

DANIEL PROJECT

TO: Lior barash

subject: web hacking scanners

Softwares:

VEGA

OWASP

NESSUS

Description:

Web Application Vulnerability Scanners are automated tools that scan web applications, normally from the outside, to look for security vulnerabilities such as Cross-site scripting, SQL Injection, Command Injection, Path Traversal and insecure server configuration



VEGA

Vega is a free way security scanner for testing the security of web application, this tool can help you find vulnerability such as SQL injections, cross site scripting blind sequer injections and more... Vega is written in JAVA and runs on LINUX and WINDOWS, but for this tutorial we go work with WINDOWS VERSION.

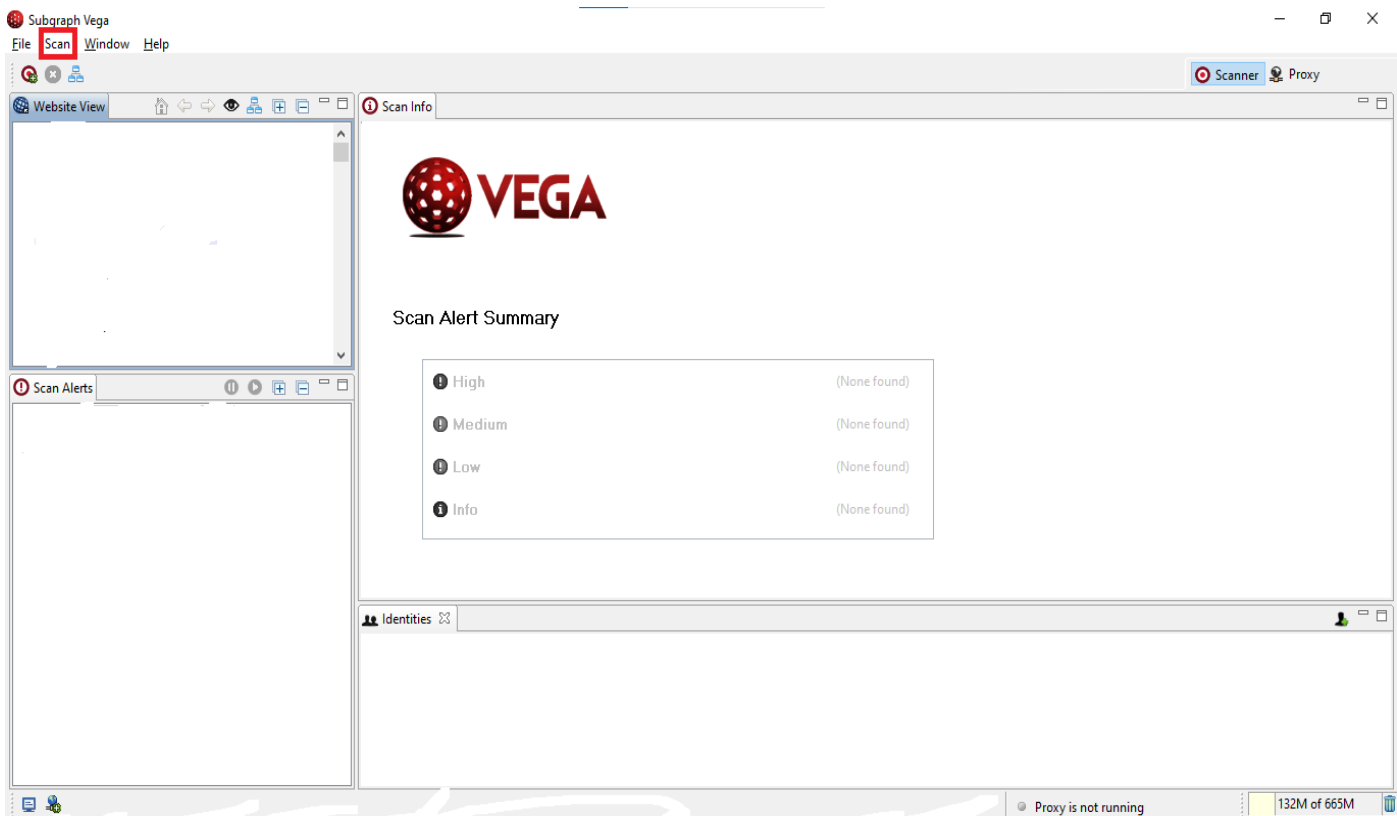
Open Source tools Advantages:

- Ease of installation and upgrade
- Bug Fixes
- Good documentation
- Development supported by large community
- free


Open Source tools Disadvantages:

- app can fall down if you scan big website
- Sometimes “mono” platform (Sponsored by Microsoft, Mono is an open source implementation of Microsoft's)

Step 1; in order to scan with “vega” you will need to select the “scan” symbol in the up




Step 2: after you select this you will chose the “START NEW SCAN” and you will enter the “URI” and you will enter the name of the web site you want to scan.



Select a Scan Target

Enter a target URI



Scan Target

☒ Enter a base URI for scan:

Enter URI to scan

☐ Choose a target scope for scan

New Scope

Edit Scopes

Web Model

☒ Include previously discovered paths from Web model

< Back

Next >

Finish

Cancel


Step 3 : after that you have 2 options

- hit finish and you scan all the website
- hit the “NEXT” button and choose the specific scan you want to see

this shows us the scanning options we have if we choose the the “NEXT” button

Select Modules

Choose which scanner modules to enable for this scan



Select modules to run:

☒ Injection Modules

☒ Eval Code Injection

☒ Shell Injection Checks

☒ Blind SQL Text Injection Differential Checks

☒ Blind SQL Injection Arithmetic Evaluation Differential Checks

☒ XML Injection checks

☒ XSS Injection checks

☒ Bash Environment Variable Blind OS Injection (CVE-2014-6271, CVE-2014-6278) Checks

☐ Blind SQL Injection Timing

☒ Remote File Include Checks

☐ Blind XPath Injection Checks

☒ HTTP Trace Probes

☒ HTTP Header Injection checks

☒ URL Injection checks

☒ Local File Include Checks

☐ Format String Injection Checks

☐ Blind OS Command Injection Timing

☐ Integer Overflow Injection Checks

☒ Cross Domain Policy Auditor

> ☒ Response Processing Modules

Select Modules

Choose which scanner modules to enable for this scan

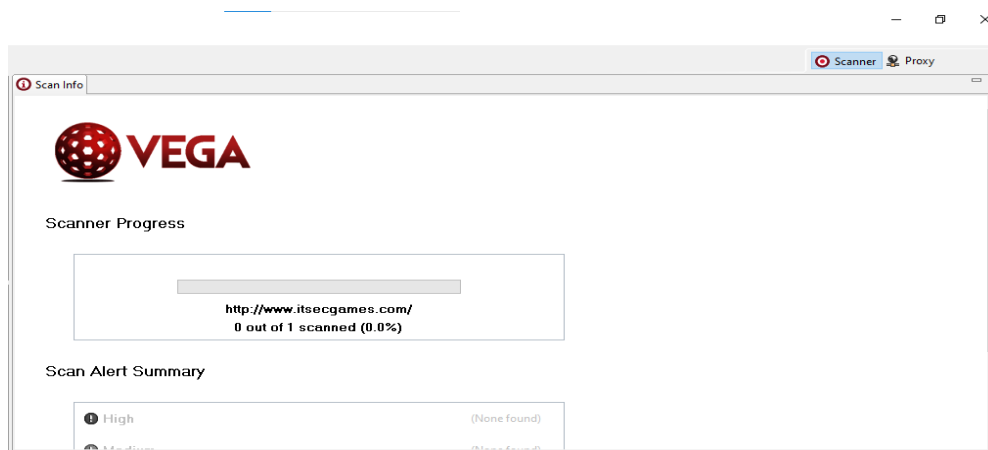


Select modules to run:

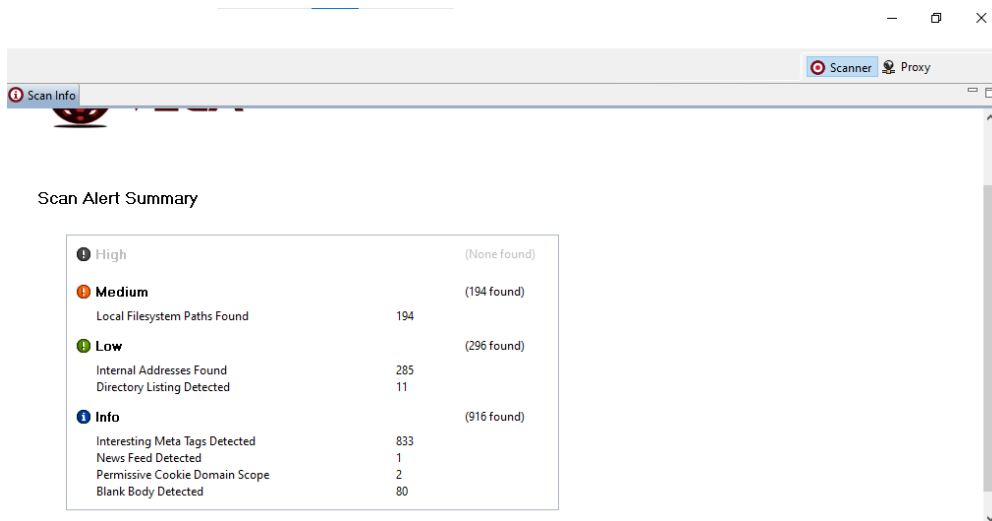
- ☒ Response Processing Modules
 - ☒ Version Control String Detection
 - ☒ Cookie Security Module
 - ☒ Unsafe Or Unrecognized Character Set
 - ☒ Cleartext Password Over HTTP
 - ☒ Path Disclosure
 - ☒ Interesting Meta Tag Detection
 - ☒ AJAX Detector
 - ☐ Social Security/Social Insurance Number Detector
 - ☐ X-Frame Options Header Not Set
 - ☐ E-Mail Finder Module
 - ☒ RSS/Atom/OPL Feed Detector
 - ☒ HTTP Header Checks
 - ☒ HTTP Authentication Over Unencrypted HTTP
 - ☒ Insecure Cross-Domain Policy
 - ☒ Source Code Disclosure Module
 - ☒ Insecure Script Include
 - ☒ Error Page Detection
 - ☒ Oracle Application Server Fingerprint Module
 - ☒ WSDL Detector
 - ☒ Form autocomplete
 - ☒ File Upload Detection
 - ☒ Cookie Scope Detection
 - ☒ Character Set Not Specified
 - ☒ Empty Response Body Module
 - ☒ Internal IP Addressess

In my exhibition ill show you the option of scanning all the scening options in a vulnerable site for scanning

In start of the scan it will look like this



it can take a while but after after is finished it will look like this :



we have the:

*high- shows us that the chances of hacking are more high

* medium- shows us that the chanes are 50% 50%

*low- shows us that the chances are low and that mean almost impossible

*info- shows us that Vega has detected that requesting this URI returned a blank response body. and this may be indicative of an error condition and should be manually investigated further

Summary

Exploring all Vega features can make the article a book but with this little exercise we can see that Vega showed itself an extraordinary web scanner tool that can be useful for directing and

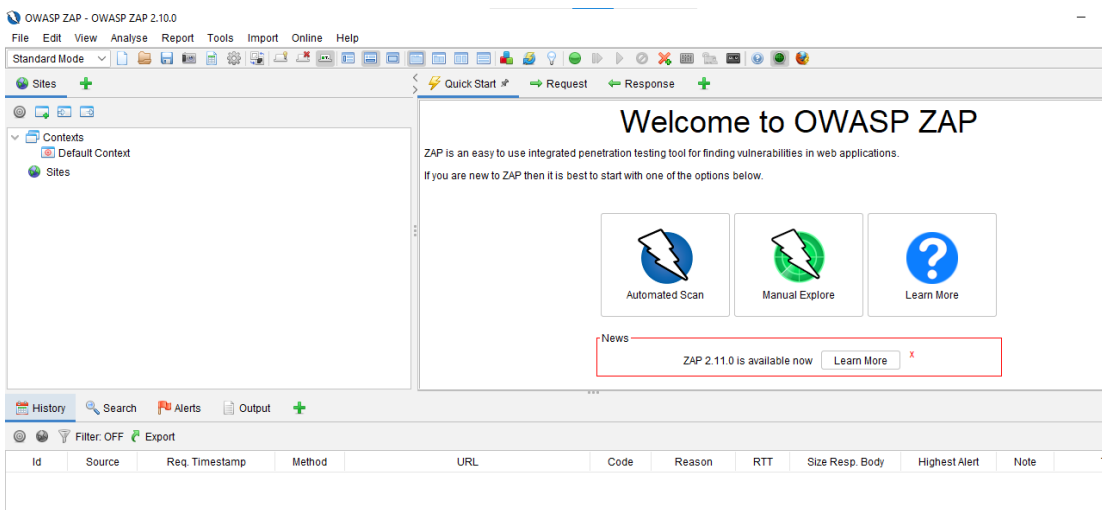
analyzing vulnerabilities in web environment. It requires some to deal with results by interpreting them correctly.

OWASP ZAP (zed attack proxy)

The OWASP ZAP ATTACK PROXY is one of the most popular free security tools . It can help you automatically find security vulnerabilities in you web applications (more popular used by developers that run sites and apps)

Owasp zap is an open source web application security scanner.

It is intended to be used by both those new to the application security as well as professional testers. When used as proxy server it allows the user to manipulate all of the traffic that passes through it, including traffic using “HTTPS”. This platform tool is written in “JAVA” and is available in all of the popular operating systems such as “Microsoft Windows”, “Linux”, and “Mac”

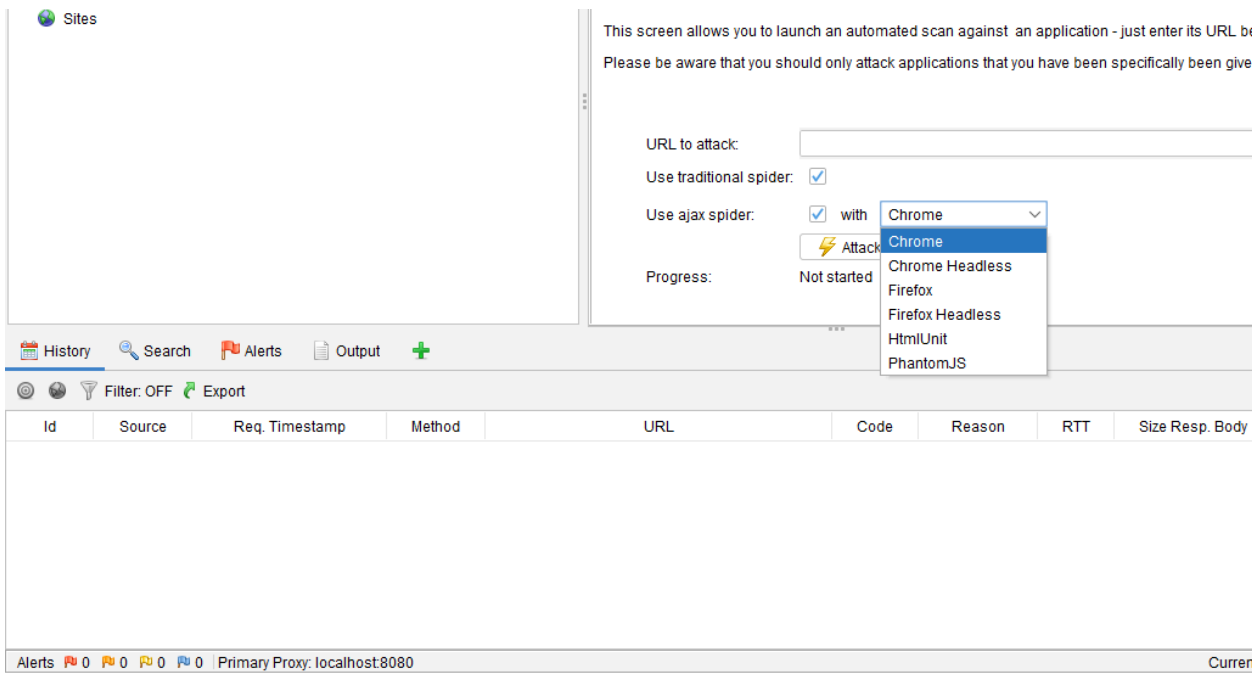


step 1: enter the app

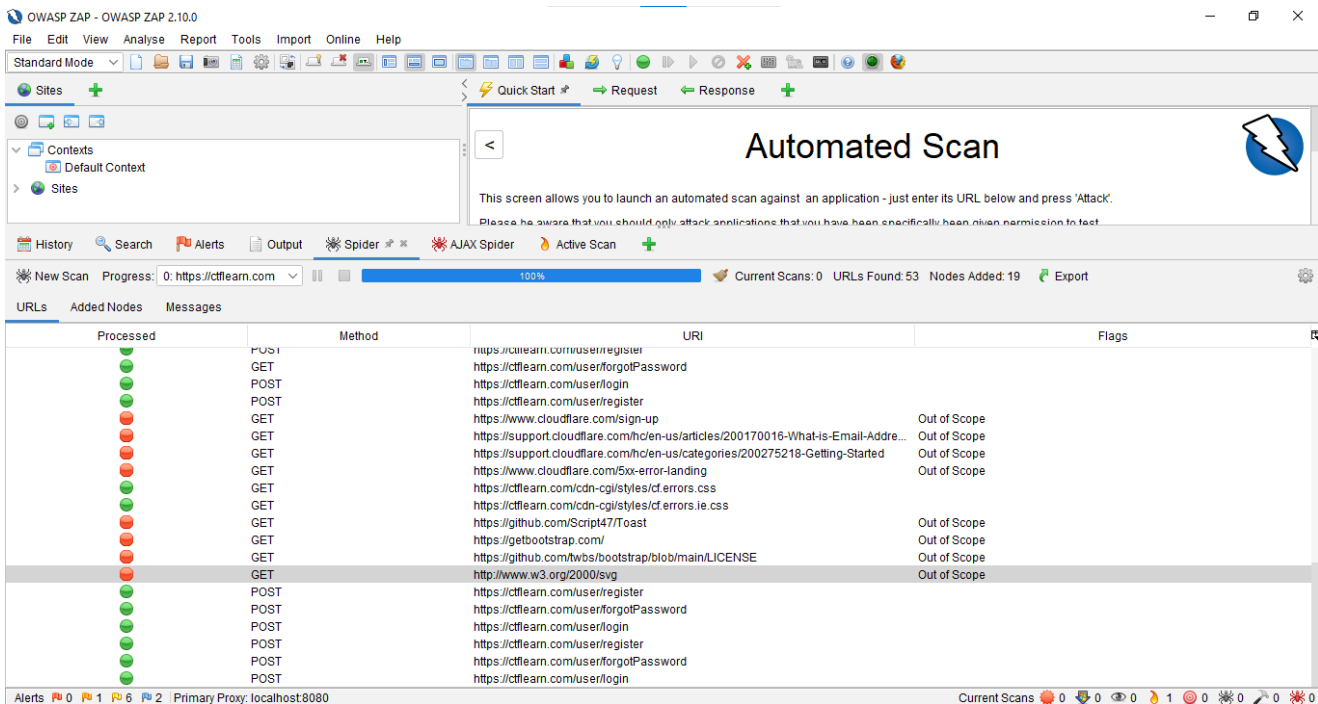
and the home screen will look like this:

1.1 for this tutorial we will choose the “Automated Scan”

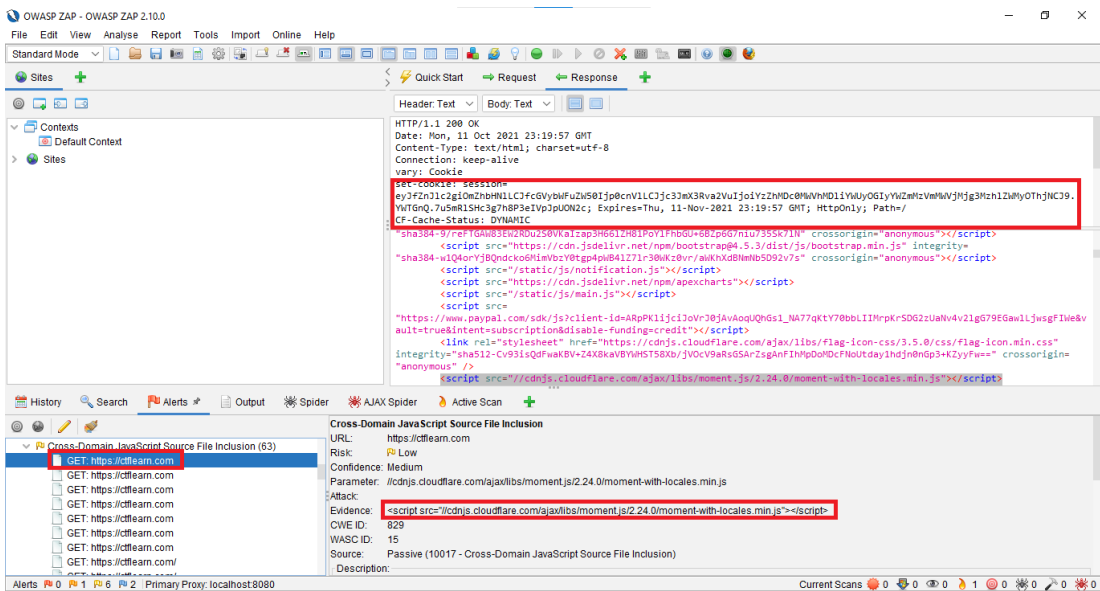
step 2: enter the “URL to attack” you want to scan and on “ajax spider” you can choose on which “web source” you want to scan and after that press “Attack”



step 3: It will automatically scan the web you chose and generate the alert report with list of possible vulnerabilities for your application



step 4: After exploring any of the vulnerabilities from the site the scanner will show us details of the vulnerabilities and also shows us the affected area by showing us the code in below



4.1 it will also provide detailed description of the vulnerabilities and solution to prevent that attack as shown in below

Solution:

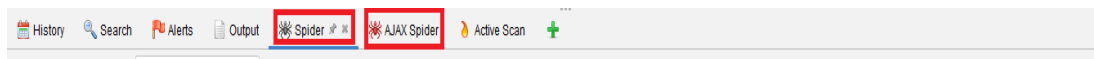
Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

Reference:

Current Scans 0 0 0 0 0

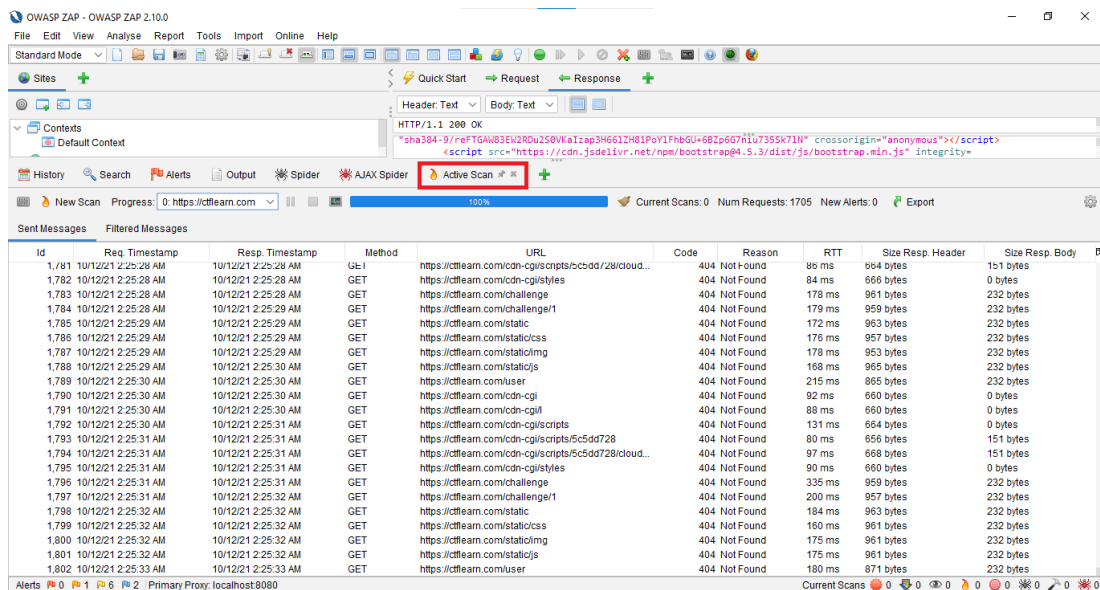
spider: the spider explores automatically the structure of web application with the list of all “URL” resources found. for each “URL” the OWASP ZAP creates a request to get the resources and then parses the response.

AJAX SPIDER: add on integrates in OWASP ZAP a crawler of “AJAX SPIDER” rich sites call “Crawljax” you can use it to identify the pages of the targeted site. you can combine it with the “normal” “spider” for better results



Active Scan:

active scanning attempts to find security holes by symbolizing real known attacks against targets in web applications. Active scanning provides a list of vulnerabilities and combined with “spider” and the scan, It can show you all the vulnerabilities OWASP ZAP can recognise including high risk vulnerabilities.



Advantages:

- list of all possible vulnerabilities
- scan all the pages of the “URL” you want and highlighting the affected area of the code vulnerability
- OWASP ZAP tool is very fast for scanning

Disadvantages:

- lack of control over connections to the system
- not much of proper validation and encoding of data sent

conclusion: In this tutorial we have seen what OWASP ZAP works in the automatic manual as we also see type of active scanning process.

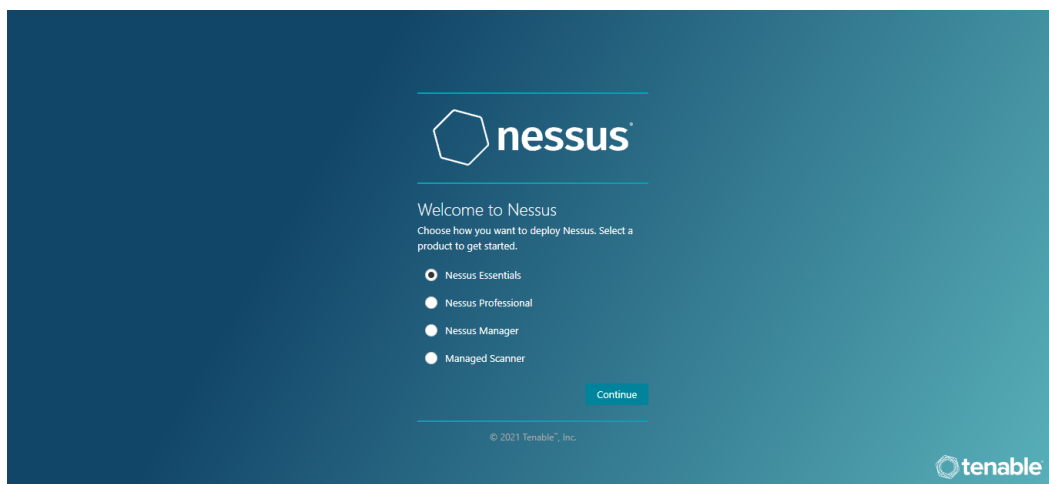
NESSUS

Nessus is an open source **network** vulnerability scanner that uses common vulnerabilities and exposures architecture for easy cross linking between compliant security tools.

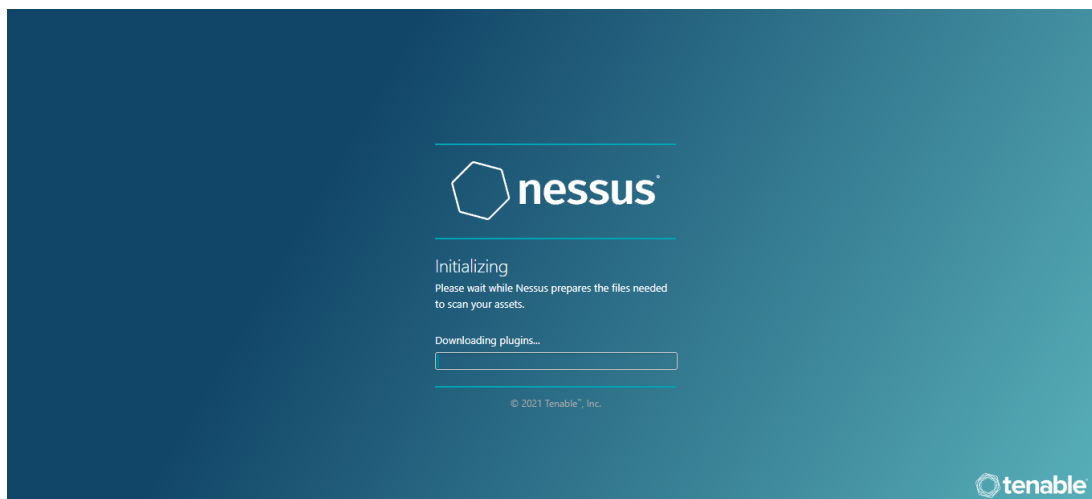
Nessus scanner should be placed in each network segment. Nessus requires port TCP/8834

Because Nessus is an open source network scanner the big difference with this tool compared to the other scanners we see before that is that when you download nessu from their site and you open the app its jumps to a web (in my case MICROSOFT EDGE) and you can scan from there, not like the tools we've seen before that

for this tutorial we will choose the “nessus essentials” because its the free version

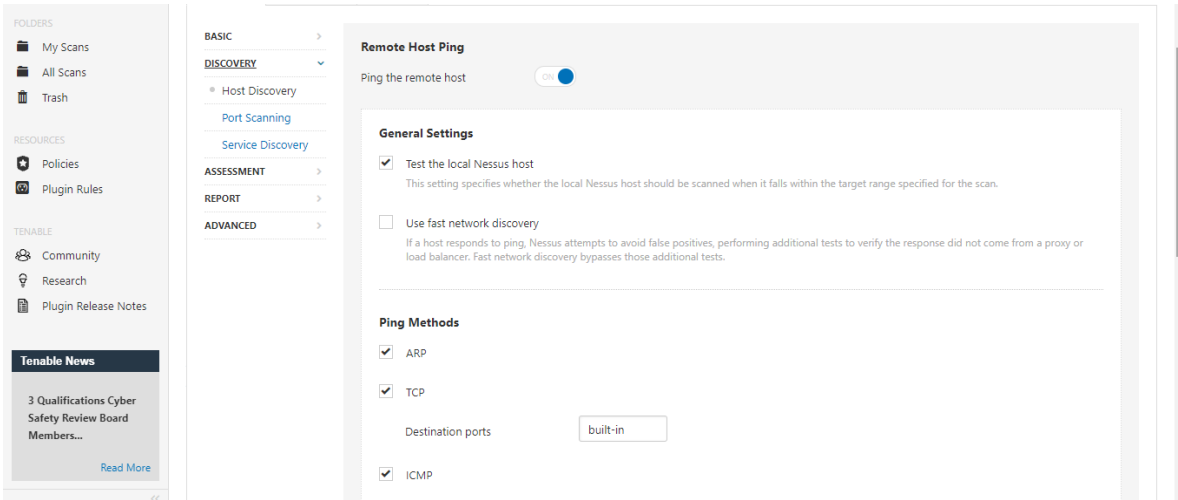


after that we will need to create our account for nessus for entering the scanner (“user name”, ”last name”, ”email”) after you will finish this steps it will send you a password to your email to verify your account.and the last thing it will download the web vulnerability scanner (10-30 min)



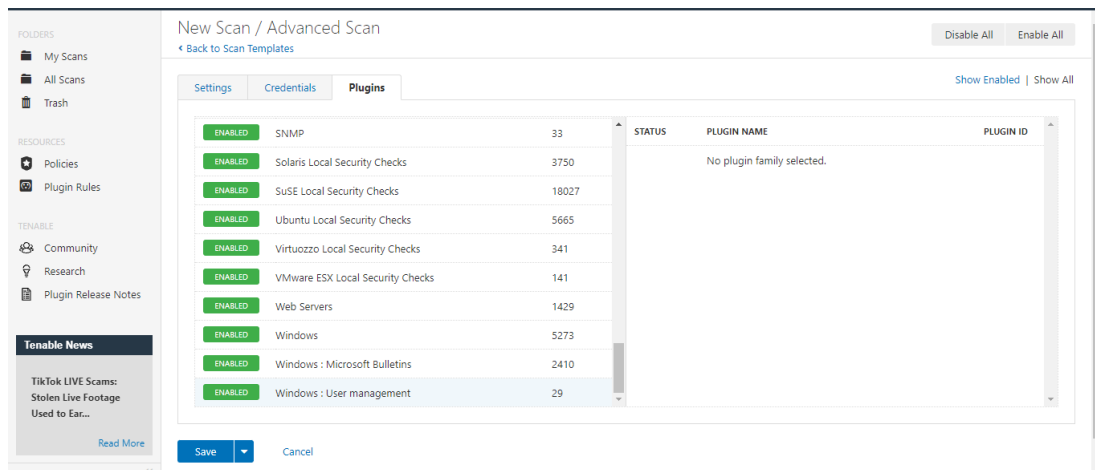
***The nessus scanner have “essential version” it can scan 16 IP addresses at one time, that means it can scan 16 machines in one scan**

Advanced scan: when you enter the “advanced scan” its going to give you options in there to choose essentially or policy to put together for future scans (name a policy descriptions test). you can see its going to ping “arp” and “tcp” and “icmp” (“udp” is off) we can also choose the range of scanning we want. but for this case we will stick with the “default” range



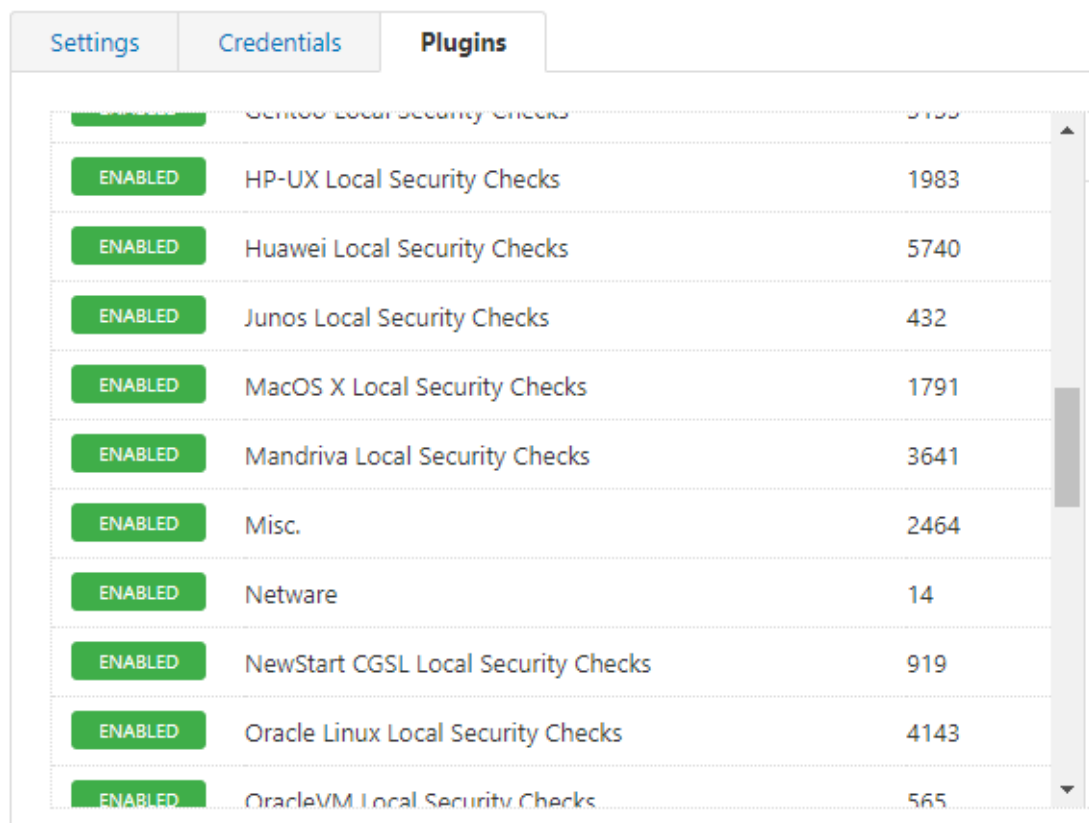
***service discovery: we can go within as well if we need credentials to log into a system**

***plugins: we can also go for plugins and by default these are all enabled. at the bottom we one that are associated specifically with “windows” we have also one ubuntu and mac ox and many more, you can pick and choose what you want to enable and disable.**



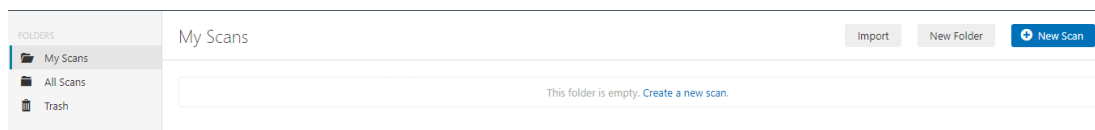
New Scan / Advanced Scan

◀ Back to Scan Templates

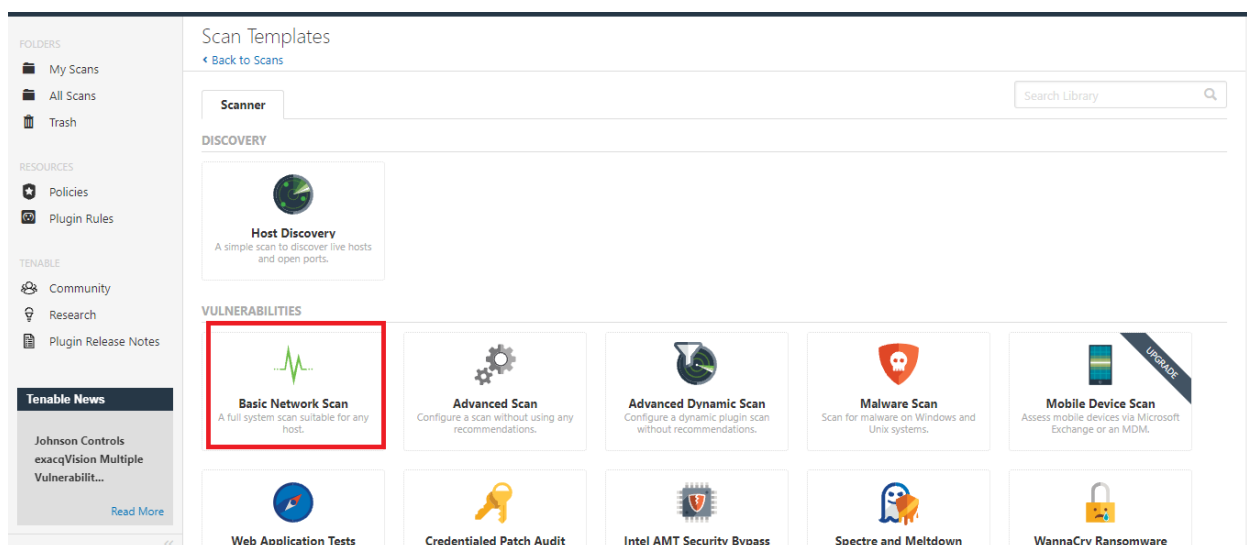


in the assessment, report, and advanced it gives you options as well but were not going to touch this

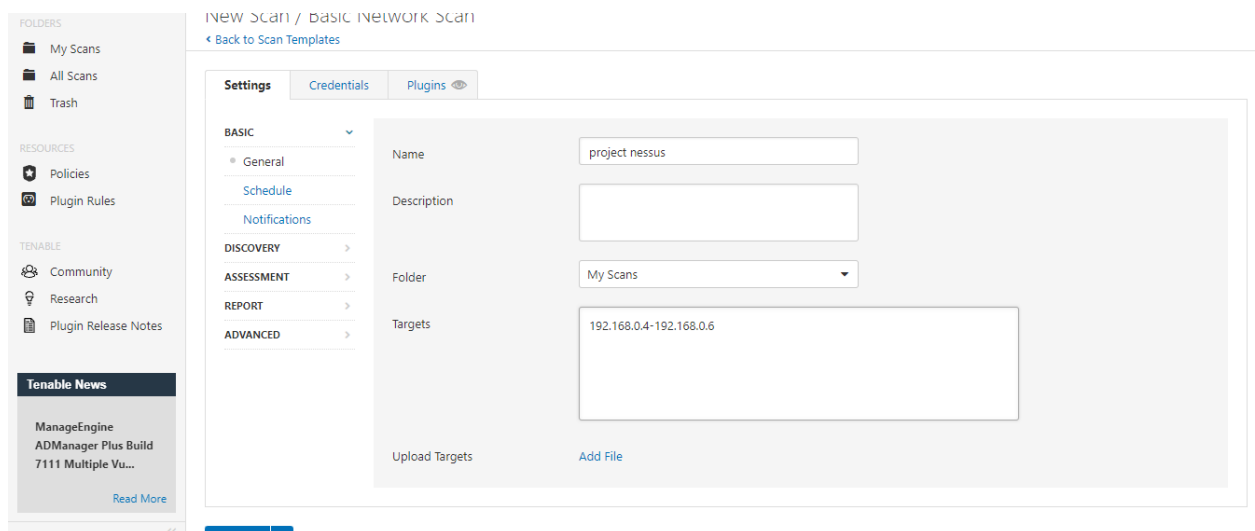
Step 1: tap and the neesus symbol and it will show you on the upper right the option of “New scan”



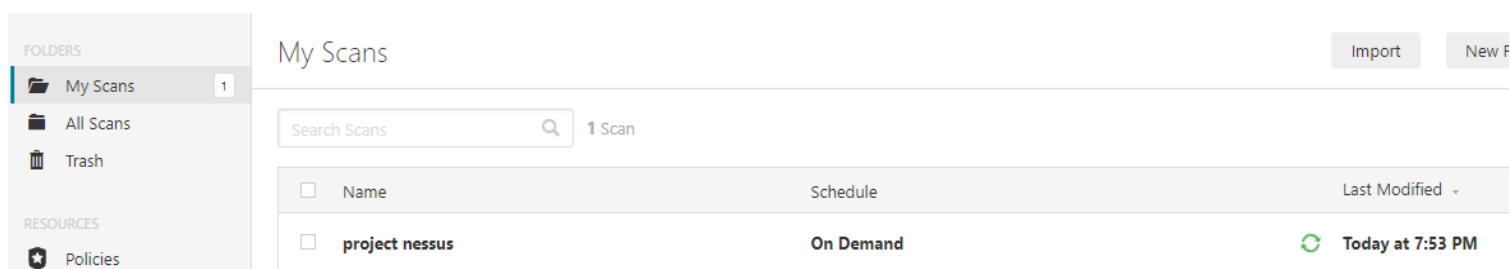
step 2: we going to choose the “basic network scan”



step 3: for this exemple i'm going to name the name the scan “project nessus” and for the target we going to scan is going to be the IP 192.168.0.4-192.168.0.6 you can write it like this or you can add them one by one in different lines and LET'S LUNCH THE MACHINE !!!



STEP 4: The scan will show up under the area of “my scans” and it shows you its running you can also choose the option of stoping it or “pause” it



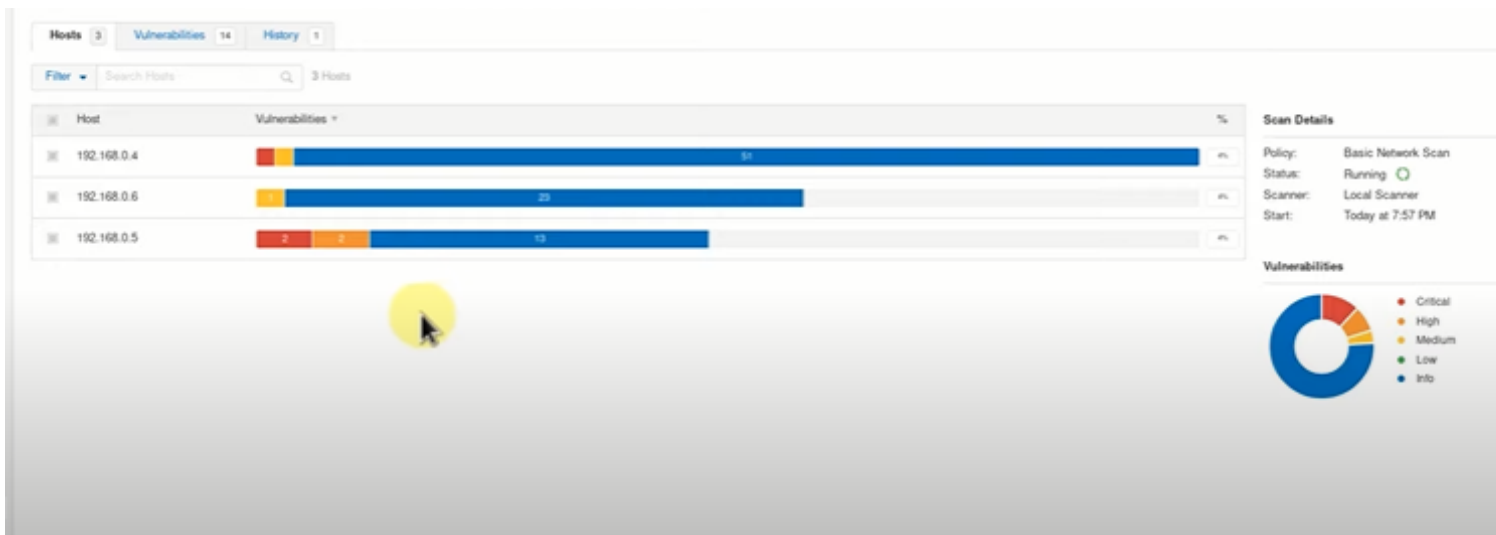
STEP 4.1 we will click into the scan and we can look at the vulnerabilities while this is running we can see our 3 hosts

RED-critical vulnerability

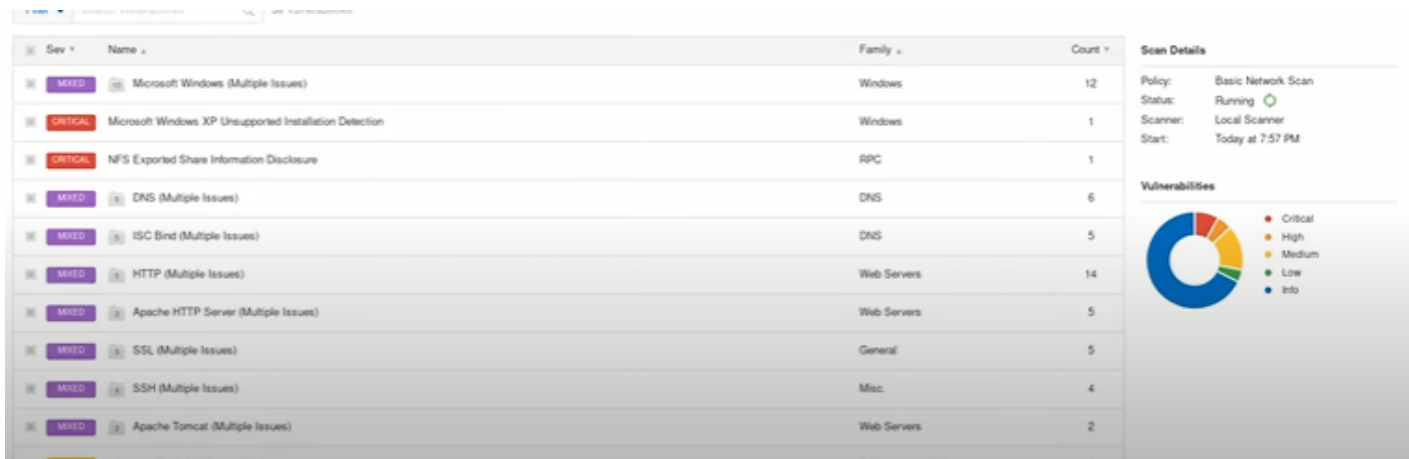
ORANGE- high vulnerability

GREEN-low vulnerability

BLUE-info



Step 5: after the scan is complete we can see the different vulnerabilities on every ip dot



We can see the vulnerabilities of the scan/ if you select specific IP dot it will breakdown these vulnerabilities of this specific scan

MIXED- “mixed” is typically going to show us a combination of different vulnerabilities of high and critical, medium and low vulnerabilities

If you enter one of the vulnerabilities it will show you the description and solution, also you can go to the website and brows it and it can show us if we can be exploited

Advantages and Disadvantages

Advantages:

Ease for use

Live result

built in templates

Disadvantages:

cost money for some of the scanners

nessus	owasp zap	vega
Platforms Supported Windows: ✓ Mac: ✗ Linux: ✗ SaaS: ✓ iPhone: ✗ iPad: ✗ Android: ✗	Platforms Supported Windows: ✓ Mac: ✓ Linux: ✓ SaaS: ✗ iPhone: ✗ iPad: ✗ Android: ✗	Platforms Supported Windows: ✓ Mac: ✗ Linux: ✓ SaaS: ✗ iPhone: ✗ iPad: ✗ Android: ✗
Support Business Hours: ✗ 24/7 Live Support: ✗ Online: ✗	Support Business Hours: ✗ 24/7 Live Support: ✗ Online: ✓	Support Business Hours: ✓ 24/7 Live Support: ✗ Online: ✓
Pricing Free Version: ✗ Free Trial: ✓	Pricing Free Version: ✓ Free Trial: ✓	Pricing Free Version: ✓ Free Trial: ✓
Training Documentation: ✗ Webinars: ✗ Live Online: ✗ In Person: ✗	Training Documentation: ✓ Webinars: ✗ Live Online: ✗ In Person: ✗	Training Documentation: ✓ Webinars: ✗ Live Online: ✗ In Person: ✗
Company Information Tenable Founded: 2002 United States www.tenable.com/products/nessus	Company Information OWASP Founded: 2001 United States www.zaproxy.org	Company Information Subgraph Founded: 2010 Canada subgraph.com/vega/

Categories Cyber Risk Management Network Monitoring Network Security Penetration Testing Vulnerability Management Vulnerability Scanners	Categories Application Security Penetration Testing	Categories Vulnerability Scanners