

RAPID

RAPPLEX

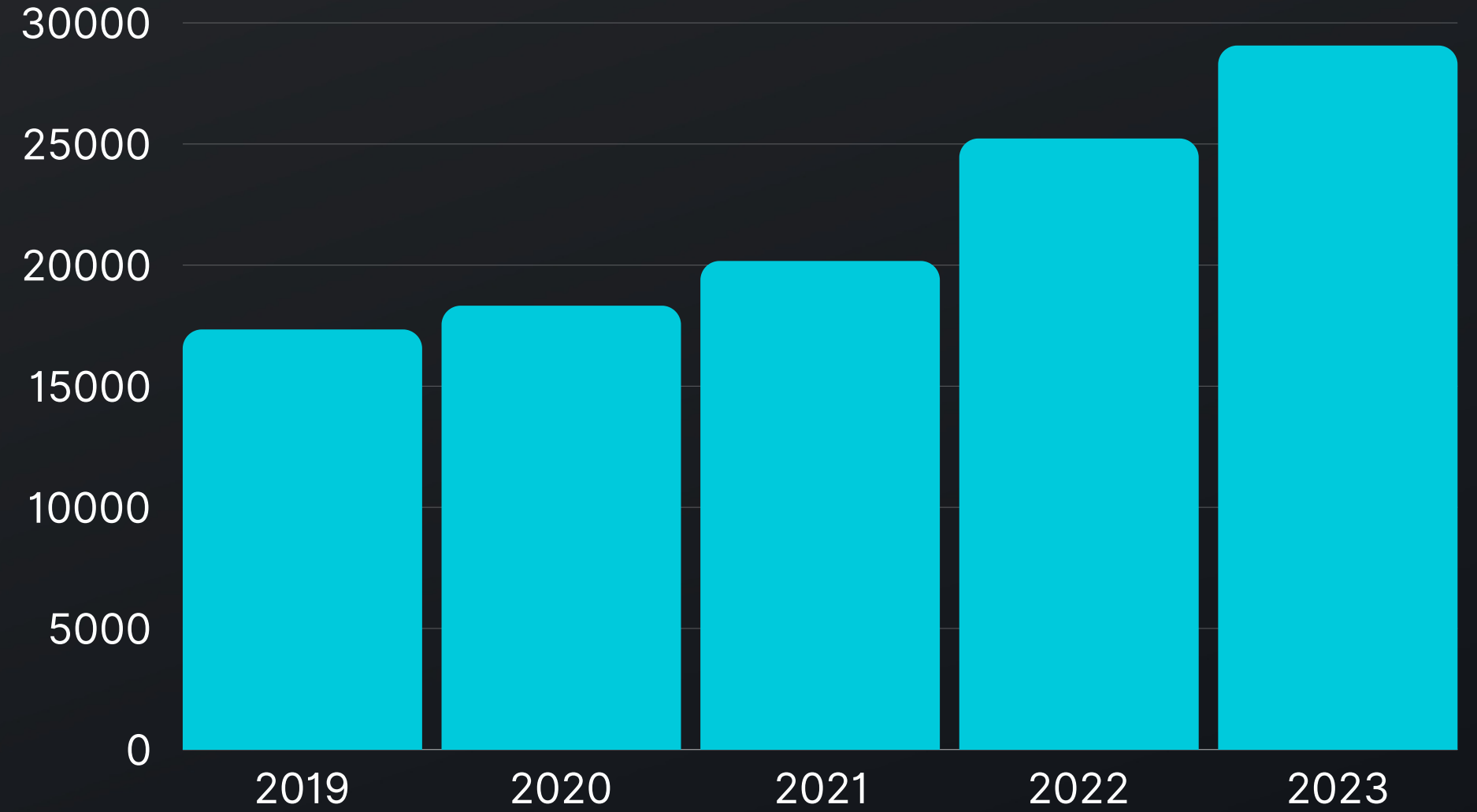
FLEXIBLE

RAPPLEX.COM

TEHDİT GRAFİĞİ

2019 ve 2023 yılları arasında raporlanan ve CVE numarası alan zafiyetlerin yıllara göre dağılımı

Grafikte de görüldüğü üzere, tespit edilen ve uluslararası kuruluşlarca onaylanan zafiyet sayısı her geçen yıl artmaktadır.



Referans: <https://noeticcyber.com/the-state-of-vulnerability-management-in-2024/>

Rapplex - Web Uygulama Güvenlik Tarayıcısı ile web sitenizi hackerlardan önce tarayın. Güvende kalın!

2024 TEHDİT BİLANÇO

22 bin zafiyet!

2024 yılı temmuz ayı itibariyle raporlanan
22 bin zafiyet CVE numarası aldı.

CVE-2024-4577 PHP RCE Argument Injection

gibi zafiyetler web sunucunuz üzerinden uzaktan kod
çalıştırılmasına sebep olabilir.

Bu durum hassas verilerinizi ve kurumsal varlığınızı tehdit eder!

Erken Tespit ve Çözüm İçin



NEDİR ?

Rapplex, gelişmiş bir web uygulama güvenlik tarayıcısıdır. Web sitenizdeki zafiyetleri kendi aktif/pasif motorları ile analiz eder ve detaylı biçimde raporlar. 15'in üstünde entegrasyona sahip olan Rapplex, CI/CD süreçleri ile tam uyumludur.

Yaptığınız taramalar sonucu oluşan verileri istatistiksel bakış açısıyla değerlendirir ve görselleştirir. Tarama karşılaştırma ve trend grafiği sayesinde güvenlik postürünüz hakkında bilgi verir.

Rapplex aynı zamanda kendi sızma testi becerilerini kullanmak isteyen uzmanlar için de gelişmiş özellikler sunar.

RAPPLEX

NEDEN KULLANILMALIDIR ?

Web teknolojilerinin devamlı gelişmesiyle birlikte dinamik web uygulamalarının derinliği ve boyutu her geçen gün artıyor. Bu durum manuel test yapmayı daha zor ve karmaşık hale getiriyor.

Tam da bu noktada Rapplex, web uygulamasındaki tüm formların doldurulması, linklerin tıklanması, site haritasının çıkartılması, kullanılan teknolojilerin tespiti, atak yüzeyinin belirlenmesi ve zafiyetlerin tespiti aşamalarını oldukça kısa sürede yaparak hem kurumunuz hem de kullanıcılar için güvenli bir ortam oluşturmanıza olanak sağlıyor.

Siz de Rapplex ile web sitenizi hackerlardan önce tarayın ve bir adım önde olun!

RAPPLEX

ilk bakış

Advanced Attack

All attacks are enabled

Engine	Injection Type	Parameter Name	Enabled
<any>	Header	<any>	☐
<any>	Cookie	<any>	☐
<any>	Url	<any>	☐
CORS Tests	Header	<any>	☒
Backup Files	Url	<any>	☒
DOM based XSS	Url	<any>	☒
Short (8.3) Files	Url	<any>	☒

Vulnerability

Auto select domain

Host
testphp.vulnweb.com
192.168.1.41
192.168.1.42
test.testinvi.ch

Scan Count 16

◀ Prev 3 / 6 Next ▶

testphp.vulnweb.com / SQL Injection

Aug

Scan	User	Started	Duration	Status	Count
60eeed95	Local User	10/19/2023 16:29:19	6m 24s	Terminated	1
b34d1964	Local User	10/19/2023 14:44:28	31s	Terminated	1
47002c3d	Local User	10/17/2023 09:47:04	15m 8s	Completed	8
a4b61af3	Local User	10/16/2023 15:44:39	5m 48s	Terminated	1
7aa0f193	Local User	10/16/2023 11:43:17	10m 33s	Completed	6
cba17349	Local User	10/16/2023 11:31:50	10m 24s	Completed	6
34c431c4	Local User	10/05/2023 10:17:54	12m 30s	Completed	3
ee7e5ad4	Local User	09/23/2023 19:59:09	27m 58s	Completed	8
b3a6a211	Local User	09/19/2023 09:16:02	13m 30s	Completed	8
8ec096fa	Local User	09/15/2023 08:55:05	14m 14s	Completed	8
33cfe423	alp@metcom	09/12/2023 13:37:51	13m 24s	Terminated	4
ec33c11d	Local User	09/07/2023 16:57:21	13m 20s	Completed	3
2f74a623	Local User	09/07/2023 13:57:49	5m 52s	Terminated	1
4096c793	Local User	09/07/2023 13:28:48	26m 13s	Completed	8
f10a0f53	Local User	09/06/2023 13:55:27	8m 35s	Terminated	3
42401b25	Local User	08/29/2023 14:20:37	13m 30s	Completed	8

Copy from

Add

Delete

Email

Add

Desktop

Asana

Azure

DefectDojo

Discord

Github

Jira

Mattermost

Slack

Teams

Telegram

Trello

OK

Report

Export to HTML

Export to PDF

View as JSON

http://testphp.vulnweb.com/

Vulnerabilities

Critical (1)

High (0)

Medium (0)

Low (0)

Information (0)

Show all

Low
%19.7

Medium
%22.5

High
%19.7

Info
%20.4

Critical
%18.3

Critical

High

Medium

Low

Information

It is possible for an intruder to penetrate and compromise the system fully and/or gain access to highly sensitive data.

An intruder can gain access to system information that could lead to more specific attacks and possibly theft or loss of private and sensitive data.

An intruder can gain access to system information that can aid and lead to more specific attacks resulting in data theft or loss of private and sensitive data.

All entries at this level simply provide additional information to that already available about the tested or not.

SQL Injection

PCI 3.2-6.5.1, OWASP 2013-A1, CWE 89, WASC 19

SQL Injection is an attack technique used to exploit applications that construct SQL statements from user-supplied input. When successful, the attacker is able to change the way the application interacts with the database.

With a successful attack, an attacker can gain:

- Unauthorized access to an application: An attacker can successfully bypass an application's authentication mechanism to have illegitimate access to it.
- Information disclosure: A SQL injection attack could lead to a complete data leakage from the database server.
- Loss of data availability: An attacker can delete records from the database server.
- Compromised data integrity: As SQL statements are also used to modify or add the record, an attacker can use SQL injection to modify or add data stored in the database.

Remediation

- Whitelisting is the best practice to validate input against blacklisting whenever it is practicable.
- Pin and create HTTP headers with which information, testpath can interact with the application for external information.

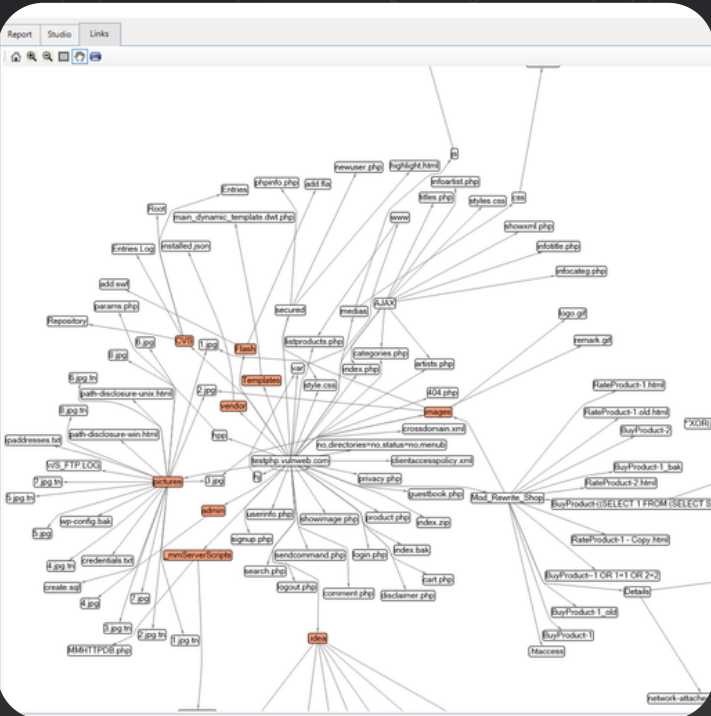
terminal

```
global> HTTP> Rapplex version 1.0 - Copyright (c) 2024

You can use TAB to complete a partially typed command or
If there is only one command that begins with the typed 1
when you hit ENTER.

clear                Clear the window
clear history        Clear the history
diff tool            Set diff tool to compare attack respon
help                Displays this
http set            Set common HTTP request headers
scan                Scan Management
update channel        Set update channel

global> http set
global> HTTP>
global> HTTP> accept charset clear exit help language
global> HTTP> show
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/536.5
Safari/536.5
Accept: text/xml,application/xml,application/xhtml+xml,
text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
```



DESTEKLENEN ZAFİYETLER

OWASP (Open Web Application Security Project) standartlarına bağlı kalan Rapplex, OWASP Top 10 zafiyetlerini tespit eder ve raporlar.

Buna ek olarak Rapplex;

- **PCI**
- **CAPEC**
- **CWE**

gibi sınıflandırmalara uygun raporlar da üretir.

01 SQL Injection

02 Cross-Site Scripting

03 Command Injection

04 SSTI

05 LFI & RFI

06 XXE

07 Code Injection

08 XPath Injection

09 HTML Injection

10 External Script Injection

01

Zafiyet Tespiti

Aktif ve pasif tarama motorları sayesinde zafiyetleri kolaylıkla tespit eder.

04

Zamanlanmış Tarama

Taramayı ayarlanan saatte başlatır.

07

Detaylı Rapor

Zafiyetlerin detaylarını, kanıtlarını ve çözüm önerilerini barındıran benzersiz rapor yapısı.

02

AutoPilot

Saniye başına yapılan HTTP istekleri, sunucu yanıt zamanına göre dinamik olarak değişir.

05

Karşılaştırma

3 taramaya kadar anında karşılaştırma imkanı sunar.

08

Entegrasyon

Jira, GitHub gibi global platformlarla entegredir.

03

Pentester Studio

Manuel testler yapmak isteyen kullanıcılar için sunulan geliştirme ortamı.

06

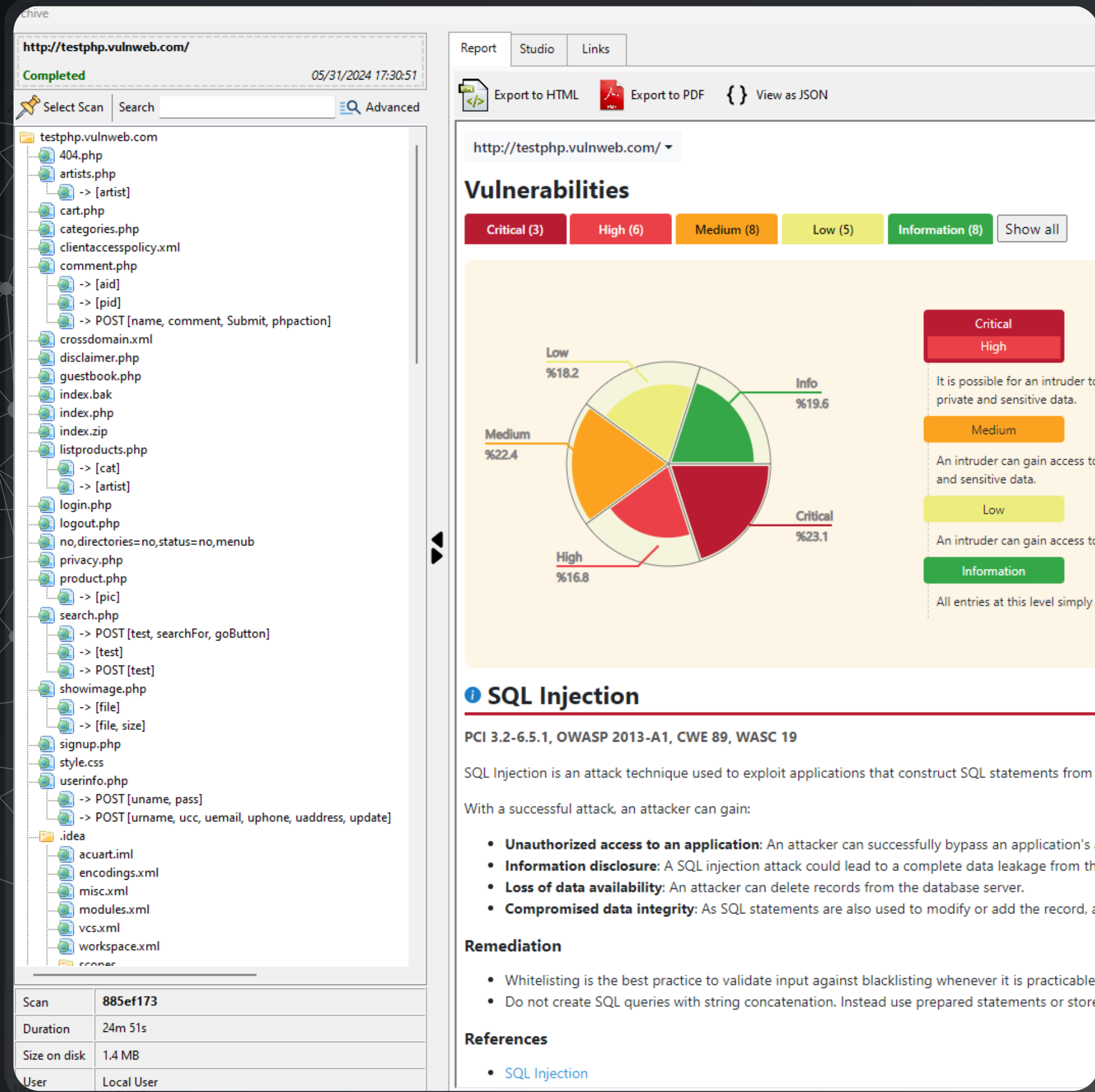
Paylaşım

Raporları farklı ortamlara aktarmadan ekibinizle paylaşın!

09

DevSecOps

Jenkins ve GitLab platformları için pipeline script üretebilen Rapplex, CI/CD süreçlerinde de ekibinizle birlikte.



Detaylı Tarama Raporu

Rapor, tarama sırasında dinamik olarak oluşur. HTML, PDF ve JSON formatlarında incelenebilir.

Site Haritası

Crawl edilen sayfalar site haritasında yer alır. Site haritasındaki linklere tıklandıkça ilgili sayfadaki zafiyetler listelenir.

Dinamik Risk Grafiği

Tespit edilen zafiyetleri risk seviyelerine göre gruplayarak yüzdesel biçimde grafikleştirir. Yönetici özeti kısmıdır.

Çözüm Önerileri

Rapplex, tespit ettiği zafiyetlerin güvenli biçimde kapatılması için çözüm önerileri ve referanslar sunar.

Zafiyet Detayları ve WAF Kuralları

Zafiyetin tespit edildiği url, parametre, payload, http istek ve yanıtını raporda gösterir. Bunlara ek olarak kanıtlar sunar. Zafiyetlere özel WAF kuralları oluşturur.

Sömürü Aracı

Zafiyetin gerçekten var olduğunun manuel testler yapmadan da tespit edilmesini sağlar.

TAM ENTE GRE

Rapplex, global platformlarla entegrasyonu sayesinde tespit edilen zafiyetlerin ilgili ekiplere atanması ve yönetimi konusunda gelişmiş imkanlar sunar.

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



GitHub



Azure



Asana

Discord



Redmine



Telegram



RAPPLEX

```
stages:
  - scan

scan:
  stage: scan
  script: |-
    #!/bin/bash
    base_endpoint="https://cloud.rapplex.com"
    token_endpoint="$base_endpoint/token"
    scan_endpoint="$base_endpoint/api/scan/create"
    sleep_interval=15

    # Get Token
    token=$(curl -sk -X POST "$token_endpoint" -d "grant_type=password&username=$2&password=$3")

    # Create Scan
    scan_response=$(curl -sk -X POST "$scan_endpoint" \
      -H "Authorization: Bearer $token" \
      -H "Content-Type: application/json" \
      -d '{"Url": "https://foo.bar", "Description": "RX", "PolicyId": "00640f182abc4"}')

    # Parse the response to get the scan ID
    scan_id=$(echo "$scan_response" | grep -oP '"Id": "\K[^"]+')

    # Check Scan Status
    while true; do
      # Get status
      status_response=$(curl -sk -X GET "$base_endpoint/api/scan/$scan_id/status" -H "Authorization: Bearer $token")

      # Get high - critical severities and scan status
      high=$(echo "$status_response" | grep -oP '"High": \K\d+')
      critical=$(echo "$status_response" | grep -oP '"Critical": \K\d+')
      status=$(echo "$status_response" | grep -oP '"Status": "\K[^"]+')

      # Check severities
      if [[ $high -gt 0 || $critical -gt 0 ]]; then
        echo "Build failed due to a vulnerability reported by Rapplex!"
        exit 1 # Fail
      fi

      # Check if scan is completed
      if [[ "$status" == "Completed" && $high -gt 0 && $critical -gt 0 ]]; then
        echo "Yay! Scan completed without any vulnerabilities! Keep up the good work!"
        exit 0
      fi
    done
```



GitLab CI/CD

Jenkins



RAPPLEX

DevSecOps

Rapplex, DevSecOps süreçlerine dahil olarak zafiyetlerin henüz geliştirme aşamasındayken tespit edilmesini ve uygulamaların son kullanıcıya ulaşmadan zafiyetlerin giderilmesini sağlar.

Bu doğrultuda GitLab CI/CD ve Jenkins platformları için pipeline script üretebilen Rapplex'in sürece dahil olması için gereken, sadece pipeline aşamalarının arasına eklenmek!

GELİŞMİŞ WEB ARAYÜZÜ

Rapplex Web modülü self-hosted web sunucu ile çalışır.

Apache ya da IIS kurulumuna ihtiyaç duymaz.

Grafiksel gösterimler ve gelişmiş özellikler ile Rapplex Web Modülü tarama yönetimini kolaylaştırır.



PERFORMANS VE ÖLÇEKLENEBİLİRLİK



Atak Yüzeyi Yönetimi

Rapplex, hedefte çalışan teknolojileri kendi pasif tarama motorlarıyla tespit eder ve yapacağı atakları bu analizlere göre dizayn eder.

MySQL veri tabanı çalışan bir hedefe MSSQL payloadları gönderilmez. Bu da daha az HTTP trafiği, daha hızlı tespit edilen zafiyetler anlamına gelir.



Throttler

Saniye başına düşen HTTP isteği sayısının kısıtlanabildiği Rapplex, hem WAF ürünlerinin tespitinden kaçınır hem de hassas konfigürasyonlu sunucuların olumsuz etkilenmesini önler.



Konumlandırma

Rapplex teknik yapısı sayesinde Windows Server/Windows 10-11 işletim sistemlerinde çalışabilir.

SoC, Sızma Testi, Yazılım Geliştirme ekipleri diledikleri mimaride Rapplex'e erişebilir.

TEKNİK BAKIŞ

Microsoft .NET Framework 4.8

Rapplex .NET Framework 4.8 ile geliştirilmektedir ve bünyesinde herhangi 3. parti bir tarama motoru barındırmamaktadır.

İşletim Sistemi Dosya Yapısı

Tarama ve diğer yapılandırma dosyaları, işletim sistemi dosya yapısında şifrelenmiş biçimde tutulur. Herhangi bir veri tabanı maliyeti bulunmamaktadır.

SignalR İle Senkronize API

SignalR kullanan hızlı API yapısı Rapplex'in web ortamını daima senkronize tutar.

API Desteği

Rapplex, kurum içi geliştirilen uygulamalar ve global çözümler ile entegrasyon için API desteği sunar.

Dahili Web Sunucu

Rapplex self-hosted web sunucuya sahiptir. Herhangi bir Apache yada IIS kurulumuna ihtiyaç duymaz.

Script Geliştirme Ortamı

Söz dizimi (Syntax), yorumlayıcı (Compiler) ve komutlar da dahil olmak üzere tamamı Rapplex ekibi tarafından geliştirilen script dili, kullanıcıya hız ve esneklik sağlar.

HEDEF KİTLE

Sızma Testi Uzmanı

Sızma testi uzmanları için özel olarak sunulan özellikler sayesinde testler artık daha hızlı ve kolay.



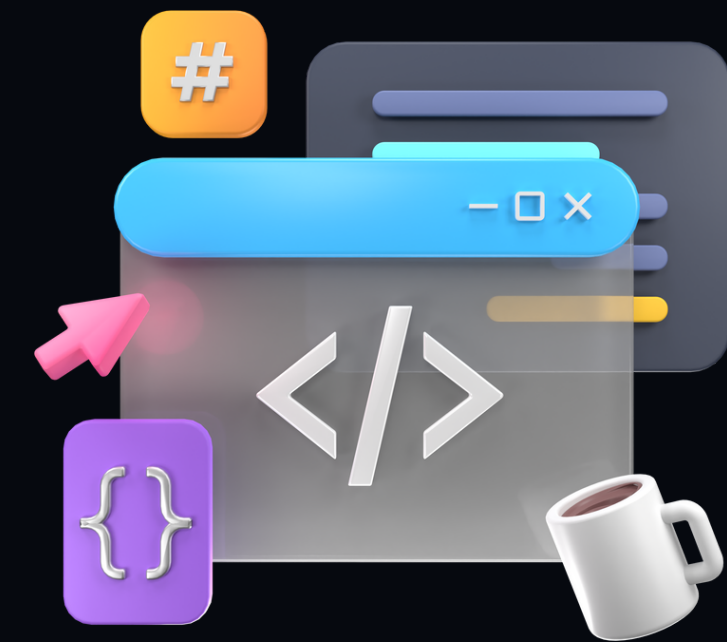
SoC Analisti

SoC analistleri tarafından yapılan periyodik taramalar, korunan sistemi daha güvenli hale getirir.



Yazılım Geliştirici

SDLC ve DevSecOps sürecine dahil olan Rapplex, zafiyeti geliştirme aşamasındayken tespit etmeyi ve daha güvenli geliştirme süreci oluşmasını sağlar.



HEDEF KİTLE

Sızma Testi Uzmanı

Sızma testi uzmanları için özel olarak sunulan özellikler sayesinde testler artık daha hızlı ve kolay.



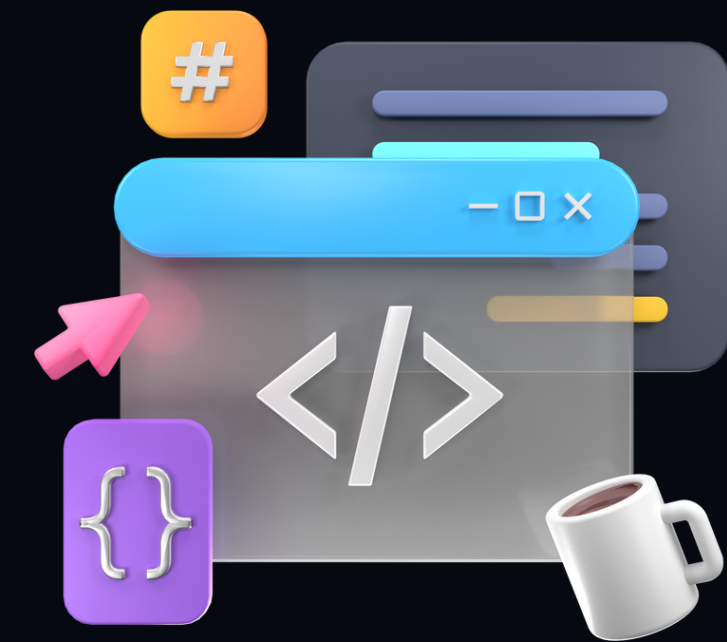
SoC Analisti

SoC analistleri tarafından yapılan periyodik taramalar, korunan sistemi daha güvenli hale getirir.



Yazılım Geliştirici

SDLC ve DevSecOps sürecine dahil olan Rapplex, zafiyeti geliştirme aşamasındayken tespit etmeyi ve daha güvenli geliştirme süreci oluşmasını sağlar.



STANDARD

Reporting
Version Tracker
Knowledgebase
Web & API Scan
Notes
Unlimited Scan

PROFESSIONAL

Reporting
Version Tracker
Knowledgebase
Web & API Scan
Notes
Unlimited Scan
Web Support
Real Time Notification
Share
Rescan
Compare
Pentester Studio
WAF Rules
Scheduled Scan



ENTERPRISE

Reporting
Version Tracker
Knowledgebase
Web & API Scan
Notes
Unlimited Scan
Web Support
Real Time Notification
Share
Rescan
Compare
Pentester Studio
WAF Rules
Scheduled Scan
Orchestrator
Protect
Copy Config

LİSANSLAMA

Rapplex, kullanıcılarına farklı senaryolarda kullanmak üzere lisanslama çeşitliliği sunar.

- Fully Qualified Domain Name (FQDN)
- Domain FIFO
- Wildcard

• FQDN

FQDN bazlı lisanslama çeşidinde Rapplex için her subdomain ayrı bir domain olarak kabul edilir.

Domain 1: <https://example.com>

Domain 2: <https://test.example.com>

• Domain FIFO

Kullanıcıların devamlı artan ve değişen domain sayıları varsa domain FIFO yöntemi tavsiye edilir.

1 yıl için 50 domain hakkı satın alan kullanıcının lisansı, tarama yaptıkça dinamik olarak oluşur.

Farklı domainlere tarama yaptıkça bu bilgiler lisansa kaydolur.

• Wildcard

Kullanıcılar tek bir ana domain altına toplanmış subdomainler altında web varlıklarını kontrol ediyor olabilirler.

Bu durumda wildcard yöntemi tavsiye edilir.

*.example.com tanımlamasının ardından example.com altındaki tüm subdomainler herhangi bir kısıtlama olmaksızın Rapplex tarafından taranabilir.

RAPID

RAPPLEX

FLEXIBLE

RAPPLEX.COM