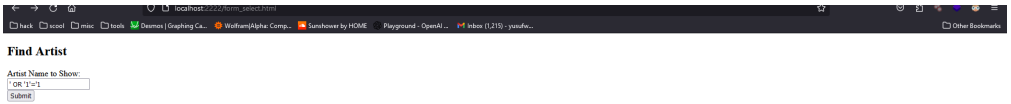
A

html page with select query and form, example shown has SQLi:

the original routine query:

```
SELECT ArtistName FROM artists WHERE ArtistName = '$name'
```



the injection query:

```
SELECT ArtistName FROM artists WHERE ArtistName = ''OR
'1' = 1'
```

which results in:

Results:

ArtistName: Hacker1

ArtistName: Hacker1

ArtistName: Hacker1

ArtistName: Hacker1

ArtistName: Hacker1

ArtistName: Hacker1

ArtistName: Hacker1

ArtistName: Hacker1

ArtistName: Hacker1

ArtistName: Hacker1

ArtistName: Hacker1

ArtistName: Hacker1

ArtistName: Hacker1

ArtistName: Hacker1

ArtistName: Hacker1

B

form with update command, example shows sqli which affects the entire table:

the original routine query:

```
UPDATE artists SET ArtistName = '$newName' where
ArtistName = '$name'
```

Artist Information Update Form

Artist Name:
' OR '1'='1
New Artist Name:
Hacker 2
Update

the injected query:

```
UPDATE artists SET ArtistName = 'Hacker 2' where
ArtistName = ''OR '1' = 1'
```

which results in:

C

the fix is to have a prepared statement.

prepared statement of part A:

```
$stmt = $conn->prepare("SELECT * FROM artists WHERE
ArtistName = ?");

$stmt->bind_param("s", $name);

$stmt->execute();

$result = $stmt->get_result();
```

so:

Find Artist

Artist Name to Show:

' OR '1'='1

Submit

results in:

```
$stmt = $conn->prepare("SELECT * FROM artists WHERE
ArtistName = ?");

$stmt->bind_param("s", $name); //$name = ' OR '1' = 1

$stmt->execute();

//$stmt is now "' OR '1' = 1", which is a string, not
valid SQL

$result = $stmt->get_result();
```

Results:

SQL Injection has been blocked!