UPES

UNIVERSITY OF TOMORROW

IT DATA SECURITY LAB FILE

Name- Dhairya Jain

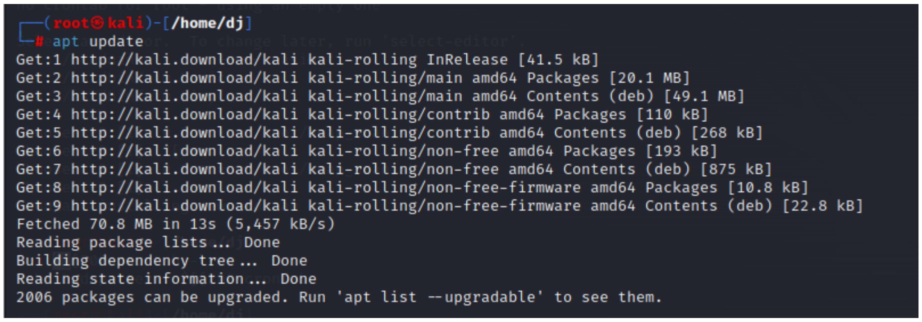
Sap ID- 500105432

Batch- CSF-B4

Experiment-6

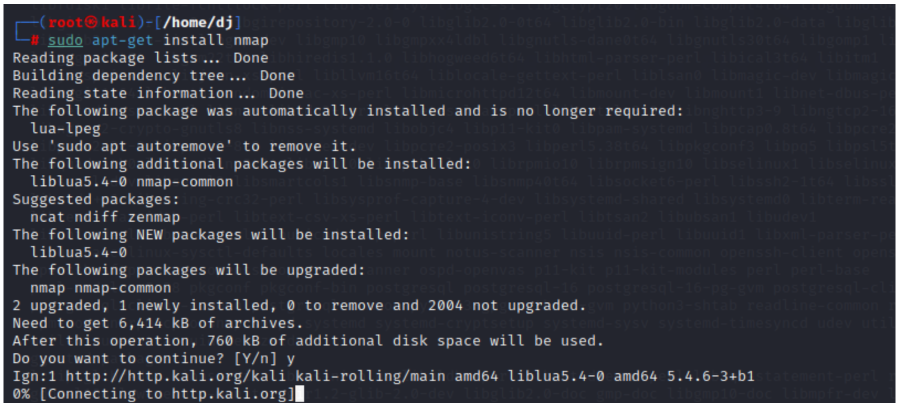
1. Network Security with Automated Testing
2. Safe3 SQL Injector

- **Setting Up the Environment**
- Update Kali Linux



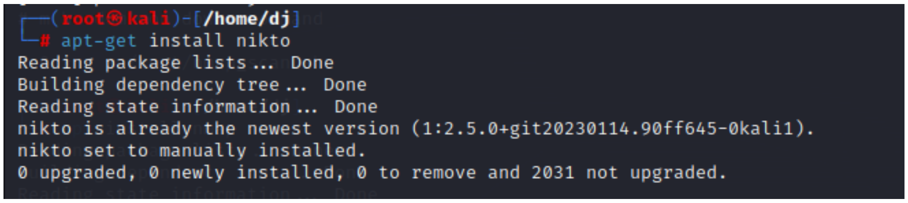
```
┌──(root㉿kali)-[/home/dj]
└─# apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.1 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [49.1 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [110 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [268 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [193 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [875 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.8 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [22.8 kB]
Fetched 70.8 MB in 13s (5,457 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
2006 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

- **Install Required Tools**
- Install Nmap



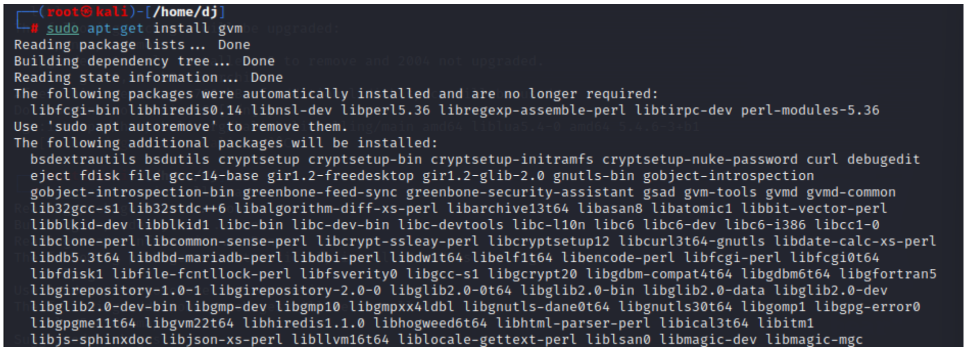
```
┌──(root㉿kali)-[/home/dj]
└─# sudo apt-get install nmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  lua-lpeg
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  liblua5.4-0 nmap-common
Suggested packages:
  ncat ndiff zenmap
The following NEW packages will be installed:
  liblua5.4-0
The following packages will be upgraded:
  nmap nmap-common
2 upgraded, 1 newly installed, 0 to remove and 2004 not upgraded.
Need to get 6,414 kB of archives.
After this operation, 760 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 liblua5.4-0 amd64 5.4.6-3+b1
0% [Connecting to http.kali.org]
```

- Install Nikto



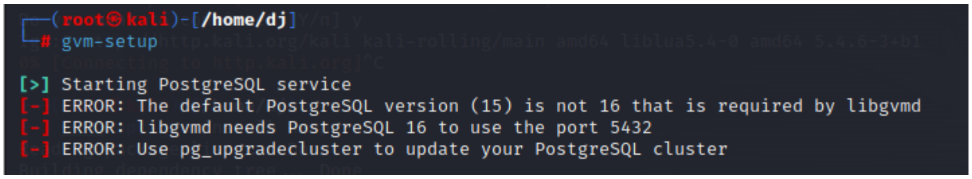
```
┌──(root㉿kali)-[/home/dj]
└─# apt-get install nikto
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nikto is already the newest version (1:2.5.0+git20230114.90ff645-0kali1).
nikto set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 2031 not upgraded.
```

- Install OpenVAS (now GVM)



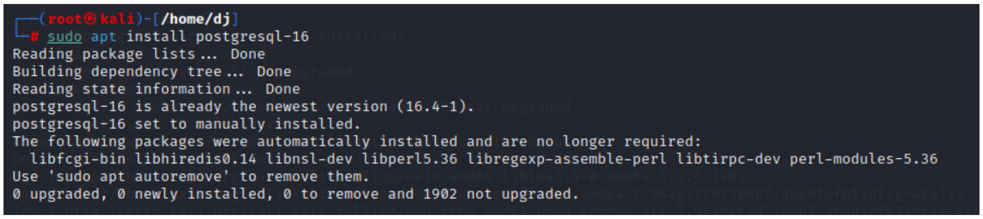
```
┌──(root㉿kali)-[/home/dj]
└─# sudo apt-get install gvm
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  libfcgi-bin libhiredis0.14 libnsl-dev libperl5.36 libregexp-assemble-perl libtirpc-dev perl-modules-5.36
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  bsdextrautils bsdutils cryptsetup cryptsetup-bin cryptsetup-initramfs cryptsetup-nuke-password curl debugedit
  eject fdisk file gcc-14-base gir1.2-freedesktop gir1.2-glib-2.0 gnutls-bin gobject-introspection
  gobject-introspection-bin greenbone-feed-sync greenbone-security-assistant gsad gvm-tools gvmd gvmd-common
  lib32gcc-s1 lib32stdc++6 libalgorithm-diff-xs-perl libarchive13t64 libasan8 libatomic1 libbit-vector-perl
  libblkid-dev libblkid1 libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev libc6-i386 libcc1-0
  libclone-perl libcommon-sense-perl libcrypt-ssleay-perl libcryptsetup12 libcurl3t64-gnutls libdate-calc-xs-perl
  libdb5.3t64 libdbd-mariadb-perl libdbi-perl libdw1t64 libelf1t64 libencode-perl libfcgi-perl libfcgi0t64
  libfdisk1 libfile-fcntllock-perl libfsverity0 libgcc-s1 libgcrypt20 libgdbm-compat4t64 libgdbm6t64 libgfortran5
  libgirepository-1.0-1 libgirepository-2.0-0 libglib2.0-0t64 libglib2.0-bin libglib2.0-data libglib2.0-dev
  libglib2.0-dev-bin libgmp-dev libgmp10 libgmpxx4ldbl libgnutls-dane0t64 libgnutls30t64 libgomp1 libgpg-error0
  libgpgme11t64 libgvm22t64 libhiredis1.1.0 libhogweed6t64 libhtml-parser-perl libical3t64 libitm1
  libjs-sphinxdoc libjson-xs-perl libllvm16t64 liblocale-gettext-perl liblsan0 libmagic-dev libmagic-mgc
```

- Gvm setup

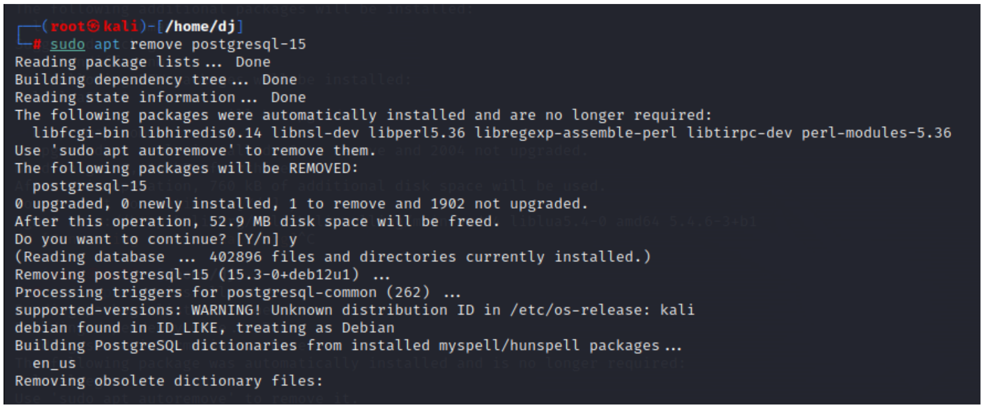


```
┌──(root㉿kali)-[/home/dj]
└─# gvm-setup

[>] Starting PostgreSQL service
[-] ERROR: The default PostgreSQL version (15) is not 16 that is required by libgvmd
[-] ERROR: libgvmd needs PostgreSQL 16 to use the port 5432
[-] ERROR: Use pg_upgradecluster to update your PostgreSQL cluster
```

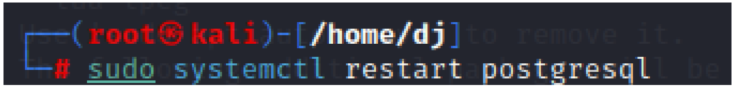
- An error occurred that postgresql 16 not installed
- Installing postgresql 16 nd removing postgresql 15



```
┌──(root㉿kali)-[/home/dj]
└─# sudo apt install postgresql-16
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
postgresql-16 is already the newest version (16.4-1).
postgresql-16 set to manually installed.
The following packages were automatically installed and are no longer required:
  libfcgi-bin libhiredis0.14 libnsl-dev libperl5.36 libregexp-assemble-perl libtirpc-dev perl-modules-5.36
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1902 not upgraded.
```

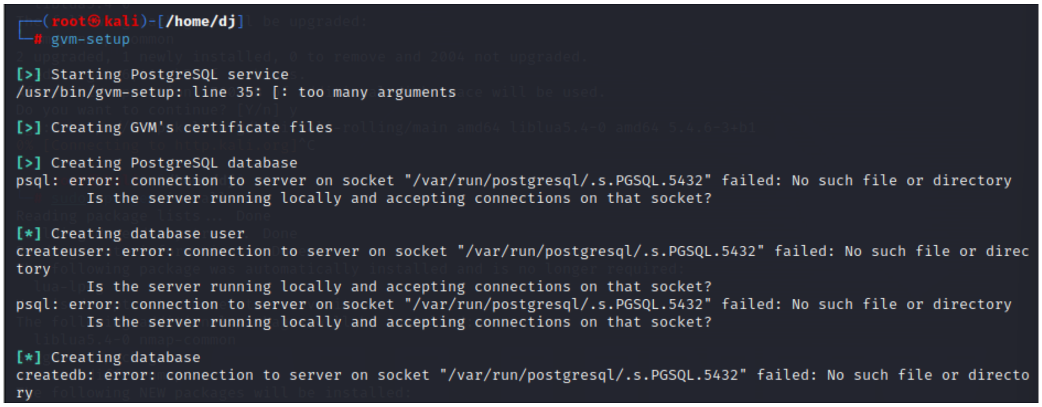


```
┌──(root㉿kali)-[/home/dj]
└─# sudo apt remove postgresql-15
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  libfcgi-bin libhiredis0.14 libnsl-dev libperl5.36 libregexp-assemble-perl libtirpc-dev perl-modules-5.36
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  postgresql-15
0 upgraded, 0 newly installed, 1 to remove and 1902 not upgraded.
After this operation, 52.9 MB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 402896 files and directories currently installed.)
Removing postgresql-15 (15.3-0+deb12u1) ...
Processing triggers for postgresql-common (262) ...
supported-versions: WARNING! Unknown distribution ID in /etc/os-release: kali
debian found in ID_LIKE, treating as Debian
Building PostgreSQL dictionaries from installed myspell/hunspell packages ...
  en_us
Removing obsolete dictionary files:
```



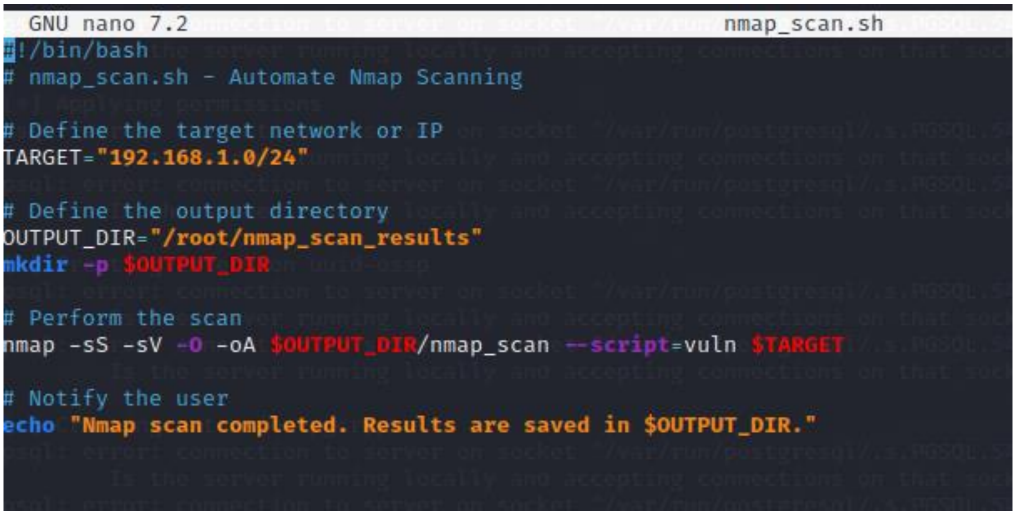
```
┌──(root㉿kali)-[/home/dj]
└─# sudo systemctl restart postgresql
```

- Now again start setup



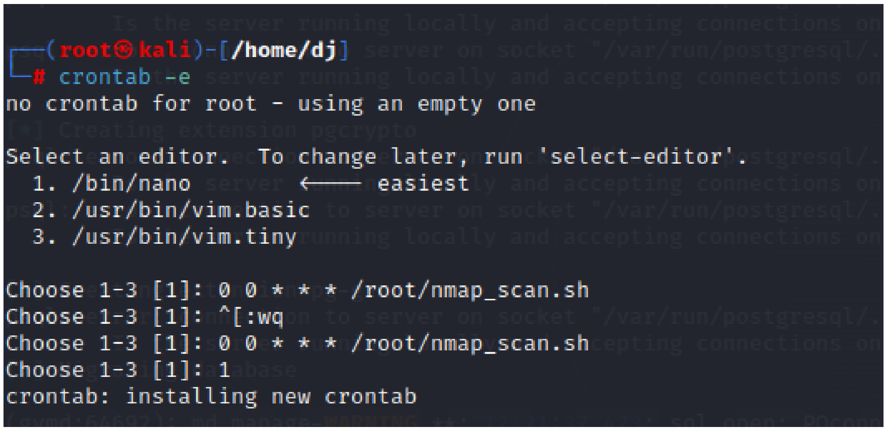
```
┌──(root㉿kali)-[/home/dj]
└─# gvm-setup
[>] Starting PostgreSQL service
/usr/bin/gvm-setup: line 35: [: too many arguments
[>] Creating GVM's certificate files

[>] Creating PostgreSQL database
psql: error: connection to server on socket "/var/run/postgresql/.s.PGSQL.5432" failed: No such file or directory
        Is the server running locally and accepting connections on that socket?

[*] Creating database user
createuser: error: connection to server on socket "/var/run/postgresql/.s.PGSQL.5432" failed: No such file or direc
tory
        Is the server running locally and accepting connections on that socket?
psql: error: connection to server on socket "/var/run/postgresql/.s.PGSQL.5432" failed: No such file or directory
        Is the server running locally and accepting connections on that socket?

[*] Creating database
createdb: error: connection to server on socket "/var/run/postgresql/.s.PGSQL.5432" failed: No such file or directo
ry
```

- **Automating Nmap for Network Scanning**
- Create a Bash Script for Nmap Scanning



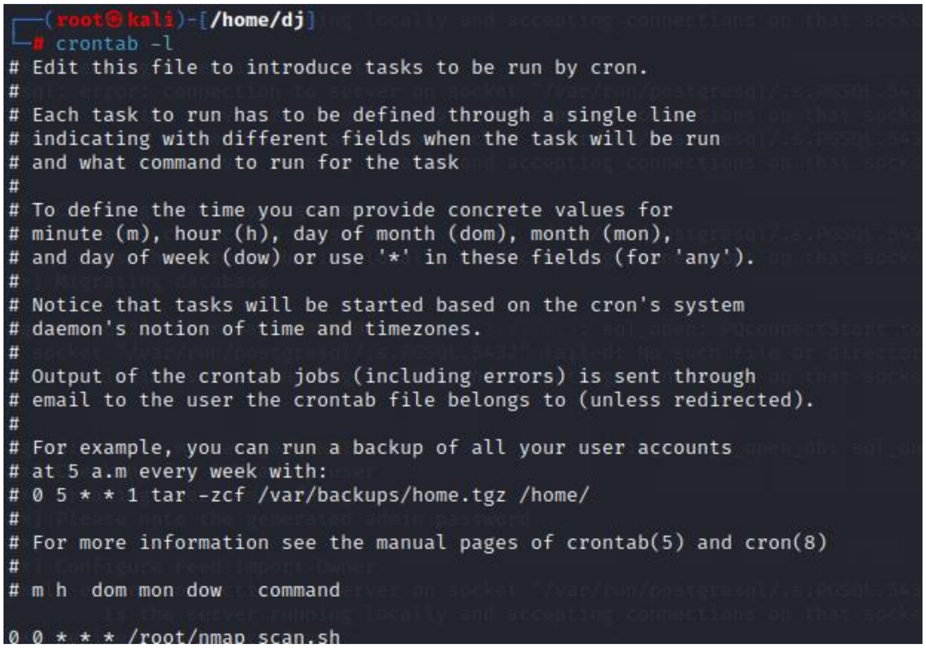
```
  GNU nano 7.2                                        nmap_scan.sh
#!/bin/bash
# nmap_scan.sh - Automate Nmap Scanning

# Define the target network or IP
TARGET="192.168.1.0/24"

# Define the output directory
OUTPUT_DIR="/root/nmap_scan_results"
mkdir -p $OUTPUT_DIR

# Perform the scan
nmap -sS -sV -O -oA $OUTPUT_DIR/nmap_scan --script=vuln $TARGET

# Notify the user
echo "Nmap scan completed. Results are saved in $OUTPUT_DIR."
```

- **Schedule the Script with Cron**
- Edit the crontab



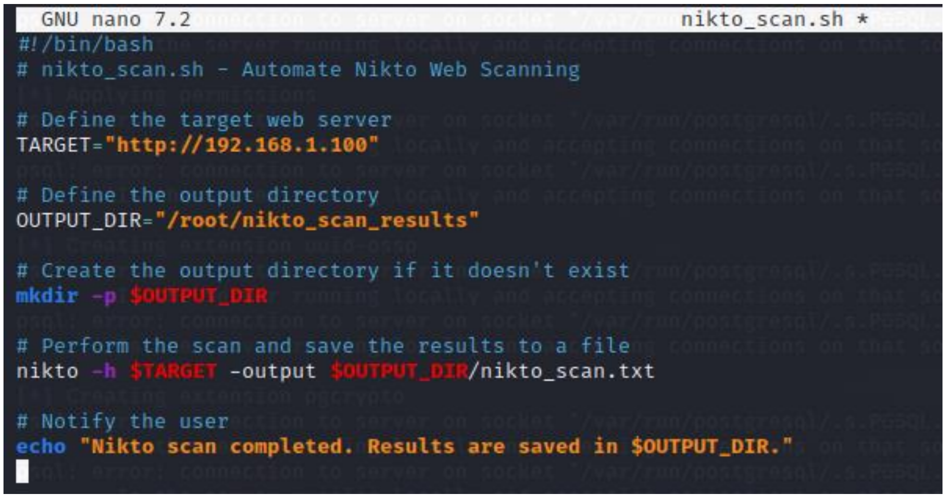
```
┌──(root㉿kali)-[/home/dj]
└─# crontab -e
no crontab for root - using an empty one

Select an editor.  To change later, run 'select-editor'.
  1. /bin/nano        <---- easiest
  2. /usr/bin/vim.basic
  3. /usr/bin/vim.tiny

Choose 1-3 [1]: 0 0 * * * /root/nmap_scan.sh
Choose 1-3 [1]: ^[:wq
Choose 1-3 [1]: 0 0 * * * /root/nmap_scan.sh
Choose 1-3 [1]: 1
crontab: installing new crontab
```

- Add a cron job to run the script daily at midnight



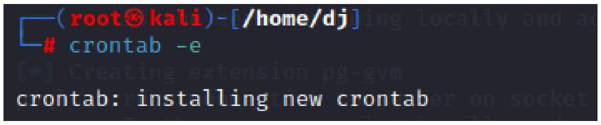
```
┌──(root㉿kali)-[/home/dj]
└─# crontab -l
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command

0 0 * * * /root/nmap_scan.sh
```

- **Automating Web Application Scanning with Nikto**
- Create a Bash Script for Nikto Scanning



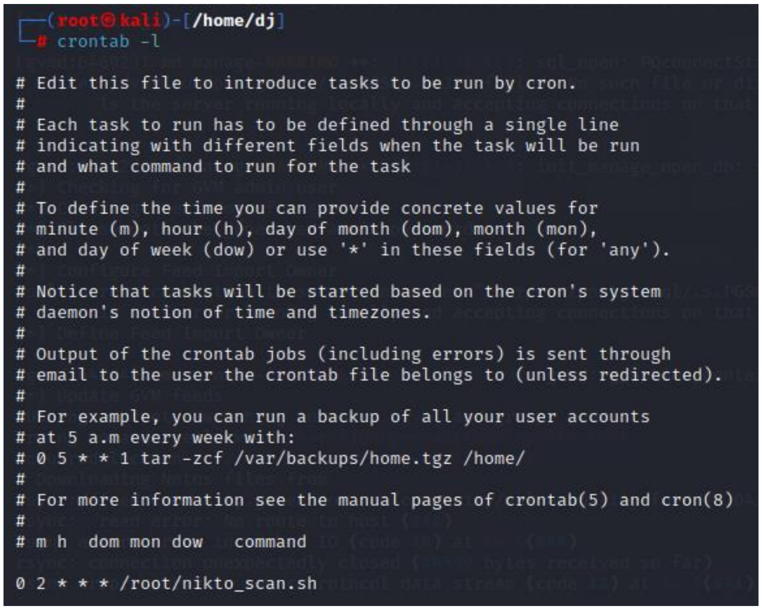
```
  GNU nano 7.2                                          nikto_scan.sh *
#!/bin/bash
# nikto_scan.sh - Automate Nikto Web Scanning

# Define the target web server
TARGET="http://192.168.1.100"

# Define the output directory
OUTPUT_DIR="/root/nikto_scan_results"

# Create the output directory if it doesn't exist
mkdir -p $OUTPUT_DIR

# Perform the scan and save the results to a file
nikto -h $TARGET -output $OUTPUT_DIR/nikto_scan.txt

# Notify the user
echo "Nikto scan completed. Results are saved in $OUTPUT_DIR."
```

- **Schedule the Script with Cron**
- Edit the crontab



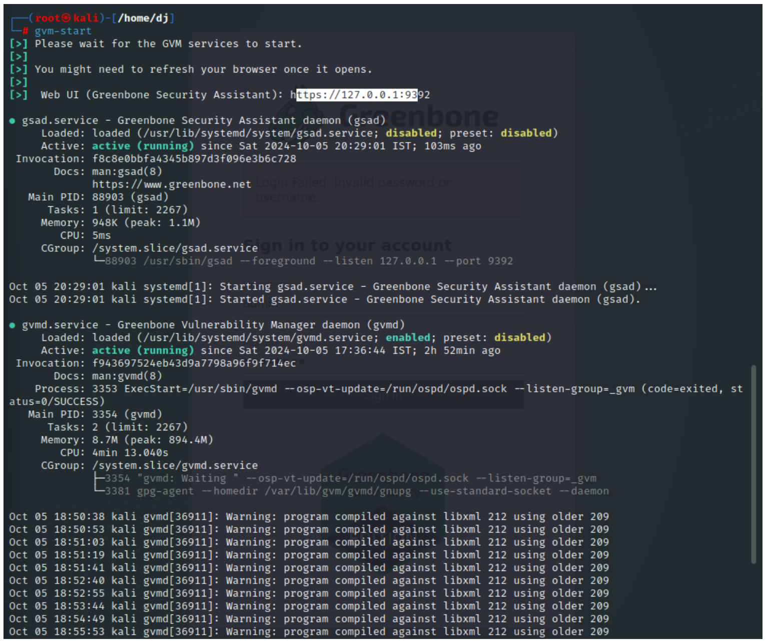
```
┌──(root㉿kali)-[/home/dj]
└─# crontab -e

crontab: installing new crontab
```

- Add a cron job to run the script every Sunday at 2 AM



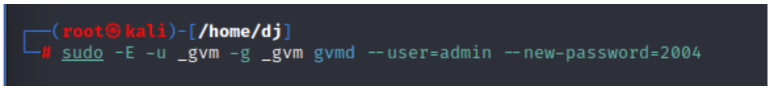
```
┌──(root㉿kali)-[/home/dj]
└─# crontab -l

# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command

0 2 * * * /root/nikto_scan.sh
```

- **Automating Vulnerability Scanning with OpenVAS**
- Start GVM



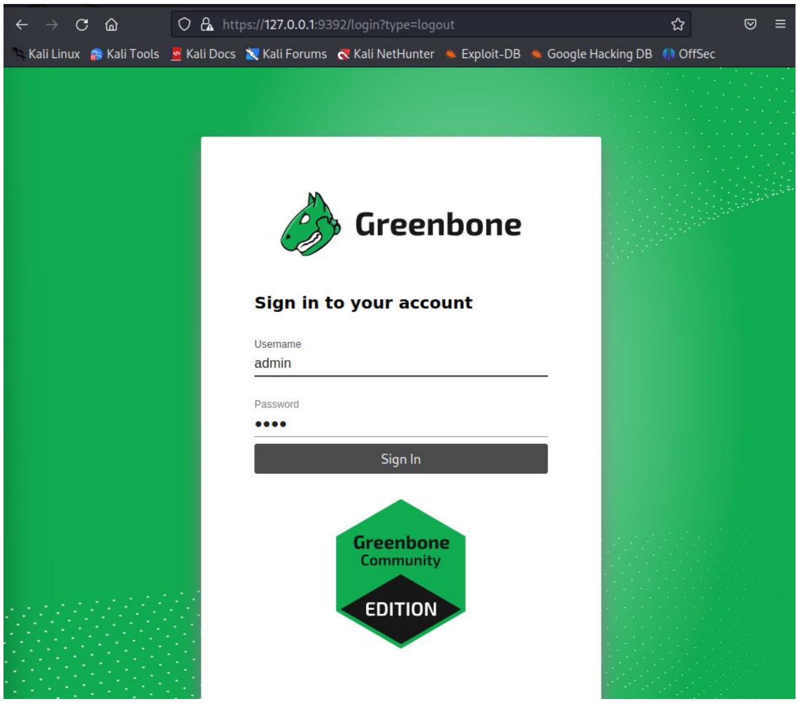
```
┌──(root㉿kali)-[/home/dj]
└─# gvm-start
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
[>]
[>]  Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

● gsad.service - Greenbone Security Assistant daemon (gsad)
     Loaded: loaded (/usr/lib/systemd/system/gsad.service; disabled; preset: disabled)
     Active: active (running) since Sat 2024-10-05 20:29:01 IST; 103ms ago
 Invocation: f8c8e0bbfa4345b897d3f096e3b6c728
       Docs: man:gsad(8)
             https://www.greenbone.net
   Main PID: 88903 (gsad)
      Tasks: 1 (limit: 2267)
     Memory: 948K (peak: 1.1M)
        CPU: 5ms
     CGroup: /system.slice/gsad.service
             └─88903 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392

Oct 05 20:29:01 kali systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gsad)...
Oct 05 20:29:01 kali systemd[1]: Started gsad.service - Greenbone Security Assistant daemon (gsad).

● gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
     Loaded: loaded (/usr/lib/systemd/system/gvmd.service; enabled; preset: disabled)
     Active: active (running) since Sat 2024-10-05 17:36:44 IST; 2h 52min ago
 Invocation: f943697524eb43d9a7798a96f9f714ec
       Docs: man:gvmd(8)
    Process: 3353 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm (code=exited, st
atus=0/SUCCESS)
   Main PID: 3354 (gvmd)
      Tasks: 2 (limit: 2267)
     Memory: 8.7M (peak: 894.4M)
        CPU: 4min 13.040s
     CGroup: /system.slice/gvmd.service
             ├─3354 "gvmd: Waiting " --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm
             └─3381 gpg-agent --homedir /var/lib/gvm/gvmd/gnupg --use-standard-socket --daemon

Oct 05 18:50:38 kali gvmd[36911]: Warning: program compiled against libxml 212 using older 209
Oct 05 18:50:53 kali gvmd[36911]: Warning: program compiled against libxml 212 using older 209
Oct 05 18:51:03 kali gvmd[36911]: Warning: program compiled against libxml 212 using older 209
Oct 05 18:51:19 kali gvmd[36911]: Warning: program compiled against libxml 212 using older 209
Oct 05 18:51:41 kali gvmd[36911]: Warning: program compiled against libxml 212 using older 209
Oct 05 18:52:40 kali gvmd[36911]: Warning: program compiled against libxml 212 using older 209
Oct 05 18:52:55 kali gvmd[36911]: Warning: program compiled against libxml 212 using older 209
Oct 05 18:53:44 kali gvmd[36911]: Warning: program compiled against libxml 212 using older 209
Oct 05 18:54:49 kali gvmd[36911]: Warning: program compiled against libxml 212 using older 209
Oct 05 18:55:53 kali gvmd[36911]: Warning: program compiled against libxml 212 using older 209
```

- Reset the gvm password



```
┌──(root㉿kali)-[/home/dj]
└─# sudo -E -u _gvm -g _gvm gvmd --user=admin --new-password=2004
```

- create a Task in GVM
- Access the GVM Web Interface
- Open your browser and navigate to https://127.0.0.1:9392.
- Log in with the credentials set during the setup.



https://127.0.0.1:9392/login?type=logout

Sign in to your account

Username: admin

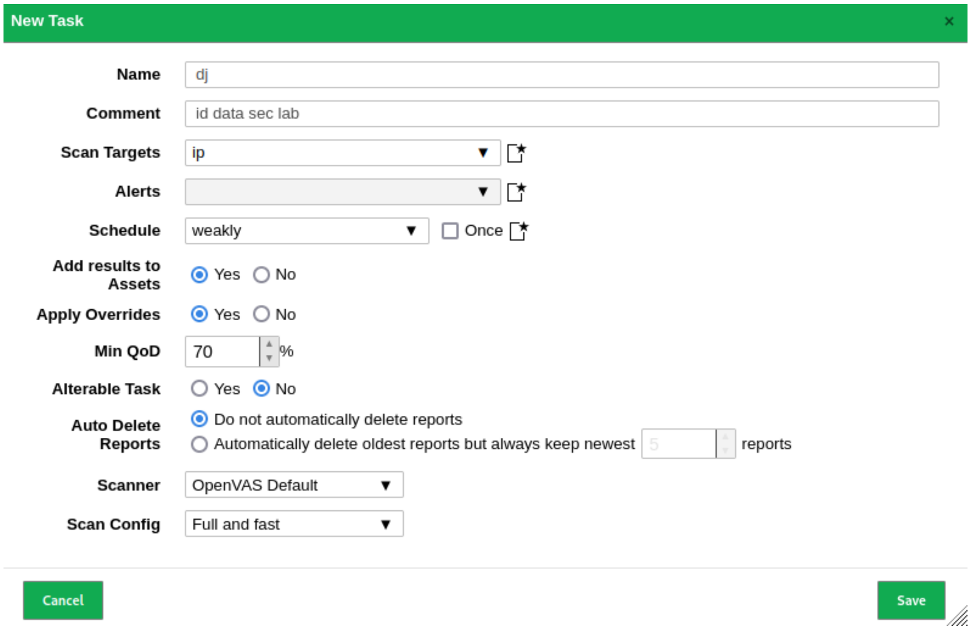
Password: ••••

- Create a New Task

➢ Go to "Scans" -> "Tasks" -> "New Task".

➢ Define the scan target (e.g., 192.168.1.0/24).

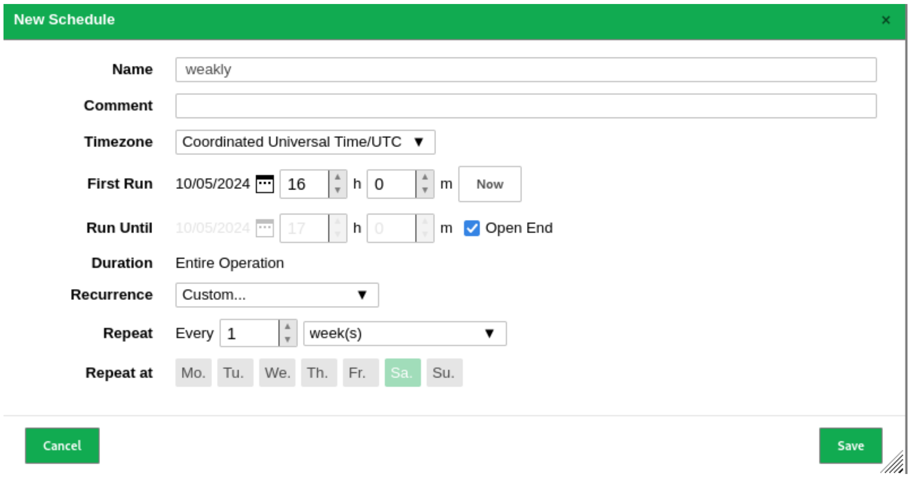
➢ Set up the scan configurations (e.g., Full and Fast)



New Task

Name	dj
Comment	id data sec lab
Scan Targets	ip ▼
Alerts	▼
Schedule	weakly ▼ □ Once
Add results to Assets	● Yes ○ No
Apply Overrides	● Yes ○ No
Min QoD	70 %
Alterable Task	○ Yes ● No
Auto Delete Reports	● Do not automatically delete reports ○ Automatically delete oldest reports but always keep newest 5 reports
Scanner	OpenVAS Default ▼
Scan Config	Full and fast ▼

- Schedule the Task:

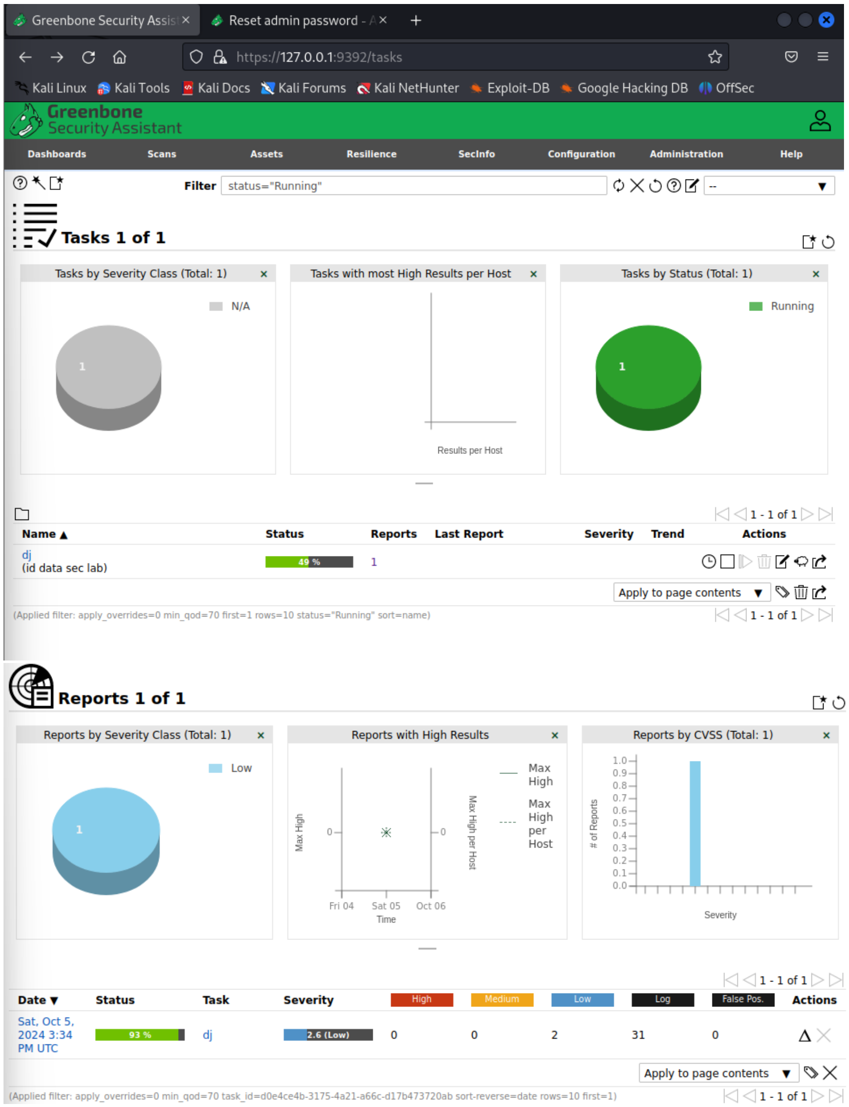


New Schedule ×

Name	weakly
Comment	
Timezone	Coordinated Universal Time/UTC ▼
First Run	10/05/2024 16 h 0 m Now
Run Until	10/05/2024 17 h 0 m ☑ Open End
Duration	Entire Operation
Recurrence	Custom... ▼
Repeat	Every 1 week(s) ▼
Repeat at	Mo. Tu. We. Th. Fr. Sa. Su.

Cancel Save

- Review and Save the Task:



Filter status="Running" --

Tasks 1 of 1

Tasks by Severity Class (Total: 1) ×
N/A
1
Tasks with most High Results per Host ×
Results per Host
Tasks by Status (Total: 1) ×
Running
1

1 - 1 of 1

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
dj (id data sec lab)	49 %	1				

Apply to page contents ▼

(Applied filter: apply_overrides=0 min_qod=70 first=1 rows=10 status="Running" sort=name)

1 - 1 of 1

Reports 1 of 1

1 - 1 of 1

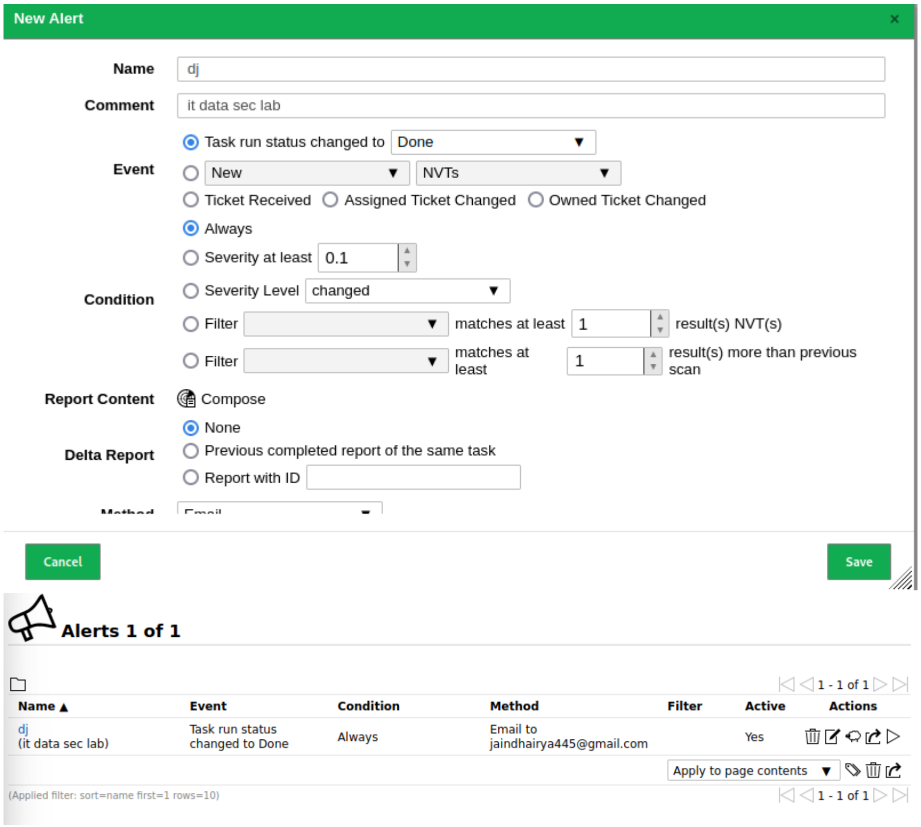
Date ▼	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Sat, Oct 5, 2024 3:34 PM UTC	93 %	dj	2.6 (Low)	0	0	2	31	0	

Apply to page contents ▼

(Applied filter: apply_overrides=0 min_qod=70 task_id=d0e4ce4b-3175-4a21-a66c-d17b473720ab sort-reverse=date rows=10 first=1)

1 - 1 of 1

- Automate Report Generation and Alerts
- Set Up Alerts
  - Go to "Configuration" -> "Alerts"
  - Configure an alert to email you the scan report or notify you via other channels



New Alert ×

Name	dj
Comment	it data sec lab
Event	● Task run status changed to Done ▼ ○ New ▼ NVTs ▼ ○ Ticket Received ○ Assigned Ticket Changed ○ Owned Ticket Changed
Condition	● Always ○ Severity at least 0.1 ○ Severity Level changed ▼ ○ Filter ▼ matches at least 1 result(s) NVT(s) ○ Filter ▼ matches at least 1 result(s) more than previous scan
Report Content	Compose
Delta Report	● None ○ Previous completed report of the same task ○ Report with ID
Method	Email ▼

Alerts 1 of 1

1 - 1 of 1

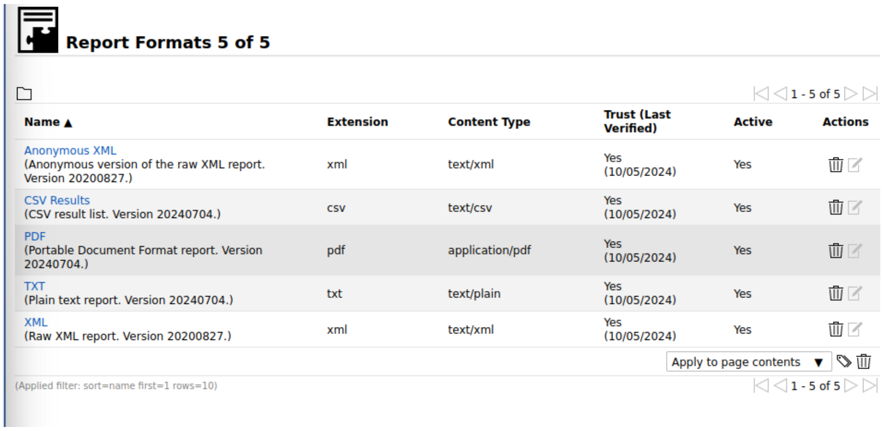
Name ▲	Event	Condition	Method	Filter	Active	Actions
dj (it data sec lab)	Task run status changed to Done	Always	Email to jaindhairya445@gmail.com		Yes	

Apply to page contents ▼

(Applied filter: sort=name first=1 rows=10)

1 - 1 of 1

- Configure Report Format:
  - Go to "Configuration" -> "Reports".
  - Choose the report format (e.g., PDF, XML) and configure the details



Report Formats 5 of 5

1 - 5 of 5

Name ▲	Extension	Content Type	Trust (Last Verified)	Active	Actions
Anonymous XML (Anonymous version of the raw XML report. Version 20200827.)	xml	text/xml	Yes (10/05/2024)	Yes	
CSV Results (CSV result list. Version 20240704.)	csv	text/csv	Yes (10/05/2024)	Yes	
PDF (Portable Document Format report. Version 20240704.)	pdf	application/pdf	Yes (10/05/2024)	Yes	
TXT (Plain text report. Version 20240704.)	txt	text/plain	Yes (10/05/2024)	Yes	
XML (Raw XML report. Version 20200827.)	xml	text/xml	Yes (10/05/2024)	Yes	

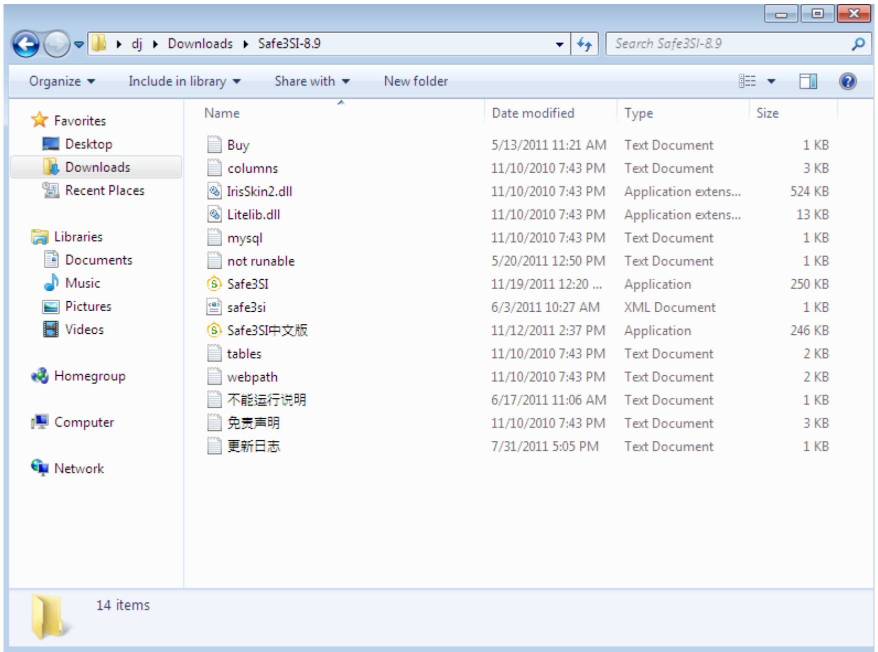
Apply to page contents ▼

(Applied filter: sort=name first=1 rows=10)

1 - 5 of 5

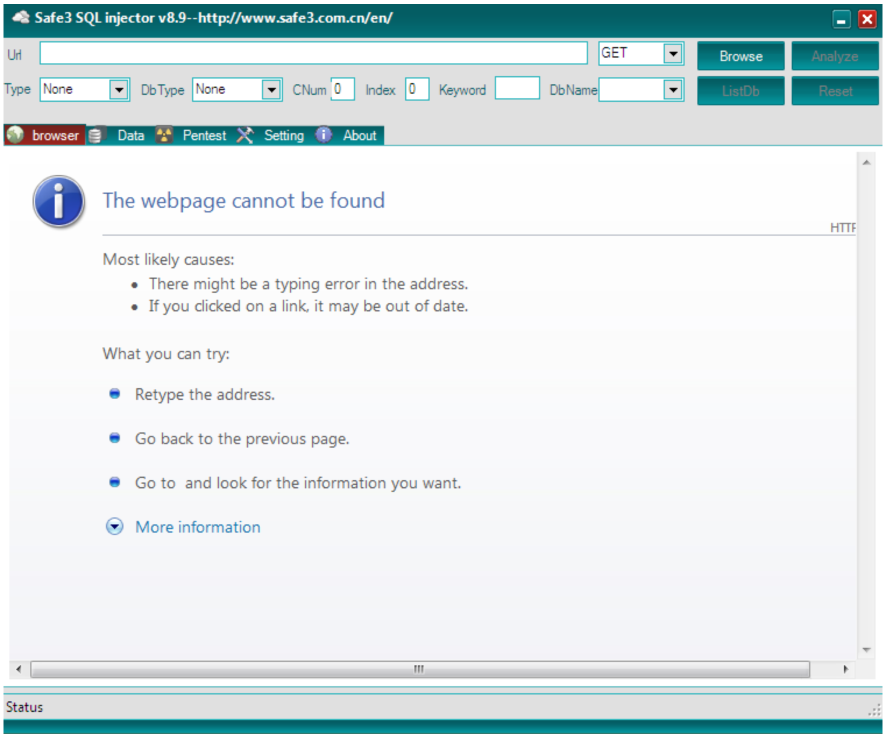
- **Workflow: Complete Automated Security Testing**
- Nmap Scan at Midnight:
  - The Nmap script runs every day at midnight, scanning your network for open ports and vulnerabilities.
  - Results are saved in /root/nmap_scan_results/ and can be reviewed daily
- Nikto Scan on Sunday at 2 AM:
  - The Nikto script runs weekly, checking your web server for vulnerabilities
  - Results are saved in /root/nikto_scan_results/ for weekly review.
- OpenVAS Weekly Scans:
  - OpenVAS runs a comprehensive scan every week, reporting on any new vulnerabilities found.
  - Alerts are configured to notify you of the results via email.
- **Reviewing and Responding to Scan Results**
- Daily/Weekly Review:
  - Regularly check the output directories for Nmap and Nikto results
  - OpenVAS reports can be reviewed directly in the GVM web interface or via email
- Respond to Vulnerabilities:
  - Prioritize vulnerabilities based on severity
  - Patch software, reconfigure services, and apply security measures as needed

- **Setting Up Safe3 SQL Injector on Windows**
- Download and Install Safe3 SQL Injector



Name	Date modified	Type	Size
Buy	5/13/2011 11:21 AM	Text Document	1 KB
columns	11/10/2010 7:43 PM	Text Document	3 KB
IrisSkin2.dll	11/10/2010 7:43 PM	Application extens...	524 KB
Litelib.dll	11/10/2010 7:43 PM	Application extens...	13 KB
mysql	11/10/2010 7:43 PM	Text Document	1 KB
not runable	5/20/2011 12:50 PM	Text Document	1 KB
Safe3SI	11/19/2011 12:20 ...	Application	250 KB
safe3si	6/3/2011 10:27 AM	XML Document	1 KB
Safe3SI中文版	11/12/2011 2:37 PM	Application	246 KB
tables	11/10/2010 7:43 PM	Text Document	2 KB
webpath	11/10/2010 7:43 PM	Text Document	2 KB
不能运行说明	6/17/2011 11:06 AM	Text Document	1 KB
免责声明	11/10/2010 7:43 PM	Text Document	3 KB
更新日志	7/31/2011 5:05 PM	Text Document	1 KB

- Launch Safe3 SQL Injector



The webpage cannot be found

Most likely causes:

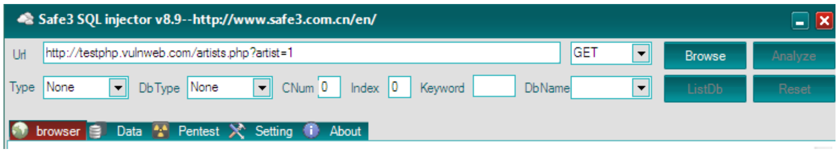
- There might be a typing error in the address.
- If you clicked on a link, it may be out of date.

What you can try:

- Retype the address.
- Go back to the previous page.
- Go to and look for the information you want.

More information

- Identifying SQL Injection Vulnerabilities with Safe3 SQL Injector
- Input the Target URL

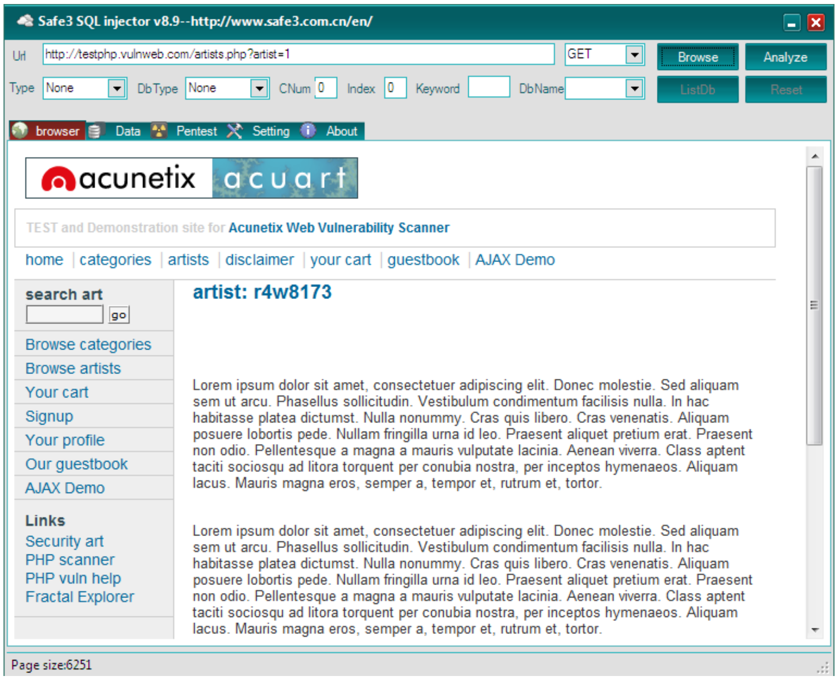


Safe3 SQL injector v8.9--http://www.safe3.com.cn/en/

Url: http://testphp.vulnweb.com/artists.php?artist=1 GET

Type: None DbType: None CNum: 0 Index: 0 Keyword: DbName:

- Test for SQL Injection



Safe3 SQL injector v8.9--http://www.safe3.com.cn/en/

Url: http://testphp.vulnweb.com/artists.php?artist=1 GET

Type: None DbType: None CNum: 0 Index: 0 Keyword: DbName:

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art

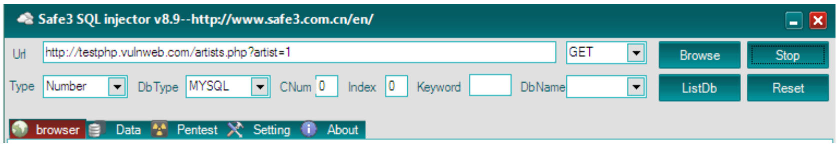
artist: r4w8173

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

Page size:6251

- Analyze the Results

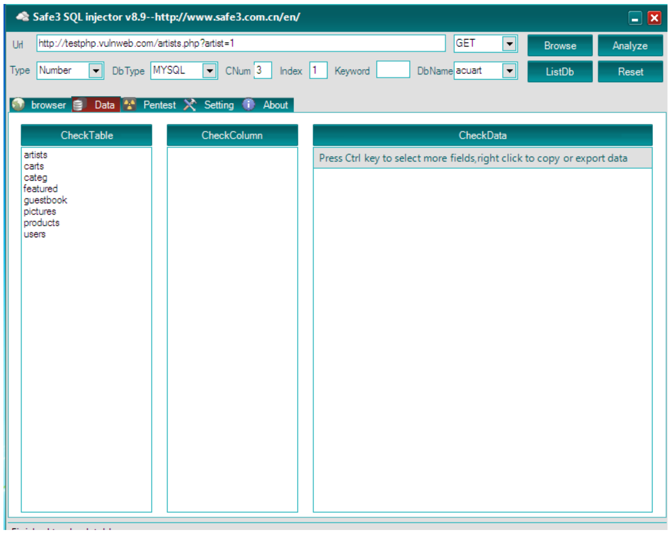


Safe3 SQL injector v8.9--http://www.safe3.com.cn/en/

Url: http://testphp.vulnweb.com/artists.php?artist=1 GET

Type: Number DbType: MYSQL CNum: 0 Index: 0 Keyword: DbName:

Type number



Safe3 SQL injector v8.9--http://www.safe3.com.cn/en/

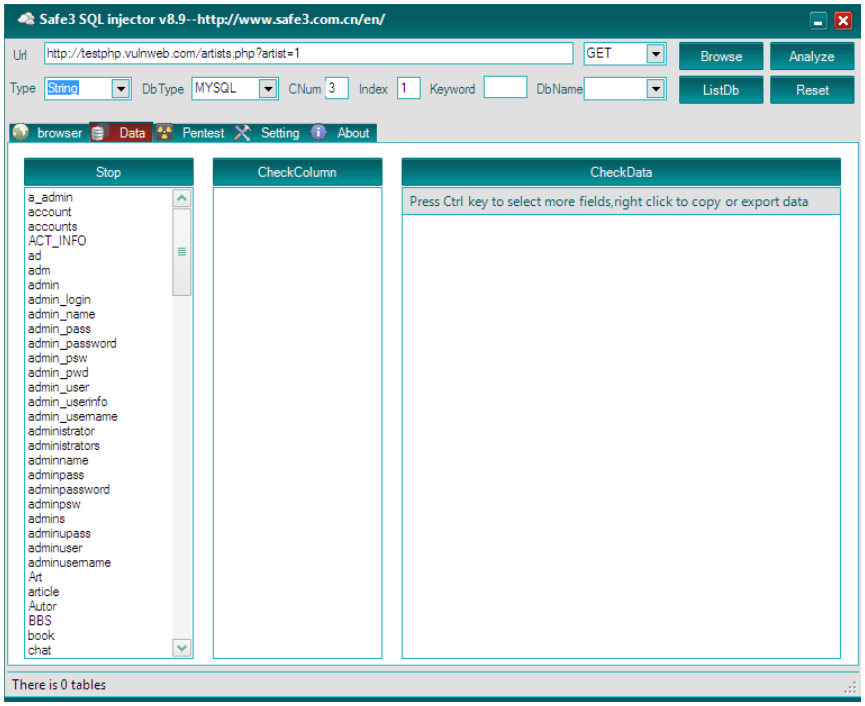
Url: http://testphp.vulnweb.com/artists.php?artist=1 GET

Type: Number DbType: MYSQL CNum: 3 Index: 1 Keyword: DbName: acuart

CheckTable:
artists
carts
categ
featured
guestbook
pictures
products
users

Press Ctrl key to select more fields,right click to copy or export data

Type- string



Url http://testphp.vulnweb.com/artists.php?artist=1 GET

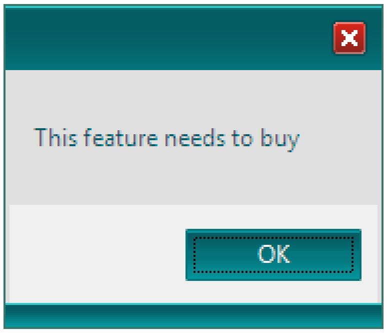
Type String DbType MYSQL CNum 3 Index 1 Keyword DbName

Press Ctrl key to select more fields,right click to copy or export data

a_admin
account
accounts
ACT_INFO
ad
adm
admin
admin_login
admin_name
admin_pass
admin_password
admin_psw
admin_pwd
admin_user
admin_userinfo
admin_username
administrator
administrators
adminname
adminpass
adminpassword
adminpsw
admins
adminupass
adminuser
adminusername
Art
article
Autor
BBS
book
chat

There is 0 tables

- **Exploiting SQL Injection with Safe3 SQL Injector**
- Extract Database Information



This feature needs to buy

Safe3 sql injector is asking to buy feature to continue to sql injection.