**CYBERSECURITY OFFENSIVE AND DEFENSIVE PROJECT**

**NAME: SHARANKUMAR VR**

**LINKEDIN:** [**https://www.linkedin.com/in/sharan-kumar-vr-4a287a376**](https://www.linkedin.com/in/sharan-kumar-vr-4a287a376)

**PROJECT-1: WAVE**

**WAVE-**WebAutomation vulnerability Explorer (***80% completed***)

The CLI based Automation tool which build for Linux operating system. Which has ability to scan Top vulnerability in a Domain(website) and report writing in Json or html format and scans for vulnerability in network configuration.

Disclaimer: *Kindly don’t scan this tool on Domains which u don’t have permission.*

Git hub: <https://github.com/rootatsharan/WAVE>

HOW TO TEST(DEMO):

**1.INSTALLATION:**

Open Linux(kali) terminal and type

**sudo apt install git**

**git clone https://github.com/rootatsharan/WAVE.git**

**cd WAVE**

**chmod +x ./MENU.sh**

**./MENU.sh**

****

**2.Create a domain with Vulnerabilities:**

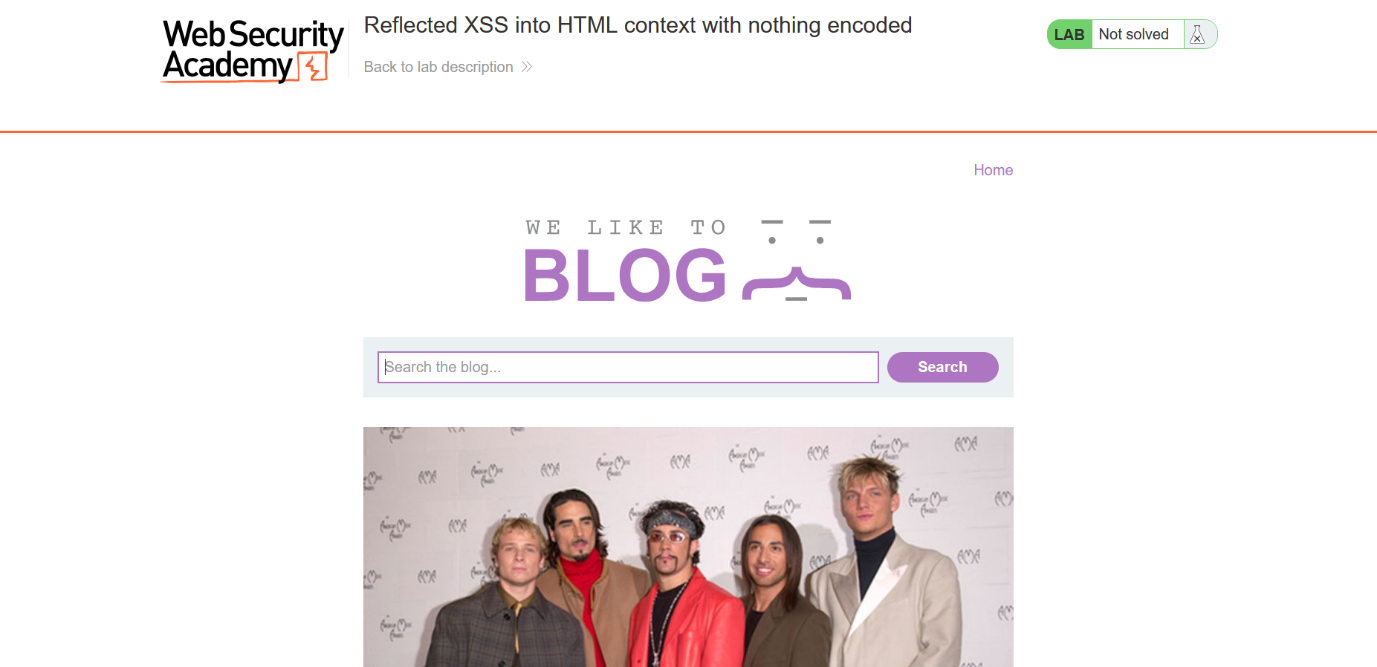
Create account(cost free) at portswigger labs: https://portswigger.net/

Select acedamy ---All content—all labs

Click on cross-site scripting and click first lab and then click access the lab

A screenshot of a computer

AI-generated content may be incorrect.



A website with XSS vulnerability is created

Type hello in search bar and copy the above link

Example:https://0ab5003403ae87ab80d7582d00880075.web-security-academy.net/?search=hello

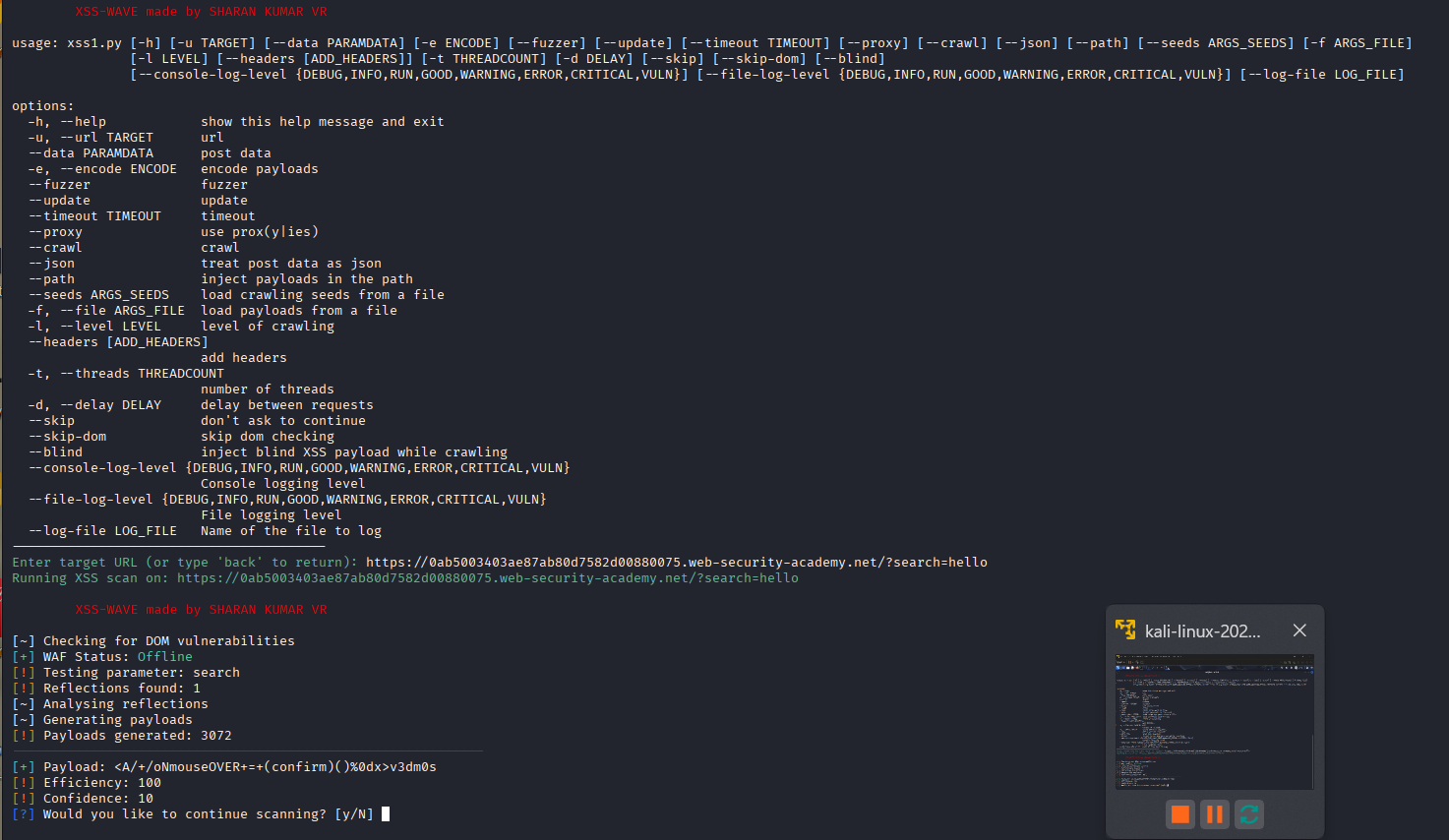
A screenshot of a computer

AI-generated content may be incorrect.

3.Testing The Domain With WAVE:

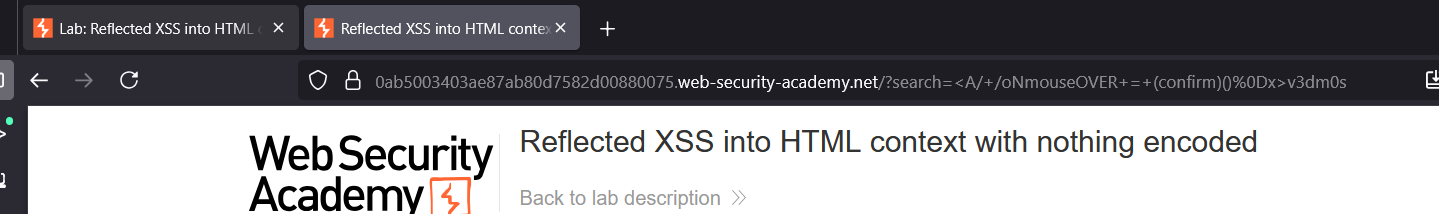
./MENU.sh

Enter 1(refer screenshot below)

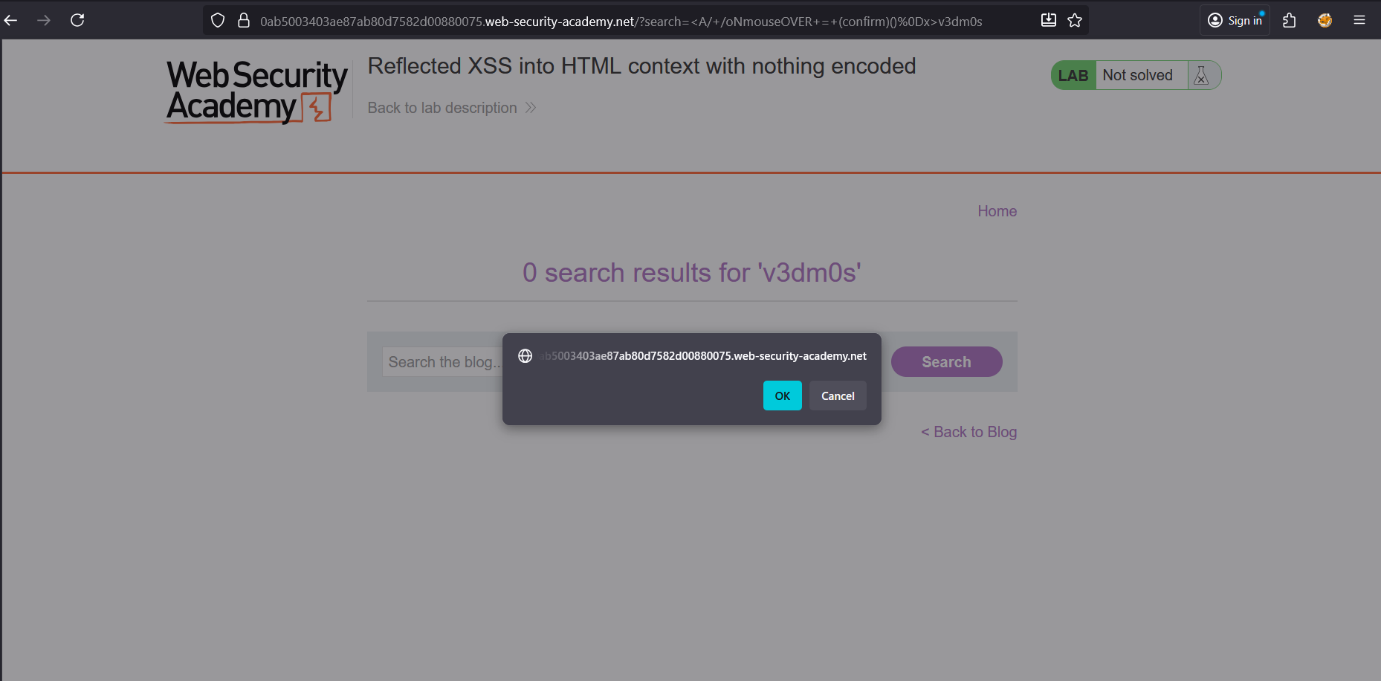


You can conform that I found a XSS in the given url

Verify it manually copy the payload and replace with hello



Now u can see the the popup like this:



THE POPUP CONFIRMS THE XSS .

Do the same thing for other section to verify it this tool is working.

Since it is 80 percentage completes some sections and report wrapping is not yet done.

**REAL-LIFE TESTING RESULT:**

VISIT :<https://www.elala.in/>

In Search box type “onmouseover=”alert(document.cookie)

This payload is used to steal the cookie of user and steal admin cookie can give access to admin account ..so it is vertical previlage escalation through

XSS.

**PROJECT-2: ECHO DEFEND**

ECHODEFEND is an automated command execution and result delivery tool built for cybersecurity operations. It fetches a remote command file (hosted via HTTP ), executes the listed CLI commands on the local system, records the results, and sends the output instantly to a chosen webhook endpoint (e.g., Slack/Discord/HTTP API).

This enables remote, centralized control and rapid sharing of execution results for red teaming, penetration testing labs, or distributed vulnerability assessment scenarios.

A screenshot of a computer screen

AI-generated content may be incorrect.

A diagram of a computer

AI-generated content may be incorrect.

HOW TO USE ECODEFEND:

1.setup Netlify Account and then link that with github:

For demo login credentials is below:

Google:sharankumarvr7@gmail.com

Password:$$SHARAN##p

Then open github and login via continue with goolge

U can see the  repositories click command\_server and download echodefend.exe on the target machine

A screen shot of a computer

AI-generated content may be incorrect.

Since the publisher unknown for this application so it is showing blue screen so click option **more info and click run anyway**

**A screenshot of a computer error

AI-generated content may be incorrect.**

**OPEN BROWSER AND GO TO** [**https://webhook.site/**](https://webhook.site/) **AND COPY THE YOUR UNIQUE URL(reciever)**

A screenshot of a computer

AI-generated content may be incorrect.

A black screen with white text

AI-generated content may be incorrect.

NOW open github and edit command.txt …enter same exact command that should be run on target host example given below

A screenshot of a computer

AI-generated content may be incorrect.

Example command : tasklist ,task kill <piid> ,sysinfo,ipconfig or run ur script like capture keystrokes for log analyses(after attack or malicious things happens)

Output: visit webhook url A screenshot of a computer

AI-generated content may be incorrect.

Here are practical **applications for your ECHODEFEND tool**:

* **Automated Vulnerability Assessment**
  + Remotely distribute and execute security testing scripts or commands (e.g., nmap scans, XSS/SQLi payloads) across multiple target machines.
  + Collect results centrally via webhook for rapid analysis.
* **Red Team Operations**
  + Trigger custom exploit/test commands on remote systems from a central script server, streamlining coordinated security tests and exercises.
* **Penetration Testing in Enterprise Networks**
  + Run routine or targeted tests (privilege escalation checks, recon commands) on endpoints automatically, collect logs via webhook integration.
* **Security Monitoring and Incident Response**
  + Push detection/response commands on compromised systems, instantly relay evidence (output/logs) back to incident responders.
* **Remote IT Management and Scripting**
  + Dispatch batch administrative tasks, updates, or queries (e.g., disk space checks, user enumeration) to a fleet of clients, automate result collection without manual login.
* **IoT/Edge Device Auditing**
  + Schedule/trigger commands on remote IoT devices or servers, gather telemetry and security posture data for compliance tracking.
* **Continuous Integration (CI/CD) Testing**
  + Integrate with DevSecOps pipelines to automate post-deployment security checks, trending results sent to dashboards/webhook endpoints.

Run artifact or file collection commands across distributed nodes, relay investigation data to central analysts securely and quickly.

* **Forensics Collection**
  + Run artifact or file collection commands across distributed nodes, relay investigation data to central analysts securely and quickly.

**THANKING YOU**