

Microservices Security Pattern

Chris Nesbitt-Smith

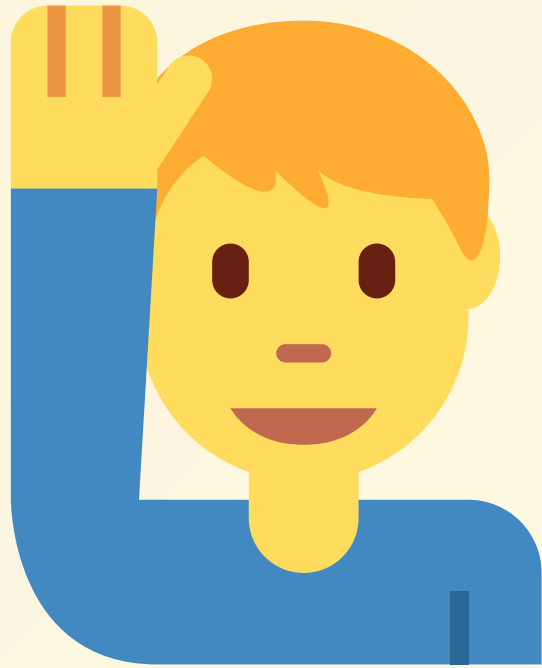
LearnK8s | Appvia



Chris Nesbitt-Smith

- **Learnk8s - Instructor**
- **Appvia - Digital Transformation Consultant**
- **Home Office (uk gov) - Consultant**
- **Opensource:**
 - **OpenZWave**
 - **Z-Wave JS**
 - **Many small projects**









sql-injection-k8s.herokuapp.com



2017

2021

A01:2017-Injection

A02:2017-Broken Authentication

A03:2017-Sensitive Data Exposure

A04:2017-XML External Entities (XXE)

A05:2017-Broken Access Control

A06:2017-Security Misconfiguration

A07:2017-Cross-Site Scripting (XSS)

A08:2017-Insecure Deserialization

A09:2017-Using Components with Known Vulnerabilities

A10:2017-Insufficient Logging & Monitoring

A01:2021-Broken Access Control

A02:2021-Cryptographic Failures

A03:2021-Injection

(New) A04:2021-Insecure Design

A05:2021-Security Misconfiguration

A06:2021-Vulnerable and Outdated Components

A07:2021-Identification and Authentication Failures

(New) A08:2021-Software and Data Integrity Failures

A09:2021-Security Logging and Monitoring Failures*

(New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey




```
92.105.22.161 - - [14/Feb/2022:03:48:55 +0000] "POST /HNAP1/ HTTP/1.1" 404 134 "-" "Mozilla/5.0"

7.53.212.184 - - [14/Feb/2022:04:11:57 +0000] "GET /.env HTTP/1.1" 404 162 "-"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0"

92.105.22.161 - - [14/Feb/2022:04:16:54 +0000] "GET /.env HTTP/1.1" 404 197 "-" "Mozilla/5.0
(X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.40

24.99.105.22.161 - - [14/Feb/2022:04:16:55 +0000] "POST / HTTP/1.1" 405 568 "-" "Mozilla/5.0
(X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36"

7.51.240.114 - - [14/Feb/2022:04:18:57 +0000] "GET /dispatch.asp HTTP/1.1" 404 134 "-"
"Mozilla/5.0 (iPad; CPU OS 7_1_2 like Mac OS X; en-US) AppleWebKit/531.5.2 (KHTML, like Gecko)
Version/4.0.5 Mobile/8B116 Safari/6531.5.2"

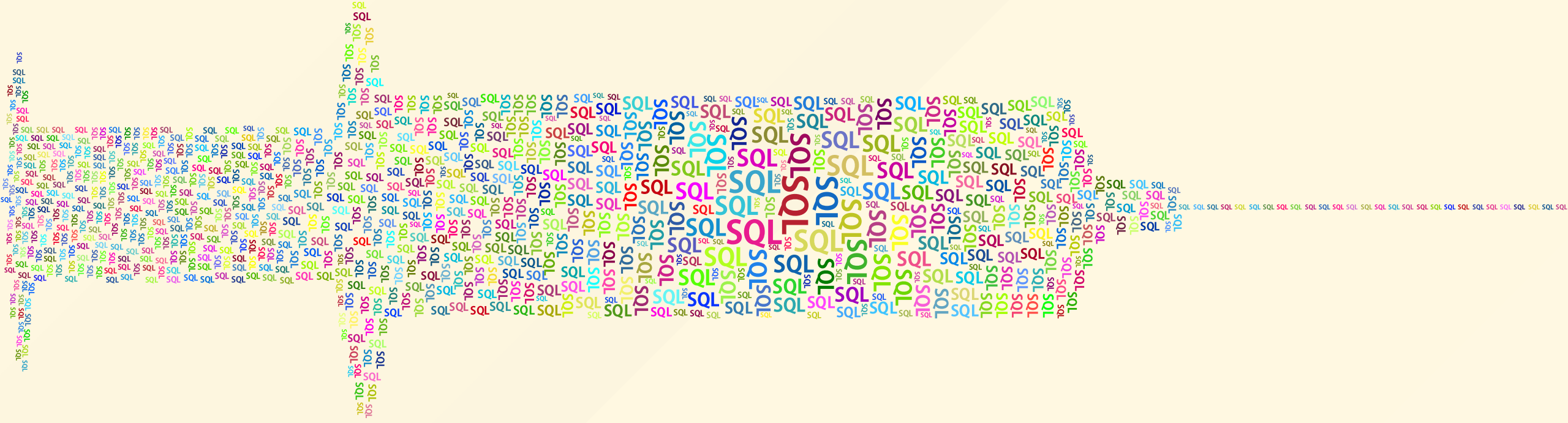
215.74.51.24 - - [14/Feb/2022:04:42:23 +0000] "HEAD / HTTP/1.0" 200 0 "-" "-"

193.246.247.130 - - [14/Feb/2022:07:38:40 +0000] "GET /icons/ubuntu-logo.png HTTP/1.1" 404 197
"http://79.155.234.179/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/98.0.4758.87 Safari/537.36"

193.246.247.130 - - [14/Feb/2022:07:38:42 +0000] "GET /favicon.ico HTTP/1.1" 404 197
"http://79.155.234.179/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/98.0.4758.87 Safari/537.36"

193.246.247.130 - - [14/Feb/2022:07:44:02 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.87
Safari/537.36"

193.246.247.130 - - [14/Feb/2022:07:44:02 +0000] "GET /icons/ubuntu-logo.png HTTP/1.1" 404 197
"http://79.155.234.179/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/98.0.4758.87 Safari/537.36"
```



```
SELECT * FROM table;
```

```
+-----+-----+-----+  
| lastname | firstname | jobtitle |  
+-----+-----+-----+  
| Jennings | Leslie   | Sales Rep |  
| Thompson  | Leslie   | Sales Rep |  
| Gerard    | Martin   | Sales Rep |  
+-----+-----+-----+
```

```
3 rows in set (0.00 sec)
```



```
SELECT name, password FROM users WHERE email = 'user@example.com';
```

```
+-----+-----+  
| name   | password           |  
+-----+-----+  
| myuser | MySecretPassw0rd! |  
+-----+-----+  
1 rows in set (0.00 sec)
```



```
INSERT INTO users (name, password, email)
VALUES('anotheruser', 'letmein', 'user2@example.com');
```

```
1 row(s) affected
```

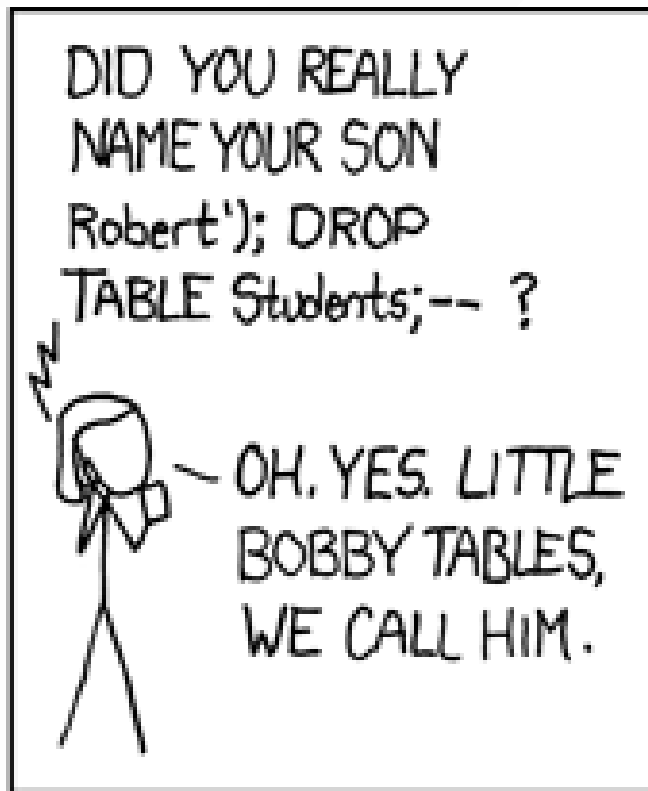
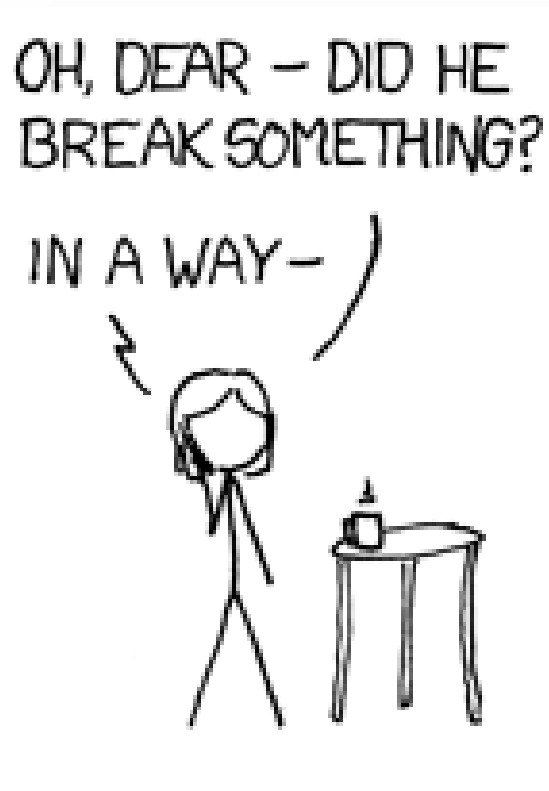
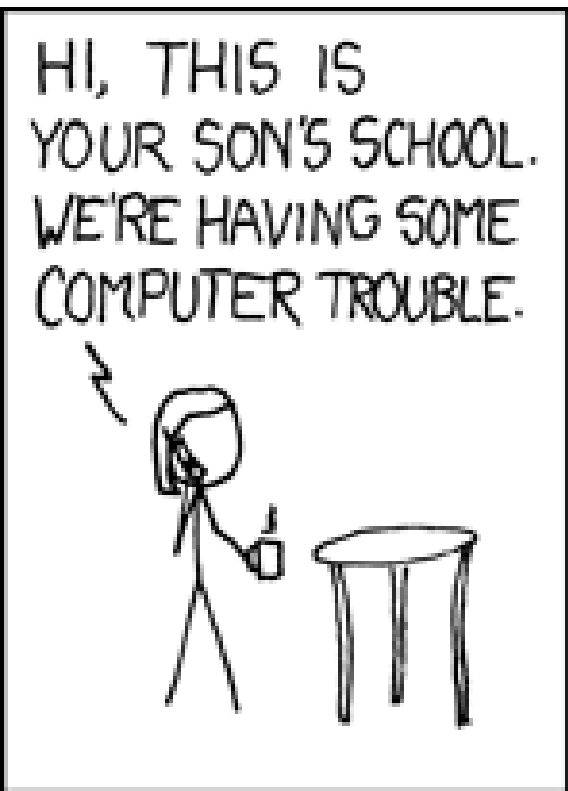


Real world

- **Tesla (2014)**
- **Cisco Prime License Manager (2018)**
- **Fortnite (2019)**







 **https://www**



- GET
- PUT
- POST
- PATCH
- DELETE
- ETC



```
POST /echo/post/json?query=hi HTTP/1.1
Host: example.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 3
```

```
a=b
```



```
POST /echo/post/json?query=hi HTTP/1.1  
a=b
```



```
$result = $con->query("SELECT * FROM products WHERE id = \"{$id}\"");
```



```
$result = $con->query("SELECT * FROM products WHERE id = \"{$_GET['id']}\"");
```



```
http://mydomain.com/products?id=unchecked things
```

```
SELECT * FROM products WHERE id = "unchecked bad things";
```






```
http://mydomain.com/products?id=1" OR id="2"
```

```
SELECT * FROM products WHERE id = "1" OR id = "2";
```



Truncate a table

```
-- http://mydomain.com/products?id=1"; TRUNCATE TABLE products; -- //  
SELECT * FROM products WHERE id = "1"; TRUNCATE TABLE products; --//";
```

Delete a row

```
-- http://mydomain.com/products?id=1"; DELETE FROM products WHERE id="1"; -- //  
SELECT * FROM products WHERE id = "1"; DELETE FROM products WHERE id="1"; --//";
```



Insert a row

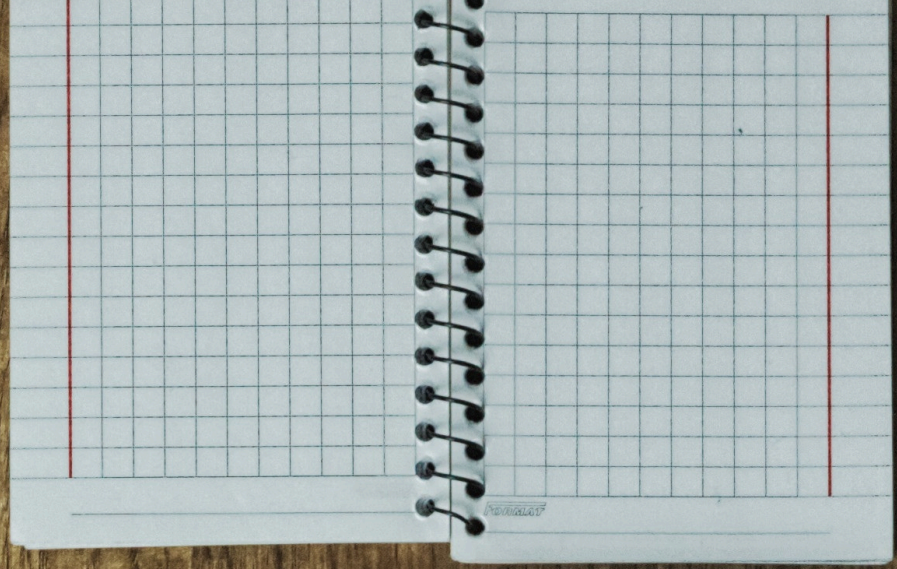
```
-- http://mydomain.com/products?id=1"; INSERT INTO payments(orderid, success) VALUES("123", "yes"); -- //  
SELECT * FROM products WHERE id = "1"; INSERT INTO payments(orderid, success) VALUES("123", "yes"); --//";
```



Encrypt

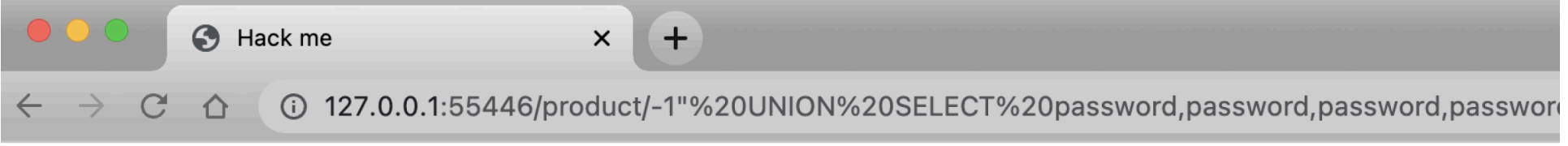
```
UPDATE customers SET email = AES_ENCRYPT(email, PRIVATEKEY);
```





Fatal error: Uncaught mysqli_sql_exception: XPATH syntax error: '::pas5w0rd' in
/var/www/html/product.php:23 Stack trace: #0
/var/www/html/product.php(23): mysqli->multi_query('SELECT * FROM p...') #1 {main} thrown
in **/var/www/html/product.php** on line **23**





[« Return to the homepage](#)

pas5w0rd
pas5w0rd

Product ID pas5w0rd

Price \$pas5w0rd

Description

pas5w0rd



```
SELECT '* * * * * root rm -rf /' INTO outfile /etc/cron.d/bad
```





```
$result = $mysqli->query(sprintf("SELECT * FROM products WHERE id = '%s'",  
    $mysqli->real_escape_string($_GET['id'])));
```





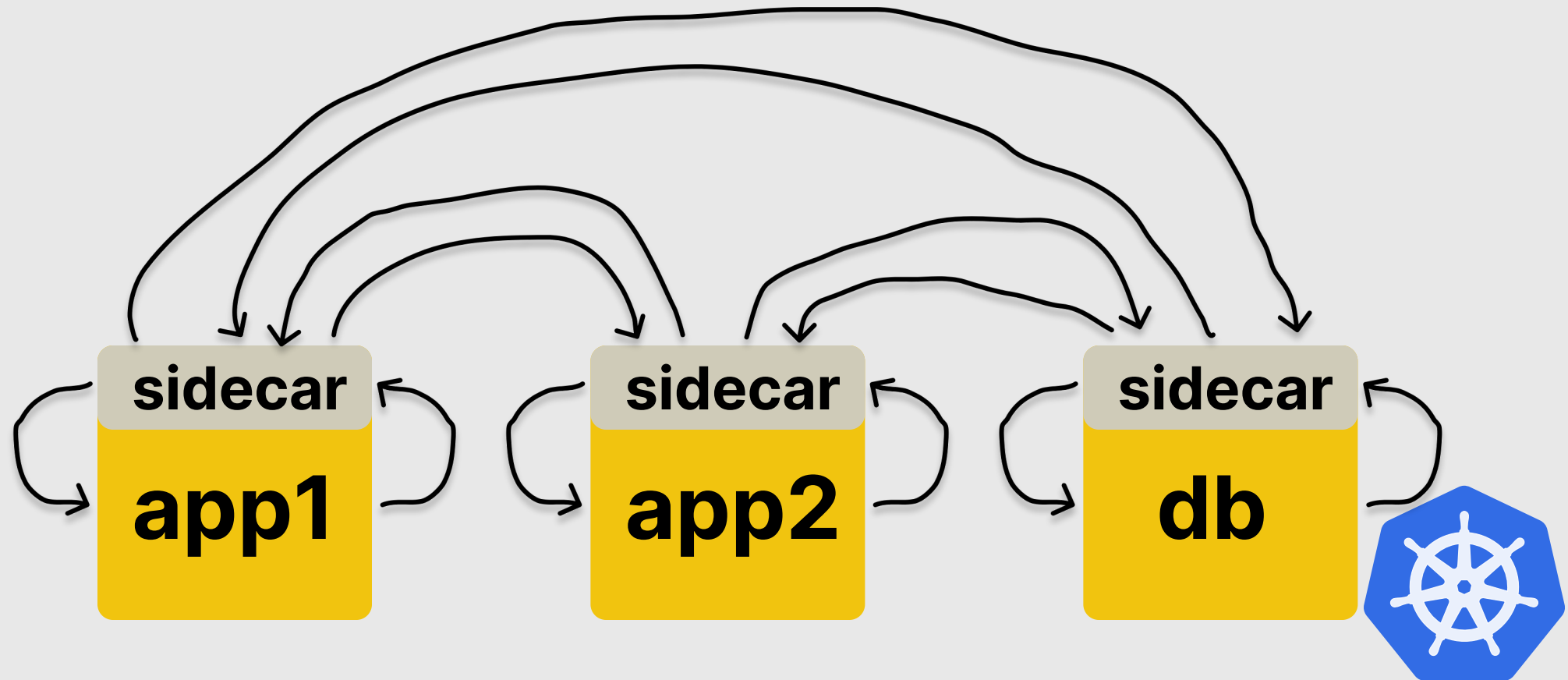












```
apiVersion: v1
kind: Pod
metadata:
  name: myapp
spec:
  containers:
    - name: myapp
      image: myapp:v1.0.0
      ports:
        - containerPort: 80
```



```
apiVersion: v1
kind: Pod
metadata:
  name: myapp
spec:
  containers:
    - name: myapp
      image: myapp:v1.0.0
    - name: nginx # <-- sidecar
      image: nginx:1.14.2
      ports:
        - containerPort: 8080
      volumeMounts:
        - mountPath: /etc/nginx
          name: nginx-config
  volumes:
    - name: nginx-config
      configMap:
        name: myapp
```



```
apiVersion: v1
kind: ConfigMap
metadata:
  name: sidecar
data:
  nginx.conf: |-
    events {}
    http {
      server {
        listen 8080 default_server;
        listen [::]:8080 default_server;

        location ~* "(\'|\")(.*)(drop|insert|md5|select|union)" {
          deny all;
        }

        location / {
          proxy_pass http://localhost:80/;
        }
      }
    }
  }
```



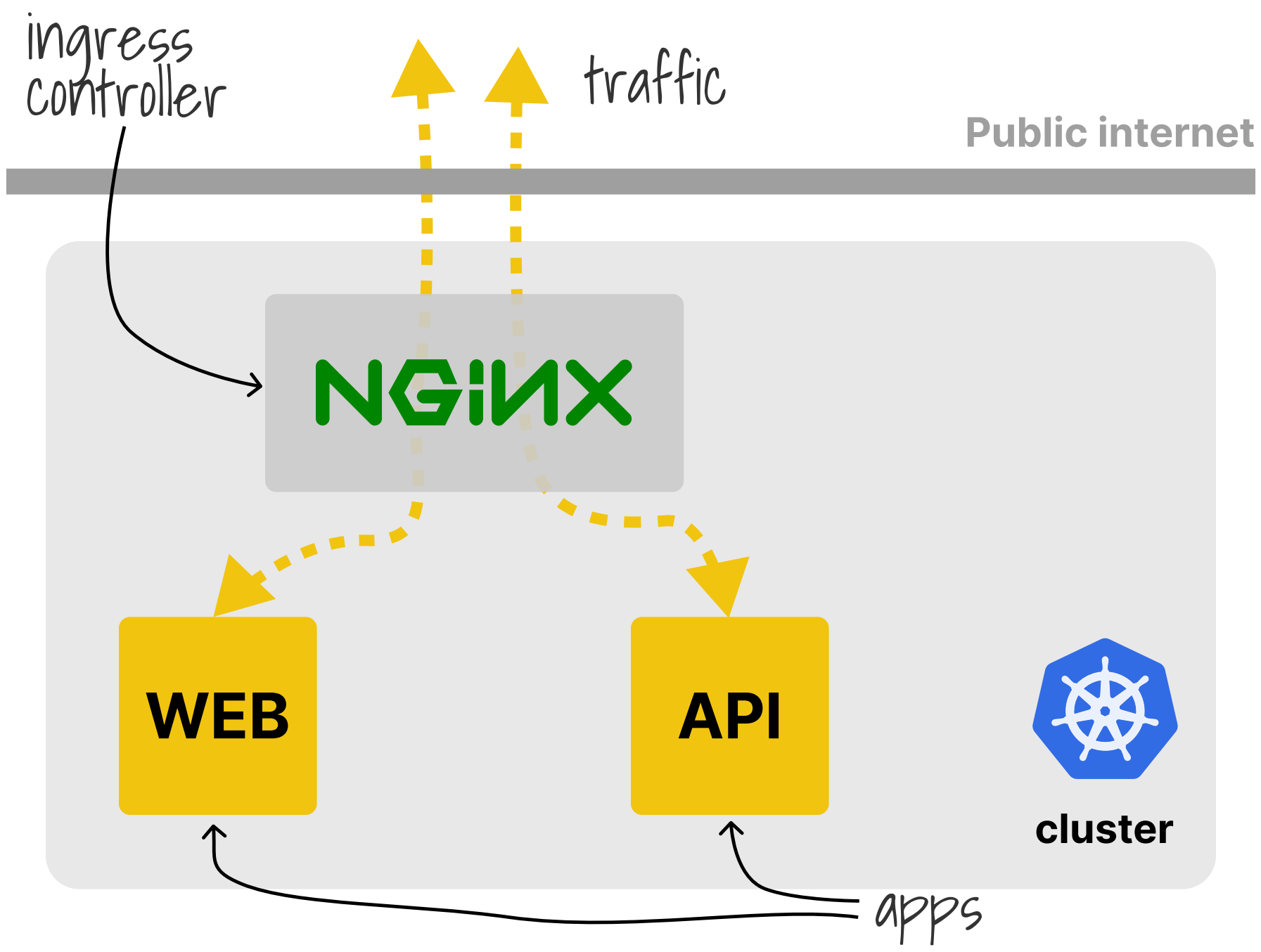
kubectl apply

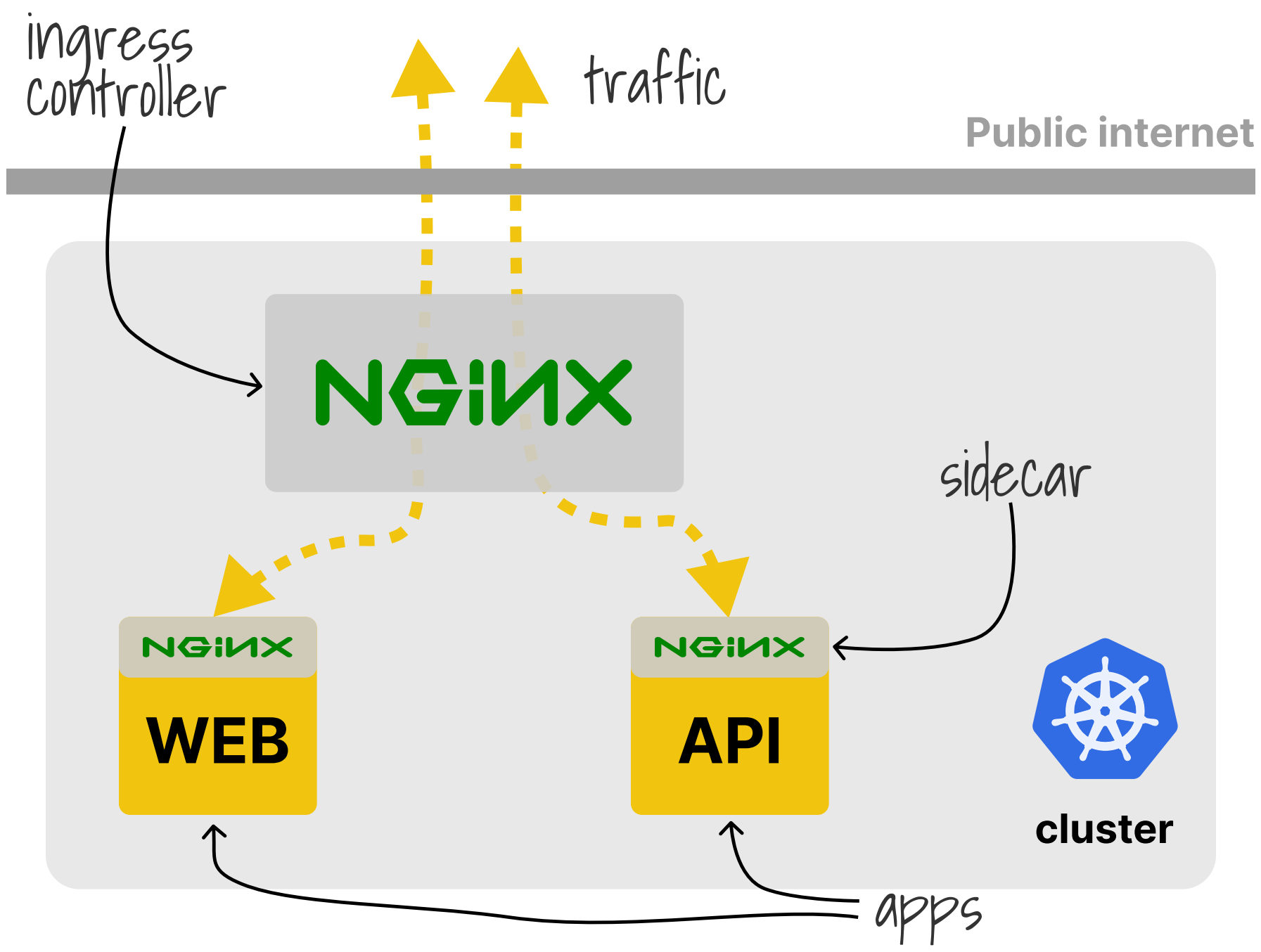


403 Forbidden

nginx/1.21.5








```
apiVersion: v1
kind: Pod
metadata:
  name: myapp
spec:
  containers:
    - name: myapp
      image: myapp:v1.0.0
      ports:
        - containerPort: 80
```



```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: myapp
spec:
  ingressClassName: nginx
  rules:
    - host: "example.com"
      http:
        paths:
          - backend:
              service:
                name: myapp
                port:
                  number: 80
            path: /
            pathType: Prefix
```



```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: myapp
  annotations:
    nginx.org/server-snippets: |
      location ~* "(\'|\")(.*)(drop|insert|md5|select|union)" {
        deny all;
      }
spec:
  ingressClassName: nginx
  rules:
    - host: "example.com"
      http:
        paths:
          - backend:
              service:
                name: myapp
                port:
                  number: 80
            path: /
            pathType: Prefix
```



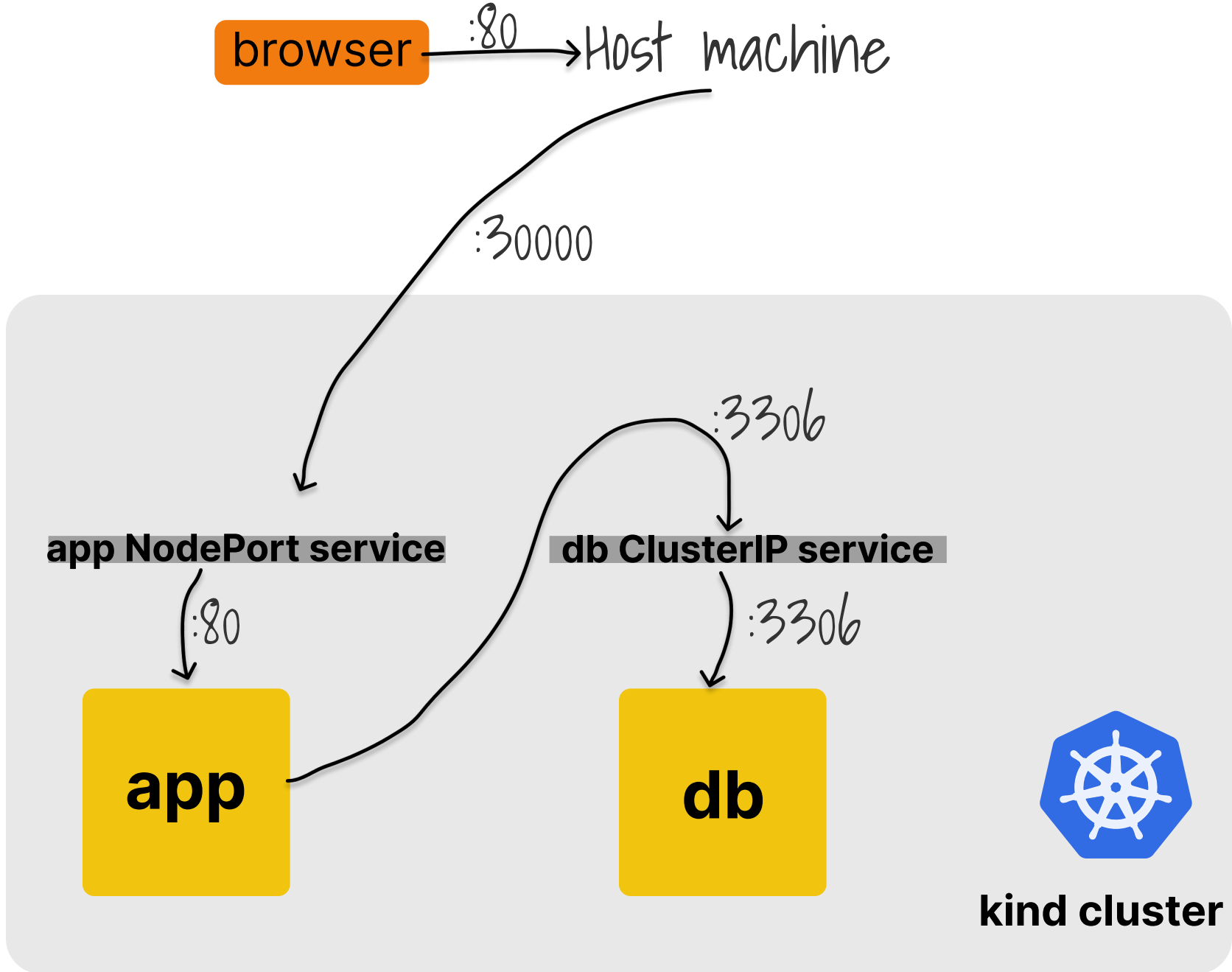
403 Forbidden

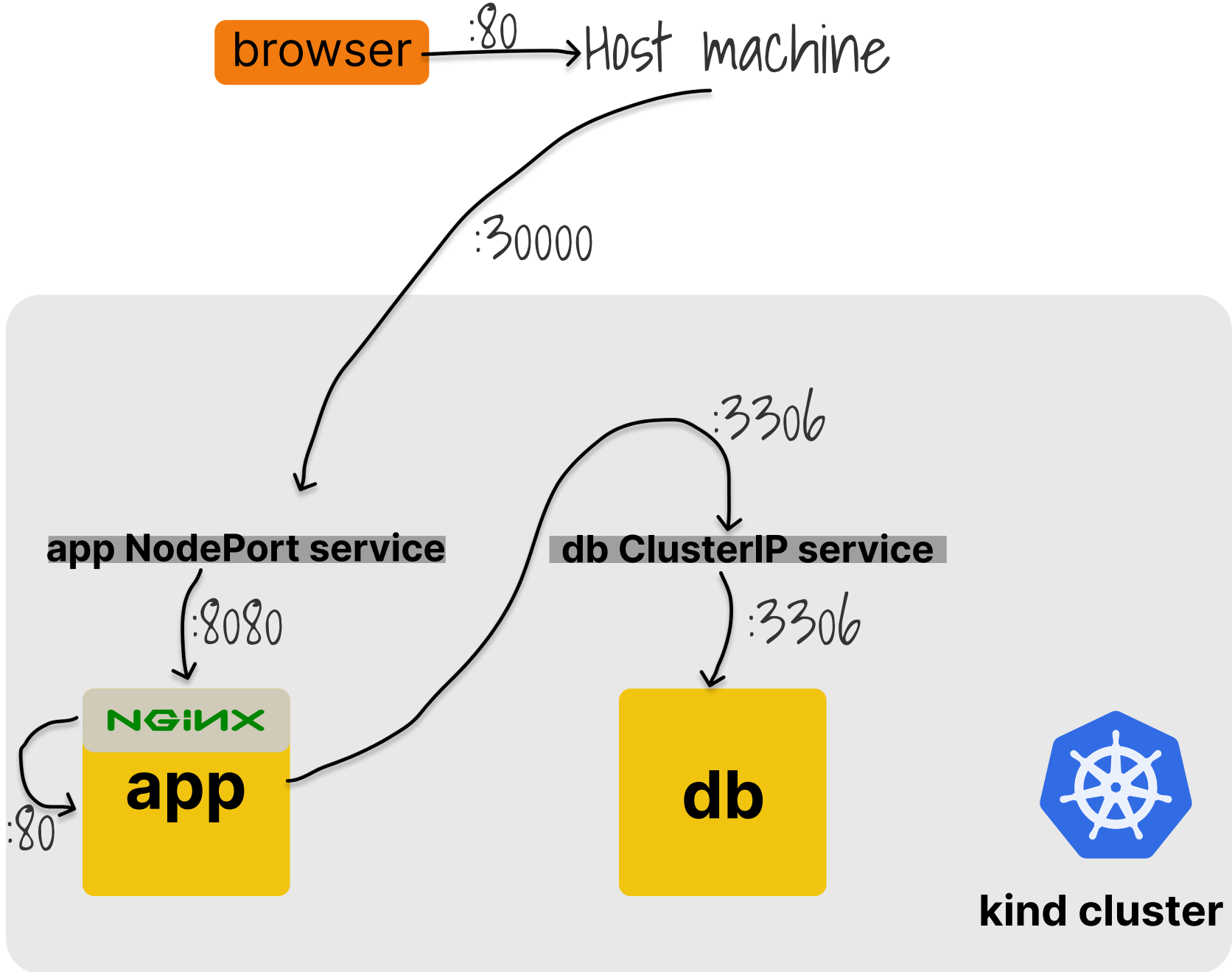
nginx/1.21.5

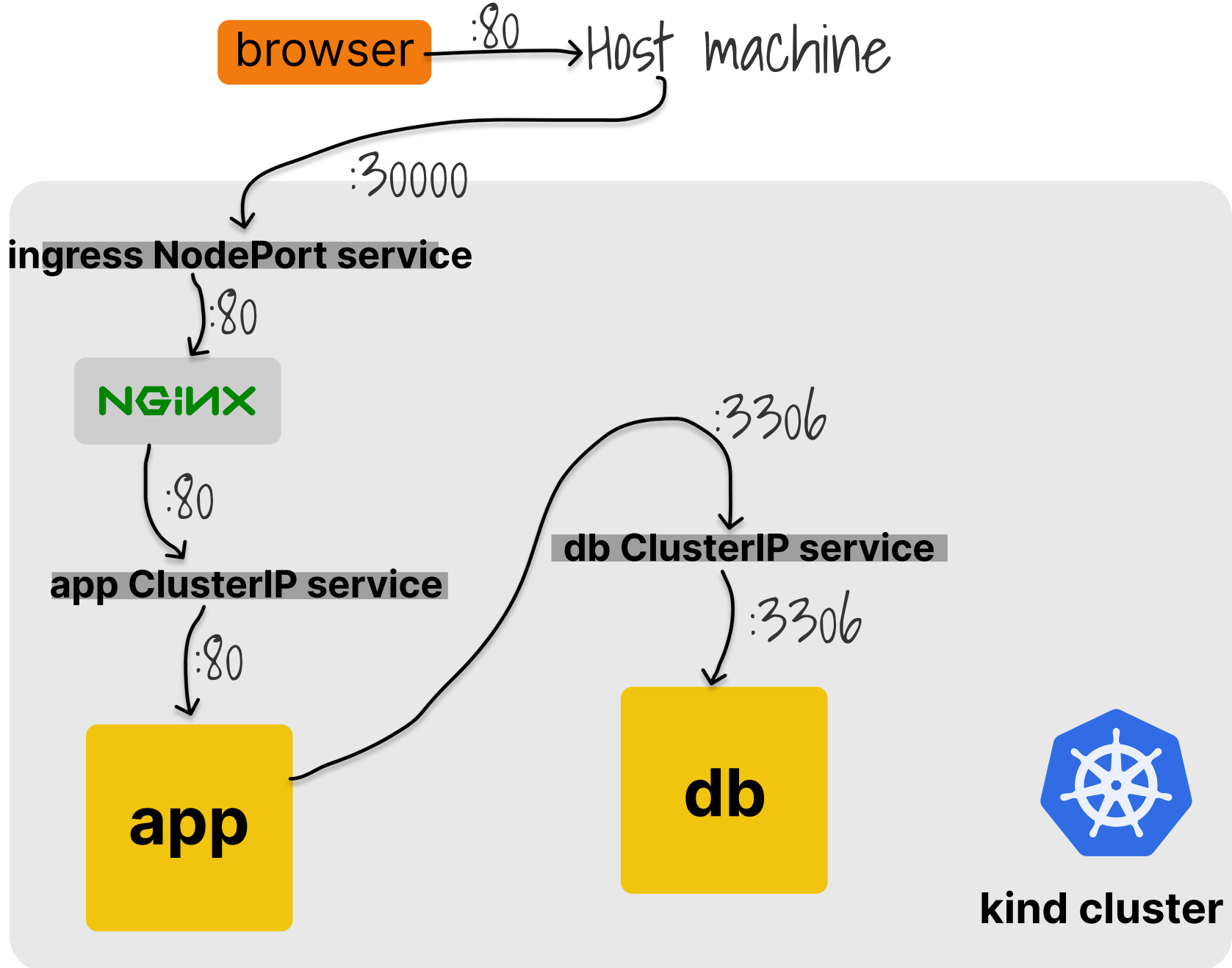


Live demo









🙏 Thanks 🙏

- cns.me
- github.com/chrisns
- nginx.com/blog
- learnk8s.io/kubernetes-resources

Chris Nesbitt-Smith

