Securing the Form Input

Mateo Prigl
SOFTWARE DEVELOPER

Overview

- Creating custom validators
- Cross-site scripting (XSS)
- CSRF token
- SQL injection
- Implementing reCAPTCHA

Demo

Creating custom validators

Cross-site Scripting (XSS)

Demo

Escaping user input

Cross-site Request Forgery (CSRF)

SQL Injection

Search Box

Form

Search by name

Luna

SUBMIT

/search?name=Luna

Server

"SELECT * FROM users WHERE name = " + Luna + ";"

SELECT * FROM users WHERE name = Luna ;

Search Box

Form

Search by name

Luna; DROP TABLE users

SUBMIT

/search?name=Luna%3B%C2%A0DROP%C2%A0TABLE%C2%A0users

Server

"SELECT * FROM users WHERE name = "

+ Luna; DROP TABLE users + ";"

SELECT * FROM users WHERE name = Luna ; DROP TABLE users;

Search Box

Form

Search by name

Luna; DROP TABLE users

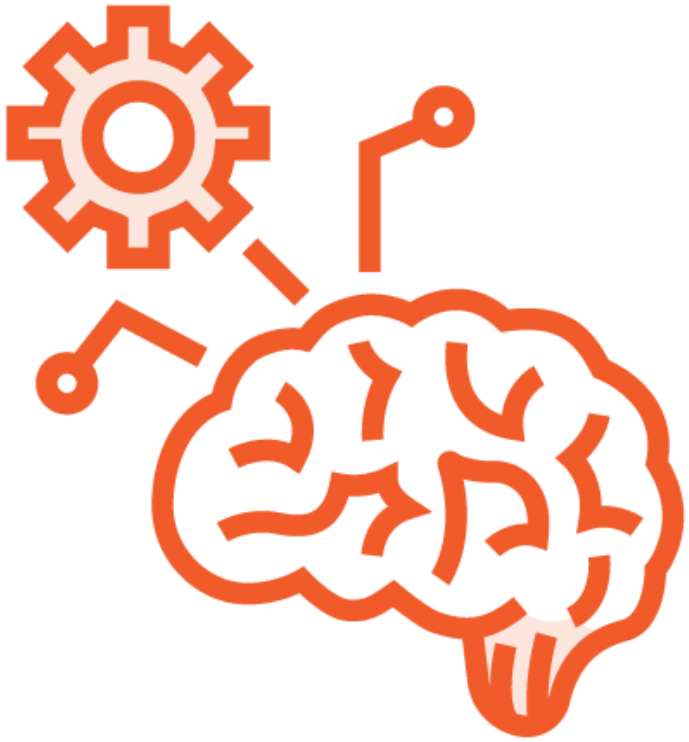
SUBMIT

/search?name=Luna%3B%C2%A0DROP%C2%A0TABLE%C2%A0users

Server

"SELECT * FROM users WHERE name = "
+ Luna; DROP TABLE users + ";"

SELECT * FROM users WHERE name = Luna ; DROP TABLE users;



CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)

Turing test by Alan Turing

Demo

Preventing spam

Implementing reCAPTCHA

Summary

- Custom validators
- Escaping user input
- CSRF tokens
- SQL injection
- Implementing reCAPTCHA