

Uygulama Laboratuvarı: Güvenlik Açığı Tarama ve Düzeltme



Tahmini süre: 30 dakika

Bu laboratuvara, GitHub'daki kodu ciddiyet sırasına göre güvenlik açıkları için nasıl kontrol edeceğini ve bu açıkları nasıl düzelttiğinizi öğreneceksiniz.

Öğrenme Hedefleri

Bu laboratuvari tamamladıktan sonra şunları yapabileceksiniz:

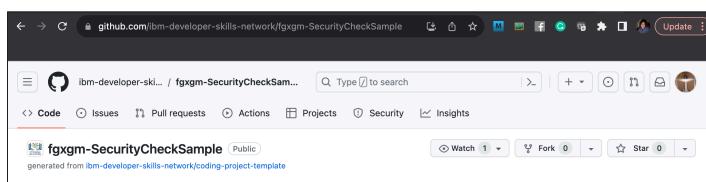
- Kodunuzda bir güvenlik açığı taraması gerçekleştirmek
- Güvenlik açığı riskini azaltma konusunda en iyi uygulamaları işselleştirmek
- Koddaki güvenlik açıklarını düzeltmek

Ön Koşullar:

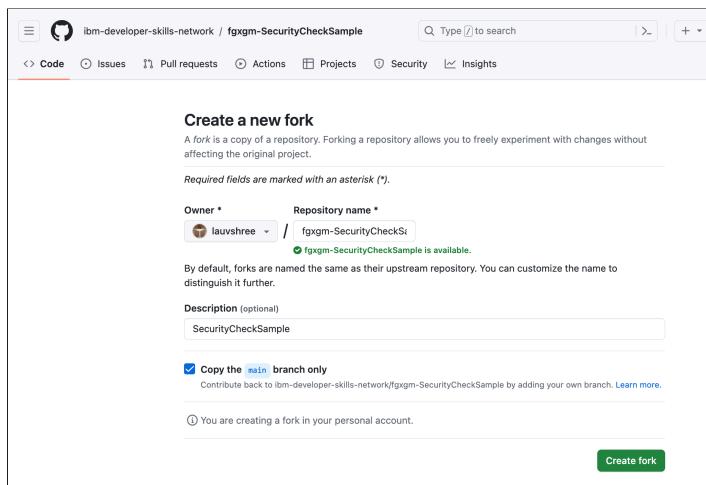
Bir GitHub hesabınızın yanı sıra GitHub hesabınızı kullanmak için kimlik doğrulaması yapılmış bir Snyk hesabınız olmalıdır. Lütfen devam etmeden önce [bu laboratuvari](#) tamamladığınızdan emin olun.

Görev 1: Bir depo kopyası alın

1. <https://github.com/ibm-developer-skills-network/fgxgm-SecurityCheckSample.git> adresine gidin.
2. Depoyu (veya repo) çatal (fork) yaparak kendi kopyanızı alın. Sadece kendi depolarınızı veya herkese açık depoları tarayabileceğinizi unutmayın. Bu depo, dockerize edilip bulutta dağıtılması gereken basit bir sunucu tarafı uygulamasına sahiptir.



3. Çatal oluşturmayı onaylamaz isteniyor. Ayrıntıları okuyun ve Create Fork butonuna tıklayarak işlemi onaylayın.



Artık kendi depo kopyanızı sahipsiniz ve bu depoda yaptığınız değişiklikler, kopyaladığınız kaynağı değiştirmeyecektir.

Görev 2: Repo'yı Tarayın

1. Artık kendi kopyanız olan depoya sahip olduğunuzu göre, <https://app.snyk.io/login> adresine gidin ve GitHub kimlik bilgilerinizi kullanarak giriş yapın.
2. Snyk'te, Projeleri Ekle butonuna tıklayın ve eklemek istediğiniz depoyu kaynak olarak GitHub seçin.

3. Forkladığınız depoyu seçin ve **Seçilen Depoları Ekle** butonuna tıklayın.

4. Proje eklendikten sonra, Snyk tarafından içe aktarılır ve taranır.

Bu birkaç saniye sürebilir. Tarama tamamlandığında, taramanın raporunu göreceksiniz.

5. Tarama tamamlandığında, aşağıdaki gibi bir sorun raporu göreceksiniz.

Görev 3: Tarama raporunu görüntüle

1. Güvenlik açıklarının nerede olduğunu ve ciddiyetini belirten ayrıntılı raporu görmek için repo adının önündeki ok simgesine tıklayın. Her dosya için gösterilen 4 farklı güvenlik açığı vardır:

- Kritik
- Yüksek
- Orta
- Düşük

2. Tarama yapılmış güvenlik açıklarını görmek için Dockerfile dosyasına tıklayın.

Lavs-GIT > Projects > Project

Lavs-GIT/fgxgm-SecurityCheckSample (main)

Lavs-GIT/fgxgm-SecurityCheckSample:Dockerfile

Created Tue 12th Sep 2023 | Snapshot taken by snyk.io 18 minutes ago | Retest now

IMPORTED BY	PROJECT OWNER	SOURCE	TARGET OS
@gmail.com	+ Add a project owner	Github	debian:11
IMAGE TAG	BASE IMAGE	REPOSITORY	MANIFEST
18.12.1	node:18.12.1	fgxgm-SecurityCheckSample	Dockerfile
ENVIRONMENT	BUSINESS CRITICALITY	LIFECYCLE	LINKED IMAGES
+ Add a value	+ Add a value	+ Add a value	+ Add a value

Recommendations for upgrading the base image

BASE IMAGE	VULNERABILITIES	SEVERITY	
Current image	node:18.12.1	430	10 C 32 H 115 M 273 L
Minor upgrades	node:18.17.1	158	0 C 0 H 1 M 157 L

Open a fix PR

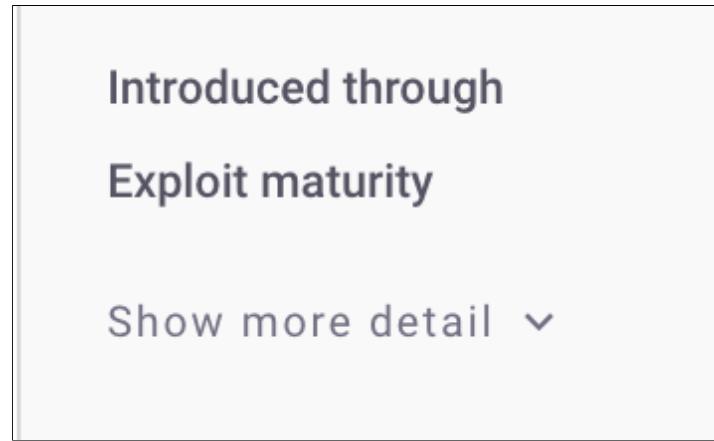
3. Sonuçlar, belirli bir tür güvenlik açığının ayrıntılı görünümünü elde etmek için ciddiyetine göre filtrelenebilir.



4. Listelenen hataları ve bunların hangi tür güvenlik açığı veya güvenlik riski olabileceğini görebilirsiniz.

C apr/libapr1 - Integer Overflow or Wraparound	SCORE 714
VULNERABILITY ***	
Introduced through	apr/libapr1@1.7.0-6+deb11u1
Fixed in	apr/libapr1@1.7.0-6+deb11u2
Exploit maturity	NO KNOWN EXPLOIT
Show more detail ▾	
Ignore	
C curl/libcurl4-openssl-dev - Exposure of Resource to Wrong Sphere	SCORE 714
VULNERABILITY ***	
Introduced through	curl/libcurl4-openssl-dev@7.74.0-1.3+deb11u3, curl@7.74.0-1.3+deb11u3 and others

5. Her hata için, hatanın sonuçları hakkında tavsiyelerde bulunan ve hatanın nasıl düzeltilebileceğini öneren ayrıntılı bir rapor görebilirsiniz.



6. Sayfanın üst kısmına kaydırığınızda, çoğunlukla en çok hatayı ortadan kaldırmak için takip edebileceğiniz büyük bir öneri olacaktır. Bu, çoğu sorunun düzeltildiği en son sürümü dayanacaktır.

Recommendations for upgrading the base image			
	BASE IMAGE	VULNERABILITIES	SEVERITY
Current image	node:18.12.1	401	10 C 32 H 109 M 250 L
Minor upgrades	node:18.17.1	150	0 C 1 I 1 M 148 L
Show more upgrade types			

7. Yukarıdaki örnekte görüldüğü gibi, node sürümünü 18.12.1'den 18.17.1'e yükseltmenizi önerir.

Görev 4: Güvenlik açıklarını düzeltin

1. GitHub'daki depoya geri dönün. Dockerfile'a tıklayarak açın ve görüntüleyin.

public	initial code
server	initial code
.gitignore	Initial commit
Dockerfile	initial code
LICENSE	Initial commit
README.md	initial code
manifest.yml	initial code
package-lock.json	initial code

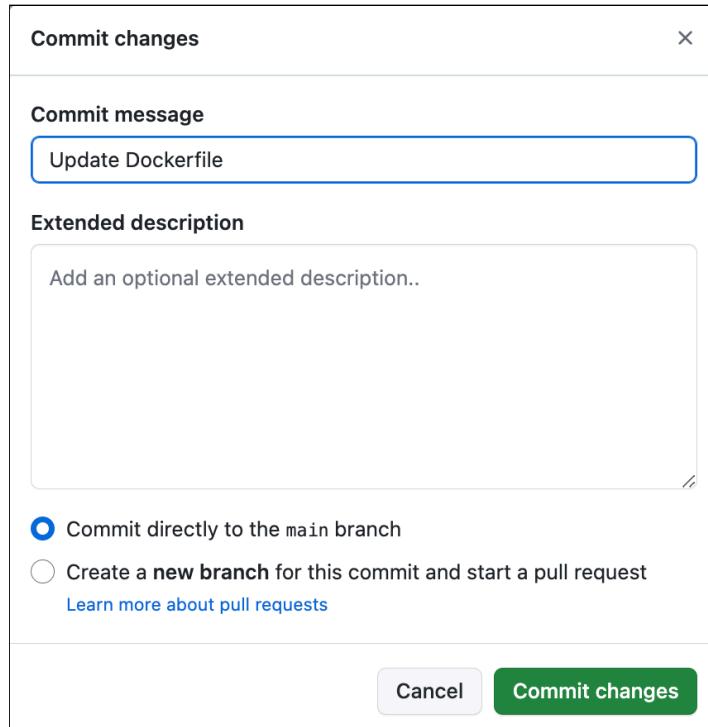
2. Sağ üstteki kalem simgesine tıklayarak düzenleyin ve node sürümünü önerildiği gibi 18.17.1 olarak değiştirin.

fgxgm-SecurityCheckSample / Dockerfile in main

Edit Preview

```
1  FROM node:18.17.1
2
3  RUN npm install -g npm@9.1.3
4
5  ADD package.json .
6  ADD index.js .
7  ADD build .
8  COPY .
9  RUN npm install
10
11 EXPOSE 8080
12
13 CMD [ "node", "index.js" ]
14
```

3. Değişiklikleri kalıcı hale getirmek için bunları deponuzda taahhüt edin.



Görev 5: Güvenlik açıklarının düzeltildiğini doğrulama

1. Snyk taramasını yaptığınız tarayıcı sekmesine geri dönün. Eğer sekmeyi kapatmışsanız, yeni bir tane açabilirsiniz.
2. Tarama yeniden çalıştırılacak ve güncellenmiş bir rapor mevcut olacaktır.
3. Yeni öneriler olup olmadığını kontrol edin.

Recommendations for upgrading the base image			
	BASE IMAGE	VULNERABILITIES	SEVERITY
Current image	node:18.17.1	150	0 C 1 H 1 M 148 L
Alternative upgrades	node:20.5.1-bookworm-slim	28	0 C 0 H 0 M 28 L
Show more upgrade types			
Open a fix PR			

4. Git üzerinde değişiklik yapın ve commit edin.
5. Tekrar tekrar önerilen değişiklikleri yapmaya devam edin ve proje raporunu tekrar kontrol edin. C, H veya M sorunları kalmadığında, projenin hazır olduğu kabul edilir.

Targets: 1	Search targets
> 0 3 lavvshree/fpxgm-SecurityCheckSample	0 C 0 H 0 M 28 L

Görev 6 (İsteğe Bağlı): Düşük öncelikli sorunları düzeltin

1. Öneriye dayanarak, L ile işaretlenmiş düşük öncelikli sorunları düzeltip düzeltmemeyeceğinizi kontrol edin.

Tebrikler! Bu laboratuvar çalışmasında, bir git kod deposunu güvenlik açıkları için taramayı ve güvenlik açıklarını düzeltmeyi öğrendiniz.

Yazar(lar)

Lavanya T S

© IBM Corporation. Tüm hakları saklıdır.