Deploy a local k8s cluster (using minikube, k3s, or anything else) and deploy the

DVWA application. Showcase/demo 3 attack surfaces as mentioned in its

documentation.

To deploy a local Kubernetes cluster and showcase/demo the DVWA (Damn Vulnerable Web Application) application along with 3 attack surfaces, I'll provide a step-by-step guide using Minikube for setting up the Kubernetes cluster and deploying DVWA. Then, I'll demonstrate three common attack vectors as mentioned in DVWA documentation.

Certainly! Here's a comprehensive answer with all the necessary commands and codes for each step:

Step 1: Setup Local Kubernetes Cluster

Install Minikube:

```
curl -LO https://storage.googleapis.com/minikube/releases/latest/minikube-linux-amd64
sudo install minikube-linux-amd64 /usr/local/bin/minikube
```

Start Minikube Cluster:

```
minikube start
```

Step 2: Deploy DVWA Application

Download DVWA Docker Image:

```
docker pull vulnerables/web-dvwa
```

Create DVWA Deployment YAML:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: dvwa-deployment
spec:
  replicas: 1
  selector:
    matchLabels:
      app: dvwa
  template:
    metadata:
      labels:
        app: dvwa
    spec:
      containers:
      - name: dvwa
        image: vulnerables/web-dvwa
        ports:
        - containerPort: 80
```

Create DVWA Service YAML:

yaml

Copy code

```
apiVersion: v1
kind: Service
```

```
metadata:
  name: dvwa-service
spec:
  selector:
    app: dvwa
  ports:
  - protocol: TCP
    port: 80
    targetPort: 80
```

Apply DVWA Deployment and Service:

```
kubectl apply -f dvwa-deployment.yaml
kubectl apply -f dvwa-service.yaml
```

Certainly! Let's delve into each of the attack vectors mentioned and how you can demonstrate them within the DVWA application deployed on Kubernetes:

1. SQL Injection:

Description:

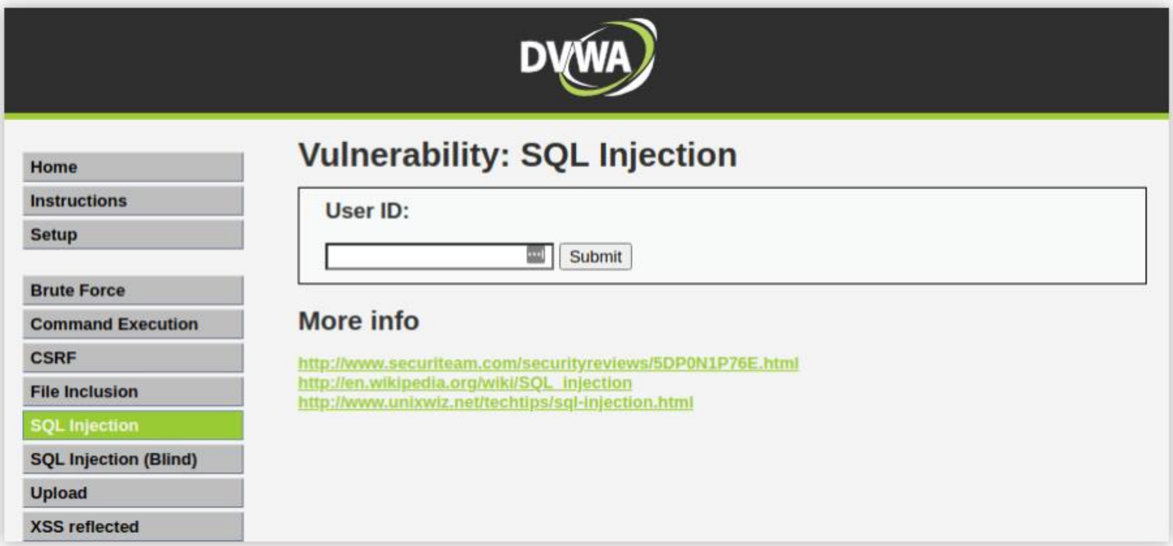
SQL Injection is a code injection technique where malicious SQL statements are inserted into input fields, allowing attackers to manipulate the backend SQL database.

Access DVWA:

Open your browser and navigate to the DVWA application deployed on your local Kubernetes cluster. You can find the IP address using minikube ip.

Navigate to SQL Injection Section:

After successfully installing DVWA, open your browser and enter the required URL `127.0.0.1/dvwa/login.php` Log in using the username "admin" and password as "password".



Vulnerability: SQL Injection

User ID:

More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

DVWA SQL Injection

Within DVWA, there's usually a dedicated section for SQL Injection. Navigate there.

Perform Basic SQL Injection:

In the input field provided for SQL injection, attempt to insert malicious SQL code. For example, try entering ' OR '1'='1' --.

SELECT * FROM users WHERE username = '' OR '1'='1' --' AND password = 'somepassword';

2. Command Injection:

Description:

Command Injection involves injecting and executing arbitrary system commands through input fields, allowing attackers to execute commands on the underlying server.

Demo Steps:

Access DVWA:

Similar to the SQL Injection demo, access the DVWA application.

Navigate to Command Injection Section:

Find the section dedicated to Command Injection within DVWA.

Perform Command Injection:

Enter a command into the input field that interacts with the underlying system. For example, try entering ; ls to list files in the directory.

If the application is vulnerable, it may execute the command and display the output.

Observe Results:

Check if the command executed successfully and if the output is displayed within the application.

3. Cross-Site Scripting (XSS):

Description:

Cross-Site Scripting (XSS) involves injecting malicious scripts into web pages viewed by other users. This can lead to various attacks such as stealing cookies, session hijacking, or defacing websites.

Demo Steps:

Access DVWA:

Again, access the DVWA application.

Navigate to XSS Section:

Look for the Cross-Site Scripting (XSS) section within DVWA.

Perform XSS Attack:

Enter a simple JavaScript code into an input field. For example, <script>alert('XSS')</script>.

If the application is vulnerable, it may execute the script when viewed by another user or when the affected page is loaded.