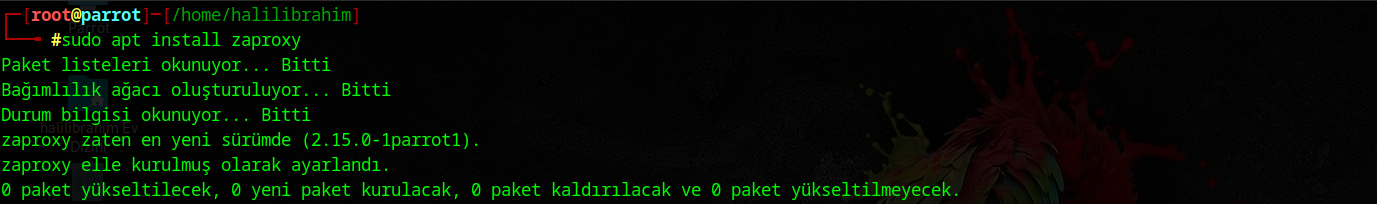
### OWASP ZAP Nedir, Nasıl Kullanılır?

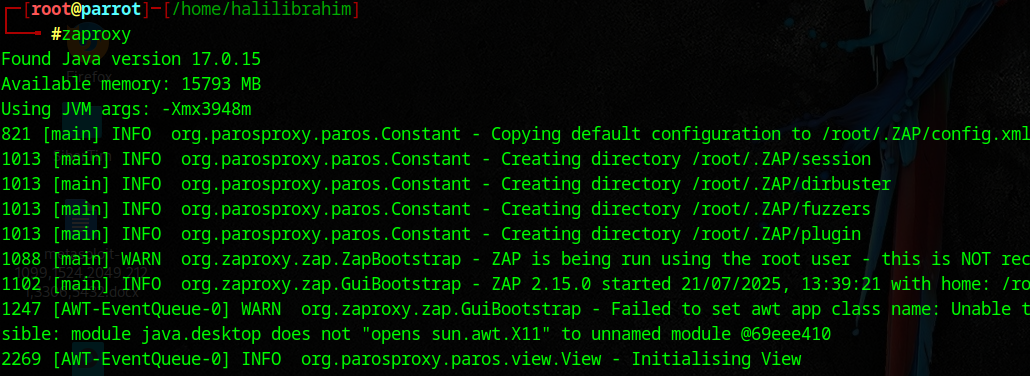
OWASP ZAP (Zed Attack Proxy), OWASP tarafından geliştirilen, açık kaynaklı ve ücretsiz bir **web uygulaması güvenlik test aracıdır**. Hem manuel hem de otomatik sızma testleri için kullanılır. ZAP, özellikle SQL Injection, XSS, CSRF, açık dizinler ve eksik güvenlik başlıkları gibi OWASP Top 10 zafiyetlerini tespit etmek amacıyla kullanılır. Proxy tabanlı çalıştığı için, tarayıcı trafiğini kendi üzerinden geçirerek uygulama ile istemci arasındaki HTTP/HTTPS isteklerini analiz edebilir, müdahale edebilir veya yeniden gönderebilir.

**ZAP kurulumu:**

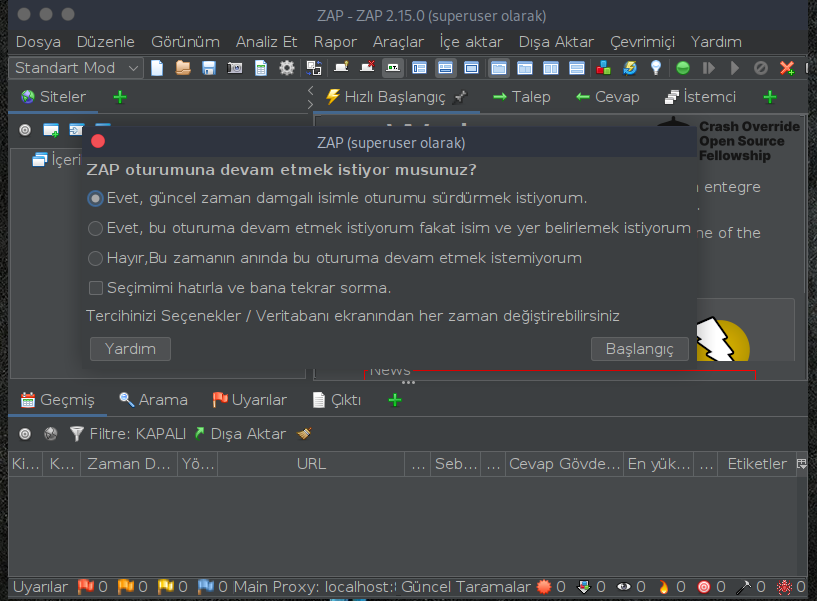
Parrot OS ve Kali Linux, siber güvenlik testleri için önceden yapılandırılmış Debian tabanlı dağıtımlardır. Bu sistemlerde OWASP ZAP çoğu zaman **önceden kurulu** gelir. Eğer sisteminizde yüklü değilse ya da **en güncel sürümü** kurmak istiyorsanız, aşağıdaki yöntemlerden biriyle kurulum gerçekleştirebilirsiniz.



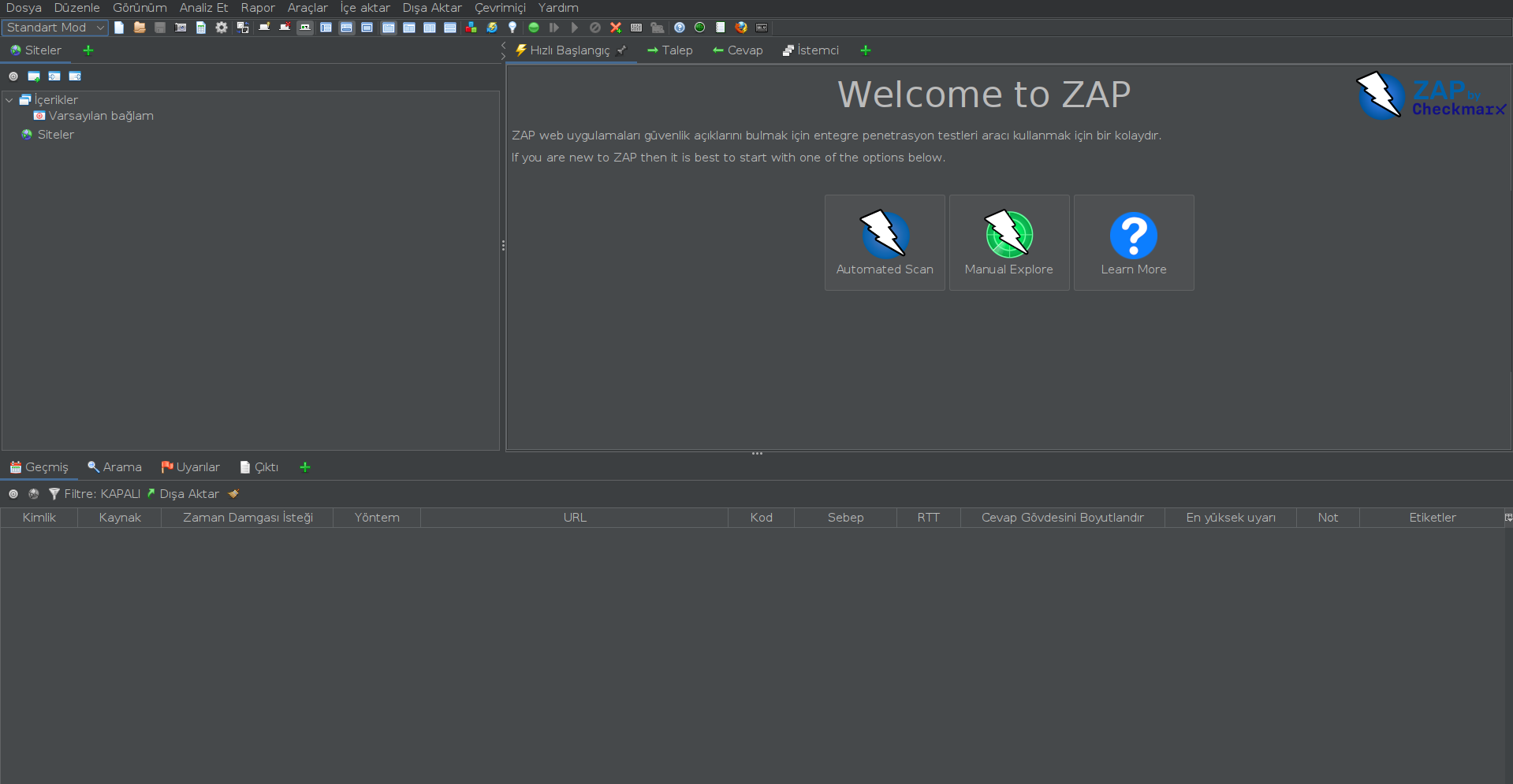
Ardından zaproxy diyerek başlatabilirsiniz.



**"Evet, güncel zaman damgalı isimle oturumu sürdürmek istiyorum." seçeneğini seçip devam ediyoruz.**



**Uygulamayı açmış olduk.**



Otomatik ve Manuel olmak üzere iki tür tarama vardır:

### Otomatik Tarama (Automated Scan)

* ZAP’in "Quick Start" bölümünden başlatılır.
* Hedef URL girildikten sonra ZAP, siteyi otomatik olarak tarar: önce bağlantıları keşfeder (spider), ardından aktif tarama ile güvenlik açıklarını test eder.
* SQL Injection, XSS gibi yaygın zafiyetleri otomatik olarak denetler.
* Kullanımı hızlı ve pratiktir, ancak her zafiyeti tespit edemez.

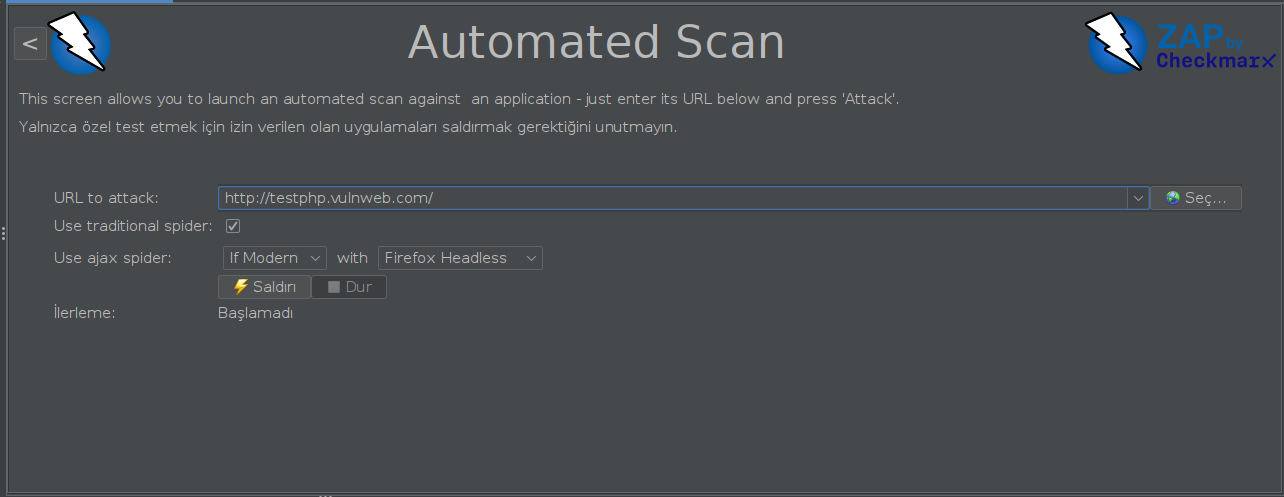
**Kullanım amacı:** Hızlı genel tarama veya ilk keşif aşamasında tercih edilir.

### Manuel Tarama (Manual Exploration)

* ZAP proxy olarak yapılandırılır ve kullanıcı siteyi tarayıcı üzerinden kendisi gezerek veri üretir.
* Tüm istek ve yanıtlar ZAP tarafından kaydedilir.
* Kullanıcı bu veriler üzerinden elle analiz yapabilir; örneğin parametre değiştirerek zafiyet testleri yapabilir, Fuzzer uygulayabilir veya özel payload’lar deneyebilir.
* Girişli alanlar, oturum kontrollü sayfalar ve özel mantık barındıran bölümler bu yöntemle test edilebilir.

**Kullanım amacı:** Detaylı analiz, özel senaryolar ve gelişmiş testler için gereklidir.

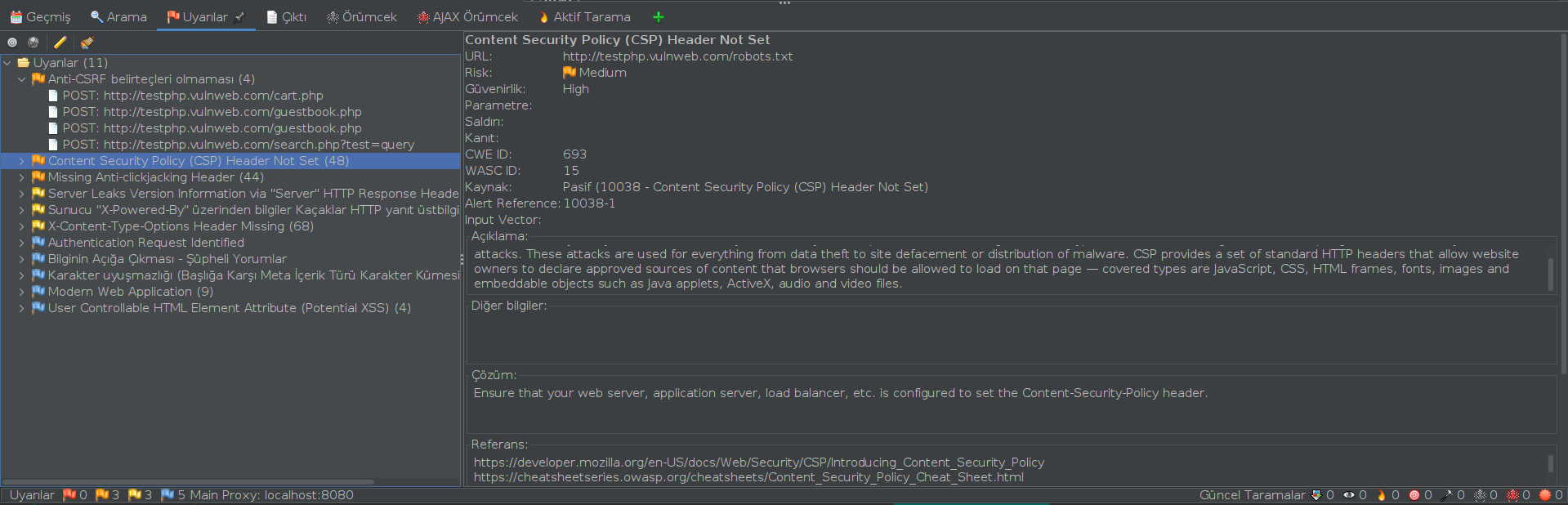
Şimdi bir otomatik scan örneği ile nasıl çalıştığına bakalım. “Automated Scan” diyip tarama ekranına gidiyoruz. Ardından hedep adresi yazıp “Saldırı” butonuna tıklıyoruz.



OWASP ZAP taraması sonucunda elde edilen zafiyetler, önem derecelerine göre **renkli bayraklarla** sınıflandırılır. Bu renkler, güvenlik açığının potansiyel etkisini hızlıca anlamak için kullanılır:

* **Kırmızı Bayrak (High)**: Kritik güvenlik açıklarıdır. Sisteme yetkisiz erişim, veri sızıntısı veya uzaktan kod çalıştırma gibi ciddi tehditler içerir. Derhal müdahale edilmelidir.
* **Turuncu Bayrak (Medium)**: Orta seviye risk taşıyan açıklardır. Genellikle bilgi sızması, güvenlik başlıklarının eksikliği veya zayıf konfigürasyon gibi durumları temsil eder.
* **Sarı Bayrak (Low)**: Düşük riskli veya yapılandırma kaynaklı potansiyel açıklardır. Güvenlik açısından iyileştirme önerisi niteliğindedir.
* **Mavi Bayrak (Informational)**: Teknik bilgiler içerir ancak doğrudan güvenlik açığı oluşturmaz. Sistem hakkında genel bilgi sağlar (örneğin sunucu tipi, yazılım versiyonu).

ZAP arayüzünün alt kısmında bu bayraklardan toplam kaç adet bulunduğu gösterilir. Örneğin "3 turuncu, 3 sarı, 5 mavi" ibaresi; orta seviye 3, düşük seviye 3 ve bilgilendirme amaçlı 5 uyarı olduğunu belirtir. Bu sayede güvenlik test raporlaması sırasında zafiyetlerin önceliklendirilmesi daha sağlıklı yapılabilir.



ZAP ile gerçekleştirdiğiniz taramalarda, “Uyarılar” sekmesi altında listelenen herhangi bir güvenlik uyarısına tıkladığınızda, o uyarıya ait **detaylı açıklama paneli** sağ tarafta görüntülenir. Bu panelde ilgili zafiyetin:

* **URL** (hangi sayfada tespit edildiği),
* **Risk seviyesi** (düşük, orta, yüksek),
* **Güvenilirlik derecesi**,
* **CWE/WASC referansları**,
* **Açıklama** (zafiyetin ne olduğu ve nasıl sömürülebileceği),
* **Çözüm önerisi** (nasıl giderileceği),
* **Referans bağlantılar** (daha fazla teknik bilgi için)

gibi bilgiler yer alır. Bu alan, hem teknik analiz hem de raporlama sürecinde kritik öneme sahiptir. Özellikle birden fazla uyarı bulunduğunda, her birini ayrı ayrı inceleyerek zafiyetlerin ciddiyetini ve nasıl düzeltileceğini değerlendirmek mümkündür.

Otomatik ve manuel taramaların yanı sıra, OWASP ZAP ile çok sayıda güvenlik test aracı da kullanılabilir. Öncelikle ZAP, hedef web uygulamasının tüm sayfalarını keşfetmek için **Spider** ve **AJAX Spider** özellikleri sunar. Bu sayede JavaScript tabanlı içerikler dâhil, tüm bağlantılar analiz edilebilir. Ayrıca tarayıcı trafiğini ZAP üzerinden geçirerek HTTP istek ve yanıtlarını gözlemleme ve müdahale etme imkânı sağlayan **proxy modu**, özellikle manuel güvenlik testleri için kritik öneme sahiptir.

ZAP, parametrelerin, URL’lerin ve form alanlarının farklı girdilerle test edilebildiği **Fuzzer** aracıyla da gelişmiş testler yapılmasına olanak tanır. Giriş sayfalarının tanımlanarak oturum yönetiminin izlenmesi ve zafiyetlerinin tespiti de mümkündür. Ek olarak, HTTP başlıklarını analiz ederek **güvenlik yapılandırması eksikliklerini** (örneğin Content Security Policy veya X-Frame-Options gibi) raporlayabilir.

ZAP, elde edilen bulguları **HTML, XML veya Markdown formatlarında dışa aktarılabilir raporlar** halinde sunar. Ayrıca desteklediği eklentiler ve API üzerinden otomasyon kabiliyeti sayesinde CI/CD süreçlerine de entegre edilebilir. Yani ZAP, yalnızca tarama aracı değil; aynı zamanda kapsamlı ve esnek bir güvenlik test platformudur.