



Beykoz University

Department of “Computer Engineering”

**“Advanced Topics in Cyber Security -
60613MEEOS-CMEo388”**

2nd Review of Project

Web Application Testing - Kali Linux

- Interim Report -

Lecturer: SHAHZAD AHMED MEMON

Leyla Abdullayeva - 1904010038

Project Description:

The project "Web Application Security Testing with Kali Linux" aims to assess the security of web applications using various tools available in Kali Linux, such as Nikto, Nmap, and XSSer. The testing involves identifying vulnerabilities in web applications and exploiting them to evaluate the effectiveness of the security controls in place. The project also includes documentation of the testing methodology, findings, and recommendations for improving the security posture of the web application.

Categories of Tools that I'll use for my project:

- Information Gathering
- Web Application Scanning
- SQL Injection
- Cross-Site Scripting (XSS)

Design and Implementation (Demo)

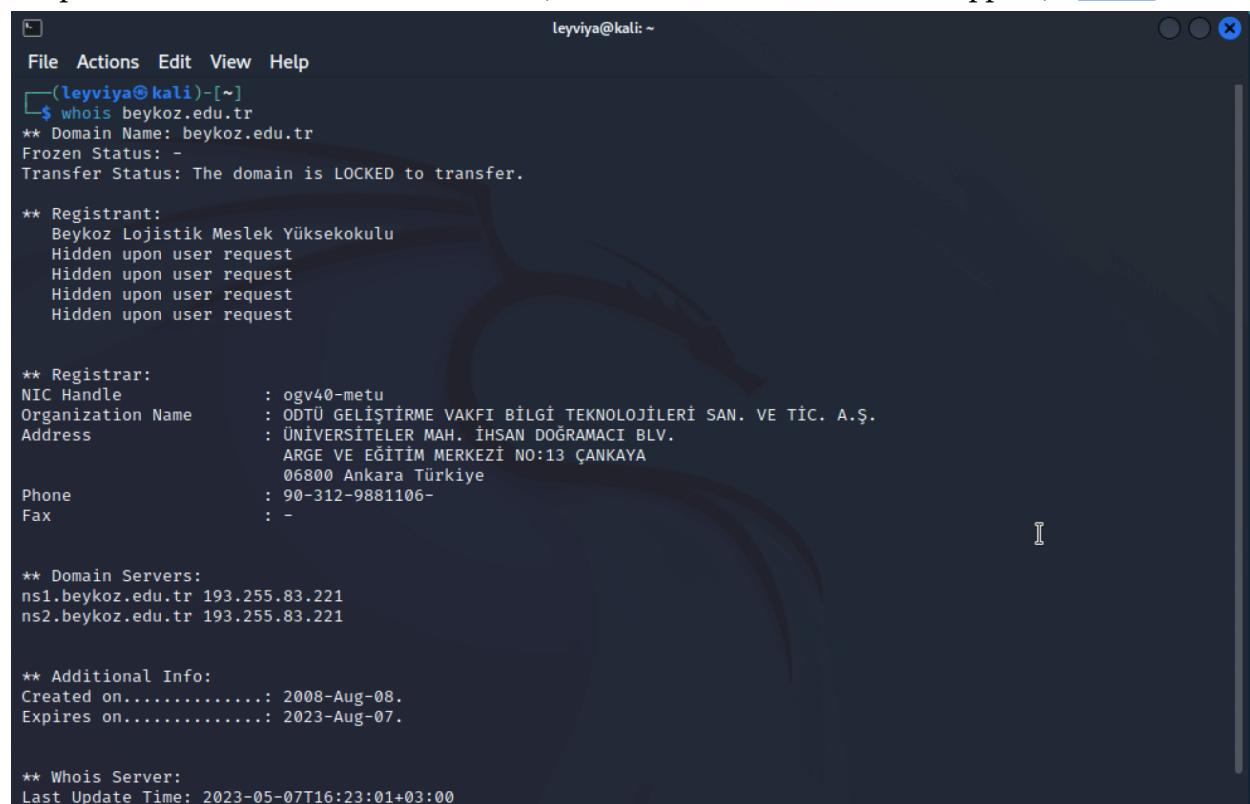
I choose only 1 tool for each category, I'll use more for final submission. I've added snapshots and screenshots of the tools that I've used with Kali Linux. Outcome analysis is provided for each.

1. Information Gathering

Whois

To identify the owner of a website or domain

Snapshot & Screenshot from Kali Linux: (Click on the link and video will appear) - [whois](#)



```
leyviya@kali: ~
File Actions Edit View Help
(leyviya@kali)-[~]
$ whois beykoz.edu.tr
** Domain Name: beykoz.edu.tr
Frozen Status: -
Transfer Status: The domain is LOCKED to transfer.

** Registrant:
Beykoz Lojistik Meslek Yüksekokulu
Hidden upon user request
Hidden upon user request
Hidden upon user request
Hidden upon user request

** Registrar:
NIC Handle : ogv40-metu
Organization Name : ODTÜ GELİŞTİRME VAKFI BİLGİ TEKNOLOJİLERİ SAN. VE TİC. A.Ş.
Address : ÜNİVERSİTELER MAH. İHSAN DOĞRAMACI BLV.
          ARGE VE EĞİTİM MERKEZİ NO:13 ÇANKAYA
          06800 Ankara Türkiye
Phone : 90-312-9881106-
Fax : -

** Domain Servers:
ns1.beykoz.edu.tr 193.255.83.221
ns2.beykoz.edu.tr 193.255.83.221

** Additional Info:
Created on.....: 2008-Aug-08.
Expires on.....: 2023-Aug-07.

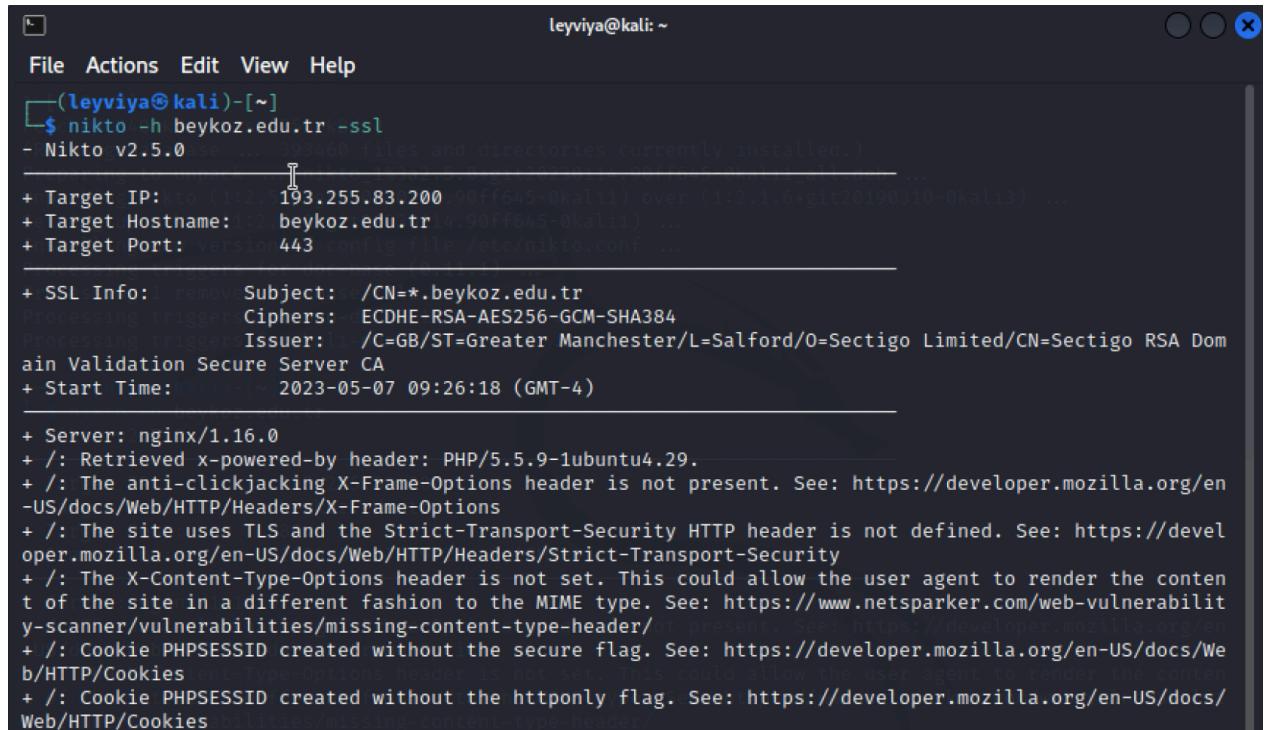
** Whois Server:
Last Update Time: 2023-05-07T16:23:01+03:00
```

2. Web Application Scanning

Nikto

To scan web servers for potential security issues and vulnerabilities

Snapshot & Screenshot from Kali Linux: (Click on the link and video will appear) - [nikto](#)



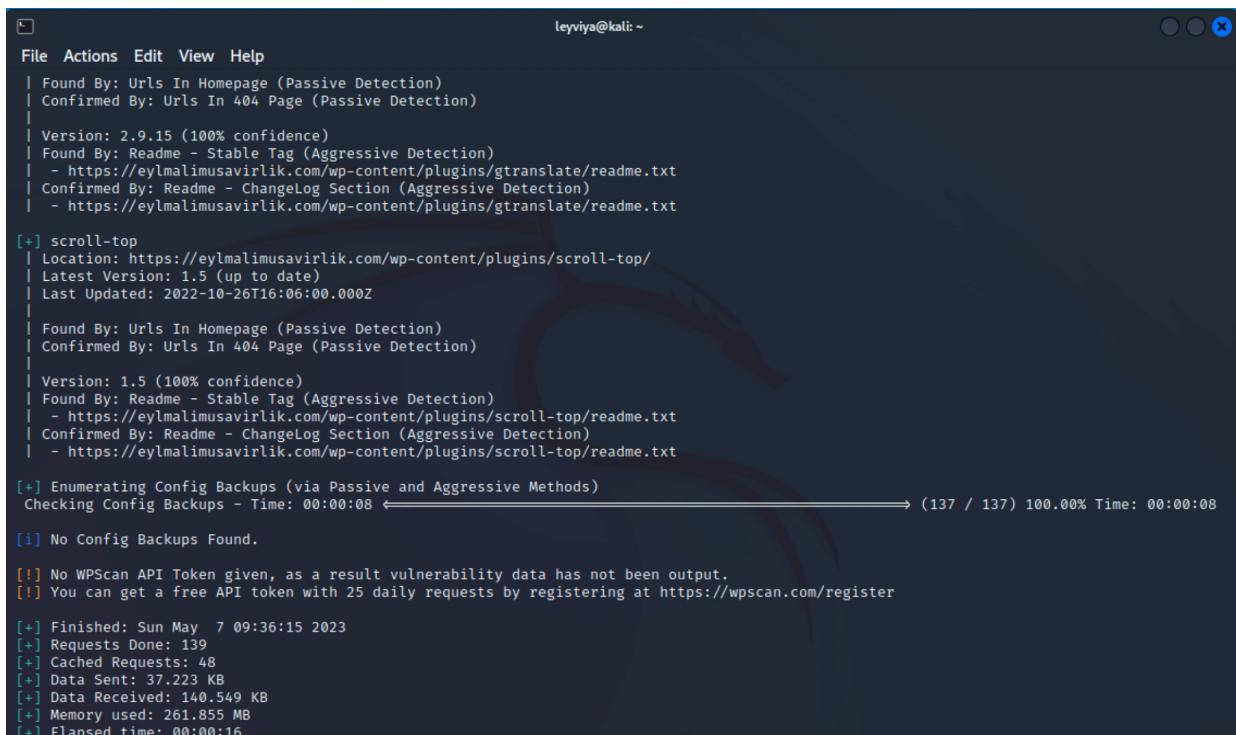
```
leyviya@kali: ~
File Actions Edit View Help
[+] (leyviya㉿kali)-[~]
$ nikto -h beykoz.edu.tr -ssl
- Nikto v2.5.0
+ Target IP: 193.255.83.200 (193.255.83.200)
+ Target Hostname: beykoz.edu.tr (193.255.83.200)
+ Target Port: 443 config file: /etc/nikto.conf ...
+ SSL Info: Subject: /CN=*.beykoz.edu.tr
  Ciphers: ECDHE-RSA-AES256-GCM-SHA384
  Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=Sectigo Limited/CN=Sectigo RSA Domain Validation Secure Server CA
+ Start Time: 2023-05-07 09:26:18 (GMT-4)

+ Server: nginx/1.16.0
+ /: Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.29.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Cookie PHPSESSID created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
```

WPScan

To scan WordPress websites for vulnerabilities

Snapshot & Screenshot from Kali Linux: (Click on the link and video will appear) - [wpscan](#)



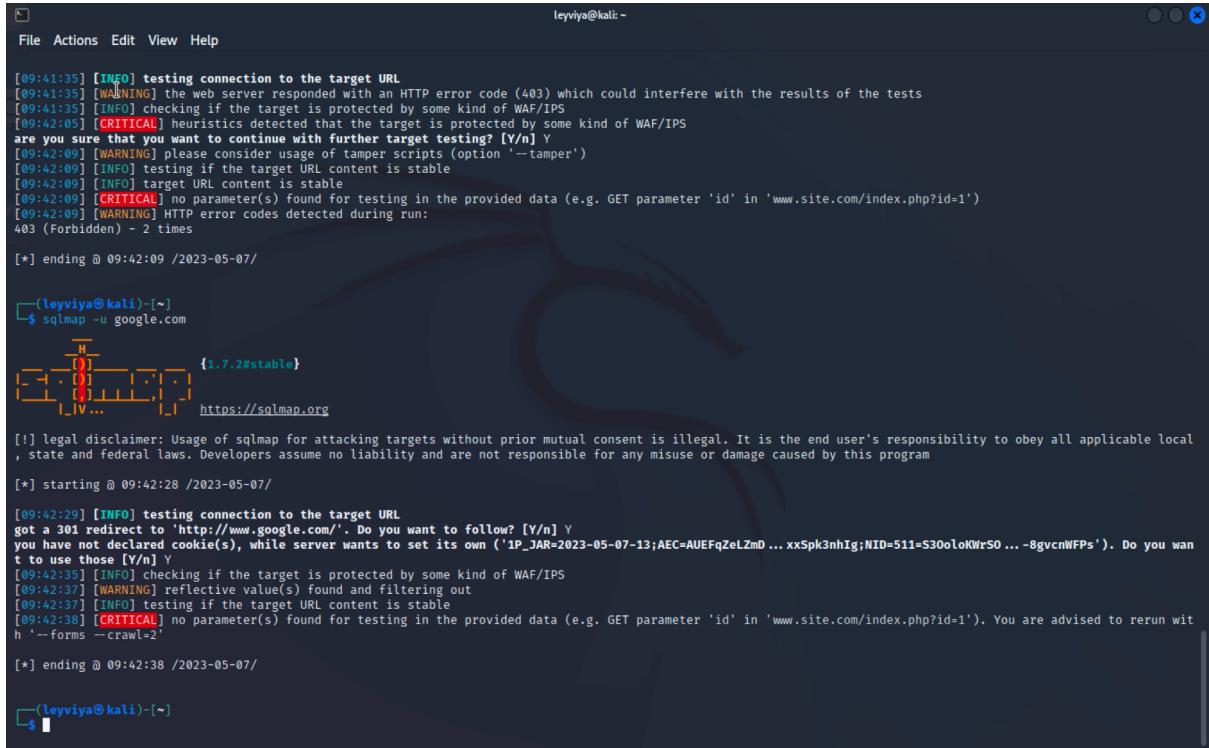
```
leyviya@kali: ~
File Actions Edit View Help
| Found By: Urls In Homepage (Passive Detection)
| Confirmed By: Urls In 404 Page (Passive Detection)
|
| Version: 2.9.15 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
|   - https://eylmalimusavirlik.com/wp-content/plugins/gtranslate/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
|   - https://eylmalimusavirlik.com/wp-content/plugins/gtranslate/readme.txt
[+] scroll-top
| Location: https://eylmalimusavirlik.com/wp-content/plugins/scroll-top/
| Latest Version: 1.5 (up to date)
| Last Updated: 2022-10-26T16:06:00.000Z
|
| Found By: Urls In Homepage (Passive Detection)
| Confirmed By: Urls In 404 Page (Passive Detection)
|
| Version: 1.5 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
|   - https://eylmalimusavirlik.com/wp-content/plugins/scroll-top/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
|   - https://eylmalimusavirlik.com/wp-content/plugins/scroll-top/readme.txt
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:08 → (137 / 137) 100.00% Time: 00:00:08
[i] No Config Backups Found.
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Sun May 7 09:36:15 2023
[+] Requests Done: 139
[+] Cached Requests: 48
[+] Data Sent: 37.223 KB
[+] Data Received: 140.549 KB
[+] Memory used: 261.855 MB
[+] Elapsed time: 00:00:16
```

3. SQL Injection

SQLmap

To detect and exploit SQL injection vulnerabilities in web applications

Snapshot & Screenshot from Kali Linux: (Click on the link and video will appear) - [sqlmap](#)



```
[09:41:35] [INFO] testing connection to the target URL
[09:41:35] [WARNING] the web server responded with an HTTP error code (403) which could interfere with the results of the tests
[09:41:35] [INFO] checking if the target is protected by some kind of WAF/IPS
[09:42:05] [CRITICAL] heuristics detected that the target is protected by some kind of WAF/IPS
are you sure that you want to continue with further target testing? [Y/n] Y
[09:42:09] [WARNING] please consider usage of tamper scripts (option '-tamper')
[09:42:09] [INFO] testing if the target URL content is stable
[09:42:09] [INFO] target URL content is stable
[09:42:09] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1')
[09:42:09] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 2 times

[*] ending @ 09:42:09 /2023-05-07/

(leyviya㉿kali)-[~]
$ sqlmap -u google.com

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local
, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 09:42:28 /2023-05-07/

[09:42:29] [INFO] testing connection to the target URL
got a 301 redirect to 'http://www.google.com/'. Do you want to follow? [Y/n] Y
you have not declared cookie(s), while server wants to set its own ('1P_JAR=2023-05-07-13;AEC=AUEFqZeLZmD ... xxSpk3nhIg;NID=511=s3OoloKWrS0 ... -8gvcnWFPs'). Do you wan
t to use those [Y/n] Y
[09:42:35] [INFO] checking if the target is protected by some kind of WAF/IPS
[09:42:37] [WARNING] reflective value(s) found and filtering out
[09:42:37] [INFO] testing if the target URL content is stable
[09:42:38] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1'). You are advised to rerun wit
h '--forms --crawl2'

[*] ending @ 09:42:38 /2023-05-07/

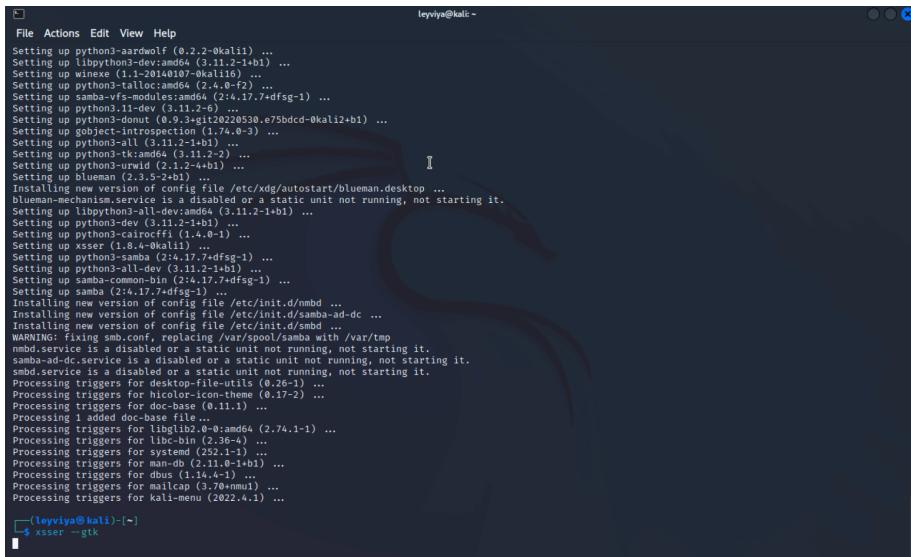
(leyviya㉿kali)-[~]
```

4. Cross-Site Scripting (XSS)

XSSer

To detect and exploit XSS vulnerabilities in web applications

Snapshot & Screenshot from Kali Linux: (Click on the link and video will appear) - [xsser](#)



```
Setting up python3-aardwolf (0.2.2-0kali1) ...
Setting up libpython3-dev-amd64 (3.11.2-1+b1) ...
Setting up winexe (1.1-201408107-0kali16) ...
Setting up python3-fallocate (2.4.0-2) ...
Setting up python3-vfslib (2.4.17.7+dfsg-1) ...
Setting up python3-nl (1.1.2-6) ...
Setting up python3-donut (0.9.3+git20220530.075bdcd-0kali2+b1) ...
Setting up gobjet-introspection (1.74.0-3) ...
Setting up python3-all (3.11.2-1+b1) ...
Setting up python3-tk (3.11.2-1+b2) ...
Setting up python3-xlib (2.1.2-4+b1) ...
Setting up blueuan (2.3.5-2+b1) ...
Installing new version of config file /etc/xdg/autostart/blueuan.desktop ...
blueuan-mechanism.service is a disabled or a static unit not running, not starting it.
Setting up libpython3-dev (3.11.2-1+b1) ...
Setting up libxkbcommon (1.4.0-1) ...
Setting up python3-cairocffi (1.4.0-1) ...
Setting up xsser (1.8.4-0kali1) ...
Setting up python3-samba (2:4.17.7+dfsg-1) ...
Setting up python3-all-dev (3.11.2-1+b1) ...
Setting up python3-xcb-util (2.1.2-1+b1) ...
Setting up samba (2:4.17.7+dfsg-1)
Installing new version of config file /etc/init.d/nmbd ...
Installing new version of config file /etc/init.d/samba-ad-dc ...
Installing new version of config file /etc/init.d/smbd ...
WARNING: Fixing smb.conf, replacing /var/spool/samba with /var/tmp
nmbd.service is a disabled or a static unit not running, not starting it.
smbd.service is a disabled or a static unit not running, not starting it.
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for locales (0.11.1) ...
Processing triggers for doc-base ...
Processing triggers for liblplib2_0-0:amd64 (2.74.1-1) ...
Processing triggers for liblc-bin (2.36-4) ...
Processing triggers for systemd (252.1-1) ...
Processing triggers for libmnl0 (1.1.0-1+b1) ...
Processing triggers for libcurl (1.14.4-1) ...
Processing triggers for mailcap (3.70-nmu1) ...
Processing triggers for kali-menu (2022.4.1) ...

(leyviya㉿kali)-[~]
$ xsser --gtk
```

REFERENCES:

- <https://www.kali.org/tools/skipfish/>
- <https://www.geeksforgeeks.org/kali-linux-web-penetration-testing-tool/>
- <https://www.geeksforgeeks.org/kali-linux-tools/#web>
- <https://www.javatpoint.com/kali-linux-web-application-tools>
- https://www.tutorialspoint.com/kali_linux/kali_linux_website_penetration_testing.htm
- <https://linuxzoo.net/>