

XSS & Database

목차



XSS 실습



Database

- Database 란

- Database 생성

Part1. XSS 실습

XSS 실습

`<script>alert('XSS');</script>`

seomj.github.io 내용:
XSS

확인

INTRODUCTION TRIP BUCKET LIST 10 VISIT

이름	내용	
<code><script>alert('XSS');</script></code>	내용	append

`XSS`

seomj.github.io 내용:
XSS

확인

INTRODUCTION TRIP BUCKET LIST 10 VISIT

이름	내용	
이름	내용	append
XSS		

XSS 실습

```
if(name.indexOf("<script>") != -1){  
    name = name.replace("<script>", "");  
    alert('공격 감지');  
}
```

문자열 내에서 특정한 문자열의 index 값을 리턴

특정 문자열을 찾아 다른 문자열로 바꾸는 메소드

이 페이지 내용:
공격 감지

확인

INTRODUCTION TRIP BUCKET LIST 10 VISIT

이름	내용
<input type="text" value="<script>alert('XSS');</script>"/>	<input type="text" value="내용"/>
<input type="button" value="append"/>	

이름
<input type="text" value="이름"/>
<input type="text" value="alert('XSS');"/>

이 페이지 내용:
XSS

확인

INTRODUCTION TRIP BUCKET LIST 10 VISIT

이름	내용
<input type="text" value="이름"/>	<input type="text" value="<script>alert('XSS');</script>"/>
<input type="button" value="append"/>	

XSS 실습

```
if(name.indexOf("<script>") != -1){
    name = name.replace("<script>", "");
    alert('공격 감지');
}
if(name.indexOf("</script>") != -1){
    name = name.replace("</script>", "");
    alert('공격 감지');
}
if(text.indexOf("<script>") != -1){
    text = text.replace("<script>", "");
    alert('공격 감지');
}
if(text.indexOf("</script>") != -1){
    text = text.replace("</script>", "");
    alert('공격 감지');
}
```

‘공격 감지’ 알림 창이 두 번씩 뜨게 됨
비슷한 구문이 반복됨

XSS 실습

```
function filterStr(str){  
    if(str.indexOf("<script>") != -1){  
        str = str.replace("<script>", "");  
        alert('공격 감지');  
    }  
    if(str.indexOf("</script>") != -1){  
        str = str.replace("</script>", "");  
        alert('공격 감지');  
    }  
    return str;  
}
```

```
name = filterStr(name);  
text = filterStr(text);
```

이름	내용	
<input type="text" value="이름"/>	<input type="text" value="내용"/>	<input type="button" value="append"/>
minjae	minjae	
min	alert('XSS');	
alert('XSS');	min	
alert('XSS');	alert('XSS');	

‘공격 감지’ 알림 창이 두 번씩 뜨게 됨

XSS 실습

```
function filterStr(str){  
    if(str.indexOf("<script>") != -1 || str.indexOf("</script>") != -1){  
        alert("공격 감지");  
    }  
    if(str.indexOf("<script>") != -1){  
        str = str.replace("<script>", "");  
    }  
    if(str.indexOf("</script>") != -1){  
        str = str.replace("</script>", "");  
    }  
    return str;  
}
```

XSS

이 페이지 내용:
XSS

확인

INTRODUCTION TRIP BUCKET LIST 10 VISIT

이름	내용	
<input type="text" value="이름"/>	<input type="text" value="내용"/>	<input type="button" value="append"/>
XSS		

XSS 실습

```
function tableCreate(){  
    var html = '';  
  
    var name = $("#inName").val();  
    var text = $("#inText").val();  
  
    name = filterStr(name, 0);  
    text = filterStr(text, 1);  
  
    html += '<tr>';  
    html += '<td>'+name+'</td>';  
    html += '<td>'+text+'</td>';  
    html += '</tr>';  
  
    $("#dynamicTable").append(html);  
  
    $("#inName").val('');  
    $("#inText").val('');
```

```
function filterStr(str, level){  
    p = str.match(/<|>|\"|'|\%|\\;|\\(|\\)|\\&|\\+|\\-/g);  
  
    if (p != null){  
        if (p.length > 0 ) {  
            alert("공격 감지");  
        }  
    }  
  
    if (level == 0 ) {  
        str = str.replace(/<|>|\"|'|\%|\\;|\\(|\\)|\\&|\\+|\\-/g, "");  
    }  
    else if (level == 1 ) {  
        str = str.replace(/</g, "&lt;");  
        str = str.replace(/>/g, "&gt;");  
    }  
    return str;  
}
```

XSS 실습

```
<script>alert('XSS');</script>
```

이 페이지 내용:
공격 감지

확인

INTRODUCTION TRIP BUCKET LIST 10 VISIT

이름	내용	
<input type="text" value="<script>alert('XSS');</script>"/>	<input type="text" value="hi"/>	<input type="button" value="append"/>

이 페이지 내용:
공격 감지

확인

INTRODUCTION TRIP BUCKET LIST 10 VISIT

이름	내용	
<input type="text" value="이름"/>	<input type="text" value="<script>alert('XSS');</script>"/>	<input type="button" value="append"/>
scriptalertXSS/script	hi	

```
name = filterStr(name, 0);  
text = filterStr(text, 1);
```

이름	내용	
<input type="text" value="이름"/>	<input type="text" value="내용"/>	<input type="button" value="append"/>
scriptalertXSS/script	hi	
	<script> alert('XSS');</script>	

XSS 실습

```
<a href="javascript:alert('XSS')">XSS</a>
```

seomj.github.io 내용:
XSS

확인

INTRODUCTION TRIP BUCKET LIST 10 VISIT

이름	내용	
<input type="text" value="이름"/>	<input type="text" value="내용"/>	<input type="button" value="append"/>
XSS		

이름	내용	
<input type="text" value="이름"/>	<input type="text" value="내용"/>	<input type="button" value="append"/>
a href=javascript:alertXSSXSS/a	XSS	

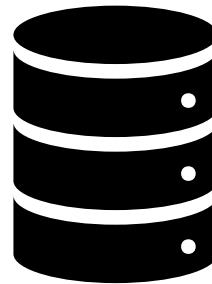
Part2. Database

Database

사용자의 질의에 대하여
즉각적인 처리와 응답

사용자가 원하는 데이터를
내용에 따라 참조

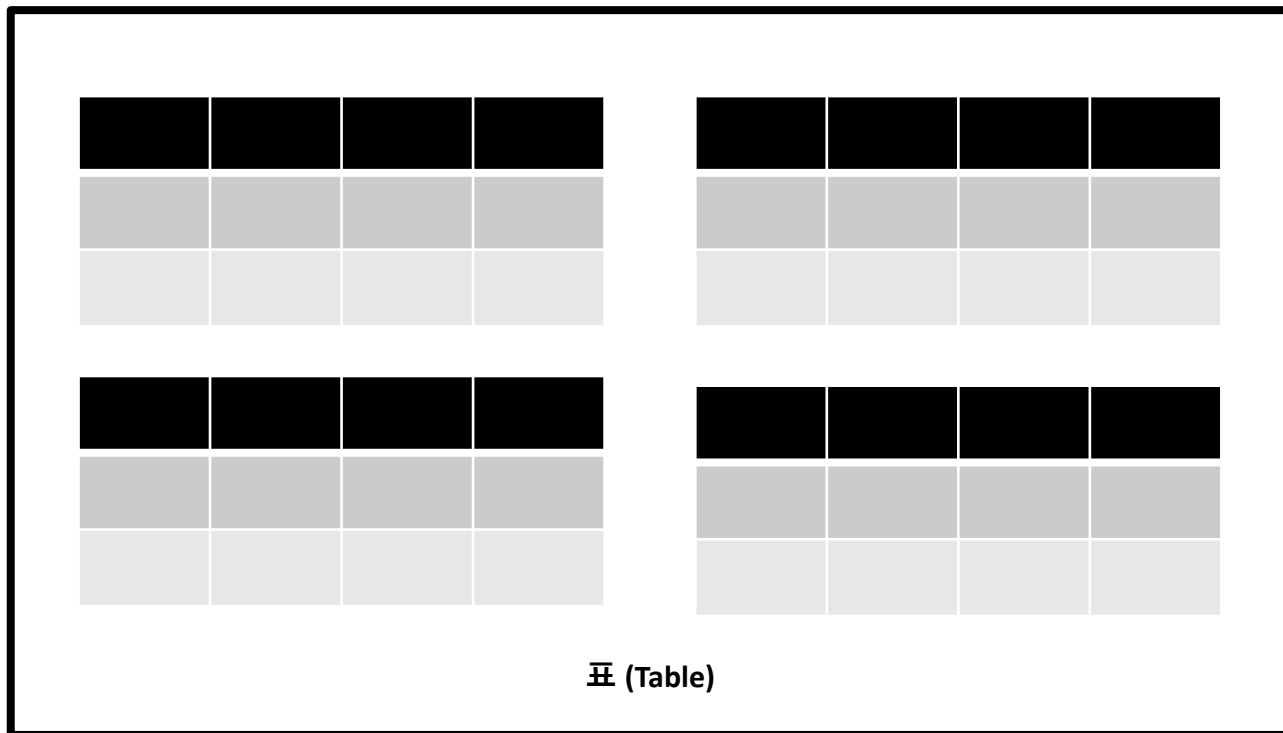
생성, 수정, 삭제를 통하여
항상 최신의 데이터를 유지



사용자들이 원하는 데이터를
동시에 공유

데이터의 논리적 구조와
응용프로그램은
별개로 동작

Database

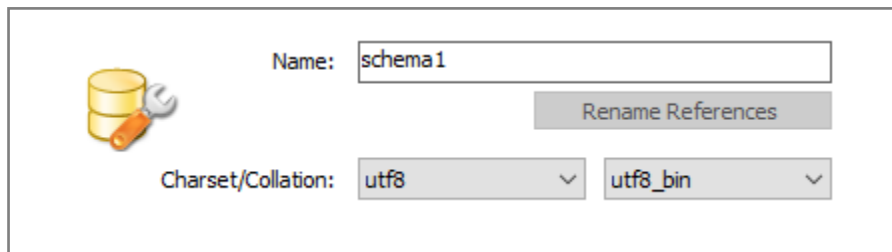


데이터 베이스 (Database)
스키마 (Schema)

Database 생성

1. 데이터 베이스 생성하기

CREATE DATABASE schema1 default CHARACTER SET UTF8;



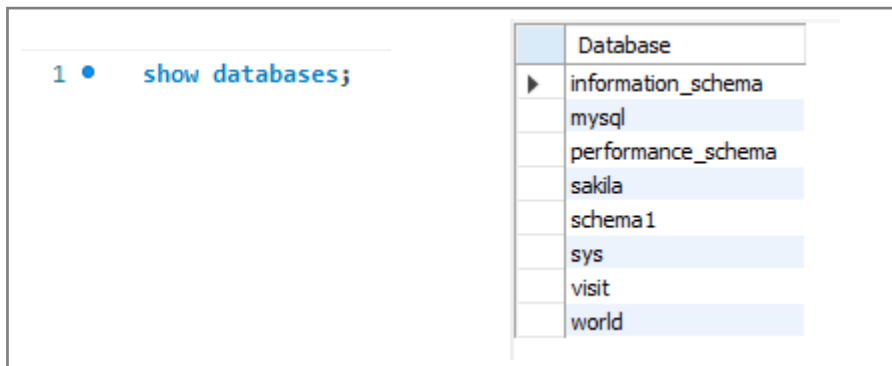
The image shows the MySQL Database Creation Wizard. On the left is an icon of a database cylinder with a wrench. The 'Name' field contains 'schema1'. Below it, the 'Charset/Collation' is set to 'utf8' and 'utf8_bin'. A 'Rename References' button is visible.

Name:

Charset/Collation:

[Rename References](#)

SHOW DATABASES;



The image shows the MySQL Query Results window. The query 'show databases;' is entered in the top pane. The bottom pane displays a table of databases.

Database
information_schema
mysql
performance_schema
sakila
schema1
sys
visit
world

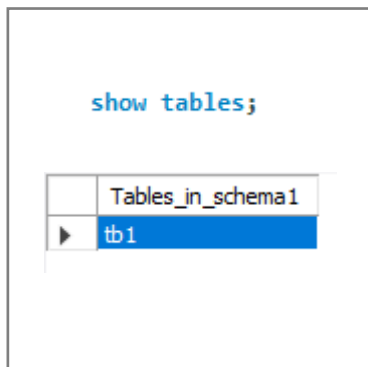
Database 생성

2. 테이블 생성하기

CREATE table tb1(칼럼이름 자료형, 칼럼이름 자료형, 칼럼이름 자료형 ...);

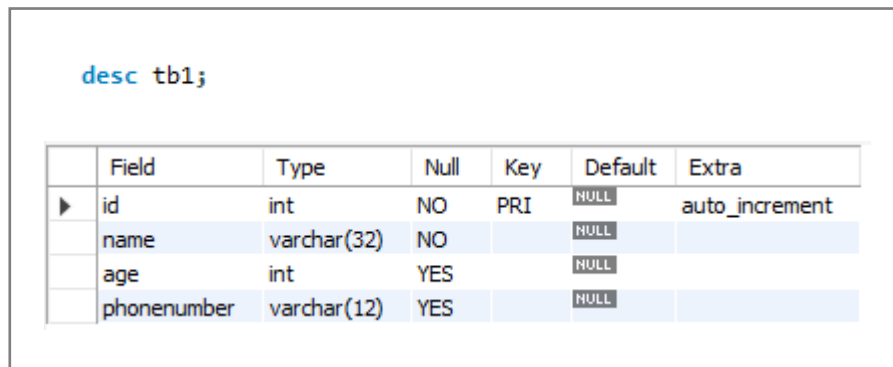
```
create table tb1(  
  id int(11) not null auto_increment,  
  name varchar(32) not null,  
  age int(11),  
  phonenumber varchar(12),  
  PRIMARY KEY(id)  
);
```

SHOW TABLES;



	Tables_in_schema1
▶	tb1

DESC tb1; (DESCRIBE tb1;)



```
desc tb1;
```

	Field	Type	Null	Key	Default	Extra
▶	id	int	NO	PRI	NULL	auto_increment
	name	varchar(32)	NO		NULL	
	age	int	YES		NULL	
	phonenumber	varchar(12)	YES		NULL	

Database 생성

3. 데이터 삽입하기

INSERT INTO tb1 (칼럼1, 칼럼2, ...) VALUES(값1, 값2, ...);

```
insert into tb1 (name, age, phonenumber) values('서민재', '21', '01020001003');
```

	id	name	age	phonenumber
▶	1	서민재	21	01020001003
✱	NULL	NULL	NULL	NULL

Database 생성

4. 데이터 선택하기

SELECT * FROM tb1 WHERE 칼럼=값;

```
select * from tb1 where age='31';
```

	id	name	age	phonenumber
▶	4	양요섭	31	01019900105
	5	이기광	31	01019900330
*	NULL	NULL	NULL	NULL

SELECT 칼럼1, 칼럼2 ... FROM tb1;

```
select name, age from tb1;
```

	name	age
▶	서민재	21
	손동운	30
	윤두준	32
	양요섭	31
	이기광	31

SELECT * FROM tb1 ORDER BY 칼럼;

```
select * from tb1 order by age;
```

	id	name	age	phonenumber
▶	1	서민재	21	01020001003
	2	손동운	30	01019910606
	4	양요섭	31	01019900105
	5	이기광	31	01019900330
	3	윤두준	32	01019890704
*	NULL	NULL	NULL	NULL

Database 생성

5. 데이터 수정하기

UPDATE tb1 SET 칼럼1 = 수정값1, 칼럼2 = 수정값2 ... WHERE 칼럼 = 값;

```
update tb1 set name='김원필', age = '27', phonenumber='01019940428' where id = 1;
```

	id	name	age	phonenumber
▶	1	김원필	27	01019940428
	2	손동운	30	01019910606
	3	윤두준	32	01019890704
	4	양요섭	31	01019900105
	5	이기광	31	01019900330
✱	NULL	NULL	NULL	NULL

Database 생성

6. 데이터 삭제하기

DELETE FROM tb1 WHERE 칼럼 = 값;

```
delete from tb1 where id = 1;
```

	id	name	age	phonenummer
▶	2	손동운	30	01019910606
	3	윤두준	32	01019890704
	4	양요섭	31	01019900105
	5	이기광	31	01019900330
⊙	NULL	NULL	NULL	NULL

Q & A

Thank you