**Acunetix**

**Acunetix Nedir?**

Acunetix, **web uygulamalarındaki güvenlik açıklarını otomatik olarak tarayan** profesyonel bir **Web Vulnerability Scanner (WVS)** yazılımıdır. Siber güvenlik uzmanları, sistem yöneticileri ve yazılım geliştiriciler tarafından **web güvenliğini test etmek** amacıyla kullanılır.  
2005 yılında geliştirilmiş olup günümüzde hem **Windows**, **Linux** hem de **bulut tabanlı** sürümleri mevcuttur. Acunetix, özellikle **OWASP Top 10** listesinde yer alan yaygın açıkları (SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Komut Enjeksiyonu vb.) hızlı ve güvenilir bir şekilde tespit edebilmesiyle bilinir.

Acunetix, hedef web sitesinin tüm yapısını (sayfalar, API’ler, formlar, linkler) tarayarak zafiyetleri bulur, her açık için **teknik ayrıntılar** ve **çözüm önerileri** sunar. Ayrıca:

* Oturum açma gerektiren sayfalarda **kimlik doğrulaması** yapabilir.
* JavaScript tabanlı modern web sitelerini tarayabilir.
* API güvenlik testi yapabilir.
* Otomatik ve özelleştirilebilir raporlar oluşturabilir.

Penetrasyon testi sürecinde hem **keşif (reconnaissance)** hem de **zafiyet analizi** aşamalarında kullanılabilir ve web uygulamalarının saldırılara karşı ne kadar savunmasız olduğunu anlamayı sağlar.

**Özellikleri**

* **Otomatik Zafiyet Taraması:** Hedef web uygulamasında binlerce bilinen güvenlik açığını tespit eder.
* **Geniş Zafiyet Kapsamı:** SQL Injection, XSS, CSRF, SSRF, Güvenli Olmayan HTTP Ayarları, Komut Enjeksiyonu vb.
* **Kimlik Doğrulama Desteği:** Giriş gerektiren alanları da tarayabilir.
* **JavaScript Destekli Tarama:** SPA (Single Page Application) ve AJAX tabanlı web siteleri tarayabilir.
* **Detaylı Raporlama:** Teknik ekipler ve yöneticiler için farklı rapor formatları.
* **API Testi:** REST ve SOAP API güvenlik testleri yapabilir.
* **Çoklu Platform Desteği:** Windows, Linux, bulut tabanlı sürümler.

**Kullanım Alanları**

* Web uygulama güvenlik testi
* Penetrasyon testi
* Yazılım geliştirme sürecinde güvenlik doğrulaması
* Güvenlik açıklarının hızlı tespiti ve raporlanması
* Kurumsal web sitelerinin periyodik güvenlik kontrolü

**Kurulum Aşamaları:**

**Windows’ta Kurulum:**

1. Acunetix Resmi Sitesi üzerinden yükleyiciyi indir.
2. Kurulum sihirbazını başlat ve yönergeleri takip et.
3. Lisans anahtarını gir veya deneme sürümünü seç.
4. Tarama için hedef web sitesinin URL’sini gir.
5. Tarama tamamlandığında raporu görüntüle.

**Linux’ta (Debian/Kali) Kurulum: **

**Temel Kullanım Adımları**

1. Hedef web sitesi adresini gir.
2. Tarama profilini seç (tam tarama, hızlı tarama, özel tarama).
3. Tarama başlat.
4. Çıkan raporda kritik, orta ve düşük seviyedeki açıkları incele.
5. Öncelikli olarak kritik açıkları kapat.

**Dikkat Edilmesi Gerekenler**

* **İzinsiz tarama yapmak yasa dışıdır.** Sadece yetki verilen sitelerde kullanılmalıdır.
* Büyük sitelerde tarama süresi uzun olabilir ve sunucuya yük bindirebilir.
* Yanlış yapılandırılmış taramalar site performansını etkileyebilir.
* Tarama öncesi hedef sistemin yedeğinin alınması tavsiye edilir.