

Uygulamalı Laboratuvar: Dinamik Analiz Kullanımı



Gereklî tahmini süre: 30 dakika

Dinamik Analiz Kullanımı laboratuvarına hoş geldiniz! Bu laboratuvar, OWASP ZAP'ı projenizin kodunun dinamik analizi için nasıl kuracağınızı, yapılandıracağınızı ve kullanacağınızı öğreneceksiniz.

Bir geliştiriciye en önemli üç hedefinin ne olduğunu sordığınızda, muhtemelen şu yanıtları alacaksınız:

- Hatasız kod yazmak
- Tasarım spesifikasyonlarına uyumak
- Güvenlik sorunlarını önlemek

Bu hedeflere ulaşmak için geliştirme ekiblerinin genellikle kodlarını kapsamlı bir şekilde gözen geçirmesi ve test etmesi gereklidir. Kod analizi, bu çözümlerden biridir. Bu laboratuvar, dinamik kod analisinin güvenlik sorunlarını önemlendirmeyi ve ZAP'ın gelen güvenlik raporlarını yorumlamayı göstericektir.

Öğrenme Hedefleri

- OWASP ZAP'ı kurmak ve yapılandırmak
- Dinamik analiz aracını kullanmak
- ZAP'tan gelen güvenlik raporlarını yorumlamak

Dinamik Kod Analizi Neden?

Dinamik Kod Analizi Nedir?

Bir uygulamanın çalışma sırasında test edilmesi ve değerlendirilmesidir. Dinamik kod taraması olarak da adlandırılan dinamik analiz, yalnızca statik analizin ortaya çıkaramayacağı karmaşık güvenlik sorunlarını belirleyebilir.

Dinamik uygulama güvenlik testi (DAST), bir web uygulamasına karşı saldırıları simülle ederek ve uygulamanın güvenlik açılarını keşfetmek için uygulamanın yanıtlarını analiz ederek uygulamayı dışarıdan içeren incelemektedir.

OWASP ZAP Kullanarak Uygulama Güvenlik Açılarını Kontrol Etme

Bu laboratuvar çalışmasında, OWASP ZAP kullanarak dinamik analiz yapma konusunda pratik deneyim kazanacaksınız. Test edeceğinizin gerçek bir uygulama, güvenlik eğitimi amaçları için geliştirilmiş olan OWASP Juice Shop uygulamasıdır. Detaylı bir tanıtım, tam özellikler listesi ve mimari genel bakış için lütfen resmi proje sayfasını ziyaret edin: <https://owasp-juice.shop>.

OWASP ZAP'ı kurma ve Juice Shop uygulamasının analizini Docker ile Cloud IDE'de çalışma konusunda sizin yönlendireceğiz, böylece her şeyi sağ paneldeki bir terminalde gerçekleştirebileceksiniz. Docker yüklü herhangi bir ortamda, geliştirici çalışma istasyonunuz dahil, bu laboratuvari kolayca tekrarlayabileceksiniz.

Bir sonraki adımlarda ZAP sunucusunu çalıştırılmak için şunları yapacaksınız:

1. Tarayıcığınız uygulamayı edinin
2. Uygulama üzerinde ZAP'ı çalıştırın
3. Tarama sonuçlarını yorumlayın

Adım 1: Güvensiz Uygulamayı Al: Juice Shop

OWASP Juice Shop uygulamasını test etmek için uygulamayı alıp çalıştırmanız gereklidir. Üst menü çubuğunda Terminal -> Yeni Terminal seçeneğine tıklayarak bir terminal açın. Aşağıdaki komutları terminal penceresine kopyalayıp yapıştırarak Juice Shop'un docker imajını alabilir ve ardından uygulamayı mevcut Cloud IDE'de çalıştırılabilirsiniz.

```
docker pull bkminnich/juice-shop
docker run --rm -p 3000:3000 bkminnich/juice-shop
```

İki komutu çalıştırıldıkten sonra, laboratuvara devam etmeden önce terminalde "info: Server listening on port 3000" mesajını görene kadar bekleyin. Bu mesajı görmüyorsanız, bu laboratuvardan çıkmayı deneyin ve ardından yeniden başlatın.

```
info: Server listening on port 3000
```

Sonraki adımda, uygulamanın web arayüzüne bakacaksınız.

Adım 2: Juice Shop UI'yi Başlat

Sonraki adımda, aşağıdaki Web Uygulaması butonuna tıklayın. Butona tıkladıktan sonra uygulamanın çalışmaya başladığını göreceksiniz!

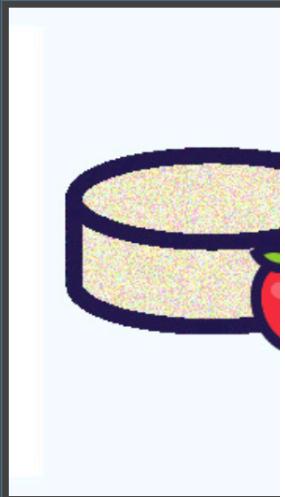
Kullanıcı arayüzü aşağıdaki görüntüye benzemelidir:



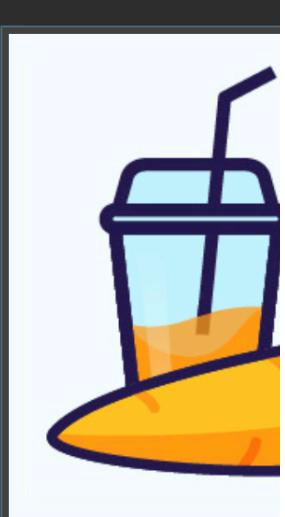
All Products

Apple Juice
(1000ml)

1.99¤

Best Juice Shop
Salesman
Artwork

5000¤



Adım 3: OWASP ZAP'ı Çalıştırın

Artık ZAP aracı bir Docker konteynerinde indirmek ve çalıştmak için hazırlısınız.

Göreviniz

1. Yeni bir terminal penceresi açmak için Terminal > Yeni Terminal seçeneğini kullanarak yeni docker komutları vermek için bir terminal açın.
2. Terminalde, OWASP ZAP'ın docker imajını indirmek için docker pull komutunu çalıştırın. (Not: Indirmek biraz zaman alabilir.)

```
docker pull softwaresecurityproject/zap-stable
```

Artık araç mevcut Cloud IDE'de kurulu olduğuna göre, Juice Shop uygulamasının bir güvenlik taramasına başlayabilirsiniz.

3. Sonra, Cloud IDE'deki çalışan uygulamanın adres çubuğuundan uygulamanın URL'sini panoa kopyalayın. Ardından aşağıdaki komutu çalıştırın ve {TARGET_URL} kısmını kopyaladığınız URL ile değiştirin.

```
docker run -t softwaresecurityproject/zap-stable zap-baseline.py -t {TARGET_URL}
```

Komutun Açıklaması

Bu komut, OWASP ZAP aracını bir Docker konteynerinde kullanarak belirtilen hedef URL üzerinde bir temel tarama başlatır. İşte komutun ayrıntılı açıklaması:

- docker run -t softwaresecurityproject/zap-stable: Bu komutu bu kısmı, Yazılım Güvenlik Projesi'nden zap-stable imajını kullanarak yeni bir Docker konteyneri çalıştırır.
- -t seçenekü, etkileşimli işlemler için yararlı olan bir sahte TTY ayırr.
- zap-baseline.py: Bu, OWASP ZAP tarafındaki sağlanan ve bir web uygulaması üzerinde temel bir tarama gerçekleştiren bir Python betiğidir. Temel tarama, uygulamanın güvenliğini değerlendirmek için yaygın güvenlik açıklarını kontrol ederek hızlı bir değerlendirme sağlamayı amaçlar.
- -t <TARGET_URL>: Bu seçenek, taramak istediğiniz hedef URL'yi belirtir. <TARGET_URL> kısmını test ettiğiniz web uygulamasının gerçek URL'si ile değiştirmeniz gereklidir (örneğin, Juice Shop uygulaması için <http://localhost:3000>).

ZAP şimdi sitenin tarama faaliyetlerine başlayacak ve bir site haritası oluşturacak, ilgili çıktılar terminalde gözden geçirilebilir. Bu işlemin gerçekleştirilmesi birkaç dakika sürecek.

Sonuçlar

Çıktı uzun olacaktır ve aşağıdaki gibi görünecektir:

```
Using the Automation Framework
Total of 13 URLs
PASS: Vulnerable JS Library (Powered by Retire.js) [10003]
PASS: In Page Banner Information Leak [10009]
PASS: Cookie No HttpOnly Flag [10010]
PASS: Cookie Without Secure Flag [10011]
PASS: Content-Type Header Missing [10019]
PASS: Information Disclosure - Debug Error Messages [10023]
PASS: Information Disclosure - Sensitive Information in URL [10024]
PASS: Information Disclosure - Sensitive Information in HTTP Referrer Header [10025]
PASS: HTTP Parameter Override [10026]
PASS: Open Redirect [10028]
PASS: Cookie Poisoning [10029]
PASS: User Controllable Charset [10030]
PASS: User Controllable HTML Element Attribute (Potential XSS) [10031]
PASS: ViewState [10032]
PASS: Directory Browsing [10033]
PASS: Heartbleed OpenSSL Vulnerability (Indicative) [10034]
PASS: HTTP Server Response Header [10036]
PASS: X-Backend-Server Header Information Leak [10039]
PASS: Secure Pages Include Mixed Content [10040]
PASS: HTTP to HTTPS Insecure Transition in Form Post [10041]
PASS: HTTPS to HTTP Insecure Transition in Form Post [10042]
PASS: User Controllable JavaScript Event (XSS) [10043]
PASS: Big Redirect Detected (Potential Sensitive Information Leak) [10044]
PASS: Retrieved from Cache [10050]
PASS: X-Chromelogger-Data (XOLD) Header Information Leak [10052]
PASS: Cookies without SameSite Attribute [10054]
PASS: CSP [10055]
PASS: X-Debug-Token Information Leak [10056]
PASS: Username Hash Found [10057]
PASS: X-AspNet-Version Response Header [10061]
PASS: PII Disclosure [10062]
PASS: Hash Disclosure [10097]
PASS: Source Code Disclosure [10099]
PASS: Weak Authentication Method [10105]
PASS: Reverse Tabnabbing [10108]
PASS: Authentication Request Identified [10111]
PASS: Verification Request Identified [10113]
PASS: Absence of Anti-CSRF Tokens [10202]
PASS: Private IP Disclosure [2]
PASS: Session ID in URL Rewrite [3]
PASS: Stats Passive Scan Rule [50003]
PASS: Insecure JSF ViewState [90001]
PASS: Java Serialization Object [9002]
PASS: Sub Resource Integrity Attribute Missing [90003]
PASS: Insufficient Site Isolation Against Spectre Vulnerability [90004]
PASS: Charset Mismatch [90011]
PASS: Application Error Disclosure [9002]
PASS: WSDL File Detection [90038]
WARN-NEW: Re-examine Cache-control Directives [10015] x 3
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/ (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/robots.txt (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/sitemap.xml (200 OK)
WARN-NEW: Cross-Domain JavaScript Source File Inclusion [10017] x 4
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/ (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/ (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/sitemap.xml (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/sitemap.xml (200 OK)
WARN-NEW: Missing Anti-Clickjacking Header [10020] x 2
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/ (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/sitemap.xml (200 OK)
WARN-NEW: X-Content-Type-Options Header Missing [10021] x 9
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/ (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/assets/public/favicon_js.ico (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/main.js (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/polyfills.js (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/robots.txt (200 OK)
WARN-NEW: Information Disclosure - Suspicious Comments [10027] x 2
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/main.js (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/vendor.js (200 OK)
WARN-NEW: Strict-Transport-Security Header Not Set [10035] x 1
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/ftp (400 Bad Request)
WARN-NEW: Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) [10037] x 9
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/ (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/assets/public/favicon_js.ico (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/main.js (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/polyfills.js (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/robots.txt (200 OK)
WARN-NEW: Content Security Policy (CSP) Header Not Set [10038] x 2
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/ (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/sitemap.xml (200 OK)
WARN-NEW: Non-Storable Content [10049] x 10
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/ftp (400 Bad Request)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/robots.txt (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/ (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/assets/public/favicon_js.ico (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/main.js (200 OK)
WARN-NEW: Deprecated Feature Policy Header Set [10063] x 6
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/ (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/main.js (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/polyfills.js (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/runtime.js (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/sitemap.xml (200 OK)
WARN-NEW: Timestamp Disclosure - Unix [10096] x 1
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/main.js (200 OK)
WARN-NEW: Cross-Domain Misconfiguration [10098] x 9
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/ (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/assets/public/favicon_js.ico (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/main.js (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/polyfills.js (200 OK)
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/robots.txt (200 OK)
WARN-NEW: Modern Web Application [10109] x 2
  https://manvigi1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/ (200 OK)
```

```
https://manvig1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/sitemap.xml (200 OK)
WARN-NEW: Dangerous JS Functions [10110] x 2
https://manvig1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/main.js (200 OK)
https://manvig1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/vendor.js (200 OK)
WARN-NEW: Session Management Response Identified [10112] x 6
https://manvig1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/ (200 OK)
https://manvig1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/ (200 OK)
https://manvig1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/robots.txt (200 OK)
https://manvig1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/sitemap.xml (200 OK)
https://manvig1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/main.js (200 OK)
WARN-NEW: Loosely Scoped Cookie [90033] x 4
https://manvig1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/ (200 OK)
https://manvig1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/ (200 OK)
https://manvig1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/robots.txt (200 OK)
https://manvig1-3000.theiadockernext-1-labs-prod-theiak8s-4-tor01.proxy.cognitiveclass.ai/sitemap.xml (200 OK)
FAIL-NEW: 0 FAIL-INPROG: 0 WARN-NEW: 16 WARN-INPROG: 0 INFO: 0 IGNORE: 0 PASS: 48
```

Adım 4: Tarama Sonuçlarını Yorumlama

Tarama sonuçlarına bakalım.

Test edilen birçok öğe PASS: ile geri döndü, bu yüzden onlara bakmayaçagınız.

Dikkatimizi uyarılaraya veya hatalara odaklayacağınız. Aşağıda geri dönen on uyarının bir özeti bulunmaktadır. Her biri zayıfeti tanımlamakta, ardından bulunduğu sayıda örneği belirtmektedir (örneğin, x 3), ve ardından zayıfeten bulunduğu URL'leri listelemektedir. Aşağıdaki özet liste oluşturmak için URL'leri kaldırıdık:

```
WARN-NEW: Re-examine Cache-control Directives [10015] x 3
WARN-NEW: Cross-Domain JavaScript Source File Inclusion [10017] x 4
WARN-NEW: Missing Anti-clickjacking Header [10020] x 2
WARN-NEW: X-Content-Type-Options Header Missing [10021] x 9
WARN-NEW: Information Disclosure - Suspicious Comments [10027] x 2
WARN-NEW: Strict-Transport-Security Header Not Set [10035] x 1
WARN-NEW: Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) [10037] x 9
WARN-NEW: Content Security Policy (CSP) Header Not Set [10038] x 2
WARN-NEW: Non-Storable Content [10040] x 10
WARN-NEW: Deprecated Feature Policy Header Set [10063] x 6
WARN-NEW: Timestamp Disclosure - Unix [10066] x 2
WARN-NEW: Cross-Domain Misconfiguration [10068] x 9
WARN-NEW: Modern Web Application [10109] x 2
WARN-NEW: Dangerous JS Functions [10110] x 2
WARN-NEW: Session Management Response Identified [10112] x 6
WARN-NEW: Loosely Scoped Cookie [90033] x 4
FAIL-NEW: 0 FAIL-INPROG: 0 WARN-NEW: 16 WARN-INPROG: 0 INFO: 0 IGNORE: 0 PASS: 48
```

Gördüğünüz gibi, bu uygulama Çapraz Alan JavaScript Kaynak Dosyası Dahil Etme, Eksik Anti-tıklama Korumalı Başlık, X-Content-Type-Options Başlığı Eksik, İçerik Güvenlik Politikası (CSP) Başlığı Ayarlanmamış, Çapraz Alan Yanlış Yapılandırması ve Gevşek Kapsamlı Çerezler gibi birkaç alanda güvenlik açıklarına sahiptir.

Güvenlik açığı adalarının yanındaki numaraları kullanarak ZAP Proxy Web sitesinde uyarı hakkında bilgi alabilirsiniz. Aşağıdaki URL'yi kullanarak:

<https://www.zaproxy.org/docs/alerts/{NUMBER}>

{NUMBER} ile uyarı numarasını değiştirdiğinizden emin olun.

Örneğin, yukarıdaki uyarı mesajında Cross-Domain JavaScript Source File Inclusion 10017 numarası ile belirtilmiştir, bu nedenle URL şu olacaktır (*üzerine tıklayın ve görün*):

<https://www.zaproxy.org/docs/alerts/10017>

Bir geliştirici olarak, göreviniz zayıfeti araştırmak, zayıf olarak belirtilen her URL'yi incelemek ve ardından koddaki zayıflıkları tek tek düzeltmektr.

Gelistirme yaşam doğallığınızın erken aşamalarında Dinamik Güvenlik Testi (DAST) aracı çalıştırırsanız, listeniz muhtemelen bu örnekteki kadar büyük olmayacağındır. Eğer DAST geliştirme sürecinin daha erken bir aşamasında yapılmış olsaydı, X-Content-Type-Options Header Missing veya Cross-Domain Misconfiguration ile ilgili dokuz ihlal olmayıabilirdi.

Sonuç

Tebrikler! Dinamik analiz üzerinde bu laboratuvarı tamamladınız; bu, güvenli uygulama geliştirmede kritik bir adımdır. Artık dinamik analiz güvenlik taramaları yaparak uygulamalarınızı daha güvenli hale getirmek için doğru yolda ilerliyorsunuz.

Dinamik analizin faydalalarını ve bir projedeki zayıflıkları tespit etmek için ne zaman kullanılacağını anladınız. Ayrıca en popüler açık kaynak dinamik analiz aracı olan OWASP ZAP ile nasıl başlayacağınızı da biliyorsunuz.

Sonraki Adımlar

Farklı zayıflıkları tespit etmek, güvenli uygulama geliştirmede atılacak ilk adımlardan sadece biridir. Düzeltici önlemler almak için bu zayıflıkların arkasındaki anlamı da anlamalısınız. Öğrenmenin en iyi yolu uygulamaktır.

Bir sonraki meydan okumanız, geliştirme ortamınızda OWASP ZAP kullanarak kodunuza güvenlik taramaları yapmak ve ardından bulduğu sorunları düzeltmektir. Daha güvenli kod yazma yolunda ilerliyorsunuz.

Author(s)

[Roxanne Li](#)
[John J. Rofrano](#)

Other Contributor(s)

© IBM Corporation. Tüm hakları saklıdır.