

RAPPLEX

**Web
Uygulamanızı
Hackerlardan
Önce
Tarayın!**



Rapplex



@RapplexOfficial



@rapplex



rapplex.com



rapplexdast



www.netcom.com.tr

Powered By

NETCOM
1986

RAPPLEX

Rapplex web uygulama güvenlik tarayıcısı, web sitelerinde zafiyet taraması yapan ve raporlayan bir yazılımdır.

Otomatize bir araç olarak kullanılabildiği gibi, manual testler yapmak isteyen pentesterlar için de hazır araçlar sunmaktadır.

Bu sayede yazılımın farklı zafiyet türlerini keşfetmesinde veya var olan tarama motorlarının geliştirilmesinde, ayrı geliştirme araçlarına ihtiyacı bulunmamaktadır.

SQL Injection, Code Injection, File Inclusion gibi zafiyetlerden faydalanmak üzere exploit (sömürü) araçları mevcuttur.

Rapplex, web uygulamalarında herkes için tehdit olabilecek zafiyetlerin, kimseye zarar vermeden tespit edilmesi noktasında hızlı, esnek, genişletilebilir bir çözüm sunmaktadır. En az çaba ile en fazla verimin alınması mantığı ile geliştirilen Rapplex, yenilenebilir ve daima çözümleyici olma misyonlarıyla hareket ederek her daim geliştirilebilir olma konusundaki kararlılığını vurgulamaktadır.

ARKANIZA YASLANIN

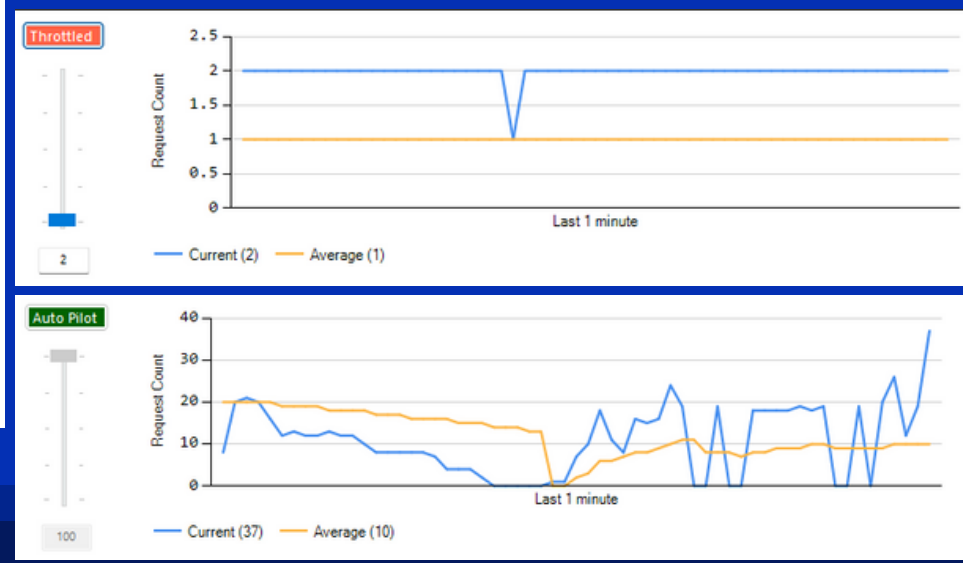
Rapplex, hedef sistemde çalışan teknolojiler hakkında sizden ön bilgi talep etmez.

ZAFİYETLER	KESİNLİK	SÖMÜRÜ ARACI	KANIT
SQL Injection	100%	☒	☒
File Upload	100%	☒	☒
Code Injection	100%	☒	☒
Command Injection	100%	☒	☒
LFI & RFI	100%	☒	☒
SSTI	100%	☒	☒
XXE	100%	☒	☒

Güçlü ve gelişmiş pasif analiz yetenekleriyle, hedef sistemi analiz eder.

Analiz sonucunda elde ettiği bulgulara dayanarak yapacağı atak vektörlerini optimize eder.

RAPPLEX AUTOPILOT İLE GÜVENLİ TARAMA



Taramanın yapılacağı hedef sistem konfigürasyonu, Rapplex tarafından yapılan çok sayıda isteğe cevap verebilecek şekilde tasarlanmamış olabilir.

Tam da bu noktada, hedeften dönen cevap sürelerinin arttığını analiz eden Rapplex Autopilot, saniyede yapılan HTTP isteklerini optimum düzeye getirir.

Bunun yanında, tarama sırasında "Auto Pilot" devre dışı bırakıldığında, "Throttler" devreye girer ve saniye başına düşen HTTP isteği sayısı dinamik olarak seçilen değere ayarlanır.

TAM ENTE GRE

Rapplex, Azure DevOps, GitHub, Jira, Slack, Asana, Trello, Gitlab, Jenkins, Redmine, Mail, Telegram, Discord gibi global platformlarla tam entegredir.



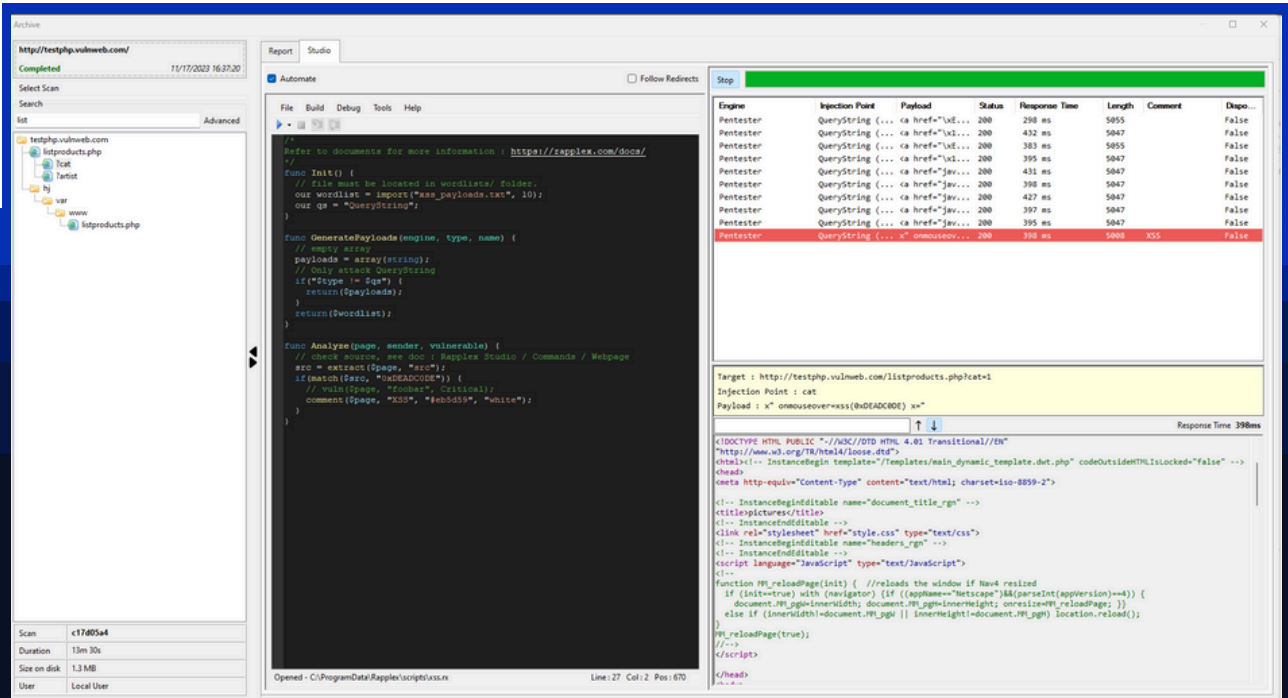
Böylelikle Rapplex, SDLC(Yazılım Geliştirme Yaşam Döngüsü) ve DevSecOps süreçlerine dahil edilerek, geliştirilen yazılım canlı sistemlerde yayınlanmaya başlamadan önce zafiyetin önüne geçilmesini sağlar.



RAPPLEX

PENTESTER STUDIO

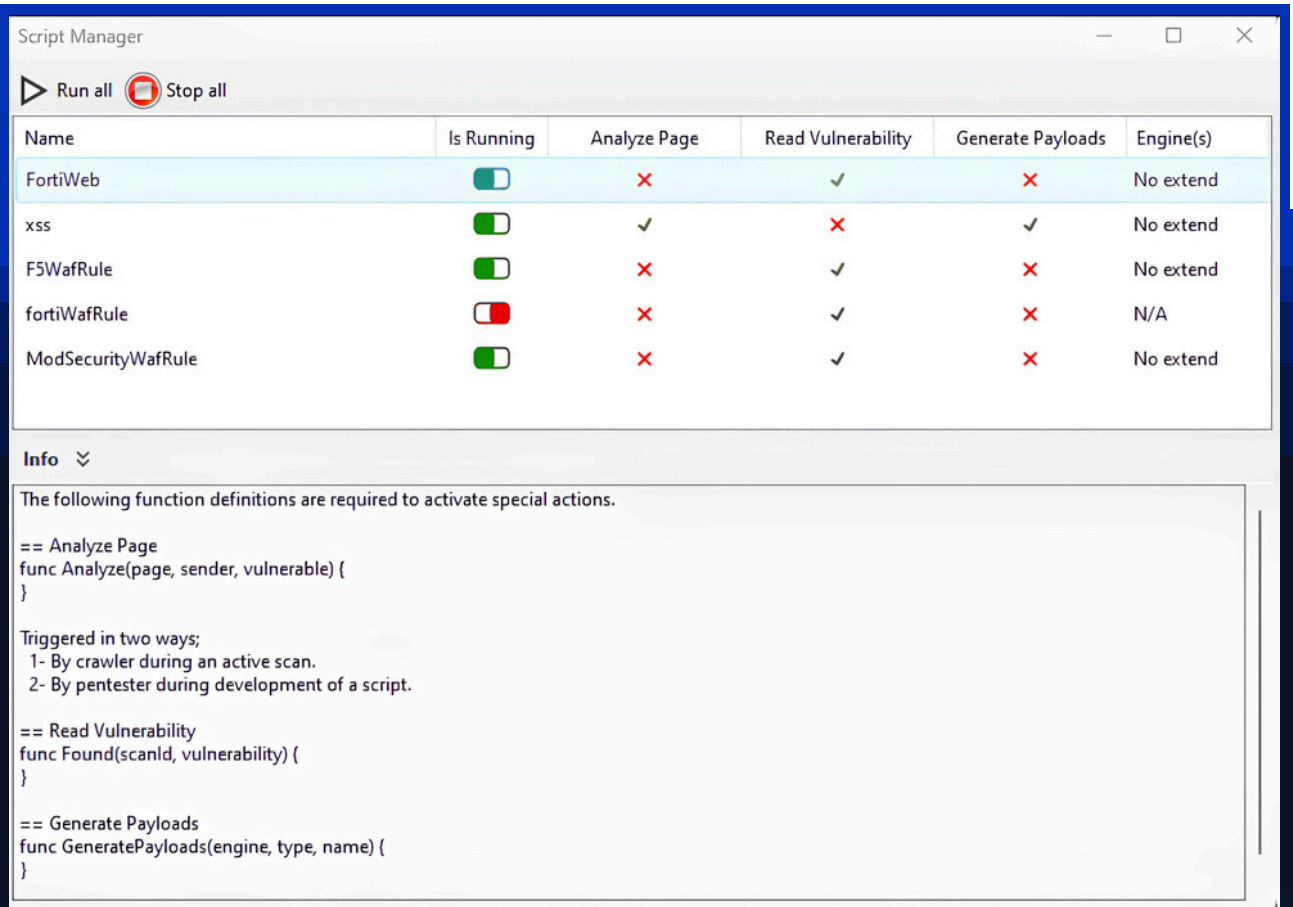
Rapplex, kendi bilgi birikimlerine ve tecrübelerine dayanarak analizler yapan sızma testleri uzmanları için de etkili çözümler sunar.



Pentester studio sızma testi uzmanlarının payload ve analiz fonksiyonları, brute force ve fuzz scriptleri yazabileceği bir geliştirme ortamı sunar. Geliştirilen analiz fonksiyonları kullanılarak zafiyetin tespit edildiğine dair belirteçler eklenebilir ya da rapora eklemeler yapılabilir.

SCRIPT MANAGER

Rapplex, Pentester Studio sayesinde script geliştirme imkanı tanır. Buna ek olarak geliştirilen scriptlerin tek ekrandan yönetilmesine olanak sağlayan Script Manager'a sahiptir.



Name	Is Running	Analyze Page	Read Vulnerability	Generate Payloads	Engine(s)
FortiWeb		✗	✓	✗	No extend
xss		✓	✗	✓	No extend
F5WafRule		✗	✓	✗	No extend
fortiWafRule		✗	✓	✗	N/A
ModSecurityWafRule		✗	✓	✗	No extend

Info ⌵

The following function definitions are required to activate special actions.

```
== Analyze Page
func Analyze(page, sender, vulnerable) {
}

Triggered in two ways;
1- By crawler during an active scan.
2- By pentester during development of a script.

== Read Vulnerability
func Found(scanId, vulnerability) {
}

== Generate Payloads
func GeneratePayloads(engine, type, name) {
}
```

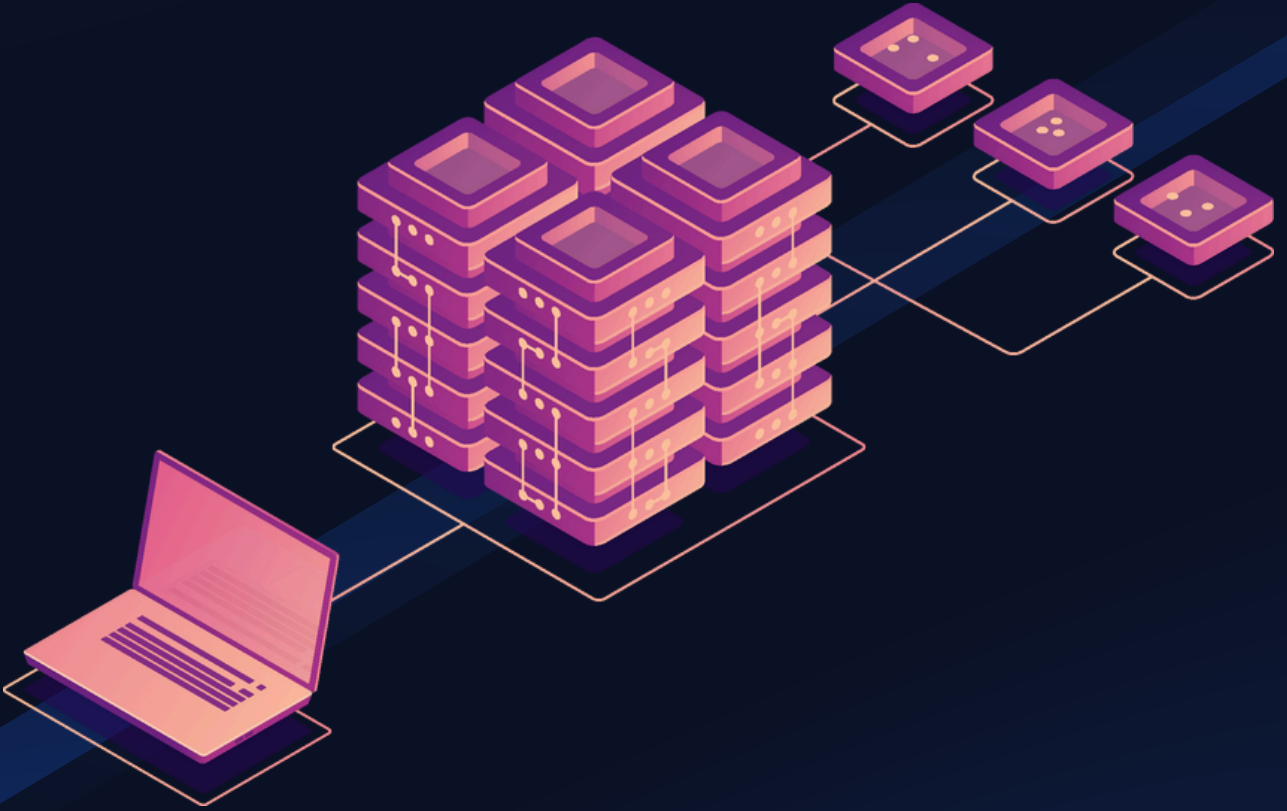
Scriptlerin tamamı tek seferde durdurulabilir ya da yeniden çalıştırılabilir.

Bunun yanında, aktif olan script her çalıştığında ilgili fonksiyonun sembolü kullanıcıya geri bildirim verir.

DENGELİ VE GÜÇLÜ

Rapplex, güçlü altyapısı sayesinde Load Balancing mantığına uygun hareket edebilir, atakları sadece kurulu olduğu server üzerinden yapmaz.

Dağıtık mimariye uygun biçimde, yapılan HTTP isteklerini dengeler. Daha dengeli ve daha güçlü bir tarama ortamı sunar.



WEB API



Rapplex, API desteęi sayesinde dięer programların kendisine entegre olabileceęi programlanabilir bir erişim sağlar.

Kurum içi geliştirilen yazılımlar, Rapplex'e kolaylıkla entegre olabilir.

ROL TABANLI ERİŞİM KONTROLÜ

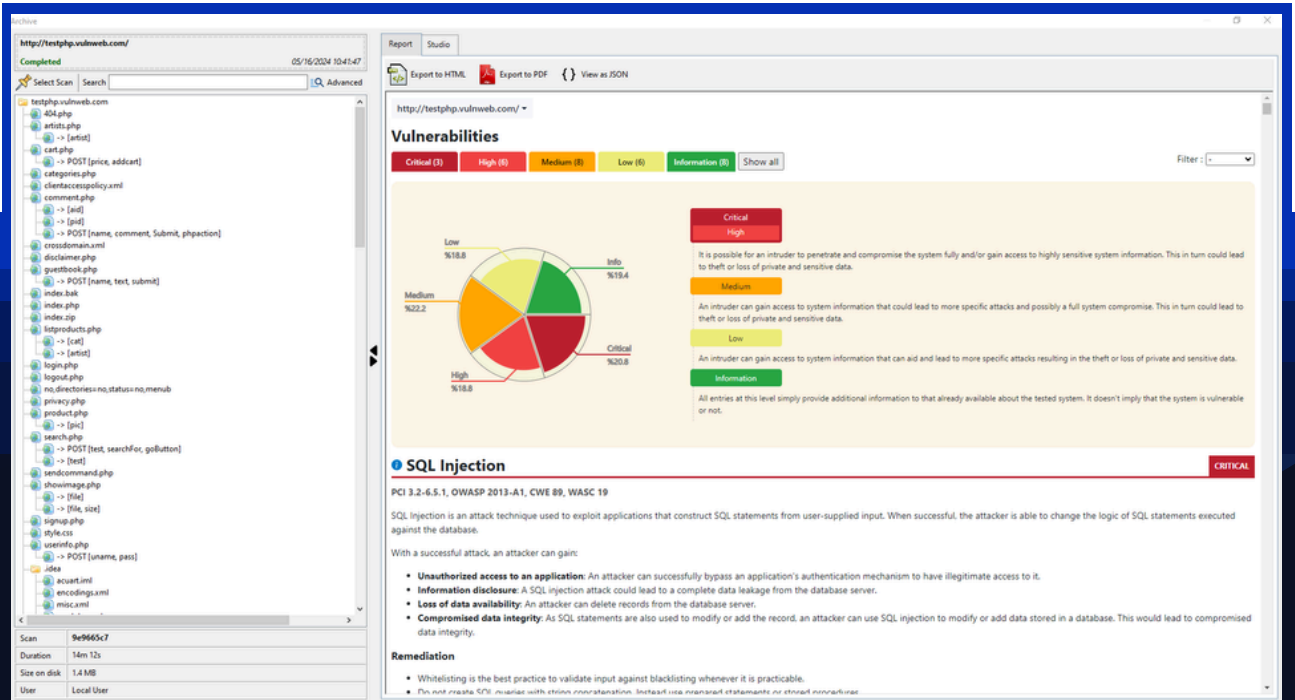


Yüzlerce ya da binlerce kullanıcının olduęu bir ortamda, Rapplex ile yapılan taramaların güvenlięi rol tabanlı erişim kontrolü ile sağlanır.

"Görmesi gereken görür" mantıęı ile hareket edilen bu yapı, aynı zamanda kullanıcıların yetki düzeyini, kişisel bilgilerini, parola bilgilerini tek ekrandan yönetilmesine imkan tanır.

ARŞİV

Belirli bir tarihte yapılan taramaların raporlarına erişim sağlanmasına imkan tanır.



Gelişmiş site haritası sayesinde, crawl edilen sayfalar özelinde hangi zafiyetin bulunduğu da incelenebilir. Detaylı arama yeteneği sayesinde sayfa adı, dosya adı, dosya uzantısı gibi filtrelerle büyük ölçekli hedeflerde tarama sonrası analiz çok daha kolaylıkla yapılabilir.

ZAMANLANMIŞ TARAMA

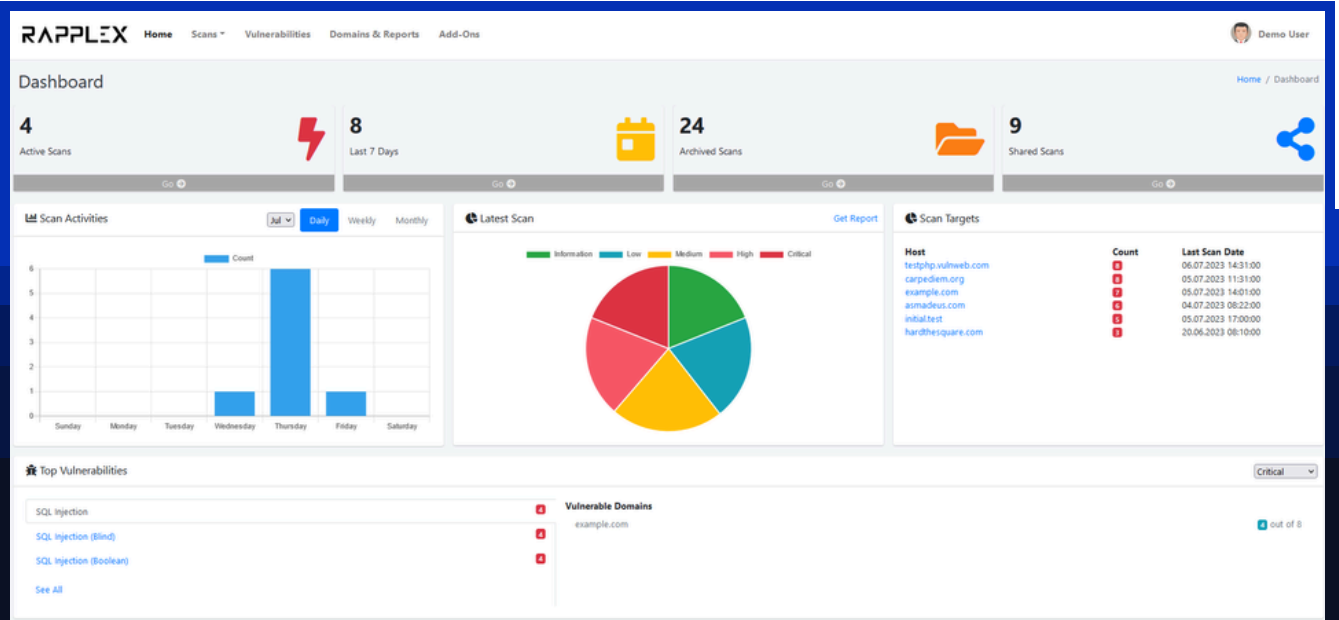
Tarama yapılacak hedef sistemler, mesai saatleri içinde yoğun kullanıma maruz kalıyor olabilir. Bu noktada Rapplex özelliklerinden biri olan zamanlanmış tarama, kullanıcılar tarafından belirlenen ve Rapplex tarafından otomatik olarak başlatılacak taramalar için bir yapı sunar. Böylelikle, mesai saatleri arasında hedef sistem ve kullanıcıların işlemlerinin zarar görmesi/yarıda kesilmesi tehlikesi ortadan kaldırılır.

VERSİYON TAKİPÇİSİ

Rapplex, WordPress gibi bilinen CMSlerin versiyonlarını checksum değerlerine göre ayırt ederek kesin versiyon bilgisini belirler. Yapılan taramalarda hedef sistemde eğer versiyon takibi yapılan bir CMS varsa, versiyona özel olarak atak vektörlerini optimize eder. Rapplex, taradığı hedef sistemdeki CMS versiyonu eski versiyonlu ise, rapora ekleyerek geliştiricileri uyarır.

GELİŞMİŞ WEB ARAYÜZÜ

Rapplex, self-hosted bir web sunucuya sahiptir. Web üzerinden erişilebilir hale gelmesi için IIS, Apache gibi teknolojilere ihtiyaç duymaz.



Detaylı istatistik grafikleri, hem zafiyet hem de hedef bazında analizler yapılmasına imkan tanır.

Kullanıcı dostu arayüzü sayesinde, tarama yönetimi kolaylıkla yürütülebilir.

Tarama ekranında yer alan detaylı site haritası ile crawl edilen sayfalar ve anlık olarak yapılan HTTP istekleri takip edilebilir.

OUT OF BAND INTERACTIONS MONITOR

Rapplex, Out of Band Monitor özelliği sayesinde, public bir servera yapılan istekleri kontrol eder ve hedefteki SSRF zafiyetlerini tespit eder.

İZOLE TARAMALAR

Her tarama kendi işlemi içinde gerçekleştirilir, böylece olası sistem kaynaklı bir kilitlenme/kesinti diğer taramaları ve ana uygulamayı etkilemez.

OTOMATİK KURTARMA

Sistem tarafında gerçekleşebilecek olası bir kilitlenme/kesinti sonrasında, taramalar Rapplex tarafından otomatik olarak kurtarılır.

RAPOR PAYLAŞIMI

Rapplex, bir kullanıcıya ait raporun başka bir kullanıcı tarafından görüntülenebilmesini de yetkilendirme ile kontrol eder.



Yetkisiz bir kullanıcı, ancak taramayı yapan ve raporun sahibi konumundaki kullanıcının yetki vermesi durumunda raporu görüntüleyebilir. Böylelikle hassas bilgiler barındıran zafiyet tarama raporu, fiziksel ortamlara aktarılmadan paylaşılabilir.

Scan #	Host
fb57b701	testphp.vulnweb.com

Share Scan
Enter comma separated email addresses
john.doe@example.com
OK Cancel

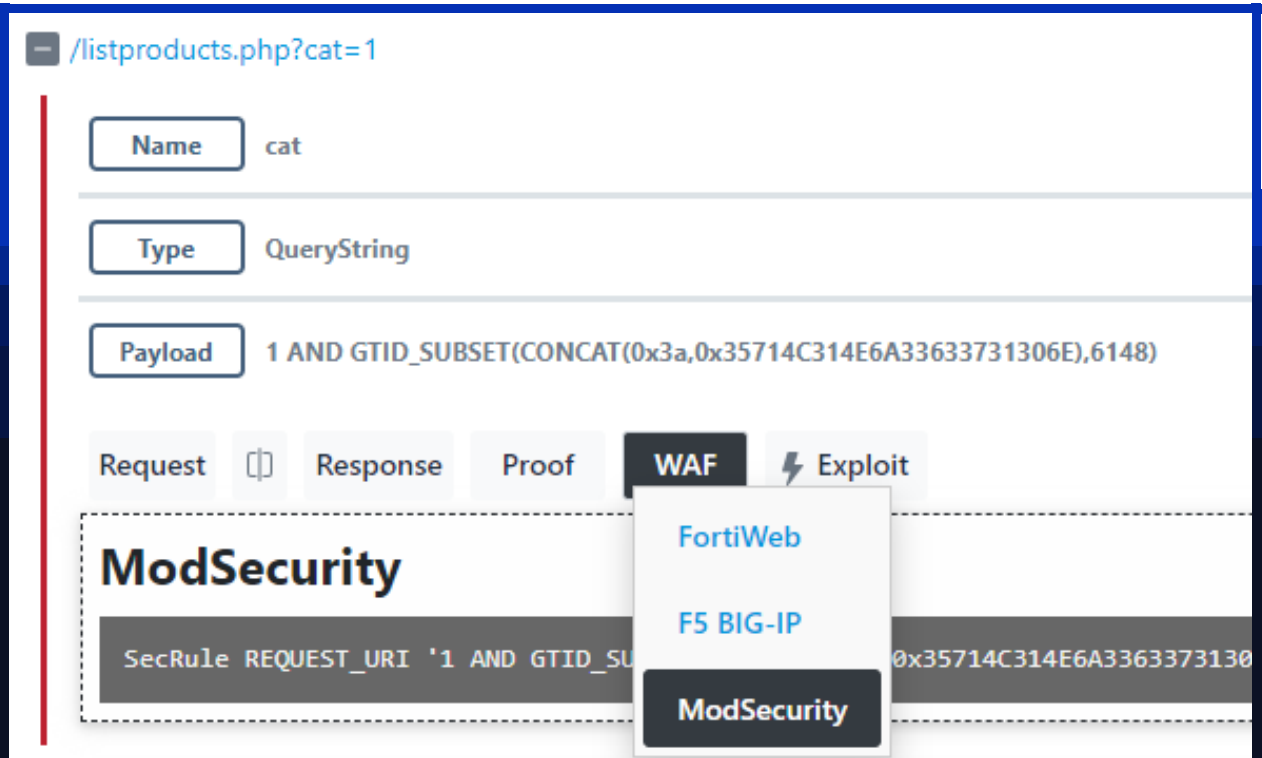
Password Protection
Enter password to protect scan
Password: ****
Retype password: ****
OK Cancel

Password Protected
Enter password to unlock scan
Password: ****
☐ Remove protection
OK Cancel

Buna ek olarak, "Protect" özelliği ile, kullanıcılar raporlarını şifreleyebilir. Paylaşım, görüntüleme gibi süreçlerde de parola koruması devrededir.

DİNAMİK WAF KURALLARI

Rapplex, WAF teknolojileri için, zafiyete özel kural üretir.



Tespit edilen zafiyetler, url, parametre, uzantı, dosya, tip gibi detaylara göre incelenerek raporlanır. Rapplex, bu detayları analiz ederek uygun WAF kuralını üretir ve rapora ekler.

FORTINET

TR7

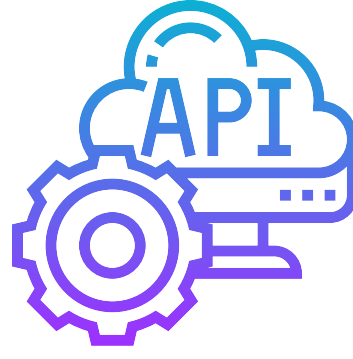
f5

modsecurity
Open Source Web Application Firewall

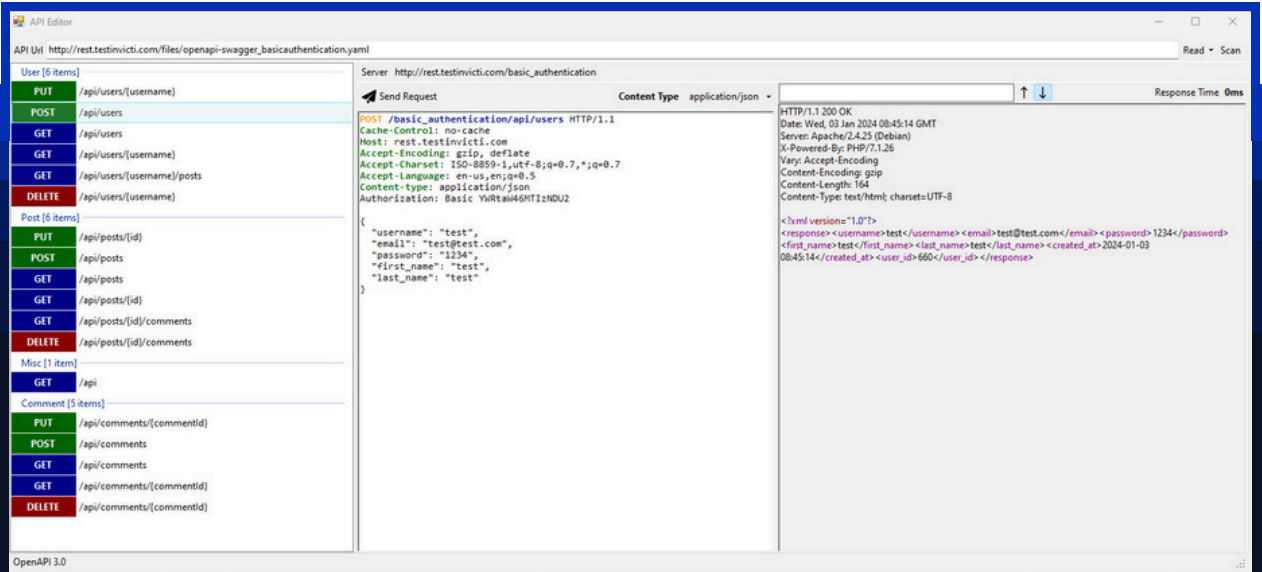
CLOUDFLARE

RAPPLEX

API SCAN



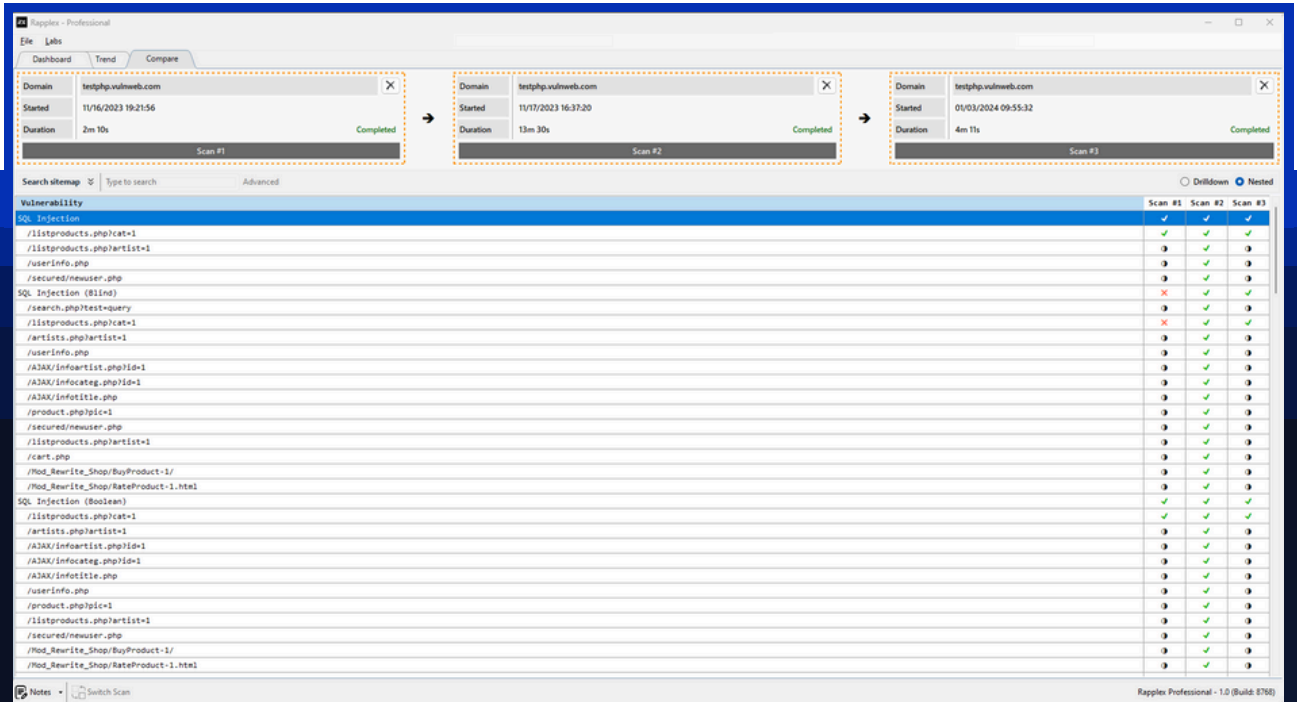
Rapplex, API servislerindeki zafiyetleri de tespit edip raporlar. API Dökümanlarını hem link hem de dosyadan okuyarak parse eder. Bunun yanında, dökümanların parse edilebilmesi için bir tarama başlatılmasına gerek duymaz.



Manuel test yapacak operatörler için API uç noktalarını, HTTP methodlarını ve parametrelerini API Editör'de hazır hale getirir.

TARAMA KARŞILAŞTIRMA

Rapplex, 3 taramaya kadar karşılaştırma imkanı sunar. Yapılan taramalar sonucunda, süre, zafiyetler, crawl edilen sayfalar, site haritası kolaylıkla karşılaştırılabilir. Senkronize arama özelliği sayesinde site haritasında detaylı incelemeler yapılabilir.



Domain	Started	Duration	Status
testphp.vulnweb.com	11/16/2023 19:21:56	2m 10s	Completed
testphp.vulnweb.com	11/17/2023 16:37:30	13m 30s	Completed
testphp.vulnweb.com	01/03/2024 09:55:32	4m 11s	Completed

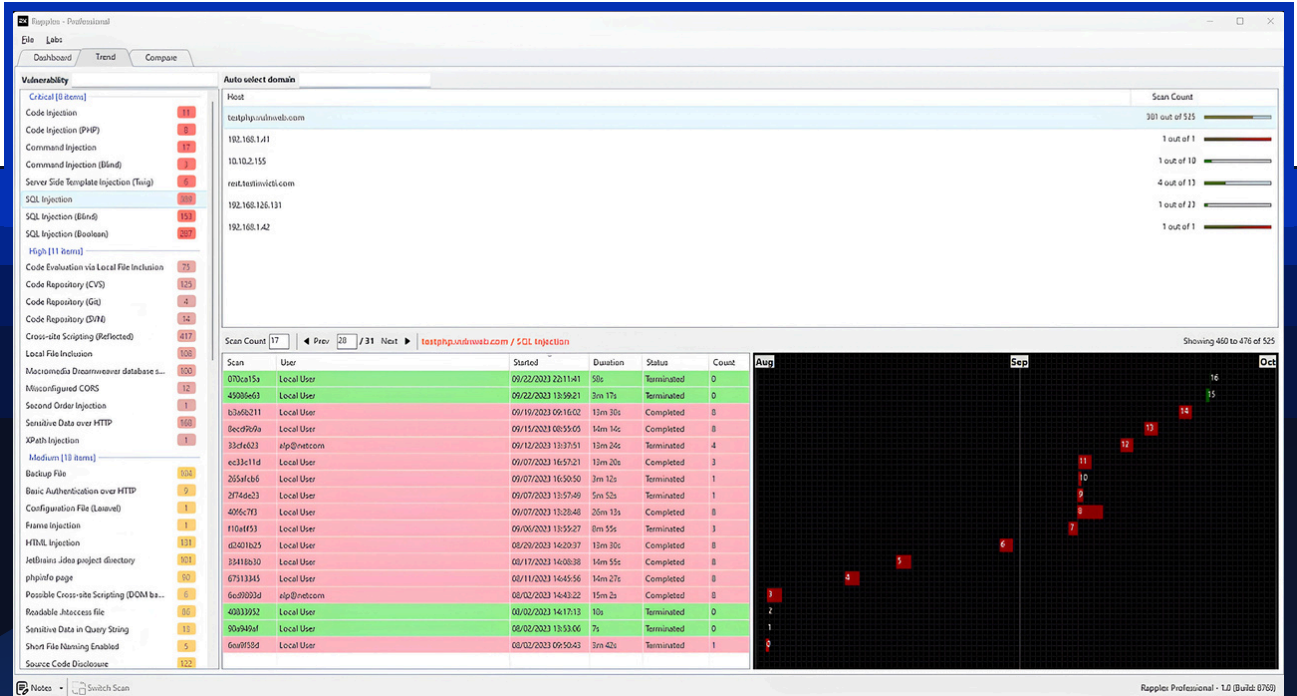
Vulnerability	Scan #1	Scan #2	Scan #3
SQL Injection	✓	✓	✓
/listproducts.php?cat=1	✓	✓	✓
/listproducts.php?artist=1	✓	✓	✓
/userinfo.php	✓	✓	✓
/secured/newuser.php	✓	✓	✓
SQL Injection (Blind)	✗	✓	✓
/search.php?test=query	✗	✓	✓
/listproducts.php?cat=1	✗	✓	✓
/artists.php?artist=1	✓	✓	✓
/userinfo.php	✓	✓	✓
/a3ax/infoartist.php?id=1	✓	✓	✓
/a3ax/infocateg.php?id=1	✓	✓	✓
/a3ax/infoitle.php	✓	✓	✓
/product.php?pic=1	✓	✓	✓
/secured/newuser.php	✓	✓	✓
/listproducts.php?artist=1	✓	✓	✓
/cart.php	✓	✓	✓
/Mod_Reurite_Shop/BuyProduct-1/	✓	✓	✓
/Mod_Reurite_Shop/RateProduct-1.html	✓	✓	✓
SQL Injection (Boolean)	✓	✓	✓
/listproducts.php?cat=1	✓	✓	✓
/artists.php?artist=1	✓	✓	✓
/a3ax/infoartist.php?id=1	✓	✓	✓
/a3ax/infocateg.php?id=1	✓	✓	✓
/a3ax/infoitle.php	✓	✓	✓
/userinfo.php	✓	✓	✓
/product.php?pic=1	✓	✓	✓
/listproducts.php?artist=1	✓	✓	✓
/secured/newuser.php	✓	✓	✓
/Mod_Reurite_Shop/BuyProduct-1/	✓	✓	✓
/Mod_Reurite_Shop/RateProduct-1.html	✓	✓	✓

Bununla birlikte, Rapplex karşılaştırma yapmak için herhangi bir session dosyasına ihtiyaç duymaz.

TREND GRAFIĐİ İLE TAKİPTE KAL

Rapplex, yapılan taramalarda tespit edilen zafiyetlere göre sınıflandırmalar yaparak Trend grafiĐini oluřturur.

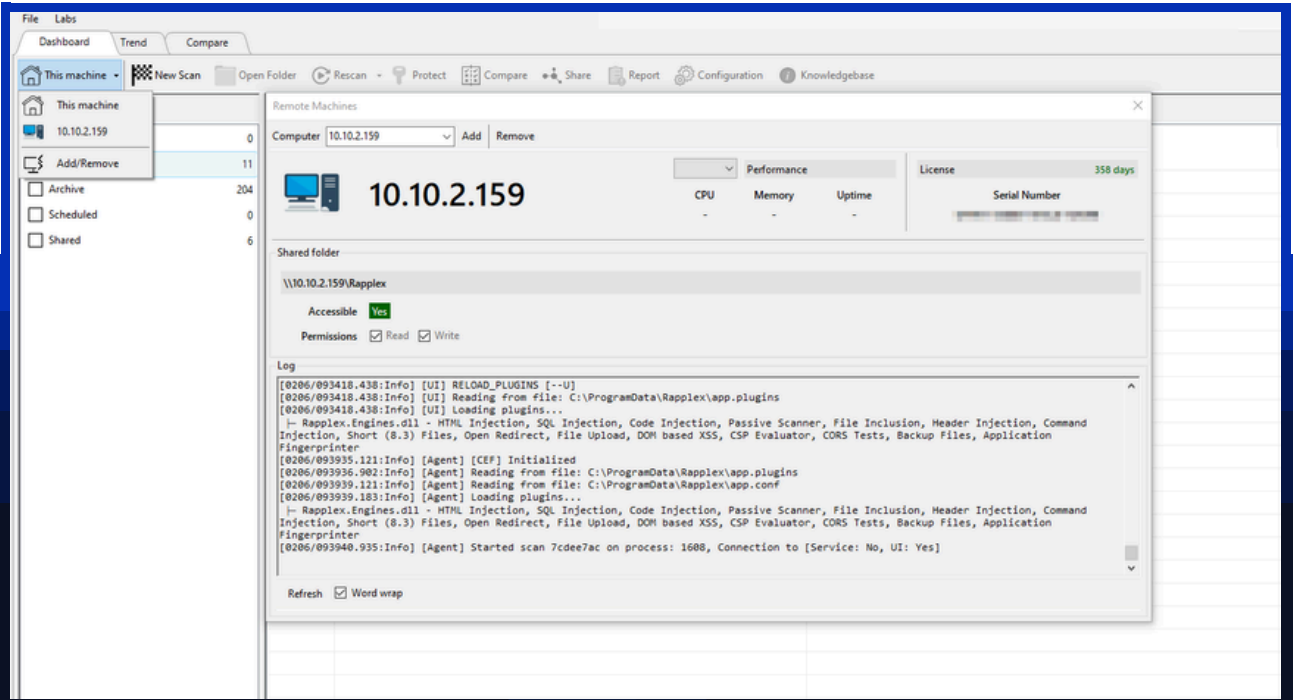
Trend grafiĐi, zafiyetin tespit edilme durumunu, tarama sũresini, tarih aralıĐını baz alarak oluřturulur. Trend grafiĐi sayesinde kullanıcılar, sistemlerinin gũvenliĐi hakkında fikir sahibi olarak ۆnlemler alabilirler.



Sıcaklık grafiĐi, zafiyetin yapılan taramaların kaçında tespit edildiĐinin gۆsterimini yapar.

ORCHESTRATOR

"Orchestrator" özelliđi, sistemdeki bağımsız makinelerin yönetimini sağlar. Bu özellik, master ve slave (köle) cihazlar arasında etkili bir koordinasyon sağlayarak sistemdeki iş yükünü dengeler ve performansı optimize eder.



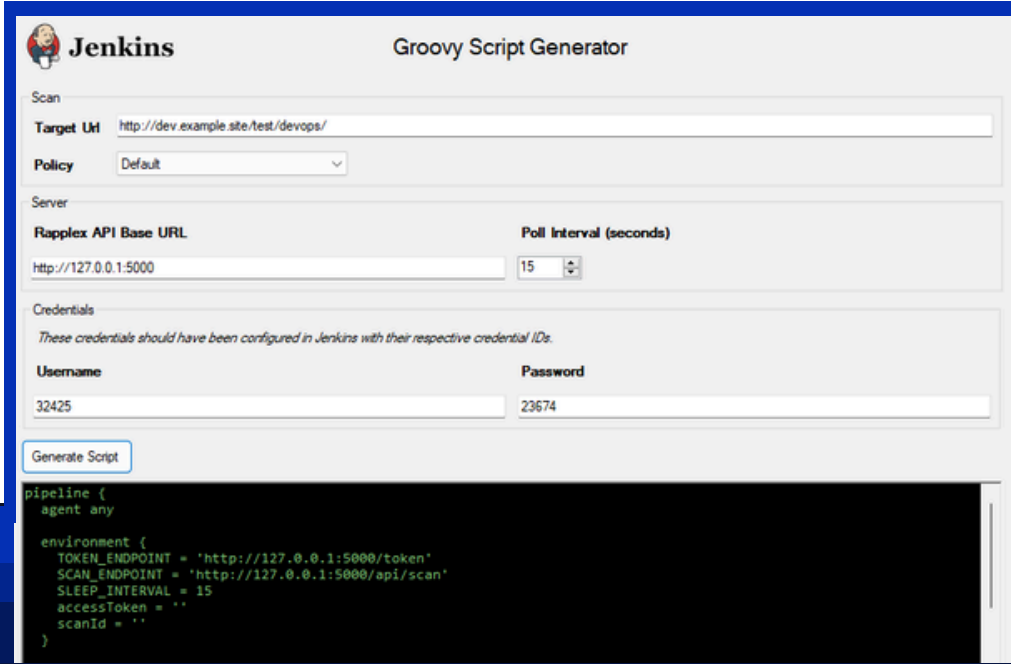
Orchestrator, merkezi bir yönetim noktası olarak çalışır. Master, farklı noktadaki Rapplex'in de kontrolünü elinde tutar. Bu kontrol tarama ve zafiyetlerin yönetimini sağlar. Bu sayede kaynak tüketimi daha verimli hale gelir ve iş yükü eşit dağılır.

Master: Ana makinede bir Enterprise lisans kurulu olmalıdır ve yalnızca alt lisanslı makineleri yönetebilir.

JENKINS

Jenkins için pipeline script üretebilen Rapplex, yazılım geliştirme sürecindeyken taramaların yönetiminin otomatize edilmesini sağlar.

Taramaların build aşamasındayken başlaması, Rapplex'in yazılım geliştirme sürecine tam olarak dahil olmasına imkan tanır.



```
pipeline {
  agent any

  environment {
    TOKEN_ENDPOINT = 'http://127.0.0.1:5000/token'
    SCAN_ENDPOINT = 'http://127.0.0.1:5000/api/scan'
    SLEEP_INTERVAL = 15
    accessToken = ''
    scanId = ''
  }
}
```

Güvenlik açıklarının henüz geliştirme aşamasındayken tespit edilmesi, erkenden önlem alınarak olası felaket senaryolarının önüne geçilmesini mümkün kılar.

Jenkins Groovy Script Generator bu bağlamda, web uygulamalarının güvenliğini artıran ve geliştirme sürecini güçlendiren bir özellik olarak öne çıkar.

RAPPLEX



Muallimköy Mah.
Deniz Cad. No: 143/5
A1 Blok Kat: 9
Ofis No: 77
Bilişim Vadisi
Gebze / Kocaeli



Kısıklı Mh. Büyük
Çamlıca Cd. Çamlıca
Deresi Sk. No:5
Üsküdar / İSTANBUL



Kızılırmak Mah. Ufuk
Üniversitesi Cad.
Farilya İş Merkez K:7
No:8/27 Çukurambar
Çankaya / ANKARA



Yunusobod district,
Firdavsiy 3 street 10-
10a, Tashkent,
Uzbekistan



www.netcom.com.tr

Powered By **NETCOM**
1986

RAPPLEX



info@rapplex.com



rapplex.com



Muallimköy Mah. Deniz Cad. No: 143/5
A1 Blok Kat: 9 Ofis No: 77
Bilişim Vadisi Gebze / Kocaeli



www.netcom.com.tr

Powered By

NETCOM
1986