Securing MongoDB from Injection Attacks

Max McCarty

@maxRmccarty https://lockmedown.com

Overview

SQL Injection Attacks

Injection Demonstration with Burp

NoSQL and the Risk of Injection Attacks

MongoDB Injection Attacks

MongoDB and the Risk of JavaScript Expressions

Handling Untrusted Data

SQL Injection Attacks


Yo!

Your destination is our priority....

Address: _____

_____

Arrive By: _____ | pm

in Party? _____

Time: 12:35 pm

Fee: $0.00

Your destination is our priority....

Address: 300 Main St

Arrive By: _____ | pm

in Party? _____

Time: 12:35 pm

Fee: $0.00

Your destination is our priority....

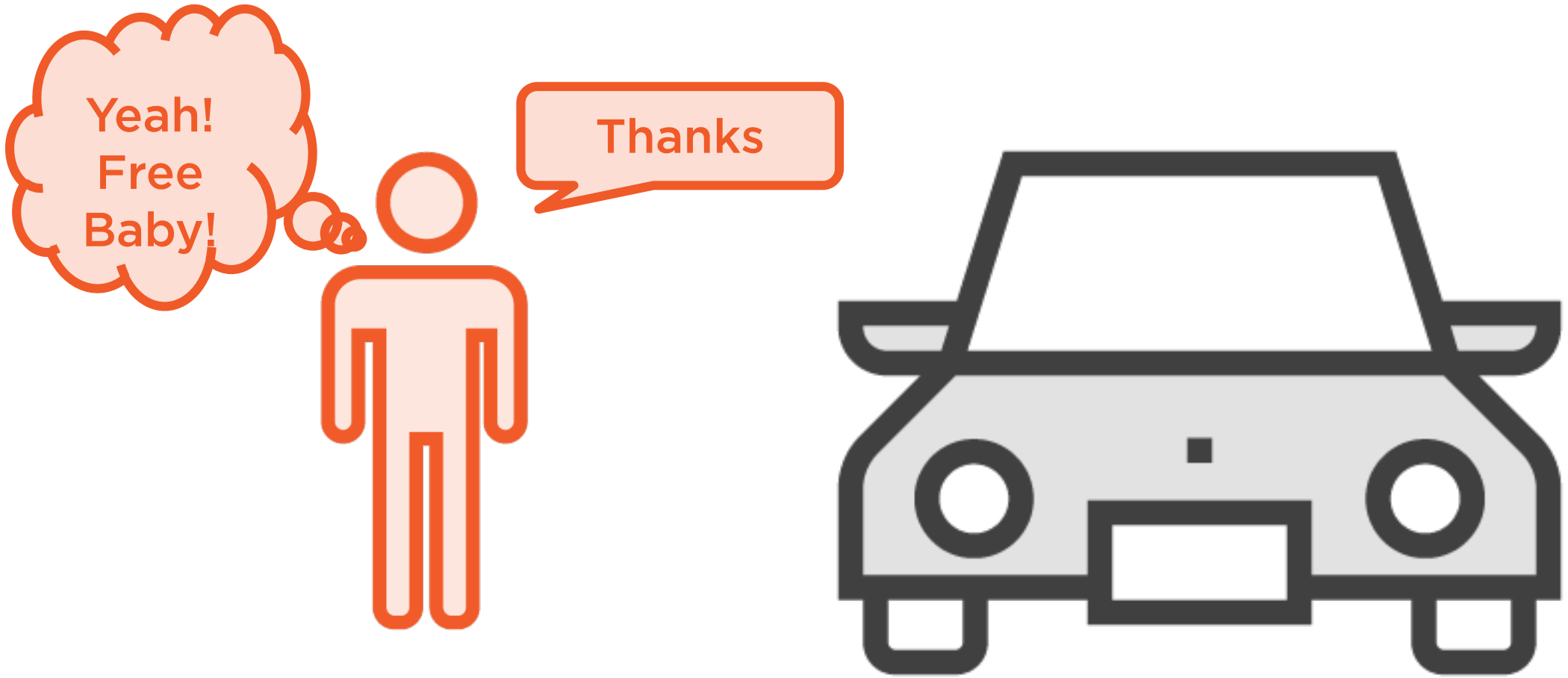
Address: 300 Main St and cost is $0.00
then return to garage

Arrive By: _____ | pm

in Party? _____

Time: 12:35 pm

Fee: $0.00


Yeah!
Free
Baby!
Thanks

SQL Injection Risk

- **Manipulate stored data**
- **Leak confidential information**
- **Grant unauthorized access or elevated privileges**

Ingredients of a SQL Injection

Search Terms: Flash Light

Search Terms:

Flash light; update products set name = ‘All your bases are belong to us'

Ingredients of a SQL Injection

SELECT * FROM Products WHERE Name =

‘Flash Light’; update products set name = ‘All your bases are belong to us'

Parameterized Query

QUERY = SELECT * FROM Products WHERE Name = @param

@param = “flash light; update products set name = ‘All your bases are belong to us'

NoSQL and the Risk of Injection Attacks

NoSQL Database

Database that provides storage and retrieval that differs from the tabular relationships of relational databases. Consist of different types such as key-value, document, graph and column based NoSQL databases.

Can stand for no SQL, non SQL or not only SQL since they may support a structured query like language.

Features of NoSQL Databases

1. **Data Flexibility**
2. **Horizontal Scalability**
3. **Finer Control over Availability**
4. **Open Source**
5. **Lower Cost**

NoSQL databases are free and clear of injection attacks?

Parameterized Query

QUERY = SELECT * FROM Products WHERE Name = @param

@param = “flash light; update products set name = ‘All your bases are belong to us'

MongoDB Injection Attacks

BSON

Short for Binary JSON, is a binary-encoded serialization of JSON-like documents.

JavaScript Expressions

An *expression* is any valid unit of code that resolves to a value.

Ingredients of a SQL Injection

SELECT * FROM Products WHERE Name =

‘Flash Light’; update products set name = ‘All your bases are belong to us'

MongoDB Query Example

```
db.products.find({$where: `this.name == ${user-input}`})
```

MongoDB Operators

$where operator

map-reduce

group command

security.javascriptEnabled

Enables or disables the server-side JavaScript execution. When disabled, you cannot use operations that perform server-side execution of JavaScript code.

mongod Configuration File

mongod-config-file.conf

```
security:
        javascriptEnabled: false
```

Execution of mongod

```
mongod   - -config /path/to/config-file.conf
```

security.javascriptEnabled

Enables or disables the server-side JavaScript execution. When disabled, you cannot use operations that perform server-side execution of JavaScript code.

mongod Configuration File

mongod-config-file.conf

```
security:
        javascriptEnabled: false
```

Execution of mongod

```
mongod   - -config /path/to/config-file.conf
```