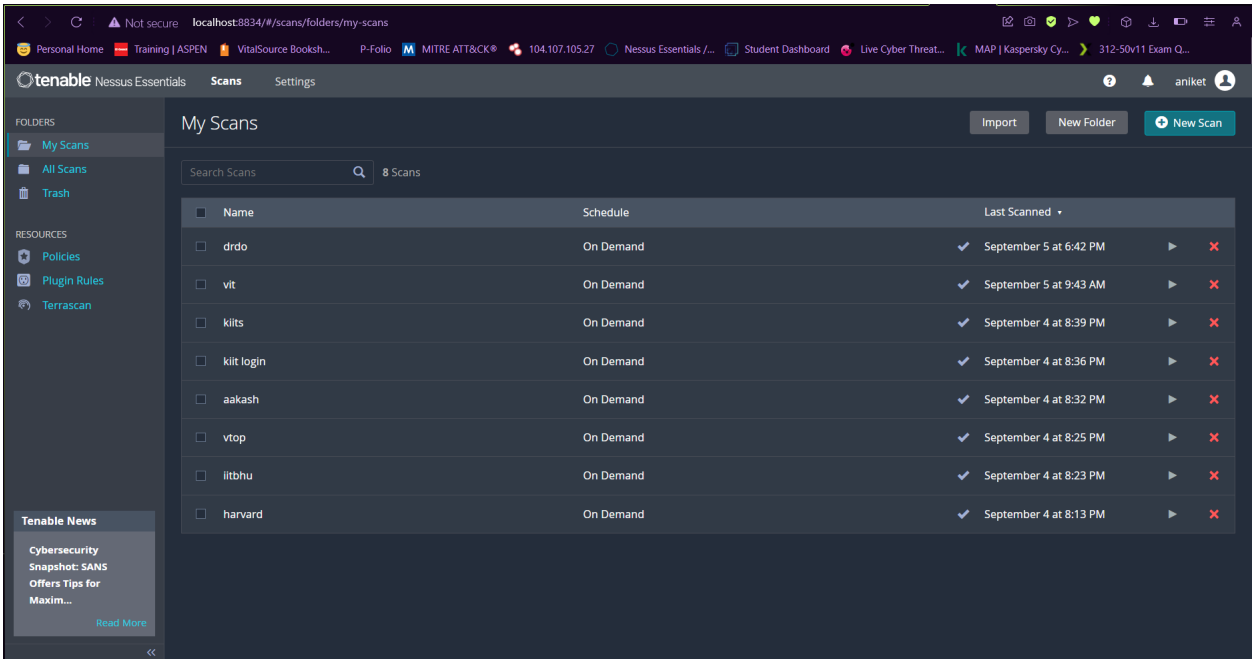
task 8

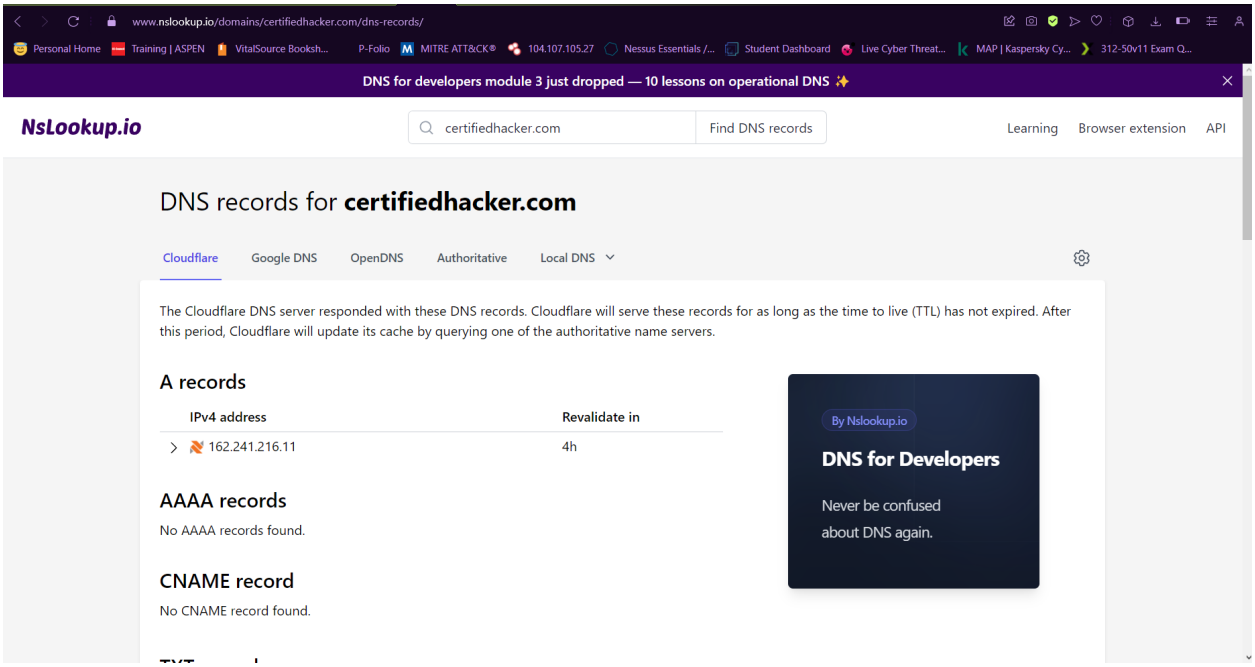
(04/09/23): Scan any website to check the vulnerabilities in the website using nessus and make a report on it

so for scanning of vulnerabilities we will use nessus tool.Nessus is a platform developed by Tenable that **scans for security vulnerabilities in devices, applications, operating systems, cloud services and other network resources**.



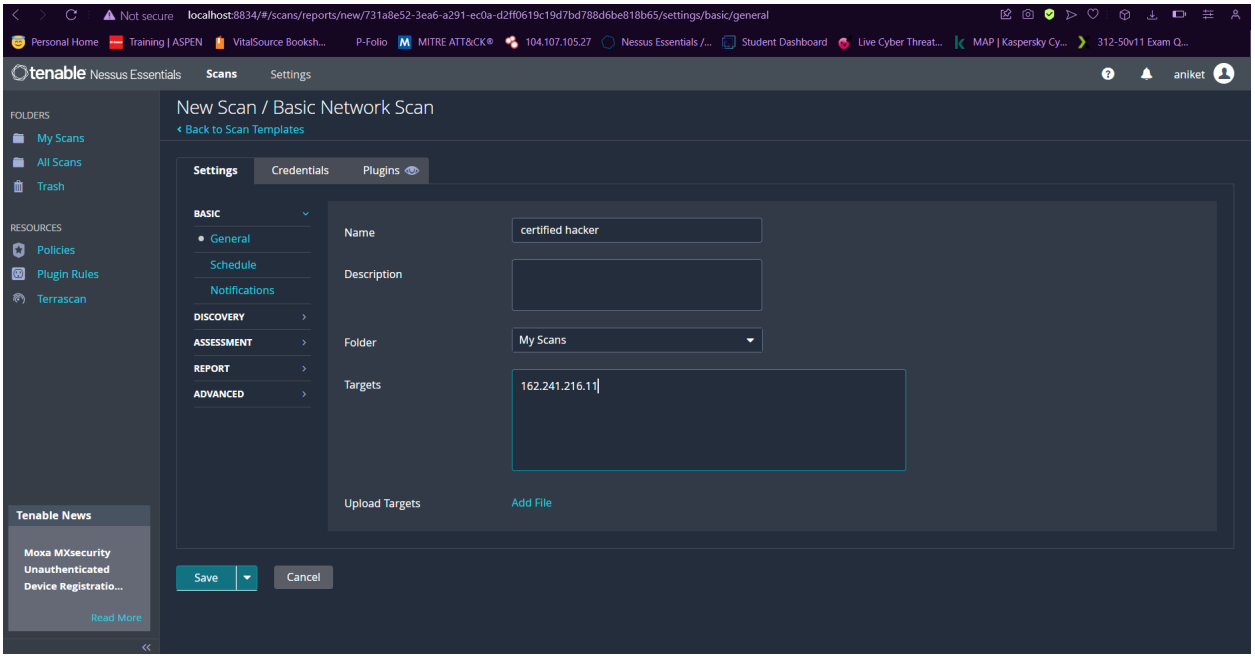
so in this i have performed the scans on many websites just out of curiosity to explore more about the tool so we will take example of some of websites one is our very favourite website vit.ac.in and one is certifiedhacker.com this website so we will go step by step

1….. we want to get the ipv4 address to start with so we will go to nslookup.io to get the ipv4 address of the website

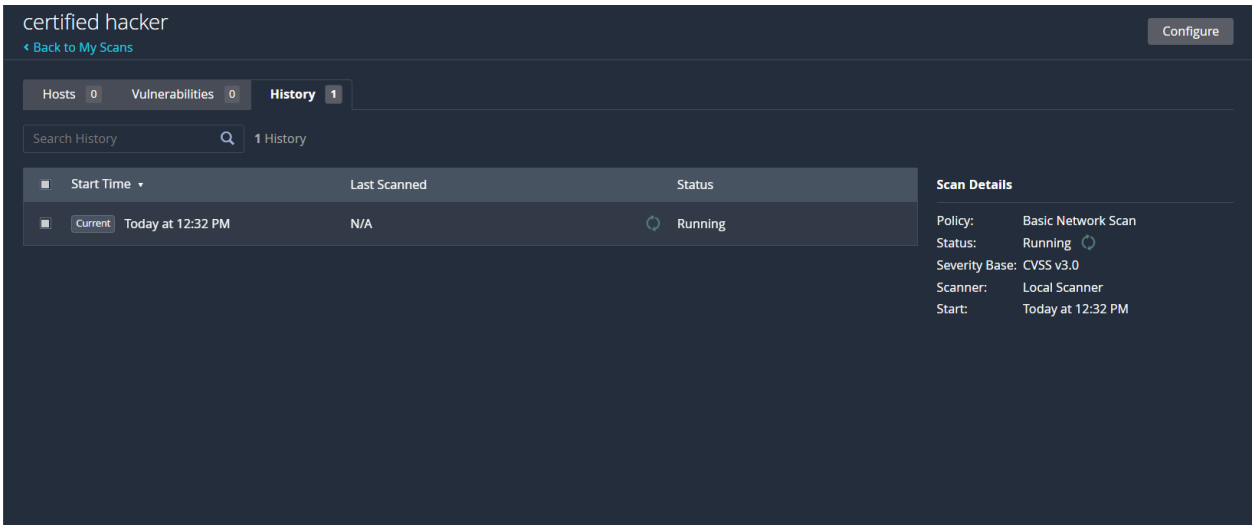


162.241.216.11

2…… now we will go back to nessus and we will click on new scan then we will click on basic network scan to start the setup phase and we will enter all the data required in this case and will click on start button

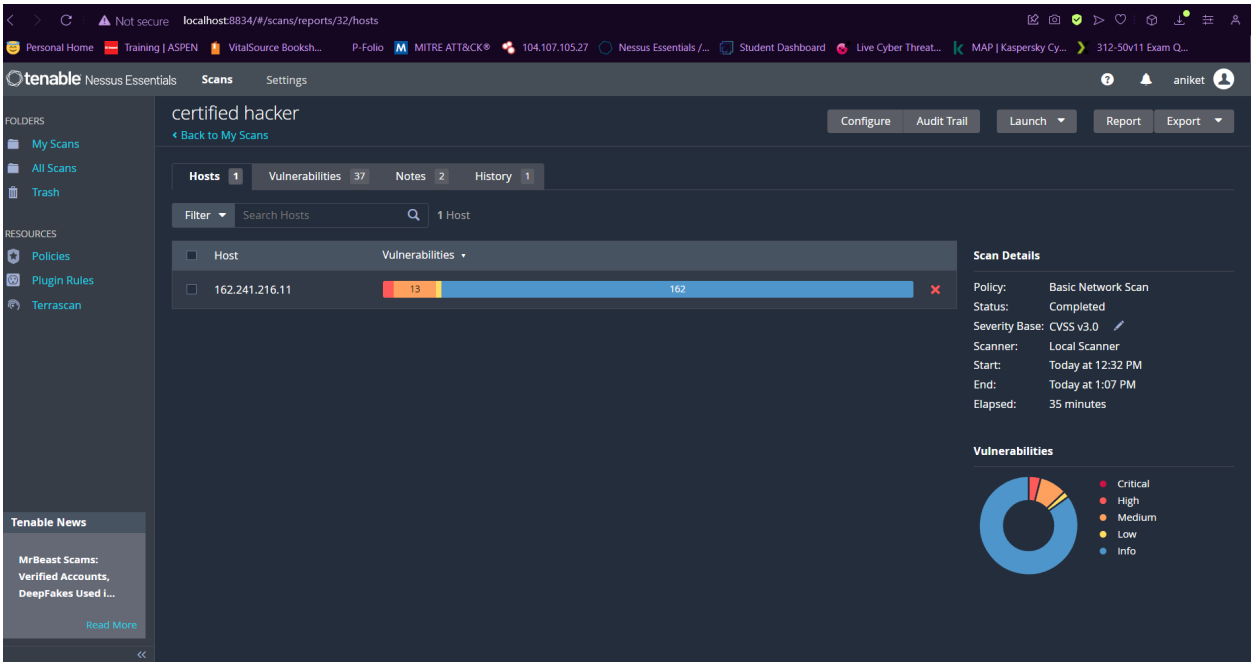


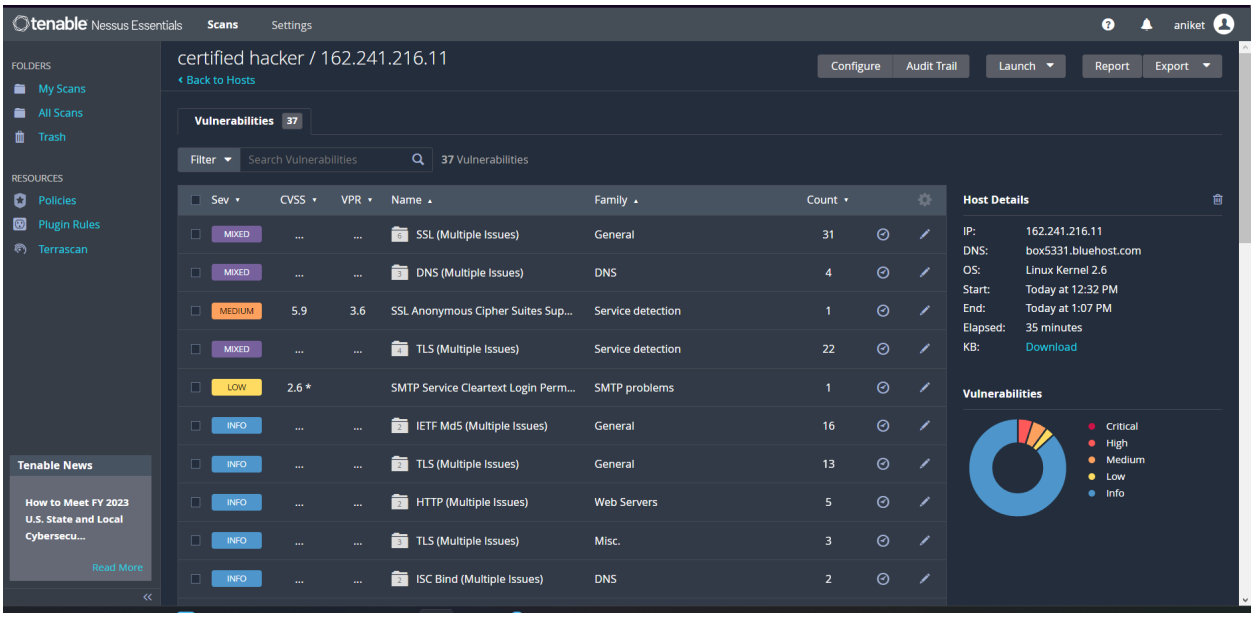
it will start scanning and will take some time as this website have a lot of open ports



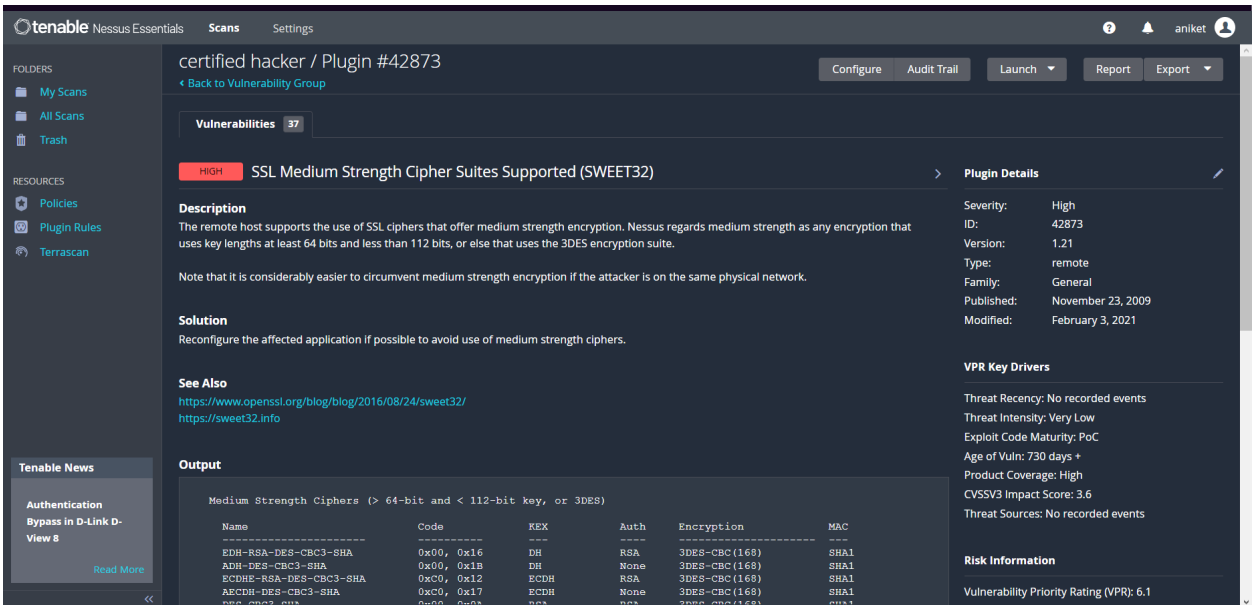
so after 35 minutes we got our final report of the scan

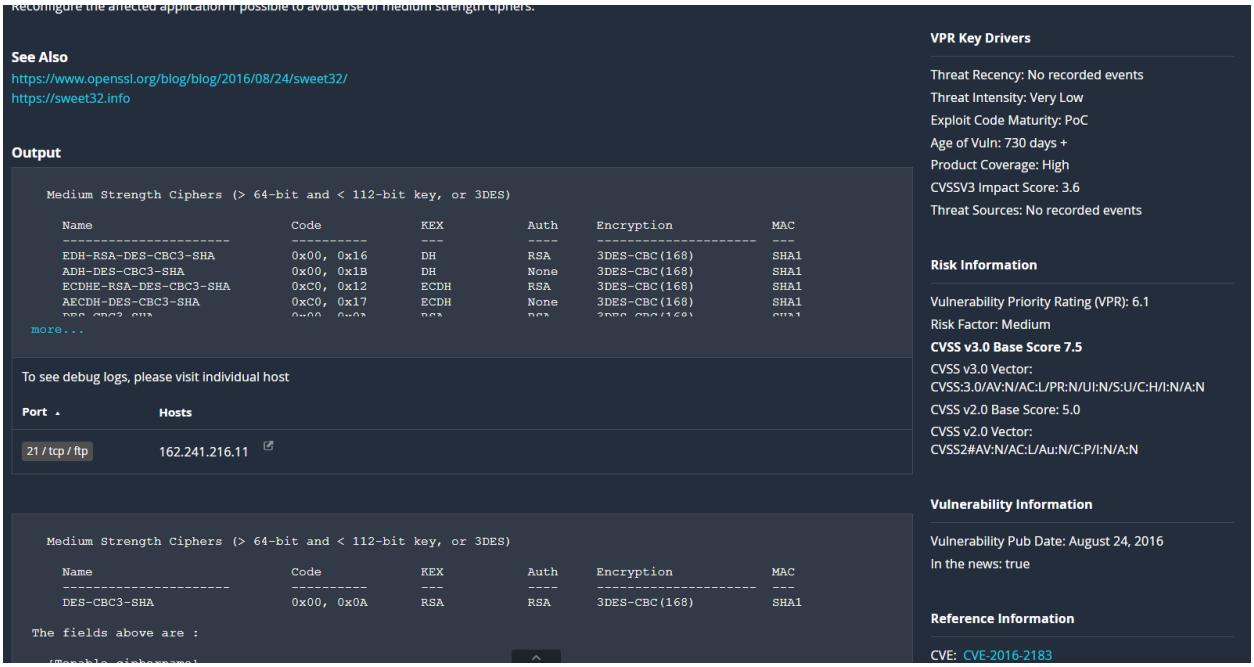
3 high 13 medium and so on





see one of the high vulnerability rating is 7.5



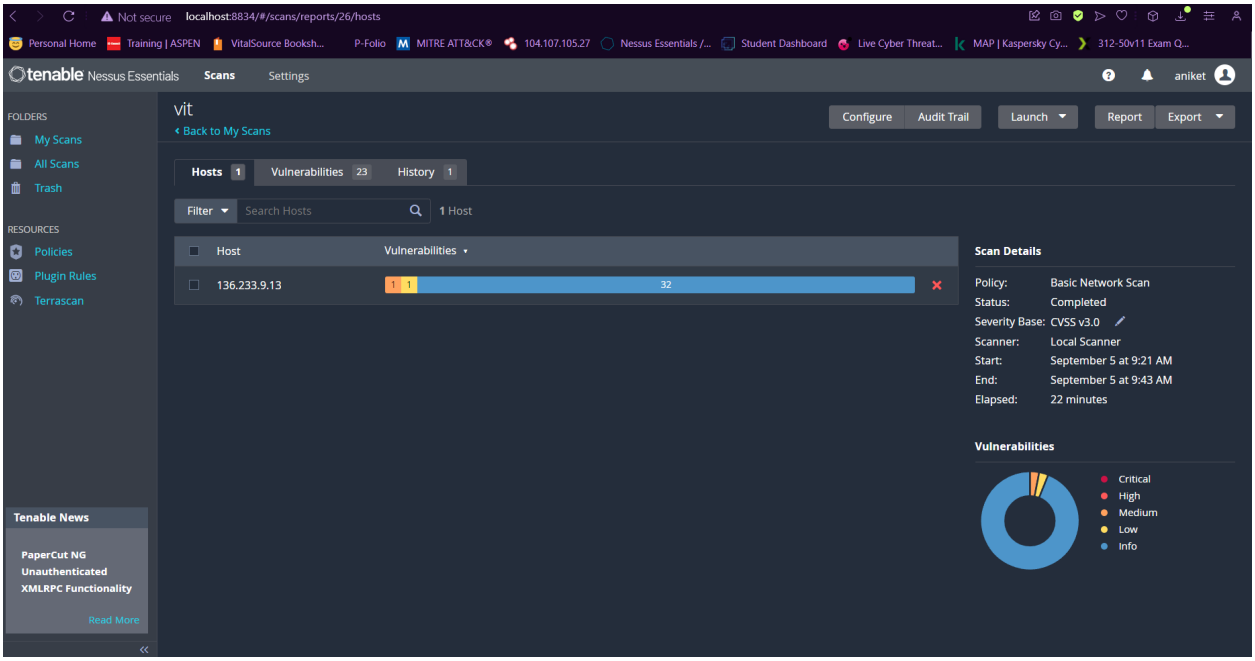


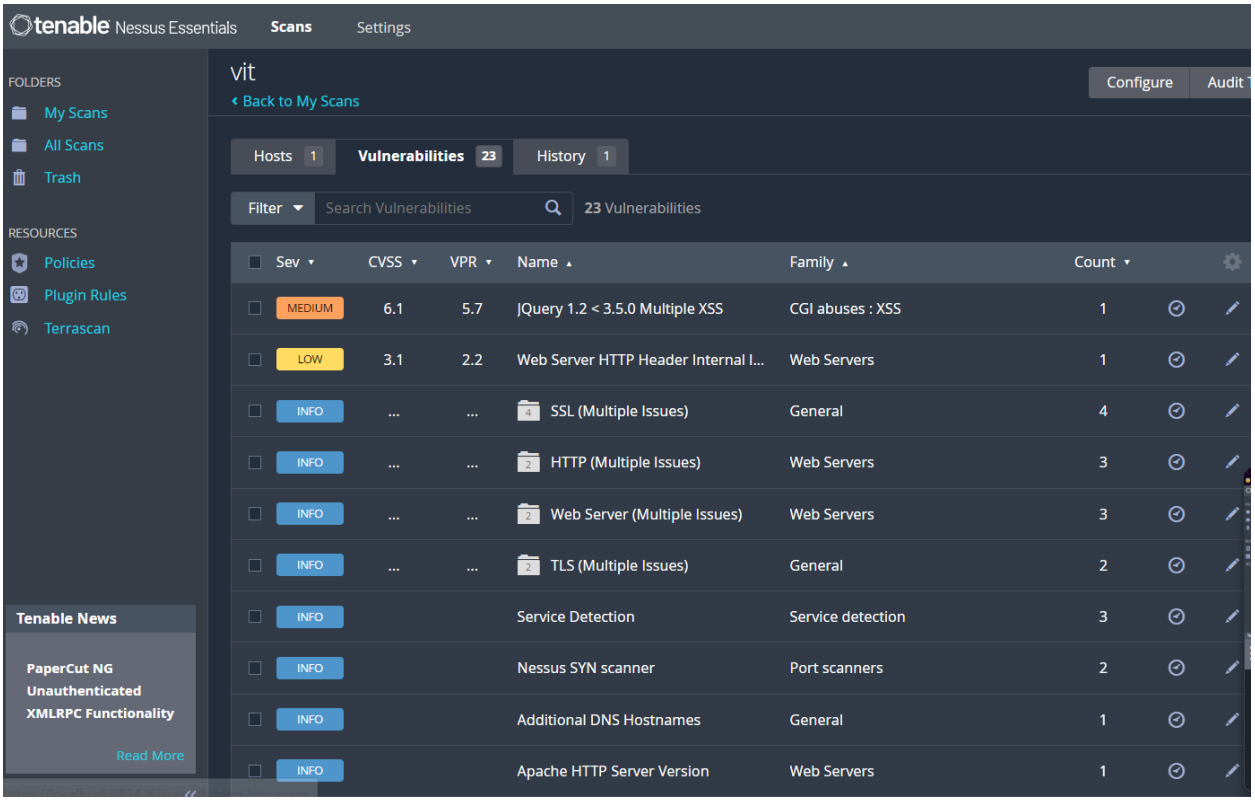
and i will upload the report too in form of html and nessus file

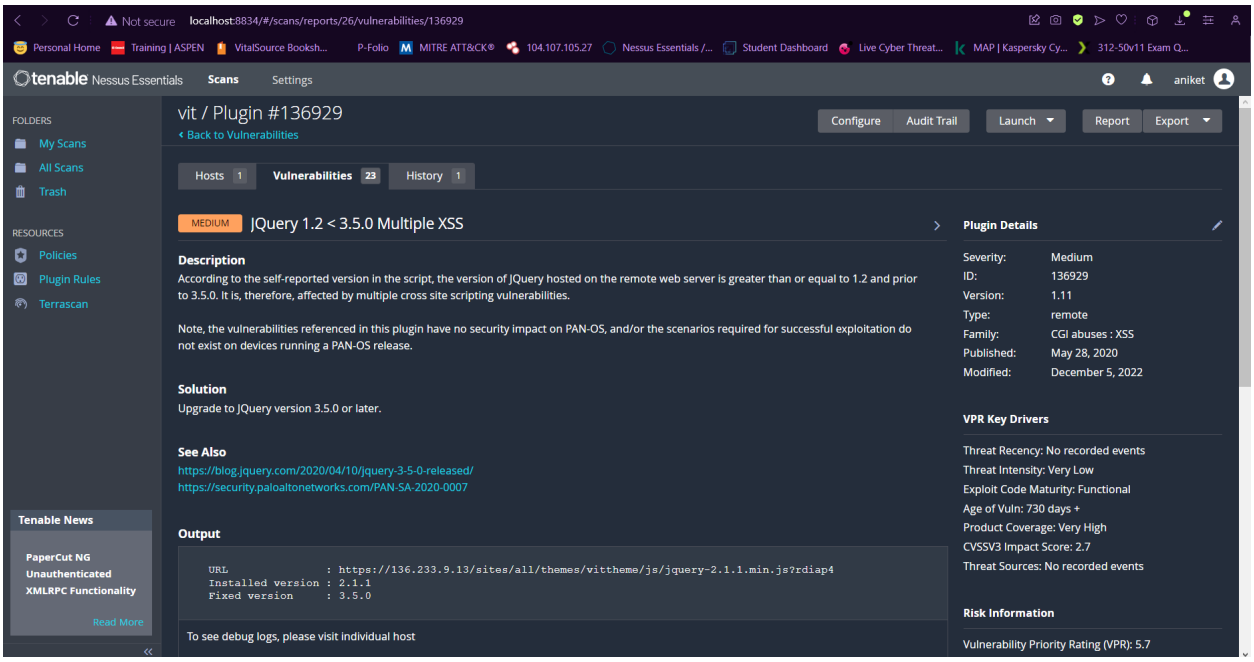
certified hacker _oopvna.html

certified hacker _q0g3na.nessus

and in similar way i have performed the same for VIT website so this is the final report of the scan


Not secure localhost:8834/#/scans/reports/26/hosts
tenable Nessus Essentials
Scans
Settings
aniket
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
vit
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 23
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
136.233.9.13
32
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: September 5 at 9:21 AM
End: September 5 at 9:43 AM
Elapsed: 22 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
PaperCut NG Unauthenticated XMLRPC Functionality
Read More


tenable Nessus Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
vit
Back to My Scans
Configure
Hosts 1
Vulnerabilities 23
History 1
Filter
Search Vulnerabilities
23 Vulnerabilities
Sev
CVSS
VPR
Name
Family
Count
MEDIUM 6.1 5.7 jQuery 1.2 < 3.5.0 Multiple XSS CGI abuses : XSS 1
LOW 3.1 2.2 Web Server HTTP Header Internal I... Web Servers 1
INFO ... ... SSL (Multiple Issues) General 4
INFO ... ... HTTP (Multiple Issues) Web Servers 3
INFO ... ... Web Server (Multiple Issues) Web Servers 3
INFO ... ... TLS (Multiple Issues) General 2
INFO Service Detection Service detection 3
INFO Nessus SYN scanner Port scanners 2
INFO Additional DNS Hostnames General 1
INFO Apache HTTP Server Version Web Servers 1
Tenable News
PaperCut NG Unauthenticated XMLRPC Functionality
Read More



vit_iwmt3r

vit_6nlfph.nessus

vit_iwmt3r.html