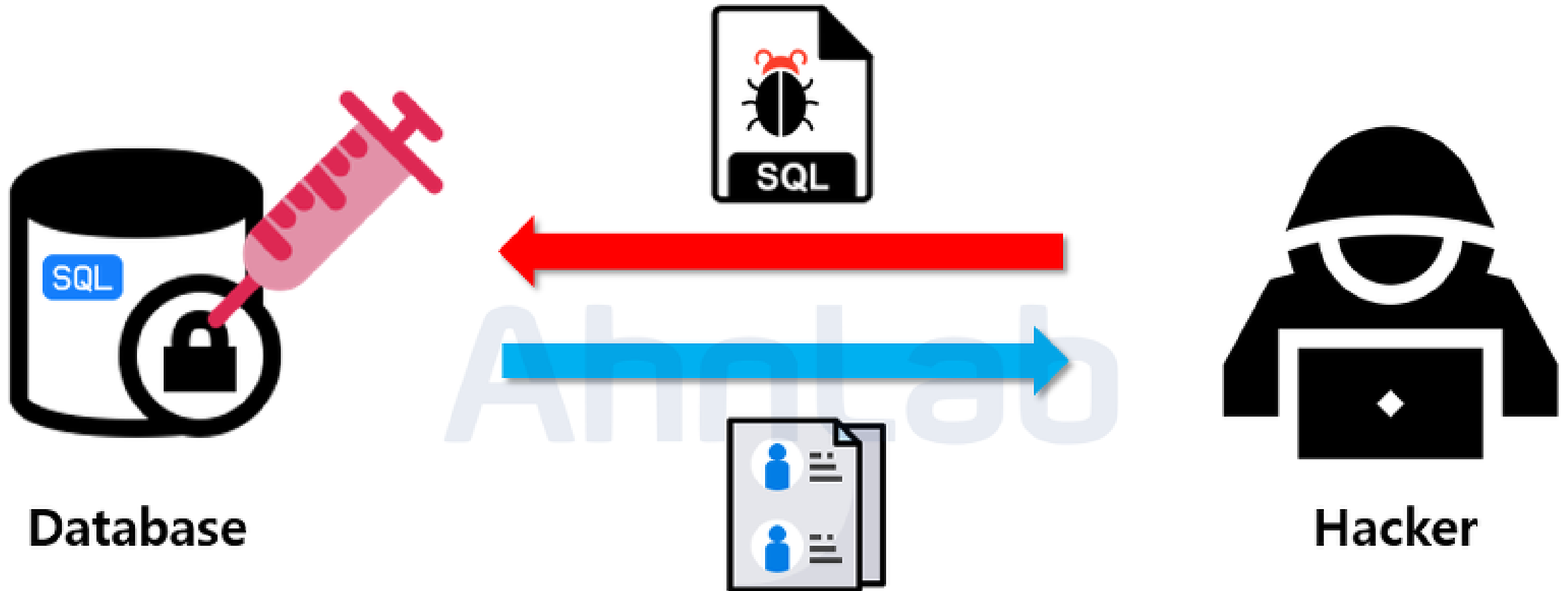
- 시스템 해킹 기법(Buffer Overflow, Race Condition)
- 시스템 해킹 절차

웹(Web)

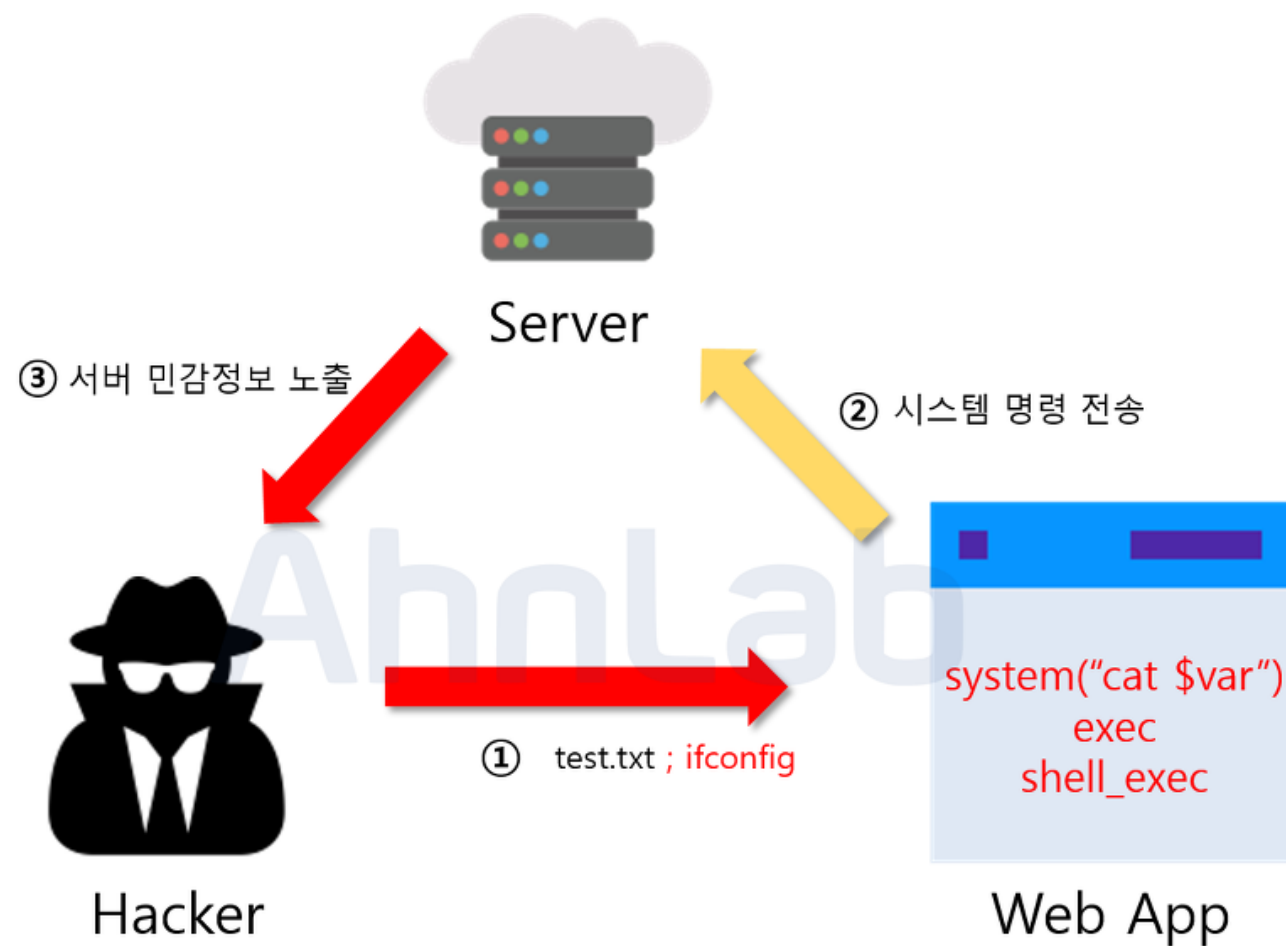
- 웹 해킹의 정의
- SQL Injection, Command Injection, XSS, 파일 업로드 취약점

SQL Injection

7



Command Injection



XSS(Cross Site Scripting)



SQL Injection

- Error Based SQL Injection
- Union Based SQL Injection
- Blind SQL Injection

SELECT * FROM Users WHERE id = 'INPUT1' AND password = 'INPUT2'



게시글 조회

① SELECT * FROM Board WHERE title LIKE '%INPUT%' OR contents '%INPUT%'

Board table

id	title	contents
1	hi	Hello
2	bye	Bye bye



① SELECT * FROM Users WHERE id = 'INPUT1' AND password = 'INPUT2'



abc123' and ASCII(SUBSTR(SELECT name FROM information_schema.tables
WHERE table_type='base table' limit 0,1,1,1)) > 100 --

(MySQL 일 경우)

조사하면서 느낀 점

S.C.P
Security Check Point