



Uygulamalı Beyaz Şapkalı Hacker Eğitimi

Bu doküman, alıntı vererek kullanılabilir ya da paylaşılabilir ancak değiştirilemez ve ticari amaçla kullanılamaz. Detaylı bilgiye <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.tr> bağlantısından erişebilirsiniz.

www.prismacsi.com

© All Rights Reserved.





Zafiyet Keşfi

Konular

- **Zafiyet Nedir?**
- **Zafiyetin Kaynağı Nedir?**
- **Zafiyet Yönetim Döngüsü**
- **Otomatize Zafiyet Tarayıcıları**
- **Zafiyet Veritabanları**
- **Sık Kullanılan Araçlar**
- **Uygulamalar**

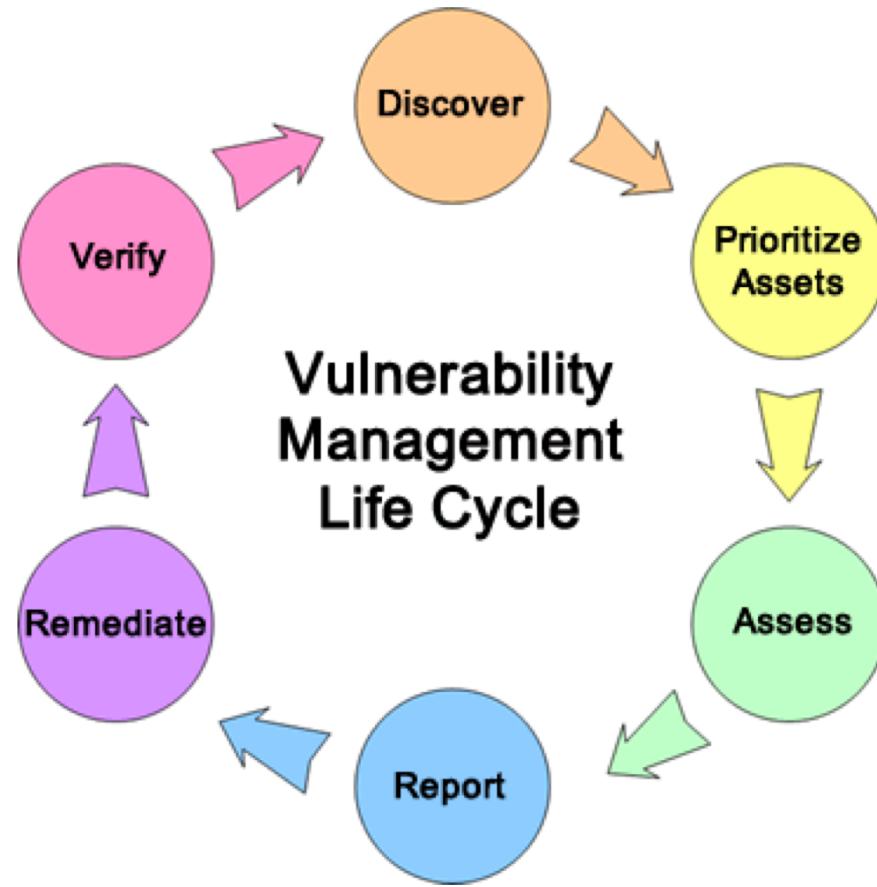
Zafiyet Nedir?

- Herhangi bir uygulamada, servis veya protokolde, daha önce yapılan arařtırmalarda tespit edilmiř veya yeni keřfedilen ve siber saldırganlar için bir atak türüne izin veren, sistemin akıřını etkileyebilecek zayıflıklardır.
- [Senaryo]

Zafiyetin Kaynağı Nedir?

- Eski sürüm / güncellenmemiş uygulama ve servisler
- Yama eksiklikleri
- Hatalı konfigürasyonlar
- Güvenli yazılım geliştirme süreç eksiklikleri
- Güvensiz ağ mimarisi tasarımları
- Insider, bilinçsizlik

Zafiyet Yönetim Döngüsü



Zafiyet Tarayıcıları

- Netsparker
- Acunetix
- Burpsuite
- Appscan
- Webinspect
- W3af
- Arachni
- Nikto
- Sqlmap
- Nessus
- Nexpose
- OpenVAS
- Qualys
- Core Impact
- Vega
- Skipfish
- Commix
- nmap



Neden ihtiya duyarız?

- Riski tanı!
- Riski yönet!
- Olası siber saldırıların bir nebze de olsa önüne geç!
- Wannacry vakası!
- Geçmişte yaşanan siber olaylardan ders çıkar!



Anahtar Kelimeler

- **POLICY:** Gerçekleştirilecek taramalar için yapılan özel ayarlamalara verilen isimdir. Örneğin ağ taramalarında kullandığını POLICY ile web uygulamaları taraması için kullandığınız POLICY farklılık gösterir.
- **PLUGIN:** Güvenlik kontrolleri için geliştirilmiş olan küçük araçlar/scriptlerdir.
- **SCAN:** Tarama işlemi

Zafiyet Veritabanları

- Zafiyet veritabanları tespit edilmiş olan zafiyetlerin listelendiği veritabanlarıdır.
- <https://nvd.nist.gov/>
- <https://www.cvedetails.com/>

2-3 CVE Details
The ultimate security vulnerability datasource
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Search

View CVE

[Log In](#) [Register](#)
Vulnerability Feeds & WidgetsNew
www.itsecdb.com

Enter a CVE id, product, vendor, vulnerability type...

Search

Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	2257	2.10
1-2	828	0.80
2-3	4161	3.90
3-4	3393	3.20
4-5	22342	20.80
5-6	20714	19.30
6-7	13996	13.10
7-8	24344	22.70
8-9	464	0.40
9-10	14663	13.70
Total	107162	

Weighted Average CVSS Score: 6.6

Vulnerability Distribution By CVSS Scores

CVSS Score Ranges	Number Of Vulnerabilities
0-1	2257
1-2	828
2-3	4161
3-4	3393
4-5	22342
5-6	20714
6-7	13996
7-8	24344
8-9	464
9-10	14663

Looking for OVAL (Open Vulnerability and Assessment Language) definitions? <http://www.itsecdb.com> allows you to view exact details of OVAL(Open Vulnerability and Assessment Language) definitions and see exactly what you should do to verify a vulnerability. It is fully integrated with cvedetails so you will be able to see OVAL definitions related to a product or a CVE entry.
Sample CVE entry with OVAL definitions : [CVE-2007-0994](#)

www.cvedetails.com provides an easy to use web interface to CVE vulnerability data. You can browse for vendors, products and versions and view cve entries, vulnerabilities, related to them. You can view statistics about vendors, products and versions of products. CVE details are displayed in a single, easy to use page, see a [sample here](#).

CVE vulnerability data are taken from National Vulnerability Database (NVD) xml feeds provided by National Institute of Standards and Technology. Additional data from several sources like exploits from www.exploit-db.com, vendor statements and additional vendor supplied data, [Metasploit](#) modules are also published in addition to NVD CVE data.

Vulnerabilities are classified by cvedetails.com using keyword matching and cwe numbers if possible, but they are mostly based on keywords.

Unless otherwise stated CVSS scores listed on this site are "CVSS Base Scores" provided in NVD feeds. Vulnerability data are updated daily using NVD feeds. Please visit nvd.nist.gov for more details.

Please contact [admin at cvedetails.com](mailto:admin@cvedetails.com) or use our [feedback forum](#) if you have any questions, suggestions or feature requests.

View CVE :

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View BID :

(e.g.: 12345)

Search By Microsoft Reference ID:

Browse :

- [Home](#)
- [Vendors](#)
- [Products](#)
- [Vulnerabilities By Date](#)
- [Vulnerabilities By Type](#)

Reports :

- [CVSS Score Report](#)
- [CVSS Score Distribution](#)

Search :

- [Vendor Search](#)
- [Product Search](#)
- [Version Search](#)
- [Vulnerability Search](#)
- [By Microsoft References](#)

Top 50 :

- [Vendors](#)
- [Vendor Cvss Scores](#)
- [Products](#)
- [Product Cvss Scores](#)
- [Versions](#)

Other :

- [Microsoft Bulletins](#)
- [Bugtraq Entries](#)
- [CVE Definitions](#)
- [About & Contact](#)
- [Feedback](#)
- [CVE Help](#)
- [FAQ](#)
- [Articles](#)

External Links :

- [NVD Website](#)
- [CVE Web Site](#)



Güvenlik Tarayıcıları

- All In One mantığı
- Network üzerindeki zafiyetleri bulmakta daha iyiler
- Daha çok sunucu/istemci tabanlı zafiyetlerin kontrollerinde kullanılıyorlar
- Uyumluluk, konfigürasyon, zafiyet testleri
- False positive durumlarla karşılaşıyor
- Test süresini ciddi oranda kısaltıyor

OpenVAS Security Scanner - DEMO

- Açık kaynak zafiyet tarama aracıdır.
- İçinde gelişmiş özellikler barındırır.
- Nessus alternatifi olarak kullanılabilir.

Greenbone Security Assistant

Logged in as Admin **admin** | Logout
Fri Jul 12 21:12:01 2013 UTC

Scan Management | Asset Management | SecInfo Management | Configuration | Extras | Administration | Help

Tasks 1 - 10 of 20 (total: 20) [No auto-refresh] [Apply overrides]

Filter: apply_overrides=1 first=1 rows=10 sort=name

Name	Status	Total	Reports			Trend	Actions
			First	Last	Threat		
aspnet.testsparker.com (Mavituna testsparker)	Done	1	Jul 11 2013	High		[Icons]	
crackme.cenzic.com (Cenzic crackmebank)	Done	1	Jul 11 2013	High		[Icons]	
demo.testfire.net (IBM altoromutual)	Done	1	Jul 11 2013	Medium		[Icons]	
demo.testfire.net (IBM altoromutual)	Done	1	Jul 11 2013	Medium		[Icons]	
firebitsbr.wordpress.com (firebitsbr.wordpress.com)	Done	1	Jul 11 2013	None		[Icons]	
php.testsparker.com (Mavituna testsparker)	Done	1	Jul 11 2013	High		[Icons]	
testasp.vulnweb.com (Acunetix acuforum)	Done	1	Jul 11 2013	Medium		[Icons]	
testaspnet.vulnweb.com (Acunetix acublog)	Done	1	Jul 11 2013	Medium		[Icons]	
testphp.vulnweb.com (Acunetix acuart)	Done	1	Jul 11 2013	High		[Icons]	

(Applied filter: apply_overrides=1 first=1 rows=10 sort=name)

Greenbone Security Assistant (GSA) Copyright 2009-2013 by Greenbone Networks GmbH, www.greenbone.net



Nmap NSE - DEMO

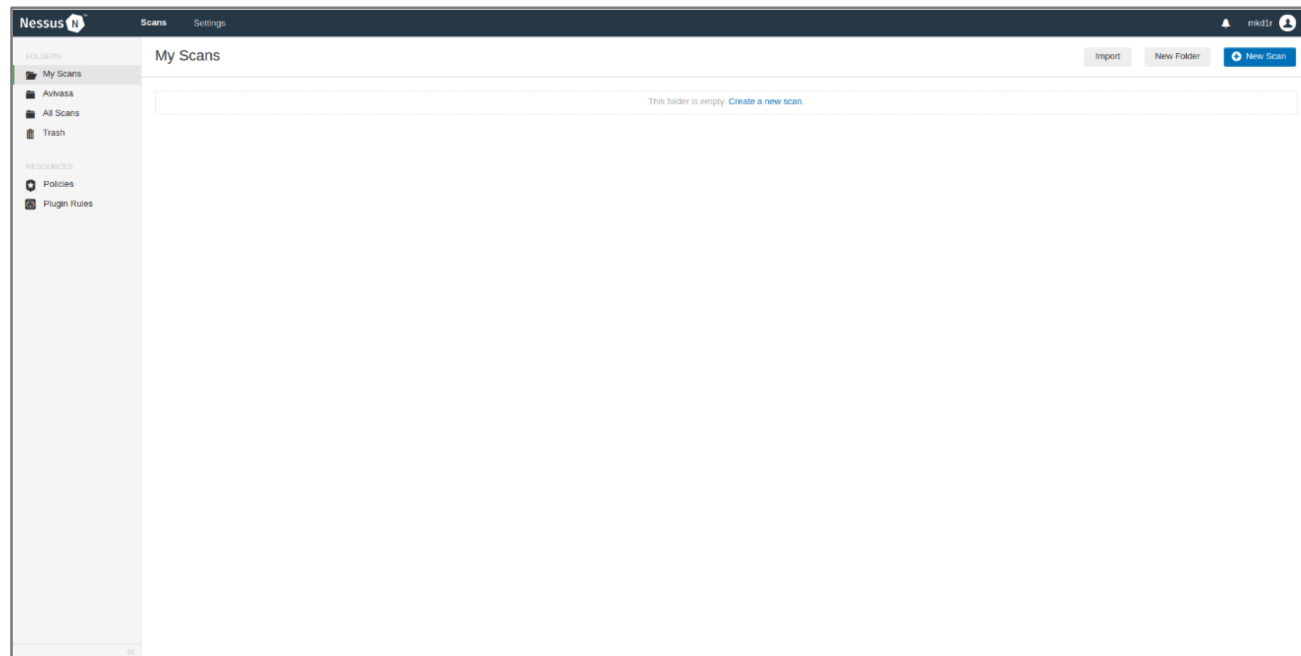
- Nmap Scripting Engine ile zafiyet taraması yapmak mümkündür.
- Açık kaynak yazılım. Siz de katkı verebilirsiniz ve üstüne modüller geliştirebilirsiniz.
- Hızlı tarama imkanı veriyor.
- Genelde tüm testlere nmap zafiyet taramaları ile başlanır.

```

root@PRISMACSI: ~
File Edit View Search Terminal Help
root@PRISMACSI:~# nmap -h
Nmap 7.70 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  
```

Nessus - Uygulama

- En sık kullanılan zafiyet tarama aracıdır.
- Penetration test vs zafiyet taraması konusuna geri dönüş!
- Lisanslı ve Free sürümleri mevcuttur.
- Free sürüm ile de birçok güvenlik kontrolünü gerçekleştirebilirsiniz.
- Web, Network, SCADA, Uyumluluk taramaları gibi seçenekler mevcuttur.
- Daha çok network taramalarında kullanılır.



Nessus - Uygulama

- Yeni Tarama Başlatma
 - Policy
 - Gelişmiş Tarama
 - Düzenlenebilir
 - Taramayı kendinize göre özelleştirebilirsiniz ve gelişmiş ayarlar yapabilirsiniz.

The screenshot displays the Nessus Scan Templates interface. The main content area is titled "Scan Templates" and shows a grid of 21 scan templates. Each template card includes an icon, a title, and a brief description. The templates are:

- Advanced Scan**: Configure a scan without using any recommendations.
- Audit Cloud Infrastructure**: Audit the configuration of third-party cloud services.
- Badlock Detection**: Remote and local checks for CVE-2016-2118 and CVE-2016-0128.
- Bash Shellshock Detection**: Remote and local checks for CVE-2014-6271 and CVE-2014-7169.
- Basic Network Scan**: A full system scan suitable for any host.
- Credentialed Patch Audit**: Authenticate to hosts and enumerate missing updates.
- DROWN Detection**: Remote checks for CVE-2016-0800.
- Host Discovery**: A simple scan to discover live hosts and open ports.
- Intel AMT Security Bypass**: Remote and local checks for CVE-2017-5689.
- Internal PCI Network Scan**: Perform an internal PCI DSS (11.2.1) vulnerability scan.
- Malware Scan**: Scan for malware on Windows and Unix systems.
- MDM Config Audit**: Audit the configuration of mobile device managers.
- Mobile Device Scan**: Assess mobile devices via Microsoft Exchange or an MDM.
- Offline Config Audit**: Audit the configuration of network devices.
- PCI Quarterly External Scan**: Approved for quarterly external scanning as required by PCI.
- Policy Compliance Auditing**: Audit system configurations against a known baseline.
- SCAP and OVAL Auditing**: Audit systems using SCAP and OVAL definitions.
- Shadow Brokers Scan**: Scan for vulnerabilities disclosed in the Shadow Brokers leaks.
- Spectre and Meltdown**: Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.
- WannaCry Ransomware**: Remote and local checks for MS17-010.
- Web Application Tests**: Scan for published and unknown web vulnerabilities.

Nessus - Uygulama

- Yeni Tarama
 - Hedef Sistemler
 - Pluginler
 - Zamanlama ayarları
 - Kaba kuvvet saldırıları
 - Gelişmiş Ayarlar

Nessus N Scans Settings rkdIn

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings Credentials Compliance Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

Description

Folder: My Scans

Targets

Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

Upload Targets Add File

Save Cancel

Nessus - Uygulama

- Tarama sonuçları birçok farklı formatta sunuluyor. Bu çıktılar ile büyük bir ağın dahi kolayca analizi yapılabilir.
 - Detaylı analiz
 - Kritiklik Seviyeleri



Nessus - Uygulama

Nessus Scans Policies admin

Test

CURRENT RESULTS: MAY 11 AT 10:34 PM

Configure Audit Trail Launch Export Filter Vulnerabilities

Hosts > 192.168.56.102 > Vulnerabilities 41 Compliance 217

Severity	Plugin Name	Plugin Family	Count
CRITICAL	CentOS 6 / 7 : openssl (CE...	CentOS Local Security Checks	1
CRITICAL	CentOS 7 : glibc (CESA-201...	CentOS Local Security Checks	1
HIGH	CentOS 7 : graphite2 (CESA...	CentOS Local Security Checks	1
HIGH	CentOS 7 : kernel (CESA-20...	CentOS Local Security Checks	1
HIGH	CentOS 7 : mariadb (CESA-...	CentOS Local Security Checks	1
MEDIUM	CentOS 5 / 6 / 7 : bind (CES...	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : ipa / libldb / li...	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : libssh2 (CES...	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : nss-util (CES...	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : samba (CES...	CentOS Local Security Checks	1

Host Details

IP: 192.168.56.102
 DNS: st91.i
 MAC: 08:00:27:db:3e:a2
 OS: Linux Kernel
 3.10.0-327.4.5.el7.x86_64 on
 CentOS Linux release 7.2.1511
 (Core)
 Start: May 11 at 10:34 PM
 End: May 11 at 10:39 PM
 Elapsed: 6 minutes
 KB: [Download](#)

Vulnerabilities

Legend: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue)



Nessus - Uygulama

Nessus Scans Settings mikiir

test / Plugin #90317 [Configure](#)

[Back to Vulnerabilities](#)

Hosts 1 Vulnerabilities 10 History 1

MEDIUM SSH Weak Algorithms Supported

Description
Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

Solution
Contact the vendor or consult product documentation to remove the weak ciphers.

See Also
<https://tools.ietf.org/html/rfc4253#section-6.3>

Output

```
The following weak server-to-client encryption algorithms are supported :
arcfour
arcfour128
arcfour256

The following weak client-to-server encryption algorithms are supported :
arcfour
arcfour128
arcfour256
```

Port	Hosts
22 / tcp / ssh	185.44.192.101

Plugin Details

Severity: Medium
ID: 90317
Version: \$Revision: 1.3 \$
Type: remote
Family: Misc.
Published: April 4, 2016
Modified: December 14, 2016

Risk Information

Risk Factor: Medium
CVSS Base Score: 4.3
CVSS Vector:
CVSS2#AV:N/AC:MAU:N/C:P/I:N/A:N

Nessus - Uygulama

- Tarama raporu aşağıdaki formatlarda sunulmaktadır ve bu formattaki çıktılar ile birlikte diğer penetration test araçları ile entegre çalışılabilmektedir.

- Formatlar

- XML
- HTML
- Nessus

The screenshot displays the Nessus web interface for a scan named 'test'. The main table lists 16 vulnerabilities with columns for severity, name, family, and count. The vulnerabilities are as follows:

Sev	Name	Family	Count
MEDIUM	SSH Weak Algorithms Supported	Misc.	1
LOW	SSH Server CBC Mode Ciphers Enabled	Misc.	1
LOW	SSH Weak MAC Algorithms Enabled	Misc.	1
INFO	Backported Security Patch Detection (SSH)	General	1
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	Nessus Scan Information	Settings	1
INFO	Nessus SYN scanner	Port scanners	1
INFO	OS Identification	General	1
INFO	Service Detection	Service detection	1
INFO	SSH Algorithms and Languages Supported	Misc.	1
INFO	SSH Protocol Versions Supported	General	1
INFO	SSH Server Type and Version Information	Service detection	1
INFO	TCP/IP Timestamps Supported	General	1
INFO	Timestamp Information	General	1

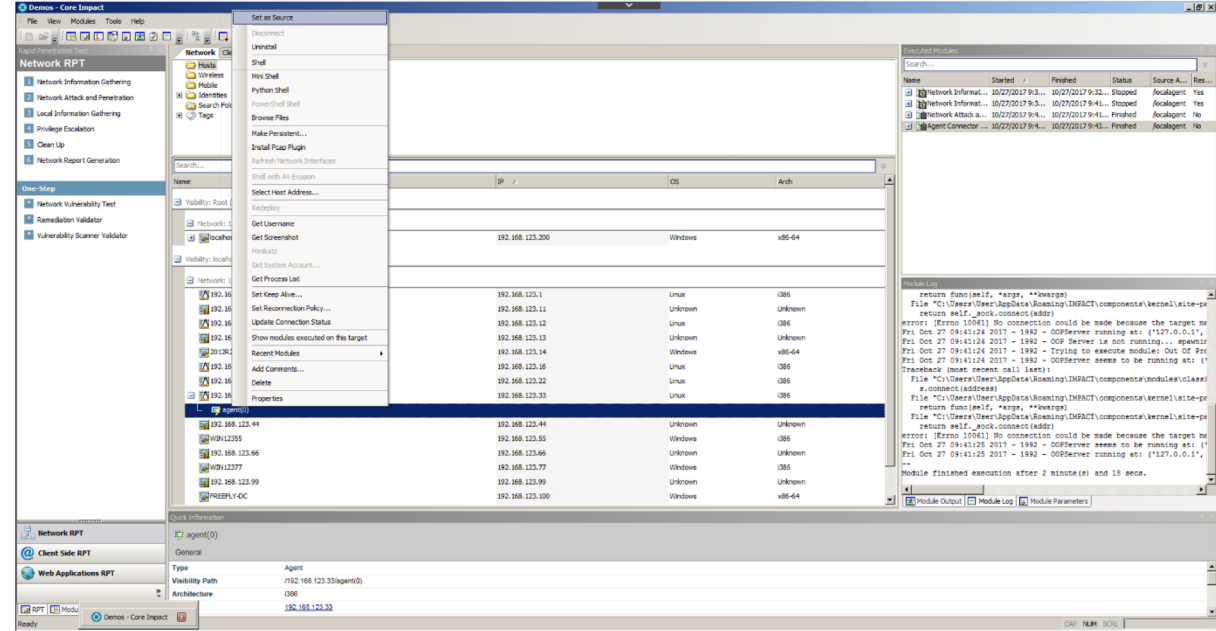
The right-hand panel shows scan details for 'test':

- Name: test
- Status: Completed
- Policy: Advanced Scan
- Scanner: Local Scanner
- Start: Today at 10:49 AM
- End: Today at 10:52 AM
- Elapsed: 3 minutes

A donut chart titled 'Vulnerabilities' shows the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue). The chart is predominantly blue, indicating a high number of information-level vulnerabilities.

Core Impact - Tanıtım

- Security Scanner
- İçerisinde ileri seviye birçok güvenlik kontrolü mevcut ve kendine has araçları da barındırıyor.
- Özel exploitler mevcuttur.
- Özel Zeroday ekibi vardır.
- Lisans bedeli 😊



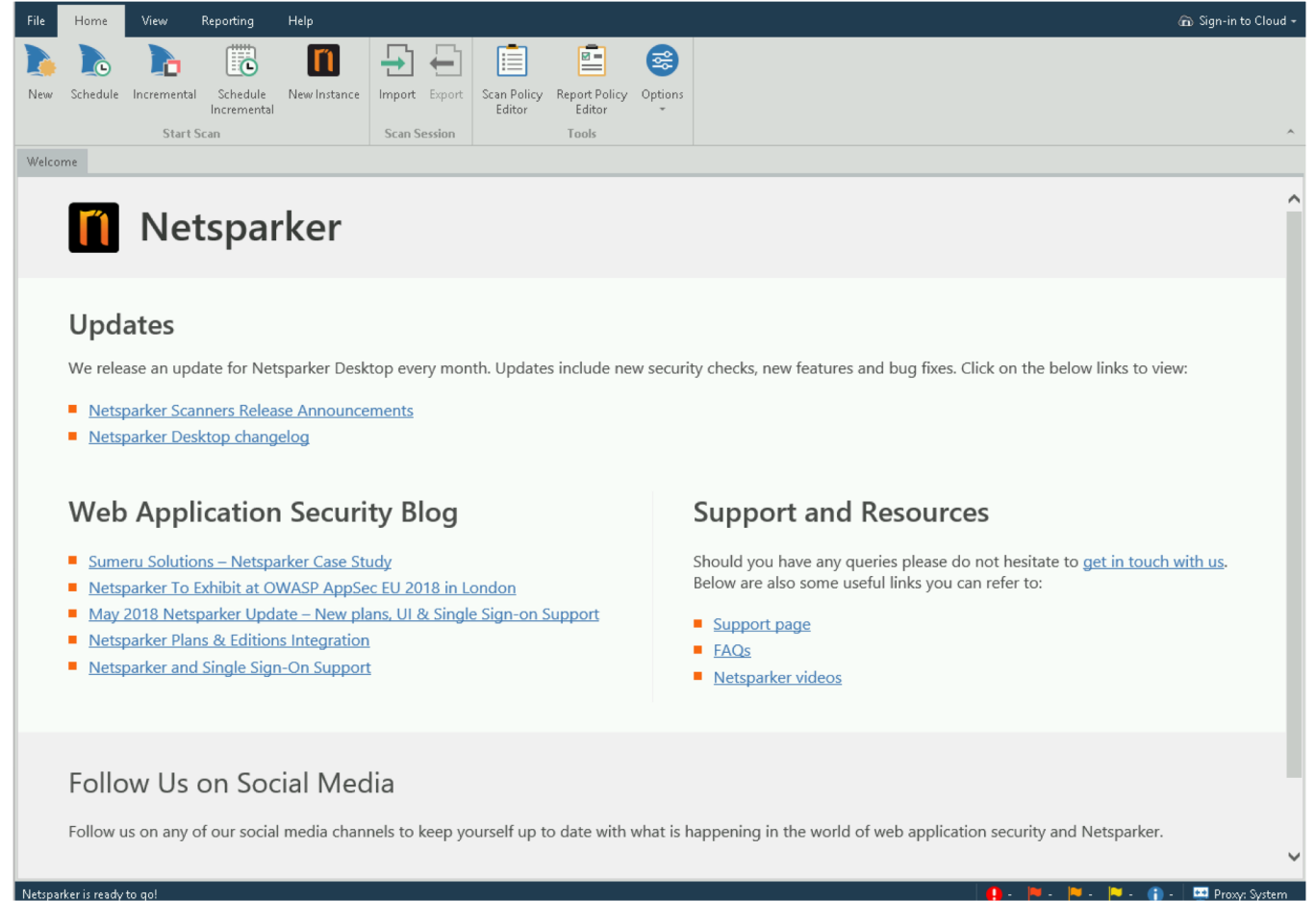


Web Güvenlik Tarayıcıları

- Web uygulamaları ve servislerinin güvenlik taramaları için kullanılıyor
- Manuel testlere de imkan sağlayanları mevcut
- Netsparker Dünya genelinde kabul edilmiş en başarılı zafiyet tarayıcısı
- Burp suite en kritik araç!

Netsparker - Uygulama

- Web uygulama güvenlik tarama aracı
- Lisanslı ve Free sürümleri mevcut
- Web teknolojileri özelinde geliştirilmiş bir yazılım.
- Netsparker Cloud ile birlikte daha gelişmiş ve entegre çözüm



File Home View Reporting Help Sign-in to Cloud

New Schedule Incremental Schedule Incremental New Instance Import Export Scan Policy Editor Report Policy Editor Options

Start Scan Scan Session Tools

Welcome

Netsparker

Updates

We release an update for Netsparker Desktop every month. Updates include new security checks, new features and bug fixes. Click on the below links to view:

- [Netsparker Scanners Release Announcements](#)
- [Netsparker Desktop changelog](#)

Web Application Security Blog

- [Sumeru Solutions – Netsparker Case Study](#)
- [Netsparker To Exhibit at OWASP AppSec EU 2018 in London](#)
- [May 2018 Netsparker Update – New plans, UI & Single Sign-on Support](#)
- [Netsparker Plans & Editions Integration](#)
- [Netsparker and Single Sign-On Support](#)

Support and Resources

Should you have any queries please do not hesitate to [get in touch with us](#). Below are also some useful links you can refer to:

- [Support page](#)
- [FAQs](#)
- [Netsparker videos](#)

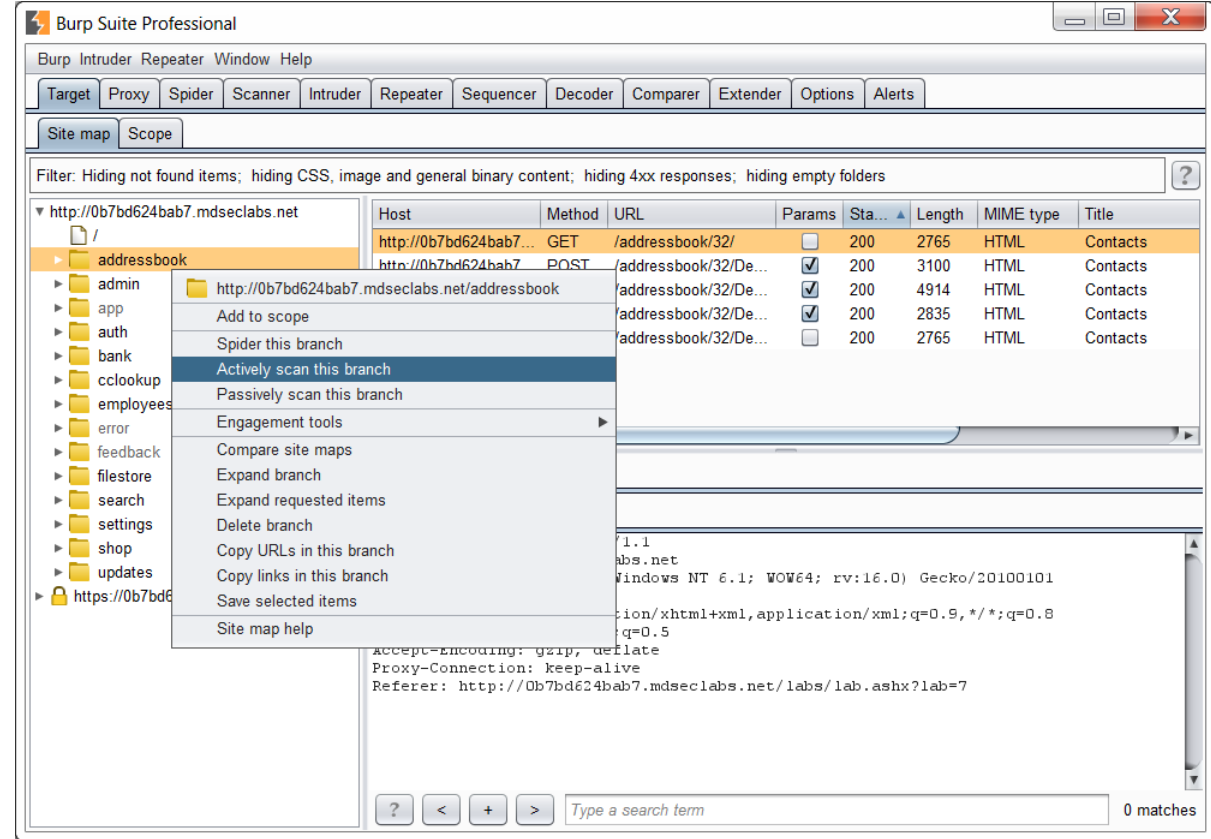
Follow Us on Social Media

Follow us on any of our social media channels to keep yourself up to date with what is happening in the world of web application security and Netsparker.

Netsparker is ready to go!

Burpsuite - Uygulama

- Web uygulama Proxy aracı ve Güvenlik Tarayıcısı
- Lisanslı ve Free sürümü var
- Web teknolojileri özelinde
- En kullanışlı araç
- Hackerların, Pentesterların eli kolu



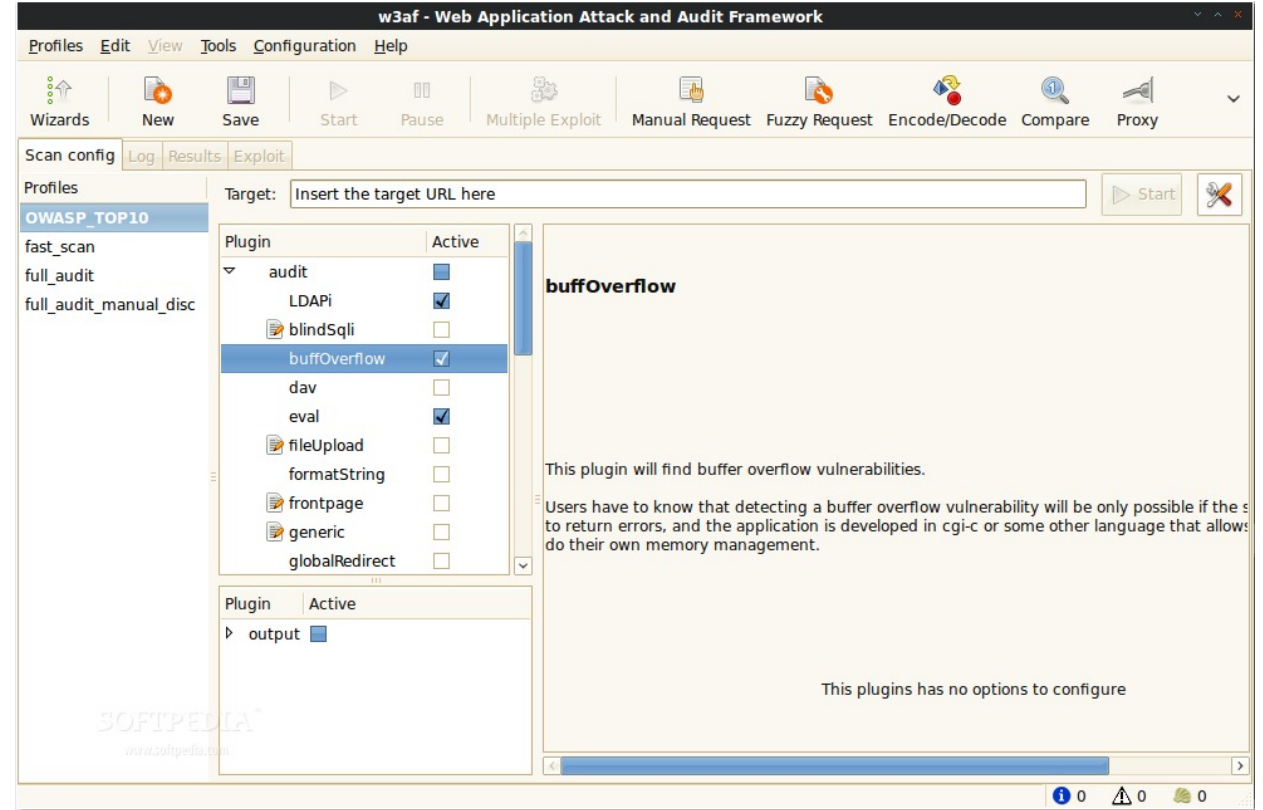
Nikto Security Scanner - Uygulama

- Web uygulama ve sunucu güvenlik tarayıcısıdır.
- Sık kullanılan pratik bir uygulamadır.
- Komut satırı üzerinden kullanılır.

```
root@PRISMACSI: ~  
File Edit View Search Terminal Help  
root@PRISMACSI:~# nikto -h  
Option host requires an argument  
  
-config+      Use this config file  
-Display+    Turn on/off display outputs  
-dbcheck     check database and other key files for syntax errors  
-Format+    save file (-o) format  
-Help       Extended help information  
-host+      target host  
-id+        Host authentication to use, format is id:pass or id:pass:realm  
-list-plugins List all available plugins  
-output+    Write output to this file  
-nossll     Disables using SSL  
-no404      Disables 404 checks  
-Plugins+   List of plugins to run (default: ALL)  
-port+      Port to use (default 80)  
-root+      Prepend root value to all requests, format is /directory  
-ssl        Force ssl mode on port  
-Tuning+    Scan tuning  
-timeout+   Timeout for requests (default 10 seconds)  
-update     Update databases and plugins from CIRT.net  
-Version    Print plugin and database versions
```

W3af Web Scanner - Uygulama


- Web uygulama güvenlik tarayıcısıdır.
- OWASP tarafından geliştiriliyor.
- İçinde politikalar mevcut ve özelleştirilmiş taramalar yapılabiliyor.
- Sık kullanılsa da oldukça kullanışlıdır.





Sqlmap – SQL Injection Scanner – Uygulama

- SQL Injection saldırıları için özel olarak geliştirilmiştir.
- Python programlama dili ile geliştirilmekte
- Açık kaynak
- Gelişmiş parametrelere ve atak methodlarına sahip

```
root@PRISMACSI: ~  
File Edit View Search Terminal Help  
root@PRISMACSI:~# sqlmap -h  
 {1.2.6#stable}  
http://sqlmap.org  
Usage: python sqlmap [options]  
Options:  
-h, --help          Show basic help message and exit  
-hh                Show advanced help message and exit  
--version          Show program's version number and exit  
-v VERBOSE        Verbosity level: 0-6 (default 1)  
Target:  
At least one of these options has to be provided to define the target(s)  
-u URL, --url=URL  Target URL (e.g. "http://www.site.com/vuln.php?id=1")  
-g GOOGLEDORK     Process Google dork results as target URLs  
Request:
```



Zafiyetler sadece uzaktan mı kontrol edilir?

- Bir tarama sadece uzaktan web uygulamasına yönelik veya bir sunucuya yönelik gerçekleştirilmek zorunda değil.
- Aynı zamanda bir sunucunun içerisine giriş yaparak işletim sistemi özelinde de tarama gerçekleştirilebilir. (RDP, SSH login → içeride tarama)
- Uyumluluk veya konfigürasyon kontrolleri gerçekleştirilebilir
- Statik kod analizi gerçekleştirilebilir

Sonuç olarak:

- **Elimizde en başta topladığımız bir çok istihbarat verisi var.**
- **Artık karşımızda var olan ve ayakta olan sistemleri tanıyoruz.**
- **Bu sistemlerde açık portları keşfettik ve bu portlar üzerinde çalışan yazılımları biliyoruz.**
- **Bu yazılımlar üstünde çalışan uygulamalarda var olan veya servisler üzerinde keşfettiğimiz açıklıkları da kenara not ettik.**
- **Şimdi sırada bu zafiyetleri nasıl kullanacağımızı kavramakta!**



UYGULAMALAR



SORULAR?