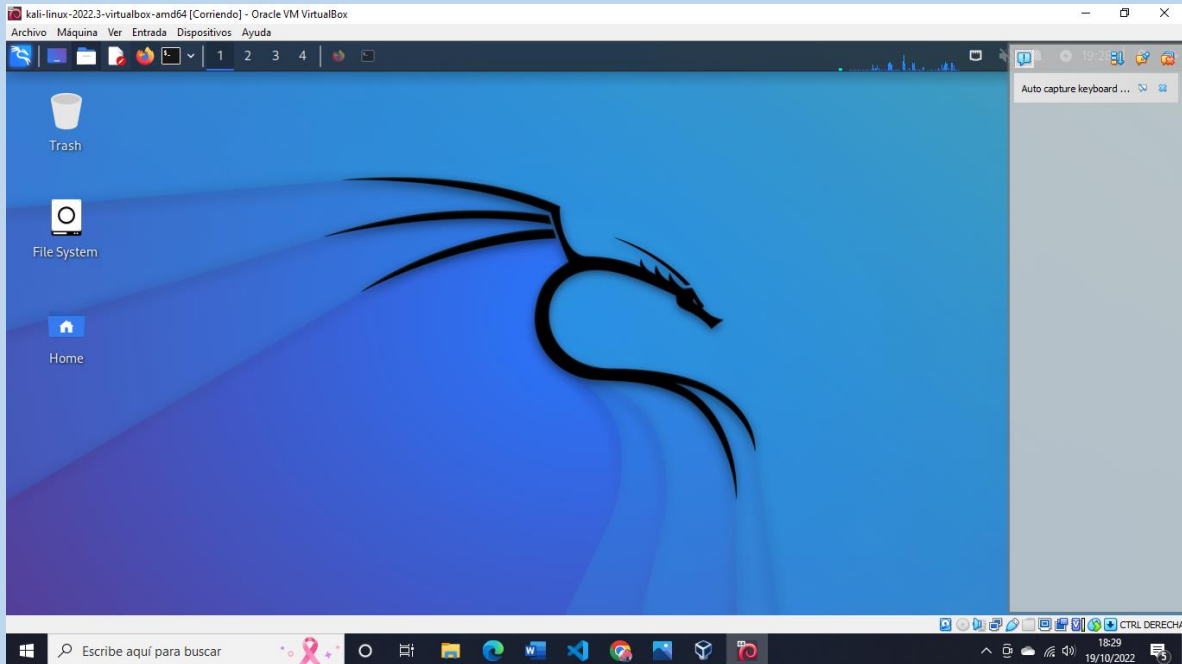
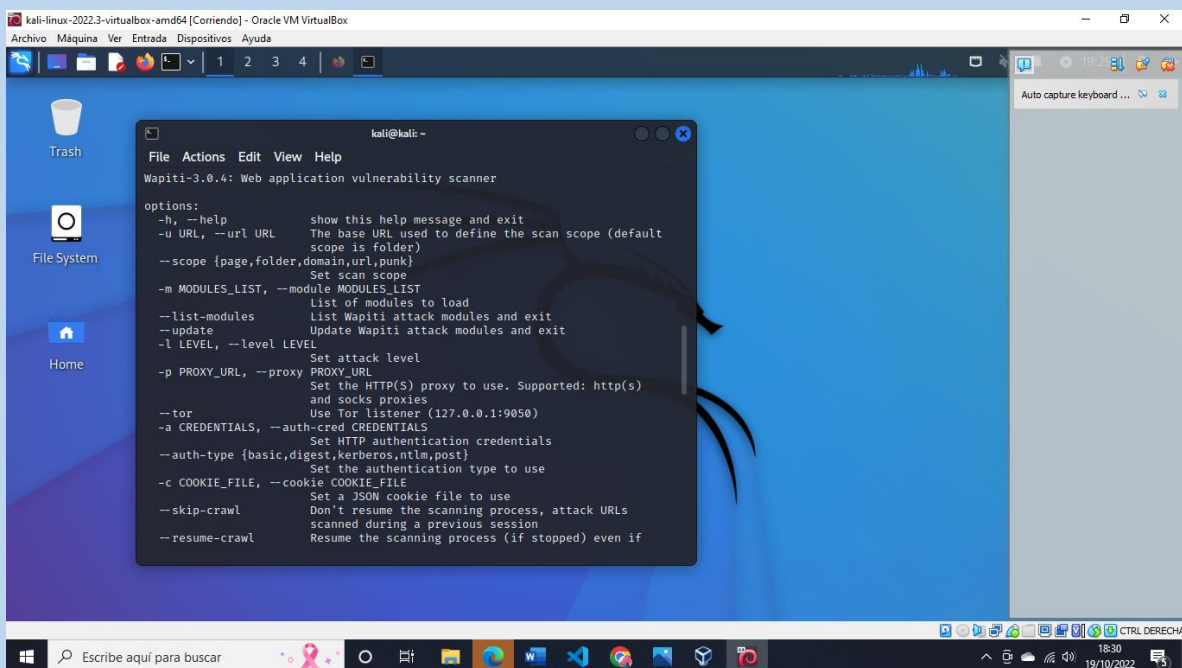


# Usando Wapiti con KALI LINUX

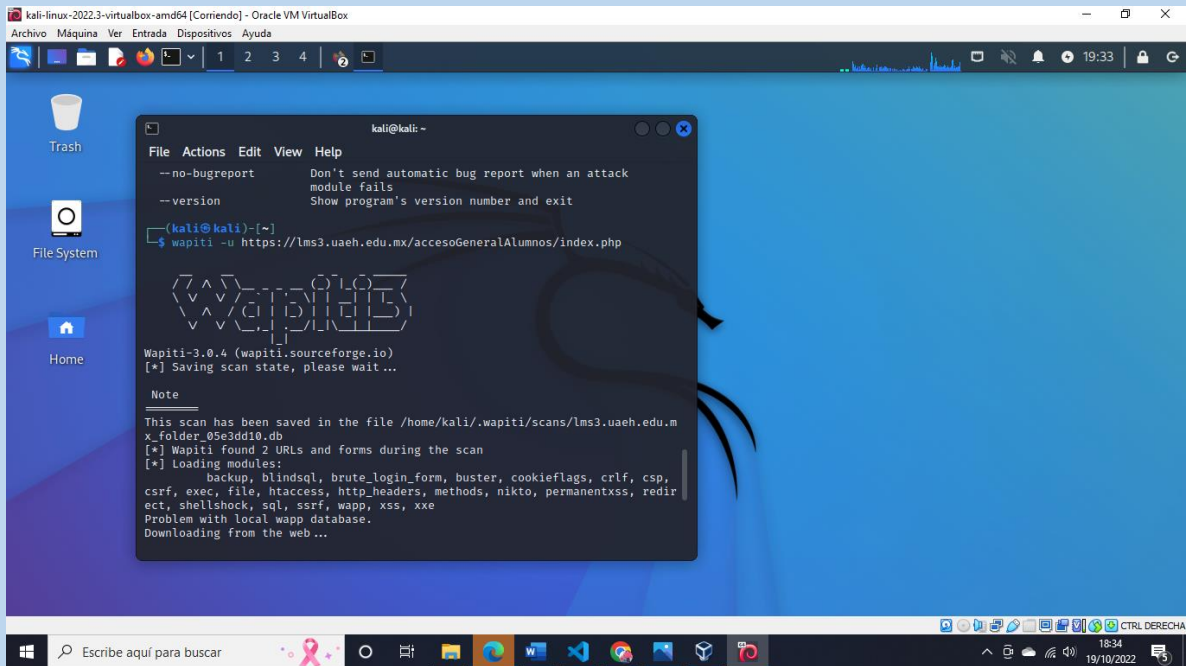
## 1.- Abrimos nuestra máquina virtual



## 2.- Escribimos en la terminal wapiti -h

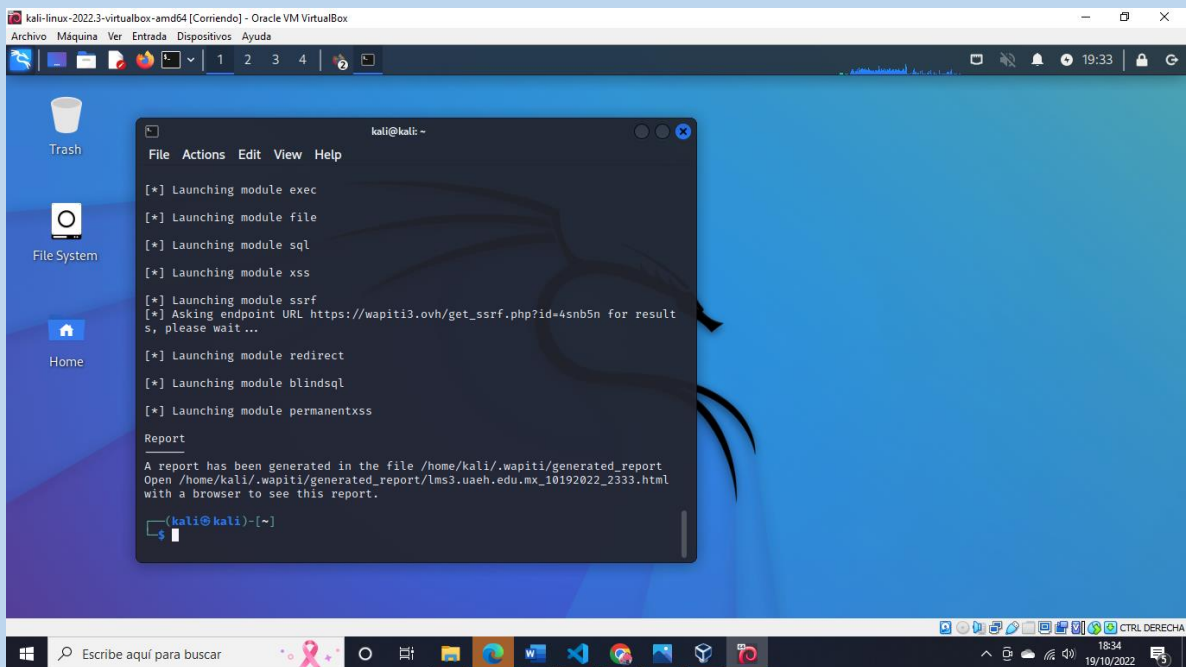


### 3.- Después con el siguiente comando wapiti -u Ponemos el URL



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the output of the command `wapiti -u https://lms3.uaeh.edu.mx/accesoGeneralAlumnos/index.php`. The output includes the Wapiti logo, version information (3.0.4), a note about saving the scan state, and a list of modules being loaded. The desktop background is blue with icons for Trash, File System, and Home. The taskbar at the bottom shows various application icons and the system clock.

```
kali@kali: ~  
File Actions Edit View Help  
--no-bugreport      Don't send automatic bug report when an attack  
--version           Show program's version number and exit  
[kali@kali]~$ wapiti -u https://lms3.uaeh.edu.mx/accesoGeneralAlumnos/index.php  
  
Wapiti-3.0.4 (wapiti.sourceforge.io)  
[*] Saving scan state, please wait...  
  
Note  
This scan has been saved in the file /home/kali/.wapiti/scans/lms3.uaeh.edu.m  
x_folder_05e3dd18.db  
[*] Wapiti found 2 URLs and forms during the scan  
[*] Loading modules:  
    backup, blindsql, brute_login_form, buster, cookieflags, crlf, csp,  
    csrf, exec, file, htaccess, http_headers, methods, nikto, permanentxss, redir  
    ect, shellshock, sql, ssrf, wapp, xss, xxe  
Problem with local wapp database.  
Downloading from the web ...
```



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the output of the command `wapiti -u https://lms3.uaeh.edu.mx/accesoGeneralAlumnos/index.php`. The output includes the Wapiti logo, version information (3.0.4), a note about saving the scan state, and a list of modules being loaded. The desktop background is blue with icons for Trash, File System, and Home. The taskbar at the bottom shows various application icons and the system clock.

```
kali@kali: ~  
File Actions Edit View Help  
[*] Launching module exec  
[*] Launching module file  
[*] Launching module sql  
[*] Launching module xss  
[*] Launching module ssrf  
[*] Asking endpoint URL https://wapiti3.ovh/get_ssrf.php?id=4snb5n for result  
s, please wait...  
[*] Launching module redirect  
[*] Launching module blindsql  
[*] Launching module permanentxss  
  
Report  
A report has been generated in the file /home/kali/.wapiti/generated_report  
Open /home/kali/.wapiti/generated_report/lms3.uaeh.edu.mx_10192022_2333.html  
with a browser to see this report.  
[kali@kali]~$
```

4.- Una vez finalizado, Wapiti nos muestra una dirección en donde podemos descargar y ver el informe de resultados

**Wapiti vulnerability report**

Target: <https://lms3.uaeh.edu.mx/accesoGeneralAlumnos/index.php>

Date of the scan: Wed, 19 Oct 2022 23:33:15 +0000. Scope of the scan: folder

---

**Summary**

Category	Number of vulnerabilities found
Backup file	0
Blind SQL Injection	0
Weak credentials	0
CRLF Injection	0
<a href="#">Content Security Policy Configuration</a>	1
Cross Site Request Forgery	0

---

Resource consumption 0

Fingerprint web technology 0

---

**Content Security Policy Configuration**

**Description**

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

**Vulnerability found in /accesoGeneralAlumnos/index.php**

Description	HTTP Request	cURL command line
CSP is not set		

---

**Solutions**

El informe nos muestra los resultados de las vulnerabilidades y las posibles soluciones que podemos implementar.