NAME/ID : ABDELKAREEM YOUSEF MAMDOH SOUBAR/19110022
SUBJECT : SECURITY LAB
ASSIGNMENT INCLUDES : SECURITY LAB (PART 1,2)
DEAD LINE : 9/1/2022

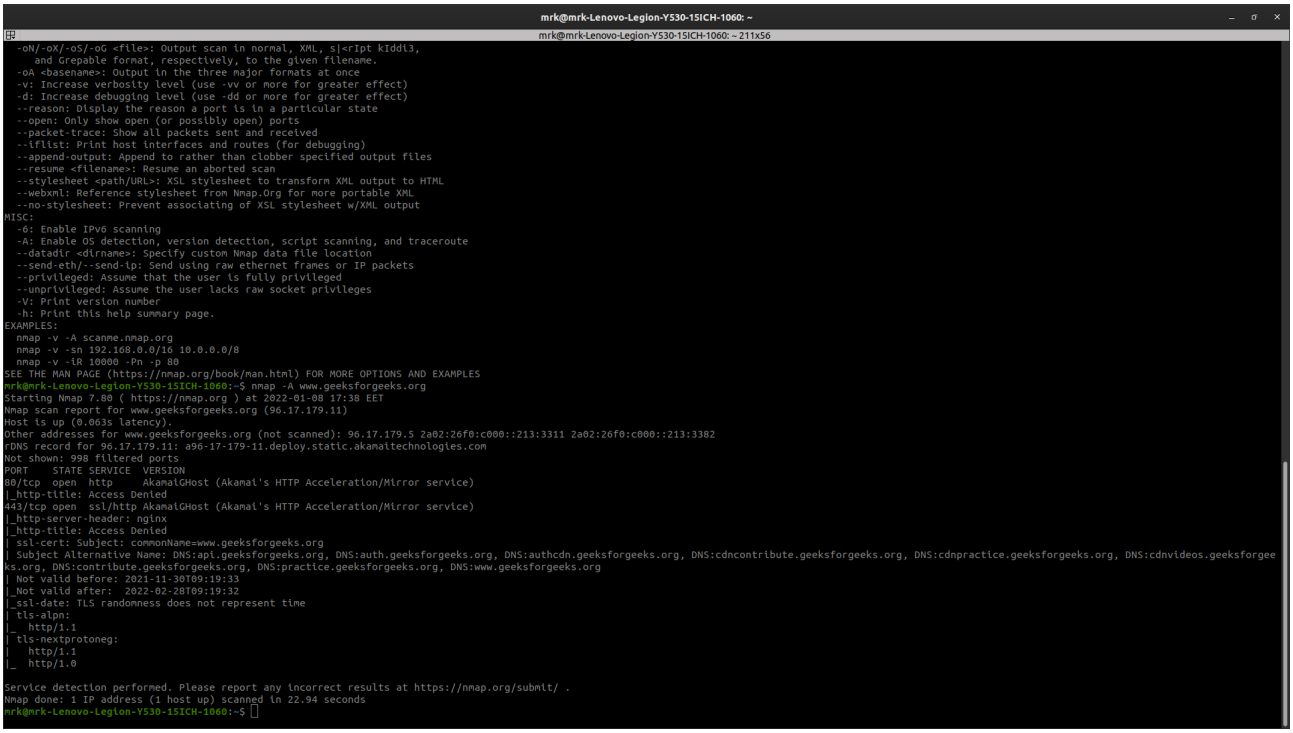
Website	Public IP	Reverse DNS
https://www.geeksforgeeks.org/	34.218.62.116	ec2-34-218-62-116.us-west-2.compute.amazonaws.com

Domain details

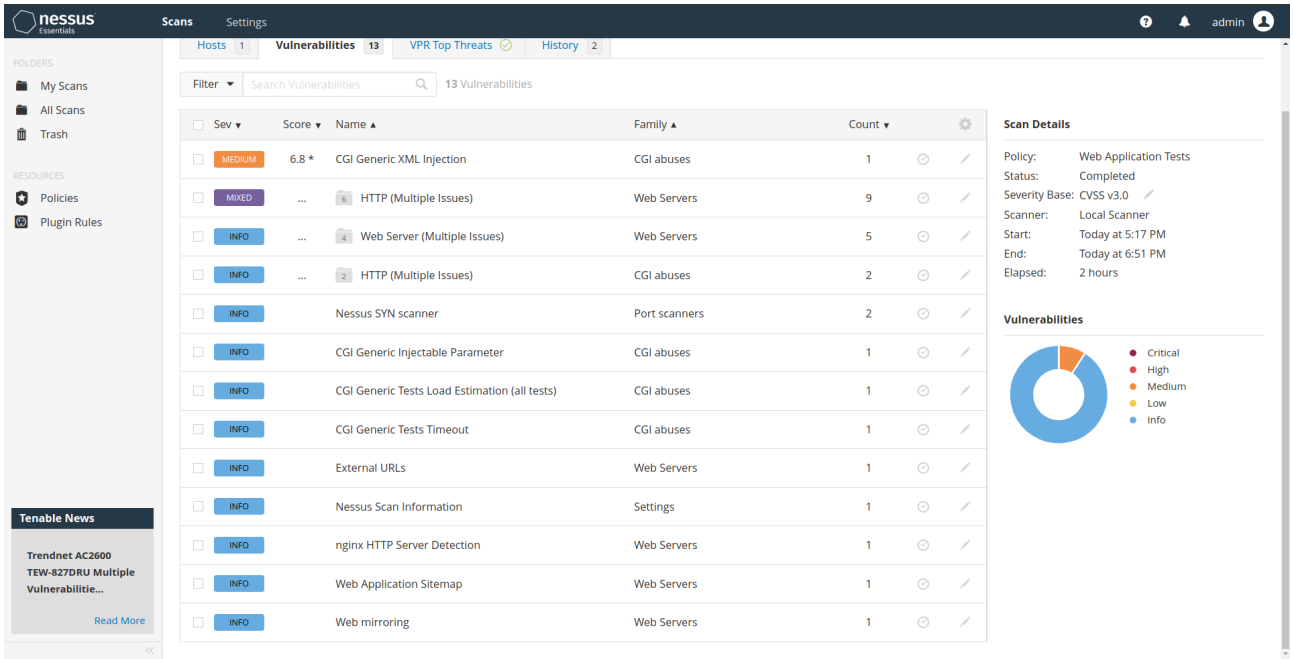
Domain Extension	org
Organization	Non-profit Organizations
TLD Type	Generic
Domain Name	geeksforgeeks.org
Title	GeeksforGeeks | A computer science portal for geeks
Description	A Computer Science portal for geeks. It contains well written, well thought and well explained computer science and programming

	articles, quizzes and practice/competitive programming/company interview Questions.
Nameservers	ns-245.awsdns-30.com, ns-869.awsdns-44.net, ns-1520.awsdns-62.org, ns-1569.awsdns-04.co.uk

it basically a website that provides a free tutorials tons of articles plus online classroom and from time to time coding competitions, and its capable of giving internship, job opportunities.
Nmap scan



nessus



risk	HSTS Missing From HTTPS Server (RFC 6797)	CGI Generic XML Injection
Port	443 / tcp / www	443 / tcp / www
Hosts	www.geeksforgeeks.org	www.geeksforgeeks.org
Output	The remote HTTPS server does not send the HTTP "Strict-Transport-Security" header.	Using the GET HTTP method, Nessus found that : + The following resources may be vulnerable to XML injection : + The 'ref' parameter of the /csharp-programming-language/ CGI :
Risk Factor	CVSS v3.0 Base Score 6.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N CVSS v2.0 Base Score: 5.8 CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N	CVSS v2.0 Base Score: 6.8 CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P
Description	The remote internet server isn't implementing HSTS, as outlined by RFC 6797. HSTS is associate degree elective response header that may be organized on the server to instruct the browser to solely communicate via HTTPS. the dearth of HSTS permits downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.	By causation specially crafted parameters to 1 or additional CGI scripts hosted on the remote net server, Nessus was ready to get a really completely different response, that suggests that it's going to are ready to modify the behavior of the appliance and directly access a SOAP back-end. An assailant is also ready to exploit this issue to bypass authentication, scan confidential knowledge, modify the remote information, or maybe head of the remote software package. Exploitation of XML injections is sometimes faraway from trivial. Note that this script is experimental and will be at risk of false positives particularly, if a PHP application uses 'strip_tags()' to sanitize user input.
Solution	Configure the remote web server to use HSTS.	Modify the affected CGI scripts so they properly escape arguments, particularly XML tags and special characters (angle brackets and slashes).

Common Vulnerabilities and Exposures (CVE)

CVE List was founded by MITRE in 1999 and it was community base project.

NVD (U.S National Vulnerability Database) was founded by NIST(National Institute of Standards and Technology) in 2005.

CVE is basically a list of recorders etch one of them has identification number and a description plus one public reference for public in the Cybersecurity community and a CVE record is use around the world with a huge request over it including the NVD.

NVD is built upon and synchronized fully with CVE list so if any update come to the CVE it goes to the NVD.

CVE and NVD are both build by the Cybersecurity and Infrastructure Security Agency (CISA), U.S. Department of Homeland Security (DHS) and both are available to the public and free to use.

The site that is related tot his is: https://www.cve.org/