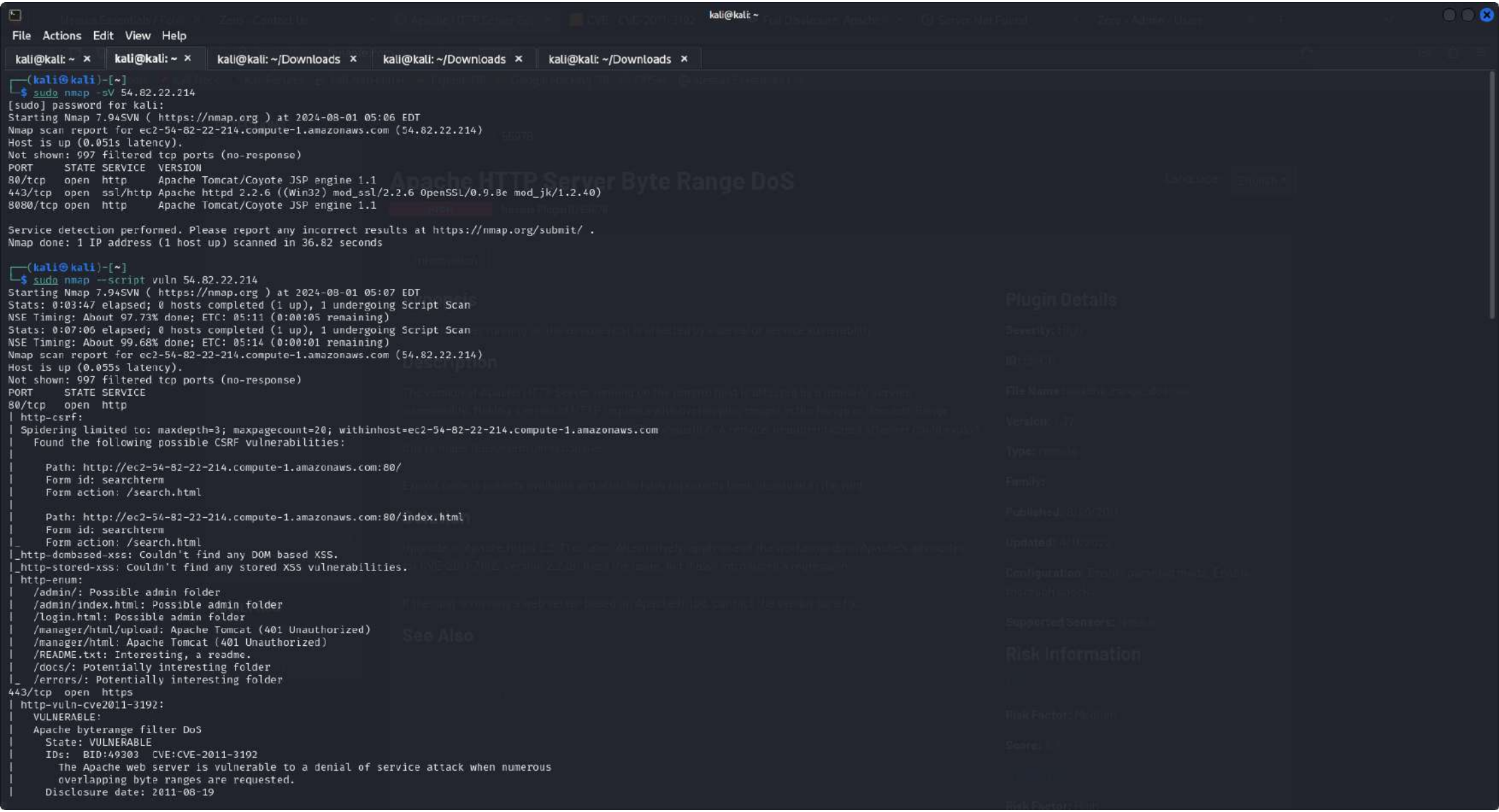
Vulnerabilities Total: 15

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	4.3*	-	85582	Web Application Potentially Vulnerable to Clickjacking
LOW	2.6*	-	34850	Web Server Uses Basic Authentication Without HTTPS
INFO	N/A	-	39446	Apache Tomcat Detection
INFO	N/A	-	47830	CGI Generic Injectable Parameter
INFO	N/A	-	49704	External URLs
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	-	50345	Missing or Permissive X-Frame-Options HTTP Response Header
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	40665	Protected Web Page Detection
INFO	N/A	-	40773	Web Application Potentially Sensitive CGI Parameter Detection
INFO	N/A	-	91815	Web Application Sitemap
INFO	N/A	-	11032	Web Server Directory Enumeration
INFO	N/A	-	10662	Web mirroring

* indicates the v3.0 score was not available; the v2.0 score is shown

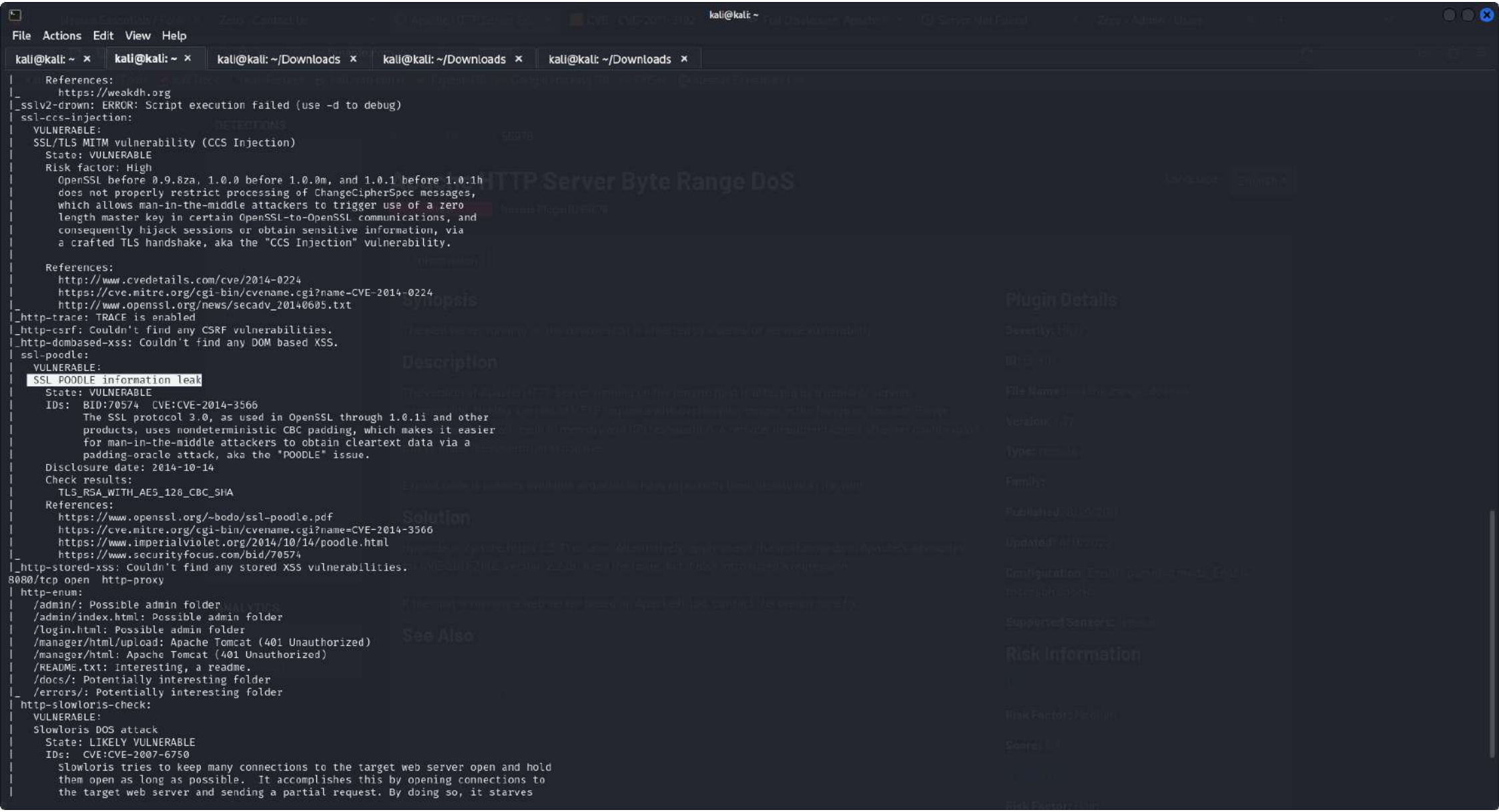

kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
kali@kali: ~/Downloads
kali@kali: ~/Downloads
kali@kali: ~/Downloads
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 54.82.22.214
[sudo] password for kali:
Starting Nmap 7.94SVN (https://nmap.org) at 2024-08-01 05:06 EDT
Nmap scan report for ec2-54-82-22-214.compute-1.amazonaws.com (54.82.22.214)
Host is up (0.051s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
80/tcp open http Apache Tomcat/Coyote JSP engine 1.1
443/tcp open ssl/http Apache httpd 2.2.6 ((Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40)
8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.82 seconds
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script vuln 54.82.22.214
Starting Nmap 7.94SVN (https://nmap.org) at 2024-08-01 05:07 EDT
Stats: 0:03:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.73% done; ETC: 05:11 (0:00:05 remaining)
Stats: 0:07:06 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.68% done; ETC: 05:14 (0:00:01 remaining)
Nmap scan report for ec2-54-82-22-214.compute-1.amazonaws.com (54.82.22.214)
Host is up (0.055s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
80/tcp open http
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=ec2-54-82-22-214.compute-1.amazonaws.com
| Found the following possible CSRF vulnerabilities:
|
| Path: http://ec2-54-82-22-214.compute-1.amazonaws.com:80/
| Form id: searchterm
| Form action: /search.html
|
| Path: http://ec2-54-82-22-214.compute-1.amazonaws.com:80/index.html
| Form id: searchterm
|_ Form action: /search.html
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
| /admin/: Possible admin folder
| /admin/index.html: Possible admin folder
| /login.html: Possible admin folder
| /manager/html/upload: Apache Tomcat (401 Unauthorized)
| /manager/html: Apache Tomcat (401 Unauthorized)
| /README.txt: Interesting, a readme.
| /docs/: Potentially interesting folder
|_ /errors/: Potentially interesting folder
443/tcp open https
| http-vuln-cve2011-3192:
| VULNERABLE:
| Apache byterange filter DoS
| State: VULNERABLE
| IDs: BID:49303 CVE:CVE-2011-3192
| The Apache web server is vulnerable to a denial of service attack when numerous
| overlapping byte ranges are requested.
| Disclosure date: 2011-08-19

kali@kali: ~

File Actions Edit View Help

kali@kali: ~ × | kali@kali: ~ × | kali@kali: ~/Downloads × | kali@kali: ~/Downloads × | kali@kali: ~/Downloads ×

```
| ssl-dh-params:
|   VULNERABLE:
|   Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
|     State: VULNERABLE
|     IDs:  BID:74733  CVE:CVE-2015-4000
|       The Transport Layer Security (TLS) protocol contains a flaw that is
|       triggered when handling Diffie-Hellman key exchanges defined with
|       the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
|       to downgrade the security of a TLS session to 512-bit export-grade
|       cryptography, which is significantly weaker, allowing the attacker
|       to more easily break the encryption and monitor or tamper with
|       the encrypted stream.
|     Disclosure date: 2015-5-19
|     Check results:
|       EXPORT-GRADE DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: mod_ssl 2.2.x/512-bit MODP group with safe prime modulus
|             Modulus Length: 512
|             Generator Length: 8
|             Public Key Length: 512
|     References:
|       https://weakdh.org
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
|       https://www.securityfocus.com/bid/74733
|
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: mod_ssl 2.2.x/1024-bit MODP group with safe prime modulus
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       http://www.cvedetails.com/cve/2014-0224
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|_      http://www.openssl.org/news/secadv_20140605.txt
```


kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
kali@kali: ~/Downloads
kali@kali: ~/Downloads
kali@kali: ~/Downloads
| References:
|_ https://weakdh.org
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
| ssl-ccs-injection:
| VULNERABLE:
| SSL/TLS MITM vulnerability (CCS Injection)
| State: VULNERABLE
| Risk factor: High
| OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
| does not properly restrict processing of ChangeCipherSpec messages,
| which allows man-in-the-middle attackers to trigger use of a zero
| length master key in certain OpenSSL-to-OpenSSL communications, and
| consequently hijack sessions or obtain sensitive information, via
| a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
| References:
| http://www.cvedetails.com/cve/2014-0224
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|_ http://www.openssl.org/news/secadv_20140605.txt
|_http-trace: TRACE is enabled
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| ssl-poodle:
| VULNERABLE:
| SSL POODLE information leak
| State: VULNERABLE
| IDs: BID:70574 CVE:CVE-2014-3566
| The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
| products, uses nondeterministic CBC padding, which makes it easier
| for man-in-the-middle attackers to obtain cleartext data via a
| padding-oracle attack, aka the "POODLE" issue.
| Disclosure date: 2014-10-14
| Check results:
| TLS_RSA_WITH_AES_128_CBC_SHA
| References:
| https://www.openssl.org/~bodo/ssl-poodle.pdf
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
| https://www.imperialviolet.org/2014/10/14/poodle.html
|_ https://www.securityfocus.com/bid/70574
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
8080/tcp open http-proxy
| http-enum:
| /admin/: Possible admin folder
| /admin/index.html: Possible admin folder
| /login.html: Possible admin folder
| /manager/html/upload: Apache Tomcat (401 Unauthorized)
| /manager/html: Apache Tomcat (401 Unauthorized)
| /README.txt: Interesting, a readme.
| /docs/: Potentially interesting folder
|_ /errors/: Potentially interesting folder
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves

Online Banking

Welcome to Zero Online Banking. Zero provides a greener and more convenient way to manage your money. Zero enables you to check your account balances, pay your bills, transfer money, and keep detailed records of your transactions, wherever there is an internet connection.

Online Banking

Click the button below to view online banking features.

More Services

Checking Account Activity

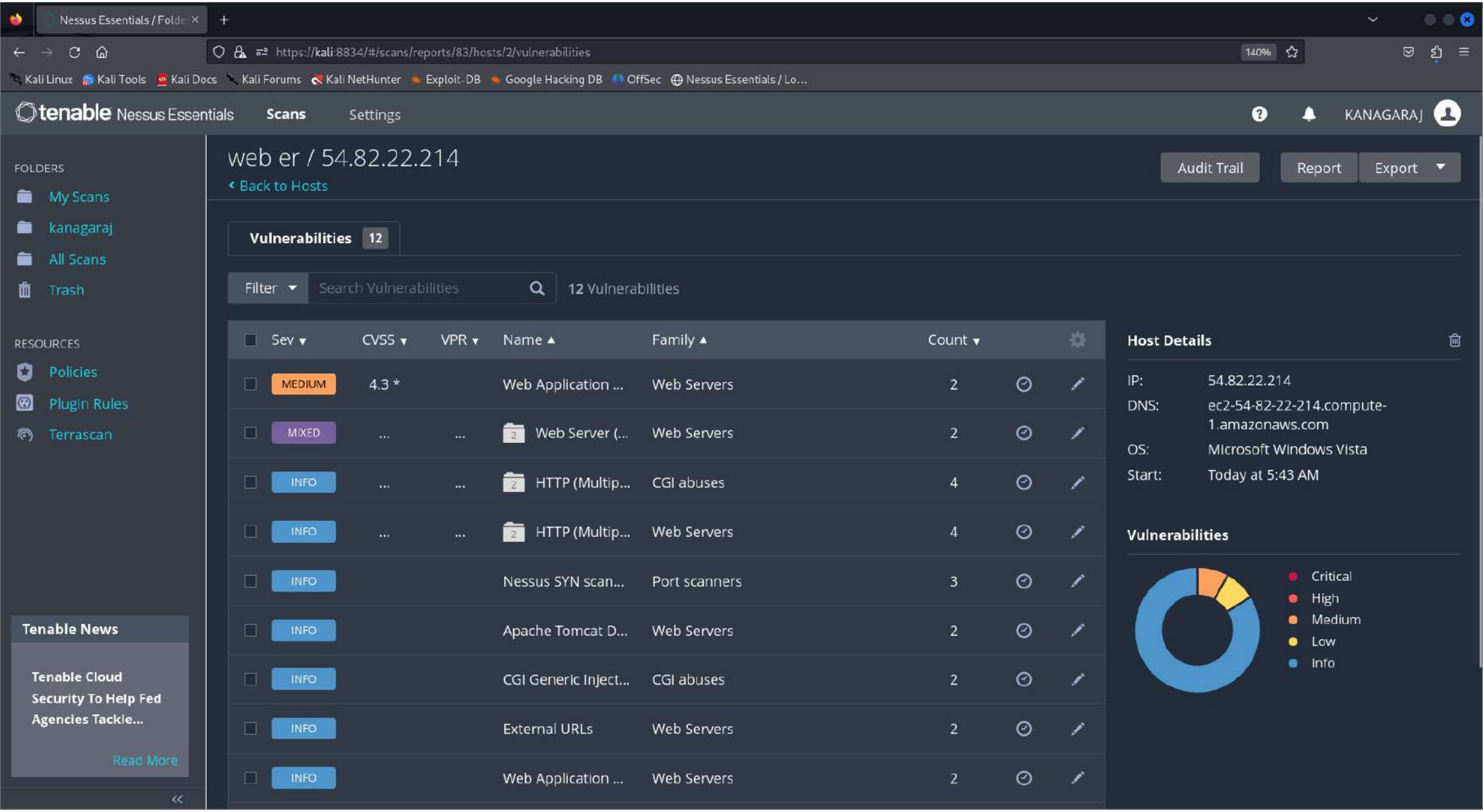
Use Zero to view the most up-to-date listings of your deposits, withdrawals, interest payments, and a number of other useful transactions.

Transfer Funds

Use Zero to safely and securely transfer funds between accounts. There is no hold placed on online money transfers, so your funds are available when you need them.

My Money Map

Use Zero to set up and monitor your personalized money map. A money map is an easy-to-use online tool that helps you manage your finances efficiently. With Money Map, you can create a budget, sort your finances into spending and savings categories, check the interest your accounts are earning, and gain new understanding of your patterns with the help of Zero's clear charts and graphs.


Nessus Essentials / Folde
https://kali:8834/#/scans/reports/83/hosts/2/vulnerabilities
140%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Nessus Essentials / Lo...
tenable Nessus Essentials
Scans
Settings
KANAGARAJ
FOLDERS
My Scans
kanagaraj
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Tenable Cloud Security To Help Fed Agencies Tackle...
Read More
web er / 54.82.22.214
Back to Hosts
Audit Trail
Report
Export
Vulnerabilities 12
Filter
Search Vulnerabilities
12 Vulnerabilities
Sev
CVSS
VPR
Name
Family
Count
MEDIUM 4.3 * Web Application ... Web Servers 2
MIXED ... ... Web Server (... Web Servers 2
INFO ... ... HTTP (Multip... CGI abuses 4
INFO ... ... HTTP (Multip... Web Servers 4
INFO Nessus SYN scan... Port scanners 3
INFO Apache Tomcat D... Web Servers 2
INFO CGI Generic Inject... CGI abuses 2
INFO External URLs Web Servers 2
INFO Web Application ... Web Servers 2
Host Details
IP: 54.82.22.214
DNS: ec2-54-82-22-214.compute-1.amazonaws.com
OS: Microsoft Windows Vista
Start: Today at 5:43 AM
Vulnerabilities
Critical
High
Medium
Low
Info