

11Kubernetes系列（十三）阻止 ingress SQL 注入、XSS 等攻击

Kubernetes系列（十三）阻止 ingress SQL 注入、XSS 等攻击

通常情况下，web 应用程序会响应来自机器人的请求、健康检查和各种绕过安全性并获得未经授权访问的尝试。

那么，如何才能过滤掉那些针对 Kubernetes 的恶意尝试呢？

Step 1

在深入研究 Kubernetes 之前，让我们回顾一下如何利用一个易受攻击的应用程序。

下面的应用程序是一个简单的电子商务网站，提供了您可以购买的商品列表。

到目前为止一切顺利，让我们点击第一项。



Product catalog

NAME	TYPE	PRICE (\$)	
pillows	bedroom linen	4000	VIEW
book shelf	furniture	3200	VIEW
pressure cooker	kitchen	12000	VIEW
shampoo	healthcare	2300	VIEW
tubelight	lighting	1200	VIEW
headphones	computers	200	VIEW
ADSL2 router	wireless devices	9090	VIEW
buffalo	animal	23000	VIEW
bicycle	vehicles	10000	VIEW

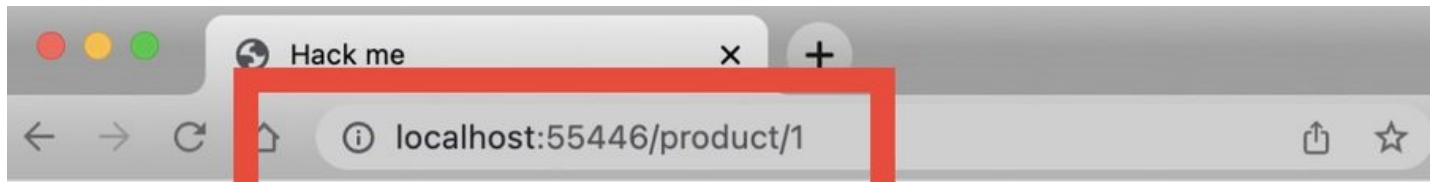
云原生拓展

Step 2

应用程序导航到路径 /product/1

"1"是用户输入，也许我们可以输入一些其他的值？

如果我们不使用数字会发生什么？



[« Return to the homepage](#)

pillows

bedroom linen

Product ID pillows

Price \$4000

云原生拓展

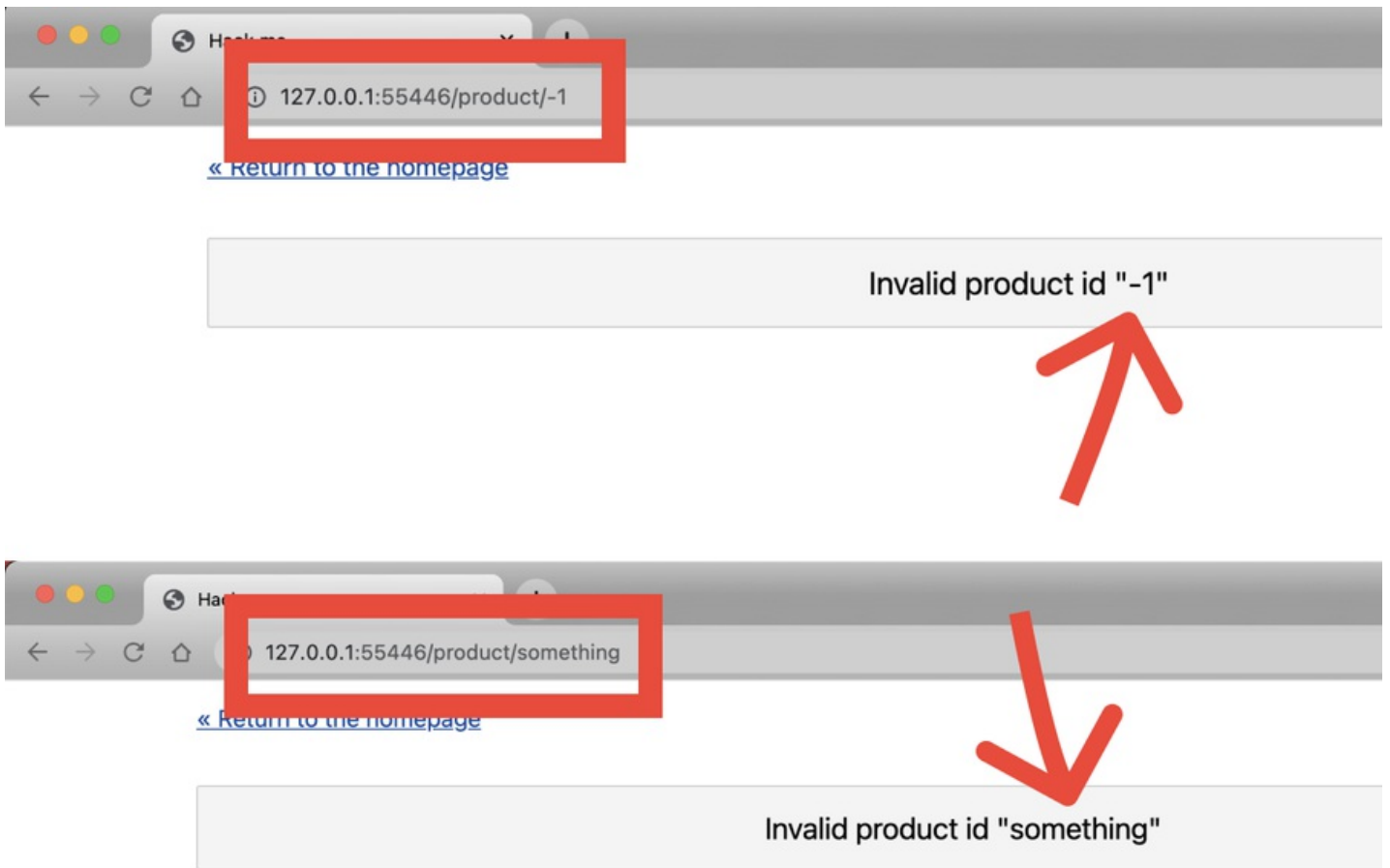
Step 3

输出表明程序并没有对输入进行转义。

我们可以假设对数据库的查询类似于:

```
SELECT * FROM some_table WHERE id = "1"
```

当我们编写恶意查询时会发生什么？



云原生拓展

Step 4

通过一些尝试，你可以针对用户查询做出如下操作:

- 忽略当前查询
- 选择用户表代替原来表
- 实现提取任意用户的用户名和密码

Original query

```
SELECT * FROM some_table WHERE id = "-1" OR 1 -- //
```

↑
injected argument

Where:

- The first quote " completes the first query
- Anything after -- // is discarded
- OR 1 is the actual query we want

云原生拓展

Step 5

下面是当我忽略现有查询并注入我自己的查询时发生的情况。

我暴露了admin用户的名称和密码。

[« Return to the homepage](#)

pas5w0rd

pas5w0rd

Product ID pas5w0rd

Price \$pas5w0rd

Description

pas5w0rd

云原生拓展

Step 6

既然你知道了这种攻击，那么如何预防它呢？

在Kubernetes，我们至少有两个可靠的选择：


1. 我们可以在流量到达容器之前过滤它
2. 我们可以过滤 ingress 的流量

让我们来看看具体做法：

1 Ingress controller

2 Sidecar proxy

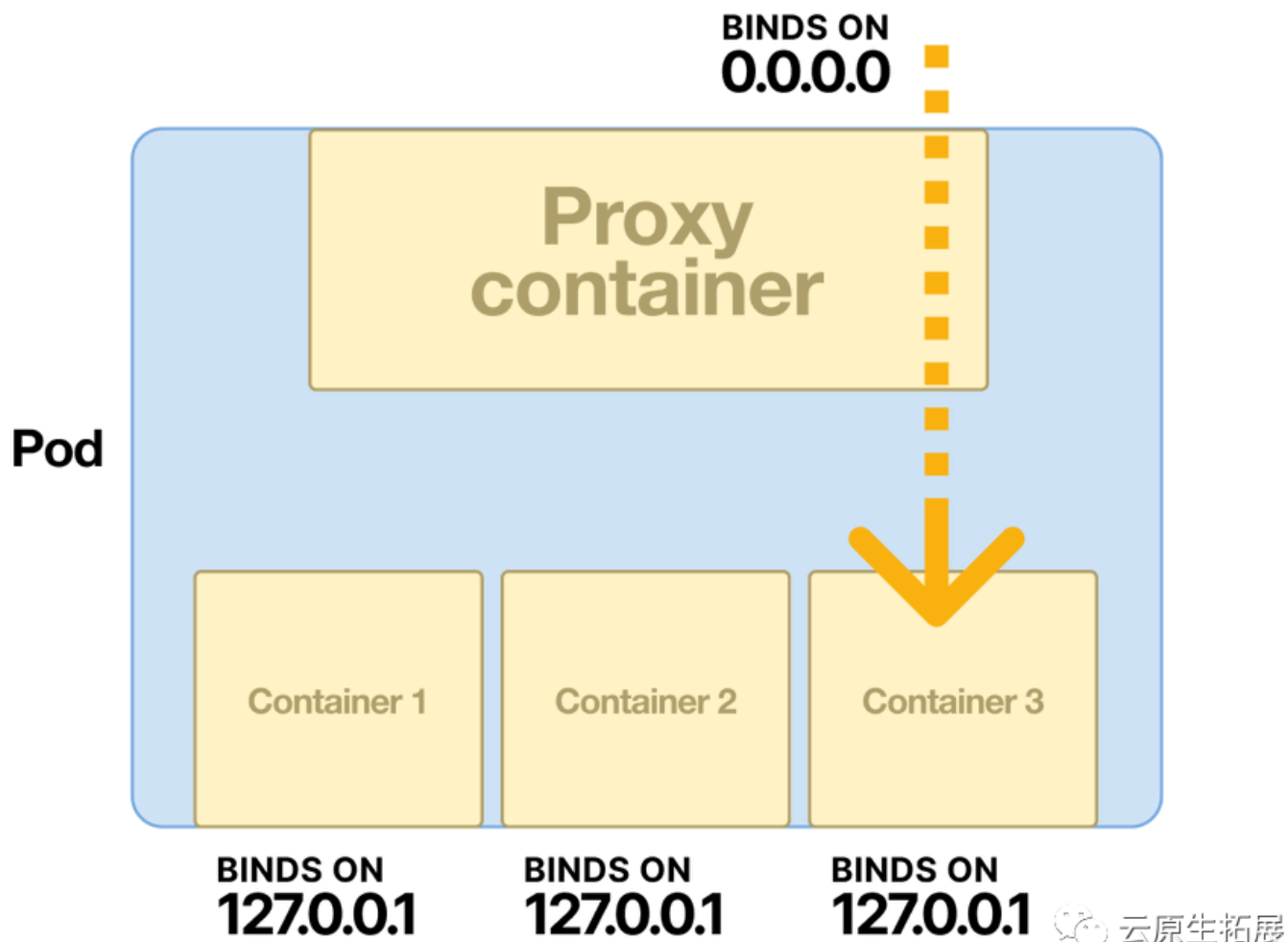
- you can combine them
- also service meshes

 云原生拓展

Step 7

您可以使用一个sidecar代理，在所有流量到达容器之前对其进行过滤。

这是 Kubernetes 中常见的部署模式



Step 8

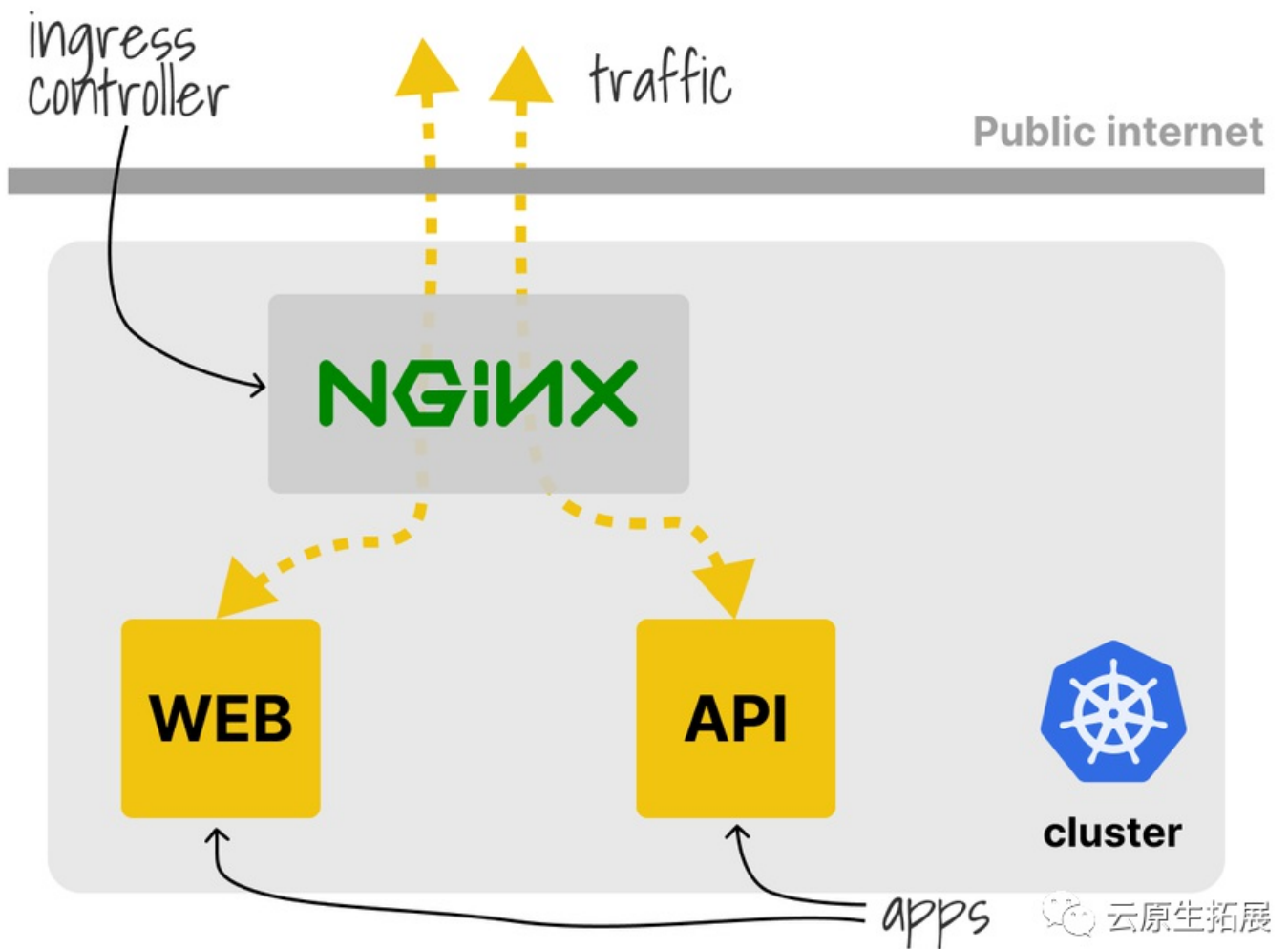
在这种情况下，sidecar NGINX 代理会阻止任何包含SQL操作符的URL到达应用程序。



Step 9

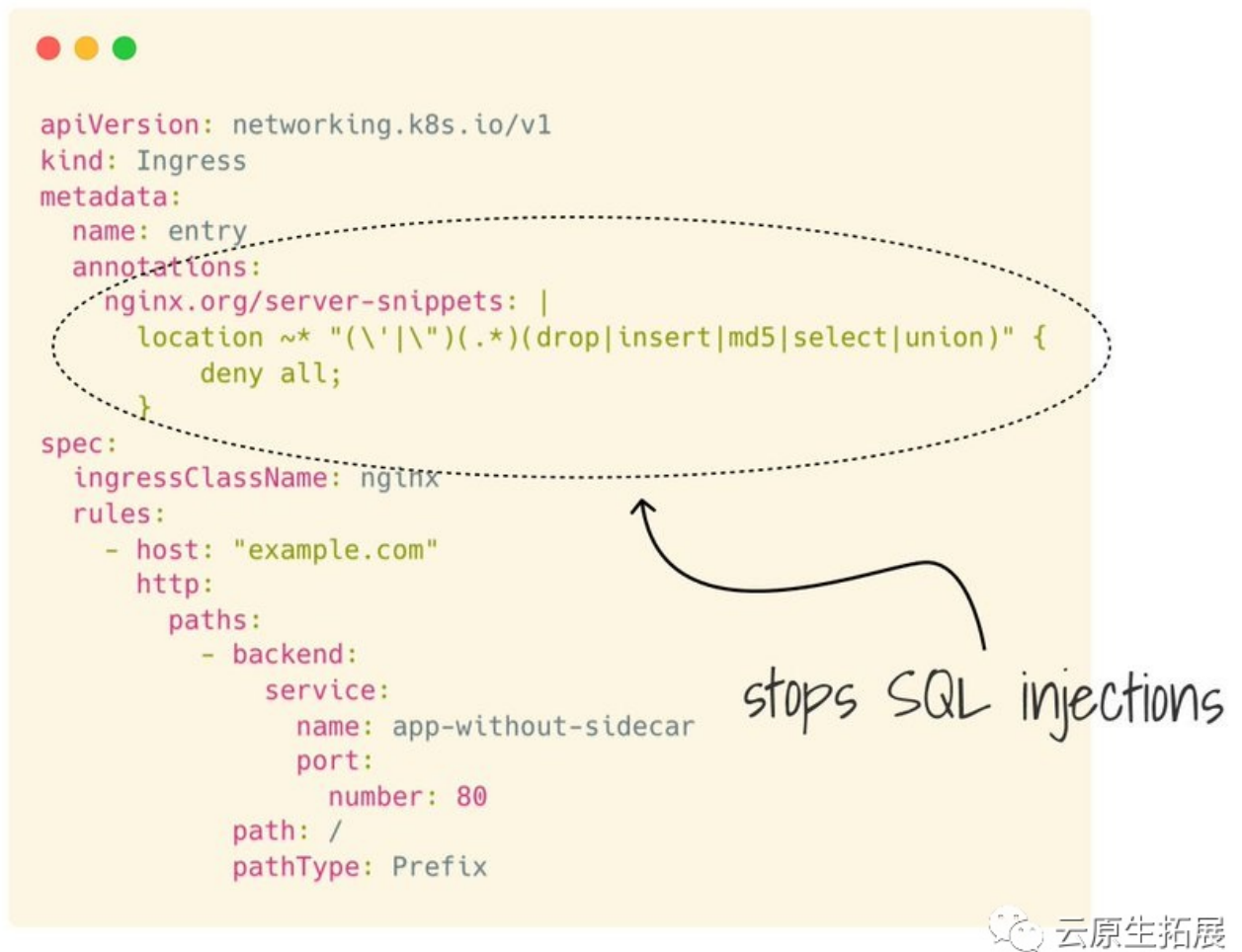
另一个选择是阻止那些针对 ingress 的恶意企图。

因为Ingress routes 会把信息传送到 Pods，我们可以在那里添加逻辑。



Step 10

在这种情况下，我使用 NGINX Ingress 控制器片段来阻止SQL注入。



Step 11

它能正常工作吗?

当然!



欢迎关注我的公众号“云原生拓展”，原创技术文章第一时间推送。