

Uygulamalı Laboratuvar: Kod Deponuzu Taramak için SNYK Kullanımı

Tahmini Süre: 30 dakika

Bu laboratuvar çalışmasında, kod deponuzu taramak için **Sneak** olarak telaffuz edilen SNYK ile tanışacaksınız.

Öğrenme Hedefleri:

Bu alıştırmayı tamamladıktan sonra şunları yapabileceksiniz:

- Kod deposunu taramak
- Kod deposu raporunu analiz etmek

Ön Koşullar

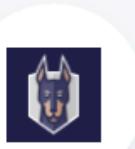
- Bir GitHub hesabınız olmalıdır. Eğer GitHub hesabınız yoksa, [bu linki](#) gidin, talimatları izleyin ve kaydolun.
- GitHub'ınızda bazı kamuya açık ve özel depolar bulunmalıdır. Eğer hiç yoksa, bir tane oluşturmalısın. Örneğin, başka bir kamuya açık depo olan <https://github.com/bitnami/containers>'nı bir kopyasını oluşturmak istiyorsanız, depoya gidin. Hesabınıza fork etmek için **Fork** butonuna tıklayın. Bu, sizin için deponun bir kopyasını oluşturacaktır.

SNYK'e bir proje ekleme

SNYK yazılımı birçok özelliğe sahiptir. Ancak, ücretsiz bir hizmet olarak sunulan kod deposu güvenlik kontrolüne odaklanacağız.

1. <https://app.snyk.io/login> adresine gidin ve GitHub ile giriş yapın.

2. Tarayıcınızda GitHub'a zaten giriş yapmışsanız, bir sonraki adıma geçin. Aksi takdirde, GitHub kimlik bilgilerinizi kullanarak giriş yapın.



Sign in to GitHub
to continue to Snyk Login

Username or email address

SPYKERSICKMUDERD

Password

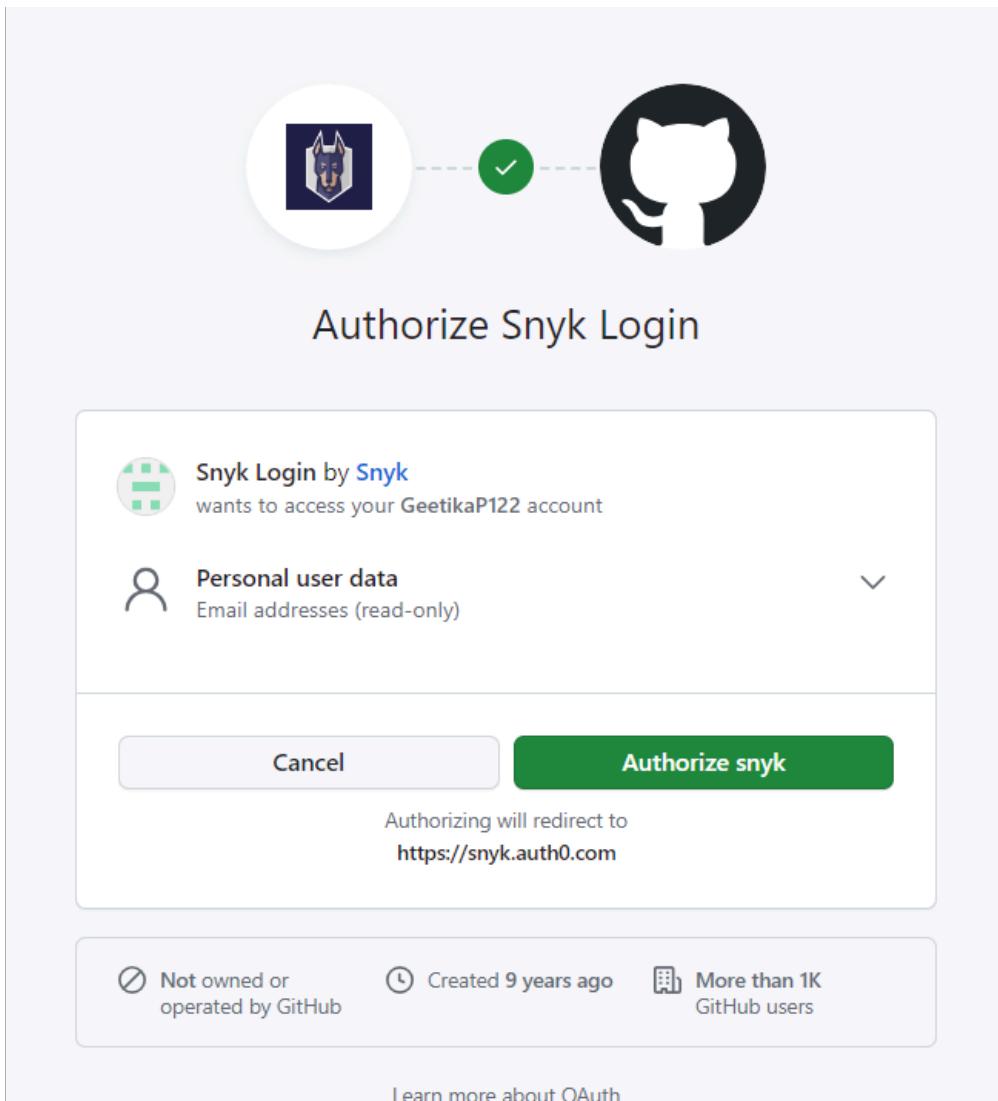
[Forgot password?](#)

[Sign in](#)

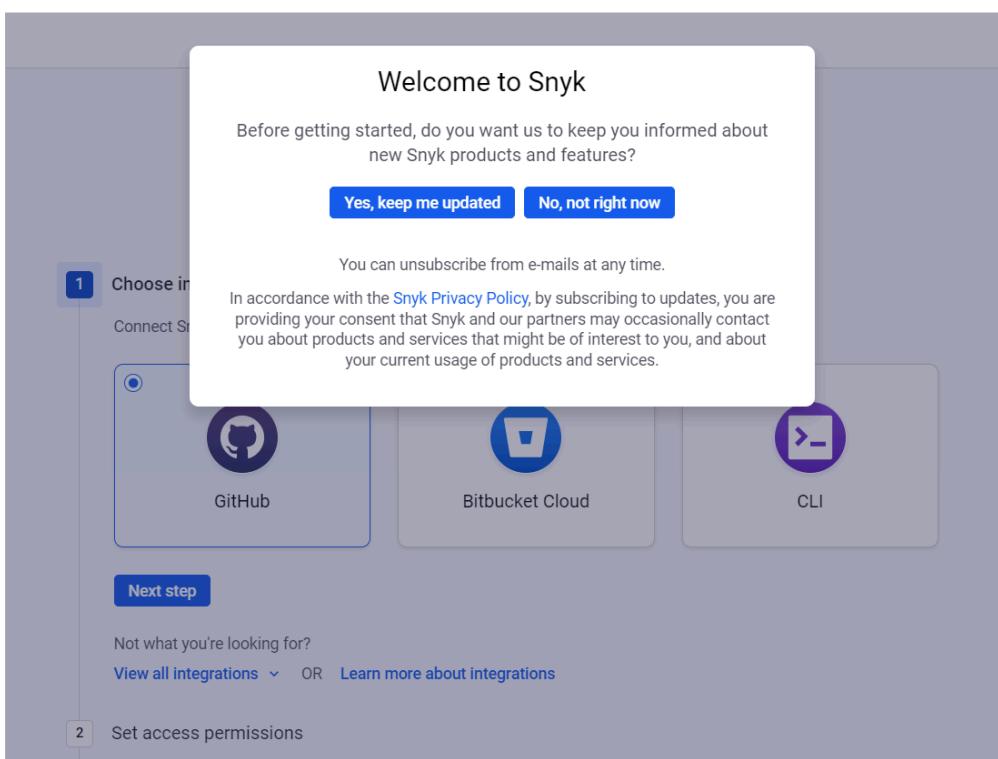
[Sign in with a passkey](#)

[New to GitHub? Create an account](#)

3. İzin verin ve snyk'in GitHub kimlik bilgilerinizi kullanarak giriş yapmasına yetki verin.



4. İlk kez giriş yaptığınızda, ürün sürümleri ve özellik güncellemeleri hakkında bilgi almak için abone olmak isteyip istemediğinizi sorar. **Hayır, şu anda değil** seçeneğine tıklayın.



5. Test etmek istediğiniz kodun konumunu seçin. Bu alıştırma için GitHub'ı seçin. Zaten bir hesabınız varsa BitBucket'ı da seçebilirsiniz.

Where is the code you want to scan?

Scan your projects for security issues

1 Choose integration method

Connect Snyk to your code and run scans directly in your workflow

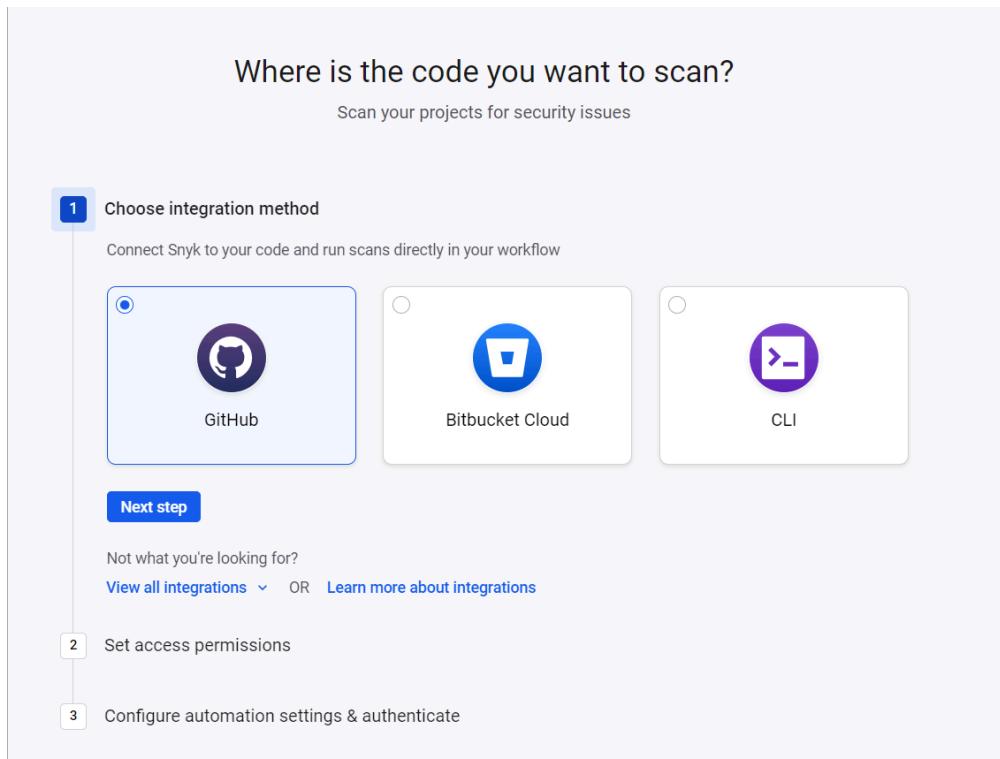
GitHub Bitbucket Cloud CLI

Next step

Not what you're looking for?
[View all integrations](#) OR [Learn more about integrations](#)

2 Set access permissions

3 Configure automation settings & authenticate



6. Hem kamu hem de özel depoları (veya repos) kullanma veya sadece kamu reposlarını kullanma seçenekleri sunulur. **Sadece kamu reposları** seçeneğini seçin.

Where is the code you want to scan?

Scan your projects for security issues

✓ Choose integration method

2 Set access permissions

Private and public repositories
Grant Snyk access to all repository types under your Github account whether private or public.

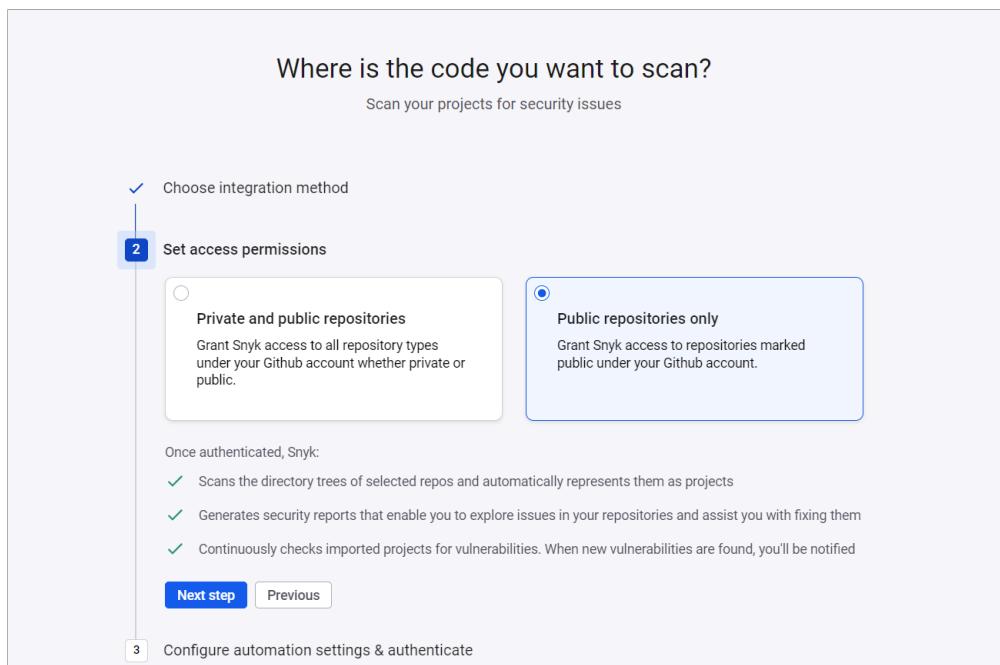
Public repositories only
Grant Snyk access to repositories marked public under your Github account.

Once authenticated, Snyk:

- ✓ Scans the directory trees of selected repos and automatically represents them as projects
- ✓ Generates security reports that enable you to explore issues in your repositories and assist you with fixing them
- ✓ Continuously checks imported projects for vulnerabilities. When new vulnerabilities are found, you'll be notified

Next step **Previous**

3 Configure automation settings & authenticate



7. Snyk'in yapmasını istediğiniz tüm tarama türlerini kontrol edin ve seçin, ardından **GitHub ile Kimlik Doğrula** seçeneğine tıklayın.

Choose integration method

Set access permissions

3 Configure automation settings & authenticate

Enabled features:

- Pull Request Checks
Test your pull requests for new issues and vulnerabilities
- New Fix Pull Requests
Automatically create pull requests for newly discovered open source issues and vulnerabilities
- Dependency Upgrade Pull Requests
Keep your packages up to date with automatic dependency upgrade pull requests
- Snyk Code
Analyze your source code for issues and vulnerabilities 

[Authenticate GitHub](#) [Previous](#)

8. GitHub, snyk'in kamu reposlarınızı kullanmasına açıkça izin vermenizi gerektirir. Bunu yapmak için **snyk'i yetkilendir** seçeneğine tıklayın.

Authorize Snyk

 **Snyk by Snyk**
wants to access your GeetikaP122 account

 **Repositories**
Public repositories

 **Organizations and teams**
Read-only access

 **Personal user data**
Email addresses (read-only)

[Cancel](#) [Authorize snyk](#)

Authorizing will redirect to
<https://app.snyk.io>

9. Sizi **Gösterge Tablosu**'na yönlendirir, burada **Projeleri Ekle** seçeneğine tıklayabilirsiniz. Seçenekleriniz şunlardır:

- GitHub
- CLI
- Kamu GitHub reposlarını izleme
- Diğer kaynaklar (BitBucket, Cloud, vb.)

The screenshot shows the Snyk dashboard for the organization 'GeetikaP122'. On the left sidebar, there are links for Projects, Integrations, Members, and Settings. The main area has a heading 'Start securing your code' with two sections: 'Connect your code' and 'Add and scan your first project'. Below these are four buttons: 'Add projects ^' (GitHub, CLI, Monitor public GitHub repos, Other), 'Collaborate on projects and build secure applications together', 'Use Snyk in the command line', and 'Learn how to install our command line tool to scan your code locally'. The 'GitHub' button is highlighted with a red box.

10. Tüm kamu reposlarınızın listelendiğini görmek için **GitHub'a** tıklayın. Kamu reposlarınızdan birini tarayabilirsiniz.

11. Reposlarını seçebilir ve seçilen reposları tarama için ekleyebilirsiniz.

This screenshot shows a modal window titled 'Which GitHub repositories do you want to test?'. It includes a search bar, a 'Cancel' button, and an 'Add selected repositories' button. The main area lists repositories under 'Personal and Organization repositories'. A repository named 'GeetikaP122' is expanded, showing a checkbox for 'containers' (which is checked) and another for 'Newfile1'. Below this is a 'Settings' section with fields for 'Add custom file location (optional)' and 'Exclude folders (Supported for Snyk Open Source and Snyk Container only, optional)'. A text input field contains '/path/to/file.ext' and a list of excluded folders includes 'fixtures, tests, __tests__, test, __test__, ci, node_mic'. The 'GitHub' icon in the top left of the modal is highlighted with a red box.

Repo boyutuna bağlı olarak, tarama biraz zaman alabilir.

12. Tekrar **Proje Ekle**'ye tıklayın ve **Kamu GitHub reposlarını izleme** seçeneğini seçin.

The screenshot shows the Snyk dashboard after scanning GitHub repositories. It features sections for 'Top pending tasks' (with a message: 'Good job! It looks like you've handled all of your tasks for today') and 'Top vulnerable projects'. The 'Top vulnerable projects' table lists five entries, each with a GitHub icon, a project name, a 'Tested' timestamp, and a 'Issues' section showing severity levels (0 Critical, 0 High, 3 Medium, 6 Low). At the bottom, there are buttons for 'View all projects' and 'Showing 1-5 of 12'. The 'GitHub' icon in the top left of the dashboard is highlighted with a red box.

13. Kamu bir URL'nin adresi yazın. Örneğin, aşağıdaki resim <https://github.com/bitnami/containers>'ı göstermektedir. **Repo ekle**'ye tıklayın ve ardından **1 reposu içe aktar**'a tıklayın.

The screenshot shows the Snyk web application. At the top, there's a purple header with the Snyk logo and a dog icon. Below it, the main title is "Monitor public GitHub repositories". A sub-instruction says "Choose the repository you'd like to check for vulnerabilities". There's a search bar with the URL "https://github.com/bitnami/containers" and a red-bordered button "+ Add repo". Below the search bar is a text input field containing "bitnami/containers" with a close button "x". A red-bordered button "Import 1 repository" is positioned below the input field. At the bottom of the form, a small note says "Not quite what you are looking for? Click here to go back."

14. Repo içe aktarılduktan sonra, güvenlik açıları için tarama başlar. Bu birkaç saniye alır, ardından depodaki kaç projenin tarandığını ve bunlarda kaç tane **Kritik**, **Yüksek**, **Orta** ve **Düşük** öncelikli güvenlik açığı bulunduğu gösteren bir rapor oluşturulur.

This screenshot shows the Snyk interface after importing two GitHub repositories: "bitnami/containers" and "GeetikaP122/containers". The left sidebar has a "Projects" section selected. The main area displays the imported targets with their respective security scores: 0 Critical (C), 0 High (H), 16 Medium (M), 18 Low (L). A message at the bottom says "Ready to import another project?" with a "Add projects" button.

Tebrikler! Snyk ile kod taramayı öğrendiniz.

Bu kod taramasını kendi depolarınızda veya pratik yapmak için diğer halka açık GitHub depolarında çalıştırmayı deneyebilirsiniz.

Yazar(lar)

Lavanya T S

