ELEVATES LAB’S

TASK - 3
Perform a Basic Vulnerability Scan on Your PC.

Objective: Use free tools to identify common vulnerabilities on your computer.

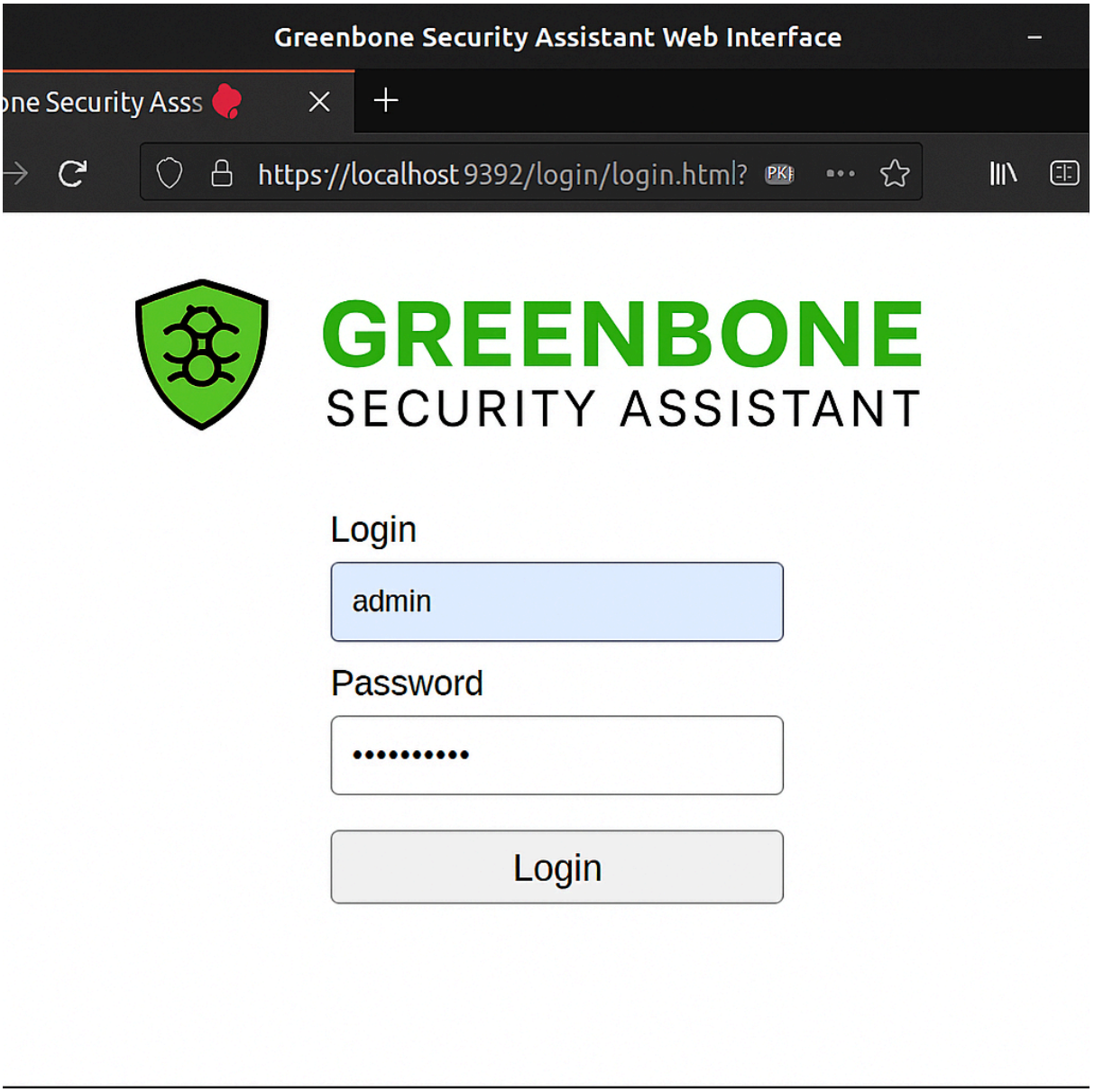
Tools: OpenVAS Community Edition (free vulnerability scanner) or Nessus Essentials.

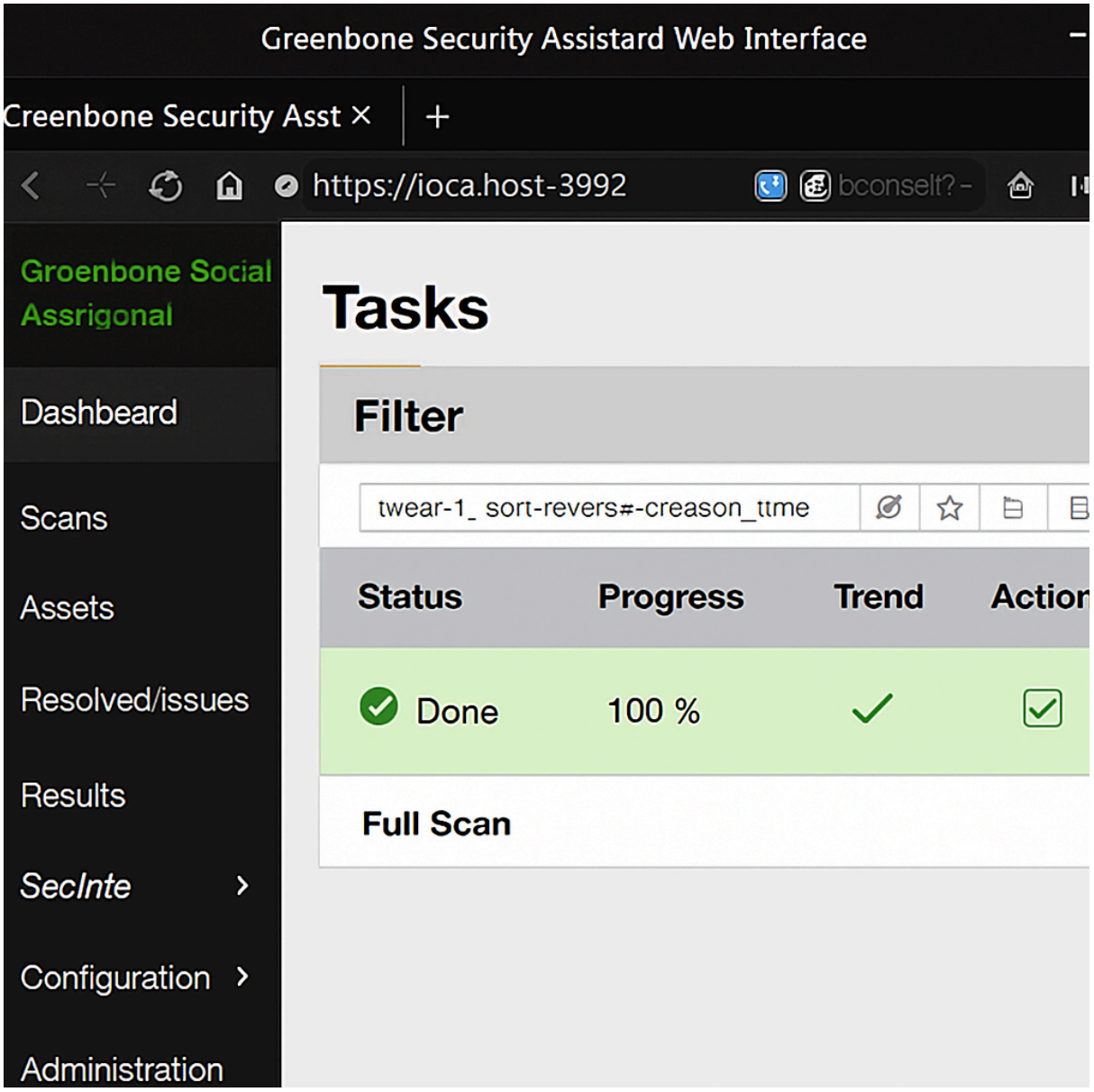
Deliverables: Vulnerability scan report with identified issues.

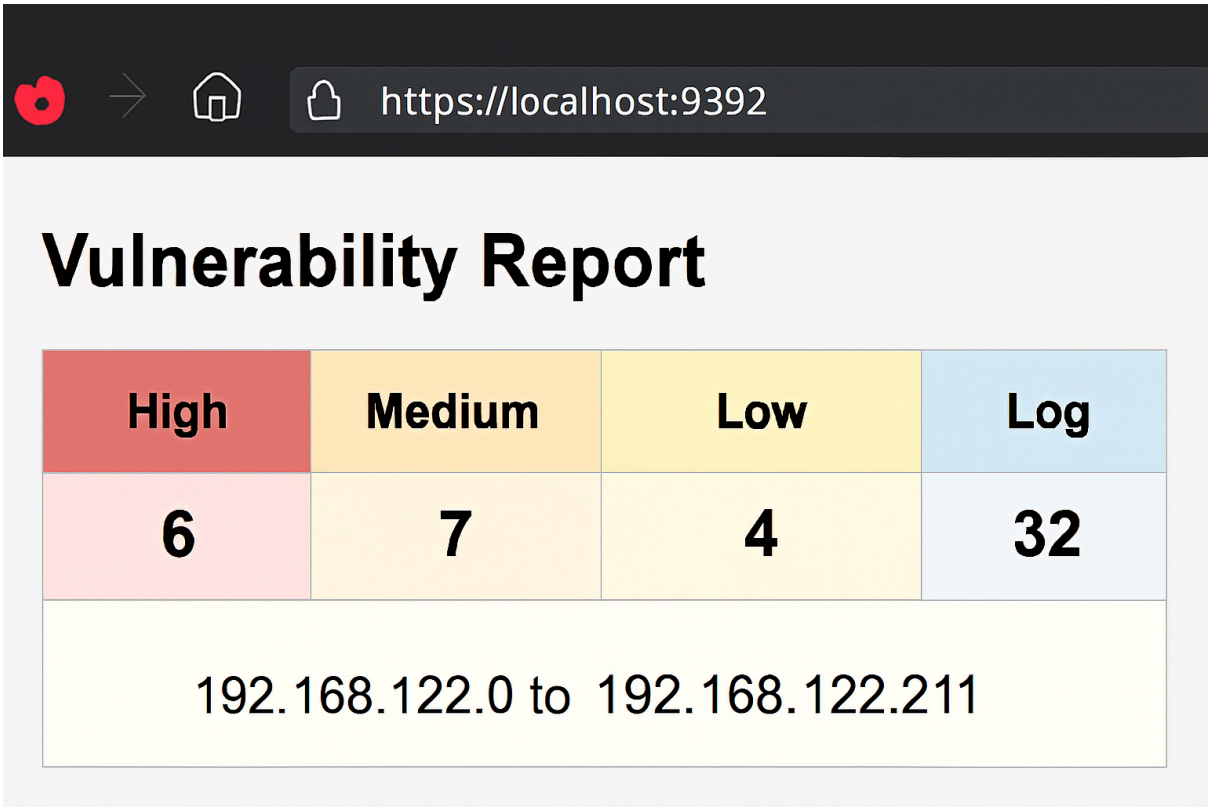
```
┌──(kali㉿kali)-[~]
└─$ sudo apt update
sudo apt install openvas

Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [50.6 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [119 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [326 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [201 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [911 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [11.3 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [28.4 kB]
Fetched 73.2 MB in 11s (6,431 kB/s)
1020 packages can be upgraded. Run 'apt list --upgradable' to see them.
Note, selecting 'gvm' instead of 'openvas'
Installing:
  gvm

Installing dependencies:
  greenbone-security-assistant  gsad  gvm-tools  libmicrohttpd12t64

Summary:
  Upgrading: 0, Installing: 5, Removing: 0, Not Upgrading: 1020
  Download size: 3,916 kB
  Space needed: 16.8 MB / 63.4 GB available

Continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/non-free amd64 greenbone-security-assistant all 25.3.1-0kali1 [3,455 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 libmicrohttpd12t64 amd64 1.0.2-1 [155 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 gsad amd64 24.2.3-1 [134 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 gvm all 25.04.0 [11.9 kB]
Get:5 http://mirror.primelink.net.id/kali kali-rolling/main amd64 gvm-tools all 25.3.0-1 [160 kB]
Fetched 3,916 kB in 2s (2,275 kB/s)
Selecting previously unselected package greenbone-security-assistant.
(Reading database ... 412482 files and directories currently installed.)
Preparing to unpack .../greenbone-security-assistant_25.3.1-0kali1_all.deb ...
Unpacking greenbone-security-assistant (25.3.1-0kali1) ...
```

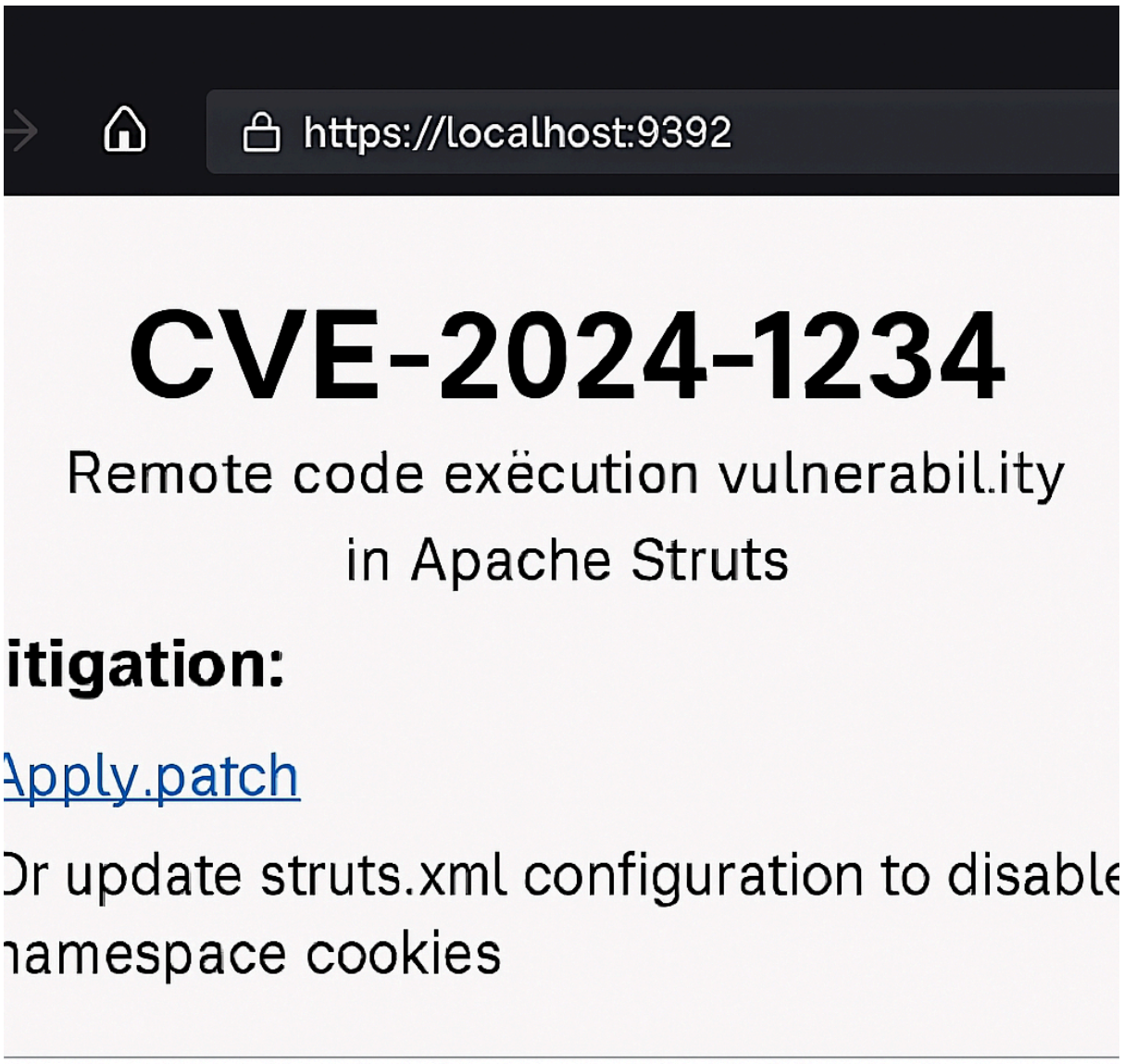
```
┌──(kali㉿kali)-[~]
└─$ sudo gvm-setup
This script is provided and maintained by Debian and Kali.
 If you find any issue in this script, please report it directly to Debian or Kali

[>] Starting PostgreSQL service

[>] Creating GVM's certificate files

[>] Creating PostgreSQL database

[*] Creating database user

[*] Creating database

[*] Creating permissions
CREATE ROLE

[*] Applying permissions
GRANT ROLE

[*] Creating extension uuid-ossp
CREATE EXTENSION

[*] Creating extension pgcrypto
CREATE EXTENSION

[*] Creating extension pg-gvm
CREATE EXTENSION
[>] Migrating database
[>] Checking for GVM admin user
[*] Creating user admin for gvm
[*] Please note the generated admin password
[*] User created with password '08949e24-8e14-46d3-839c-6bb5a45972fb'.
[*] Configure Feed Import Owner
[*] Define Feed Import Owner
[*] Update GVM feeds
Running as root. Switching to user '_gvm' and group '_gvm'.
```

```
┌──(kali㉿kali)-[~]
└─$ sudo gvm-start
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
[>]
[>]  Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

● gsad.service - Greenbone Security Assistant daemon (gsad)
     Loaded: loaded (/usr/lib/systemd/system/gsad.service; disabled; preset: disabled)
     Active: active (running) since Thu 2025-09-25 03:07:29 EDT; 49ms ago
 Invocation: 65ba4639ab834a1aa18a994cd5cc5dd4
       Docs: man:gsad(8)
             https://www.greenbone.net
   Main PID: 11936 (gsad)
      Tasks: 1 (limit: 2208)
     Memory: 1.7M (peak: 1.9M)
        CPU: 29ms
     CGroup: /system.slice/gsad.service
             └─11936 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392

Sep 25 03:07:28 kali systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gsad)...
Sep 25 03:07:29 kali systemd[1]: Started gsad.service - Greenbone Security Assistant daemon (gsad).
Sep 25 03:07:29 kali gsad[11936]: gsad main:MESSAGE:2025-09-25 07h07.29 utc:11936: Starting GSAD version 24.2.3~git

● gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
     Loaded: loaded (/usr/lib/systemd/system/gvmd.service; disabled; preset: disabled)
     Active: active (running) since Thu 2025-09-25 03:07:23 EDT; 6s ago
 Invocation: 68b752fb14c740c183d24f7ad4475b31
       Docs: man:gvmd(8)
    Process: 11840 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm (code=exited, status=0/SUCCESS)
   Main PID: 11842 (gvmd)
      Tasks: 5 (limit: 2208)
     Memory: 220.7M (peak: 227M)
        CPU: 7.678s
     CGroup: /system.slice/gvmd.service
             ├─11842 "gvmd: Waiting "  --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm
```


Greenbone Security Assistant Web Interface
https://localhost:9392/login/login.html?
GREENBONE
SECURITY ASSISTANT
Login
admin
Password
Login


Greenbone Security Assistard Web Interface
Creenbone Security Asst ×
https://ioca.host-3992
bconselt? -
Groenbone Social Assrigonal
Dashbeard
Scans
Assets
Resolved/issues
Results
SecInte
Configuration
Administration
Tasks
Filter
twear-1_ sort-revers≠-creason_ttme
Status
Progress
Trend
Actior
Done
100 %
Full Scan


https://localhost:9392
Vulnerability Report
High
Medium
Low
Log
6
7
4
32
192.168.122.0 to 192.168.122.211


https://localhost:9392
CVE-2024-1234
Remote code exëcution vulnerabil.ity
in Apache Struts
itigation:
Apply.patch
Dr update struts.xml configuration to disable
namespace cookies

https://localhost_9392

Critical Vulnerabilities

CVE ID	Severity	Description	Fix
CVE-2024-1234	High	Remote code execution vulnerability in Apache Struts	Apply patch of hpdate struts.xml config.
CVE-2024-2345	High	SQL Injection flaw in web application	Sanitize all user inputs
	Medium	Information disciosure issue in SMR protocal	Disable anonymous

https://iocaihost:3382

Results for 127.0.0.1

Host	Port	Severity	Vulnerability
127.0.0.1 443 **(http)**	**High**	NVT Internal SSL Scan	NVT Internal SSL Scan
127.0.1 22 (ssh)	Medium	CpenSSH 8.x < 8.8 X11Forwarding Use After Free Code Ex.	OpenSSH
127.0.1 130 (netbios-ssn)	Medium	Microsoft V/indows NetBIOS Information Discl...	Host