

Plan de Seguridad Informática

2021

Índice

01

Consideraciones Generales

02.

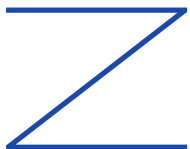
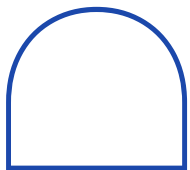
Recomendaciones

03.

Práctica de ataque

04.

Conclusiones



Para la elaboración del Plan de Seguridad se tendrán en cuenta las siguientes consideraciones.

- 1.El PS es un documento el cual será accesible a todo el personal que requiera su utilización, por lo que la información que en él se incluye debe ser ordinaria. No se incluirá información clasificada, la cual, de ser necesario, formará parte de un documento independiente.
- 2.Su redacción será simple, clara y libre de ambigüedades para que sea comprensible por todo el personal que lo requiera.
- 3.Se mantendrá permanentemente actualizado sobre la base de los cambios que se produzcan en las condiciones consideradas durante su elaboración.

RECOMENDACIONES

En esta sección se establecen las recomendaciones generales que debe cumplir el personal que forma parte del departamento de TI.

A01. Se seguirá una política que indique revisar periódicamente los permisos en el sistema para verificar si existe algún detalle con los privilegios del usuario, para así garantizar que estos mismos no excedan los definidos durante alguna actualización aprobada formalmente.

A02. Se hará uso del protocolo TLS para el cifrado de datos en tránsito, además de priorización de cifrado por parte del servidor y parámetros seguros.

A03. Para la configuración de la Base de Datos, se deberán validar los comandos utilizados, con la ayuda de una lista de comandos permitidos, para así evitar la inyección de datos en la misma.

A04. Hacer uso del Modelo de Amenazas de forma constante, al momento de realizar algún cambio, para así reconocer lo que puede salir mal y así identificar problemas de diseño e implementación.

A05. Antes del deploy de cualquier característica y/o aplicación, verificar que se han eliminado demos o aplicaciones de ejemplo que vienen por defecto.

RECOMENDACIONES

A06. Se seguirá una política que indica que de forma trimestral actualizaremos nuestra versión de nuestros sistemas, esto incluye el sistema operativo, el servidor web / de aplicaciones, el sistema de administración de bases de datos, las aplicaciones, las API y todos los componentes, los tiempos de ejecución y las bibliotecas.

A07. Se implementará la autenticación multifactor para evitar el relleno automatizado de credenciales, la fuerza bruta y los ataques de reutilización de credenciales robadas.

A08. Se seguirá una política que indica que cada vez que se realice algún cambio, tanto en código, como en configuración, haya un proceso de revisión de los mismo, para que de esta forma se descarte la posibilidad de que se pueda introducir código o configuración malintencionado.

A09. Asegurarse de que las transacciones de alto valor tengan una pista de auditoría con controles de integridad para evitar la manipulación o eliminación, como tablas de base de datos de solo apéndice o similares.

A10. Registrar todos los flujos de red aceptados y bloqueados del firewall, además de deshabilitar las redirecciones HTTP.

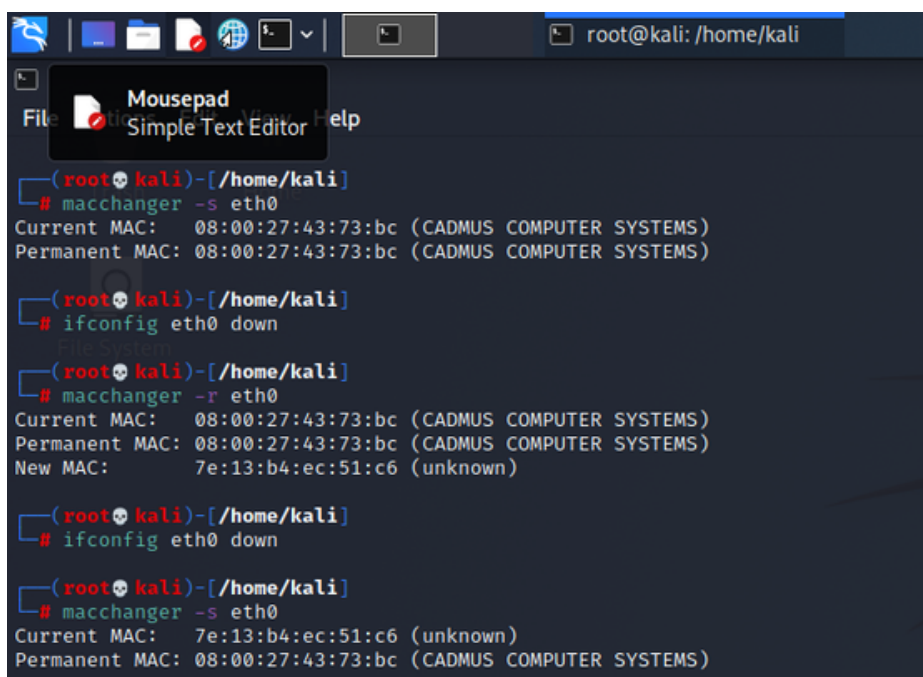
PRÁCTICA

Como práctica de seguridad de software, se realizaron 2 procedimientos, uno es el cambio de la dirección MAC y la otra es WPScan, la cual es una herramienta que nos ayuda a encontrar vulnerabilidades de página hechas en WordPress.

01

MacChanger

Esta herramienta es muy fácil de usar y consta de un par de comandos, los cuales son:



```
(root@kali)~[/home/kali]
# macchanger -s eth0
Current MAC: 08:00:27:43:73:bc (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 08:00:27:43:73:bc (CADMUS COMPUTER SYSTEMS)

(root@kali)~[/home/kali]
# ifconfig eth0 down

(root@kali)~[/home/kali]
# macchanger -r eth0
Current MAC: 08:00:27:43:73:bc (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 08:00:27:43:73:bc (CADMUS COMPUTER SYSTEMS)
New MAC: 7e:13:b4:ec:51:c6 (unknown)

(root@kali)~[/home/kali]
# ifconfig eth0 down

(root@kali)~[/home/kali]
# macchanger -s eth0
Current MAC: 7e:13:b4:ec:51:c6 (unknown)
Permanent MAC: 08:00:27:43:73:bc (CADMUS COMPUTER SYSTEMS)
```

PRÁCTICA

01

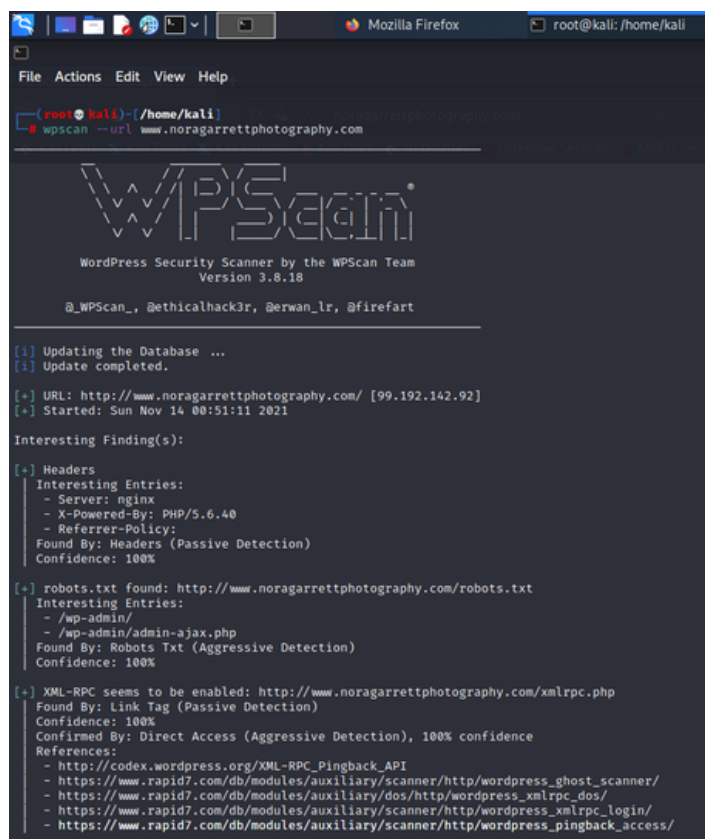
WPScan - Instalación

Ahora bien, primero que nada para hacer uso de esta herramienta, es recomendable actualizar el sistema con un "apt update" para luego hacer la instalación mediante el comando "apt install wpscan".

02.

WPScan - Escaneo

Una vez lista la instalación, ya solo sería encontrar una página web, hecha en WordPress, y simplemente utilizar el comando " wpscan --url http://example.com "



```
(root@kali)~# wpscan --url www.noragarrettphotography.com

WPScan
WordPress Security Scanner by the WPScan Team
Version 3.8.18
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[i] Updating the Database ...
[i] Update completed.

[+] URL: http://www.noragarrettphotography.com/ [99.192.142.92]
[+] Started: Sun Nov 14 00:51:11 2021

Interesting Finding(s):

[+] Headers
Interesting Entries:
- Server: nginx
- X-Powered-By: PHP/5.6.40
- Referrer-Policy:
Found By: Headers (Passive Detection)
Confidence: 100%

[+] robots.txt found: http://www.noragarrettphotography.com/robots.txt
Interesting Entries:
- /wp-admin/
- /wp-admin/admin-ajax.php
Found By: Robots Txt (Aggressive Detection)
Confidence: 100%

[+] XML-RPC seems to be enabled: http://www.noragarrettphotography.com/xmlrpc.php
Found By: Link Tag (Passive Detection)
Confidence: 100%
Confirmed By: Direct Access (Aggressive Detection), 100% confidence
References:
- http://codex.wordpress.org/XML-RPC_Pingback_API
- https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
- https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
- https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
- https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
```

PRÁCTICA - RESULTADOS

Como bien se puede observar en las siguientes capturas, la página utilizada no tenía ningún tipo de seguridad, ya que me dió desde diferentes archivos del proyecto, así como las tecnologías utilizadas junto con las versiones de cada uno; incluso me llegó a dar el login de "/wp-admin" junto con un usuario.

```
File Actions Edit View Help
root@kali:/home/kali

Found By: Direct Access (Aggressive Detection)
Confidence: 100%

[-] The external WP-Cron seems to be enabled: http://www.noragarretphotography.com/wp-cron.php
Found By: Direct Access (Aggressive Detection)
Confidence: 60%
References:
- https://www.iplocation.net/defend-wordpress-from-ddos
- https://github.com/wpscanteam/wpscan/issues/1299

[-] WordPress version 5.8.2 identified (Latest, released on 2021-11-10).
Found By: WP Generator (Passive Detection)
- http://www.noragarretphotography.com/feed/, <generator>https://wordpress.org/?v=5.8.2/</generator>
- http://www.noragarretphotography.com/comments/feed/, <generator>https://wordpress.org/?v=5.8.2/</generator>
- http://www.noragarretphotography.com/homepage/feed/, <generator>https://wordpress.org/?v=5.8.2/</generator>

[-] WordPress theme in use: patt1
Location: http://www.noragarretphotography.com/wp-content/themes/patt1/
Style URI: http://www.noragarretphotography.com/wp-content/themes/patt1/style.css?ver=5.8.2
Style Name: Patt1
Style URI: http://delicousthemes.com/
Description: Creative / Portfolio One-Page Theme ...
Author: Madalin Tudose
Author URI: http://delicousthemes.com/

Found By: CSS Style In Homepage (Passive Detection)
Confirmed By: CSS Style In 404 Page (Passive Detection)

Version: 2.9.17 (80% confidence)
Found By: Style (Passive Detection)
- http://www.noragarretphotography.com/wp-content/themes/patt1/style.css?ver=5.8.2, Match: 'Version: 2.9.17'

[-] Enumerating all Plugins (via Passive Methods)
[-] Checking Plugin Versions (via Passive and Aggressive Methods)

[+] Plugin(s) Identified:

[-] addons-for-visual-composer
Location: http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/
Latest Version: 2.8 (up to date)
Last Updated: 2021-09-03T13:05:00.000Z

Found By: Urls In Homepage (Passive Detection)
Confirmed By: Urls In 404 Page (Passive Detection)

Version: 2.8 (100% confidence)
Found By: Query Parameter (Passive Detection)
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/assets/css/lvca-frontend.css?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/assets/css/lcomoon.css?ver=2.8

[-] wordpress-seo
Location: http://www.noragarretphotography.com/wp-content/plugins/wordpress-seo/
Last Updated: 2021-11-02T09:10:00.000Z
[-] The version is out of date, the latest version is 17.5

Found By: Comment (Passive Detection)
Version: 17.4 (100% confidence)
Found By: Comment (Passive Detection)
- http://www.noragarretphotography.com/, Match: 'optimized with the Yoast SEO plugin v17.4 -'
Confirmed By:
Readme - Stable Tag (Aggressive Detection)
- http://www.noragarretphotography.com/wp-content/plugins/wordpress-seo/readme.txt
Readme - Changelog Section (Aggressive Detection)
- http://www.noragarretphotography.com/wp-content/plugins/wordpress-seo/readme.txt

[-] wp-content-copy-protector
Location: http://www.noragarretphotography.com/wp-content/plugins/wp-content-copy-protector/
Last Updated: 2021-11-09T12:47:00.000Z
[-] The version is out of date, the latest version is 3.4.2

Found By: Urls In Homepage (Passive Detection)
Confirmed By: Urls In 404 Page (Passive Detection)

Version: 3.4.1 (100% confidence)
Found By: Readme - Stable Tag (Aggressive Detection)
- http://www.noragarretphotography.com/wp-content/plugins/wp-content-copy-protector/readme.txt
Confirmed By: Readme - Changelog Section (Aggressive Detection)
- http://www.noragarretphotography.com/wp-content/plugins/wp-content-copy-protector/readme.txt

[-] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:41

[+] 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 Nov 14 00:52:34 2021
[-] Requests Done: 213
[-] Cached Requests: 7
[-] Data Sent: 50.291 KB
[-] Data Received: 18.194 MB
[-] Memory used: 217.473 MB
[-] Elapsed time: 00:01:23
```

```
Minimize all open windows and show the desktop
root@kali:/home/kali

- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/assets/css/lvca-frontend.css?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/assets/css/lcomoon.css?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/includes/addons/accordion/css/style.css?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/assets/css/slick.css?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/includes/addons/carousel/css/style.css?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/includes/addons/clients/css/style.css?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/includes/addons/heading/css/style.css?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/includes/addons/odometers/css/style.css?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/includes/addons/piecharts/css/style.css?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/includes/addons/posts-carousel/css/style.css?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/includes/addons/pricing-table/css/style.css?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/includes/addons/services/css/style.css?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/includes/addons/stats-bar/css/style.css?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/includes/addons/tabs/css/style.css?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/includes/addons/team/css/style.css?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/includes/addons/testimonials/css/style.css?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/assets/css/flexslider.css?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/includes/addons/portfolio/css/style.css?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/assets/js/jquery.waypoints.min.js?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/assets/js/lvca-frontend.min.js?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/assets/js/accordion.min.js?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/assets/js/slick.min.js?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/assets/js/jquery.stats.min.js?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/includes/addons/odometers/js/odometer.min.js?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/includes/addons/piecharts/js/piechart.min.js?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/includes/addons/posts-carousel/js/posts-carousel.min.js?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/includes/addons/spacer/js/spacer.min.js?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/includes/addons/stats-bar/js/stats-bar.min.js?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/assets/js/tabs.min.js?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/assets/js/jquery.flexslider.min.js?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/includes/addons/testimonials-slider/js/testimonials.min.js?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/assets/js/isotope.pkgd.min.js?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/assets/js/imagesloaded.pkgd.min.js?ver=2.8
- http://www.noragarretphotography.com/wp-content/plugins/addons-for-visual-composer/includes/addons/portfolio/js/portfolio.min.js?ver=2.8

[-] contact-form-7
Location: http://www.noragarretphotography.com/wp-content/plugins/contact-form-7/
Latest Version: 5.5.2 (up to date)
Last Updated: 2021-10-25T04:38:00.000Z

Found By: Urls In Homepage (Passive Detection)
Confirmed By:
Urls In 404 Page (Passive Detection)
Hidden Input (Passive Detection)

Version: 5.5.2 (100% confidence)
Found By: Query Parameter (Passive Detection)
- http://www.noragarretphotography.com/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.5.2
Confirmed By:
```


CONCLUSIÓN

Es cierto que la práctica realizada anteriormente, es simplemente una landing page, que en cierta forma de poco sirve saber las tecnologías que utiliza junto con sus versiones. Apesar de que incluso se podía acceder a un login por medio de wp-admin, prácticamente todos los datos, los tiene de forma pública en la misma página, pero luego uno se pone a pensar si envés de una simple landing page, eso fuese una pequeña tienda en línea, o alguna página que almacene datos, ciertamente estarían en un gran problema.

Por una parte he de decir que a lo largo de este parcial, ha sido muy interesante, ya que no solo las recomendaciones de la OWASP te hacen ver muchas otras vulnerabilidades de forma general, que se pueden aplicar como las diferentes prácticas que se pueden encontrar en internet, y eso me hace reflexionar sobre lo demasiado expuestos que llegamos a estar, y que por otra parte me hace ver lo muy bien que debemos estar formados para poder desarrollar software y/o proyectos que tengamos para el futuro.