



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

```
mrk@mrk-Lenovo-Legion-Y530-15ICH-1060: ~
nmap -h
nmap -oN /path/to/output: Output scan in normal, XML, sscript kiddi3,
and Greppable format, respectively, to the given filename.
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
--6: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -IR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
mrk@mrk-Lenovo-Legion-Y530-15ICH-1060: ~$ nmap -A www.geeksforgeeks.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-08 17:38 EET
Nmap scan report for www.geeksforgeeks.org (96.17.179.11)
Host is up (0.063s latency).
Other addresses for www.geeksforgeeks.org (not scanned): 96.17.179.5 2a02:2ef0:c000::213:3311 2a02:2ef0:c000::213:3302
DNS record for 96.17.179.11: a96-17-179-11.deploy.static.akamaitechnologies.com
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http    AkamaiGhost (Akanal's HTTP Acceleration/Mirror service)
|_ http-title: Access Denied
443/tcp   open  ssl/http AkamaiGhost (Akanal's HTTP Acceleration/Mirror service)
|_ http-server-header: nginx
|_ http-title: Access Denied
|_ ssl-cert: Subject: commonName=www.geeksforgeeks.org
|_ Subject Alternative Name: DNS:api.geeksforgeeks.org, DNS:auth.geeksforgeeks.org, DNS:authcdn.geeksforgeeks.org, DNS:cdncontribu.geeksforgeeks.org, DNS:cdnpractice.geeksforgeeks.org, DNS:cdnvideos.geeksforgeeks.org, DNS:contribu.geeksforgeeks.org, DNS:practice.geeksforgeeks.org, DNS:www.geeksforgeeks.org
|_ Not valid before: 2021-11-30T09:19:33
|_ Not valid after: 2022-02-28T09:19:32
|_ ssl-date: TLS randomness does not represent time
|_ tls-alpn:
|_   http/1.1
|_   http/1.1
|_   http/1.0
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.94 seconds
mrk@mrk-Lenovo-Legion-Y530-15ICH-1060: ~$
```

nessus

nessus

Essentials

Scans

Settings

Hosts 1

Vulnerabilities 13

VPR Top Threats

History 2

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Tenable News

Trendnet AC2600

TEW-827DRU Multiple Vulnerabilitie...

Read More

Filter

Search Vulnerabilities

13 Vulnerabilities

Sev	Score	Name	Family	Count
MEDIUM	6.8 *	CGI Generic XML Injection	CGI abuses	1
MIXED	...	HTTP (Multiple Issues)	Web Servers	9
INFO	...	Web Server (Multiple Issues)	Web Servers	5
INFO	...	HTTP (Multiple Issues)	CGI abuses	2
INFO	...	Nessus SYN scanner	Port scanners	2
INFO	...	CGI Generic Injectable Parameter	CGI abuses	1
INFO	...	CGI Generic Tests Load Estimation (all tests)	CGI abuses	1
INFO	...	CGI Generic Tests Timeout	CGI abuses	1
INFO	...	External URLs	Web Servers	1
INFO	...	Nessus Scan Information	Settings	1
INFO	...	nginx HTTP Server Detection	Web Servers	1
INFO	...	Web Application Sitemap	Web Servers	1
INFO	...	Web mirroring	Web Servers	1

Scan Details

Policy: Web Application Tests

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 5:17 PM

End: Today at 6:51 PM

Elapsed: 2 hours

Vulnerabilities

Donut chart showing vulnerability distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue)

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 each one of them has identification number and a description plus one public reference for public in the Cybersecurity community and a CVE record is used 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 comes to the CVE it goes to the NVD.

CVE and NVD are both built 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 to this is: <https://www.cve.org/>

