XSS & SQLi

for ICEWALL Mentoring

조성준

Contents

- Code Injection
- XSS
- SQL injection

Code Injection

나의 이름은 _____이다.

➔ 나의 이름은 조성준이다.

➔ 나의 이름은 뭔지 모르겠고, PPT를 만드는 중이다.

Code Injection

alert("_____");

➔ alert("Hello World");

➔ alert("Hello World"); location.href="https://www.naver.com/"; // ");

SELECT * FROM USER_TABLE WHERE id="____" and pw="____";

➔ SELECT * FROM USER_TABLE WHERE id="user" and pw="password";

➔ SELECT * FROM USER_TABLE WHERE id="admin"; -- " and pw="____";

XSS

http://127.0.0.1/0520/login/login_test_get.php?ID=aaaaaa&PW=bbbb

http://127.0.0.1/0520/login/signup.html

XSS

https://youtu.be/XqUoxXQ9i_c

https://youtu.be/bIUyqDwvzXc

NAVER XSS 취약점 예시 보여주기

SQL Injection

SELECT * FROM USER_TABLE WHERE id="____" and pw="____";

➔ SELECT * FROM USER_TABLE WHERE id="user" and pw="password";

➔ SELECT * FROM USER_TABLE WHERE id="admin"; /* " and pw="____";

데이터베이스 조작 가능

- ID/PW, 카드정보 등 개인정보 유출
- 타인 계정으로 로그인
- 실시간 쿼리 정보 노출(MITM SQL INJECTION)

SQL Injection

SELECT * FROM Login WHERE id='$ID' and pw='$PW’

SELECT * FROM Login WHERE id='aaaa' and pw='' or 1=1 #’

SELECT * FROM Login WHERE id='aaaa' and pw='' OR pw LIKE 'b%' #

추천 과제

SQLi : https://los.eagle-jump.org/ 문제 풀기

XSS : http://xss-game.appspot.com/ 문제 풀기