Índice general

1 Práctica 11: Auditoría de seguridad en WordPress con WPScan

En esta práctica vamos a realizar una auditoría de seguridad sobre nuestra instalación de WordPress con la que hemos estado trabajando en las prácticas anteriores.

La herramienta que vamos a utilizar para realizar la auditoría de nuestro sitio web WordPress es `wpscan`.

1.1 Contenedor Docker con WPScan

Vamos a utilizar una imagen *Docker* que ya contiene la utilidad WPScan. El archivo Dockerfile que se ha utilizado para crear la imagen está disponible en el repositorio GitHub del proyecto.

La imagen de WPScan está disponible en *Docker Hub*:

- https://hub.docker.com/r/wpscanteam/wpscan/

Para consultar todas las acciones que podemos realizar con ÑWPScan podemos consultar la ayuda ejecutando el siguiente comando:

```
docker run -it --rm wpscanteam/wpscan --help
```

La salida que obtendremos será similar a esta:

```
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.13
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

Usage: wpscan [options]
```

```
        --url URL                                   The URL of the blog to
            scan
                                                    Allowed Protocols: http,
                                                        https
                                                    Default Protocol if none
                                                        provided: http
                                                    This option is mandatory
                                                        unless update or
                                                       help or hh or version
                                                        is/are supplied
    -h, --help                                      Display the simple help
       and exit
        --hh                                        Display the full help
            and exit
        --version                                   Display the version and
            exit
    -v, --verbose                                   Verbose mode
        --[no-]banner                               Whether or not to
            display the banner
                                                    Default: true
    -o, --output FILE                               Output to FILE
    -f, --format FORMAT                             Output results in the
       format supplied
                                                    Available choices: cli-
                                                       no-colour, cli-no-
                                                       color, json, cli
        --detection-mode MODE                       Default: mixed
                                                    Available choices: mixed
                                                       , passive, aggressive
        --user-agent, --ua VALUE
        --random-user-agent, --rua                  Use a random user-agent
            for each scan
        --http-auth login:password
    -t, --max-threads VALUE                         The max threads to use
                                                    Default: 5
        --throttle MilliSeconds                     Milliseconds to wait
            before doing another web request. If used, the max threads will
             be set to 1.
        --request-timeout SECONDS                   The request timeout in
            seconds
                                                    Default: 60
        --connect-timeout SECONDS                   The connection timeout
            in seconds
```

```
                                                Default: 30
      --disable-tls-checks                      Disables SSL/TLS
         certificate verification, and downgrade to TLS1.0+ (requires
         cURL 7.66 for the latter)
      --proxy protocol://IP:port                Supported protocols
         depend on the cURL installed
      --proxy-auth login:password
      --cookie-string COOKIE                    Cookie string to use in
         requests, format: cookie1=value1[; cookie2=value2]
      --cookie-jar FILE-PATH                    File to read and write
         cookies
                                                Default: /tmp/wpscan/
                                                   cookie_jar.txt
      --force                                   Do not check if the
         target is running WordPress or returns a 403
      --[no-]update                             Whether or not to update
          the Database
      --api-token TOKEN                         The WPScan API Token to
         display vulnerability data, available at https://wpscan.com/
         profile
      --wp-content-dir DIR                      The wp-content directory
          if custom or not detected, such as "wp-content"
      --wp-plugins-dir DIR                      The plugins directory if
          custom or not detected, such as "wp-content/plugins"
  -e, --enumerate [OPTS]                        Enumeration Process
                                                Available Choices:
                                                 vp   Vulnerable plugins
                                                 ap   All plugins
                                                 p    Popular plugins
                                                 vt   Vulnerable themes
                                                 at   All themes
                                                 t    Popular themes
                                                 tt   Timthumbs
                                                 cb   Config backups
                                                 dbe  Db exports
                                                 u    User IDs range. e.
                                                    g: u1-5
                                                      Range separator to
                                                          use: '-'
                                                      Value if no
                                                         argument
                                                         supplied: 1-10
                                                 m    Media IDs range. e
```

```
                                                    .g m1-15
                                                      Note: Permalink
                                                          setting must be
                                                           set to "Plain"
                                                           for those to
                                                          be detected
                                                      Range separator to
                                                           use: '-'
                                                      Value if no
                                                          argument
                                                          supplied: 1-100
                                                  Separator to use between
                                                       the values: ','
                                                  Default: All Plugins,
                                                      Config Backups
                                                  Value if no argument
                                                      supplied: vp,vt,tt,cb
                                                      ,dbe,u,m
                                                  Incompatible choices (
                                                      only one of each
                                                      group/s can be used):
                                                   - vp, ap, p
                                                   - vt, at, t
      --exclude-content-based REGEXP_OR_STRING    Exclude all responses
          matching the Regexp (case insensitive) during parts of the
          enumeration.
                                                  Both the headers and
                                                      body are checked.
                                                      Regexp delimiters are
                                                       not required.
      --plugins-detection MODE                    Use the supplied mode to
           enumerate Plugins.
                                                  Default: passive
                                                  Available choices: mixed
                                                      , passive, aggressive
      --plugins-version-detection MODE            Use the supplied mode to
           check plugins' versions.
                                                  Default: mixed
                                                  Available choices: mixed
                                                      , passive, aggressive
  -P, --passwords FILE-PATH                       List of passwords to use
       during the password attack.
                                                  If no --username/s
```

```
                                                    option supplied, user
                                                     enumeration will be
                                                    run.
    -U, --usernames LIST                            List of usernames to use
        during the password attack.
                                                    Examples: 'a1', 'a1,a2,
                                                    a3', '/tmp/a.txt'
        --multicall-max-passwords MAX_PWD           Maximum number of
           passwords to send by request with XMLRPC multicall
                                                    Default: 500
        --password-attack ATTACK                    Force the supplied
           attack to be used rather than automatically determining one.
                                                    Available choices: wp-
                                                    login, xmlrpc, xmlrpc
                                                    -multicall
        --login-uri URI                             The URI of the login
           page if different from /wp-login.php
        --stealthy                                  Alias for --random-user-
           agent --detection-mode passive --plugins-version-detection
           passive
```

Es posible obtener una salida mucho más detallada ejecutando el siguiente comando:

```
docker run -it --rm wpscanteam/wpscan --hh
```

En este caso la salida será la siguiente:

```
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 3.8.13
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________
```

```
Usage: wpscan [options]
        --url URL                                  The URL of the blog to
           scan
                                                   Allowed Protocols: http,
                                                       https
                                                   Default Protocol if none
                                                       provided: http
                                                   This option is mandatory
                                                       unless update or
                                                      help or hh or version
                                                       is/are supplied
    -h, --help                                     Display the simple help
       and exit
        --hh                                       Display the full help
           and exit
        --version                                  Display the version and
           exit
        --ignore-main-redirect                     Ignore the main redirect
            (if any) and scan the target url
    -v, --verbose                                  Verbose mode
        --[no-]banner                              Whether or not to
           display the banner
                                                   Default: true
        --max-scan-duration SECONDS                Abort the scan if it
           exceeds the time provided in seconds
    -o, --output FILE                              Output to FILE
    -f, --format FORMAT                            Output results in the
       format supplied
                                                   Available choices: cli-
                                                      no-colour, cli-no-
                                                      color, json, cli
        --detection-mode MODE                      Default: mixed
                                                   Available choices: mixed
                                                      , passive, aggressive
        --scope DOMAINS                            Comma separated (sub-)
           domains to consider in scope.
                                                   Wildcard(s) allowed in
                                                      the trd of valid
                                                      domains, e.g: *.
                                                      target.tld
                                                   Separator to use between
                                                       the values: ','
```

```
        --user-agent, --ua VALUE
        --headers HEADERS                           Additional headers to
           append in requests
                                                    Separator to use between
                                                        the headers: '; '
                                                    Examples: 'X-Forwarded-
                                                       For: 127.0.0.1', 'X-
                                                       Forwarded-For:
                                                       127.0.0.1; Another:
                                                       aaa'
        --vhost VALUE                               The virtual host (Host
           header) to use in requests
        --random-user-agent, --rua                  Use a random user-agent
           for each scan
        --user-agents-list FILE-PATH                List of agents to use
           with --random-user-agent
                                                    Default: /usr/local/
                                                       bundle/gems/
                                                       cms_scanner-0.13.0/
                                                       app/user_agents.txt
        --http-auth login:password
    -t, --max-threads VALUE                         The max threads to use
                                                    Default: 5
        --throttle MilliSeconds                     Milliseconds to wait
           before doing another web request. If used, the max threads will
            be set to 1.
        --request-timeout SECONDS                   The request timeout in
           seconds
                                                    Default: 60
        --connect-timeout SECONDS                   The connection timeout
           in seconds
                                                    Default: 30
        --disable-tls-checks                        Disables SSL/TLS
           certificate verification, and downgrade to TLS1.0+ (requires
           cURL 7.66 for the latter)
        --proxy protocol://IP:port                  Supported protocols
           depend on the cURL installed
        --proxy-auth login:password
        --cookie-string COOKIE                      Cookie string to use in
           requests, format: cookie1=value1[; cookie2=value2]
        --cookie-jar FILE-PATH                      File to read and write
           cookies
                                                    Default: /tmp/wpscan/
```

```
                                                    cookie_jar.txt
        --cache-ttl TIME_TO_LIVE                    The cache time to live
           in seconds
                                                    Default: 600
        --clear-cache                               Clear the cache before
           the scan
        --cache-dir PATH                            Default: /tmp/wpscan/
           cache
        --server SERVER                             Force the supplied
           server module to be loaded
                                                    Available choices:
                                                       apache, iis, nginx
        --force                                     Do not check if the
           target is running WordPress or returns a 403
        --[no-]update                               Whether or not to update
            the Database
        --api-token TOKEN                           The WPScan API Token to
           display vulnerability data, available at https://wpscan.com/
           profile
        --wp-content-dir DIR                        The wp-content directory
            if custom or not detected, such as "wp-content"
        --wp-plugins-dir DIR                        The plugins directory if
            custom or not detected, such as "wp-content/plugins"
        --interesting-findings-detection MODE       Use the supplied mode
           for the interesting findings detection.
                                                    Available choices: mixed
                                                       , passive, aggressive
        --wp-version-all                            Check all the version
           locations
        --wp-version-detection MODE                 Use the supplied mode
           for the WordPress version detection, instead of the global (--
           detection-mode) mode.
                                                    Available choices: mixed
                                                       , passive, aggressive
        --main-theme-detection MODE                 Use the supplied mode
           for the Main theme detection, instead of the global (--
           detection-mode) mode.
                                                    Available choices: mixed
                                                       , passive, aggressive
    -e, --enumerate [OPTS]                          Enumeration Process
                                                    Available Choices:
                                                     vp   Vulnerable plugins
                                                     ap   All plugins
```

```
                                                    p     Popular plugins
                                                    vt    Vulnerable themes
                                                    at    All themes
                                                    t     Popular themes
                                                    tt    Timthumbs
                                                    cb    Config backups
                                                    dbe   Db exports
                                                    u     User IDs range. e.
                                                        g: u1-5
                                                          Range separator to
                                                              use: '-'
                                                          Value if no
                                                             argument
                                                             supplied: 1-10
                                                    m     Media IDs range. e
                                                        .g m1-15
                                                          Note: Permalink
                                                             setting must be
                                                              set to "Plain"
                                                              for those to
                                                             be detected
                                                          Range separator to
                                                              use: '-'
                                                          Value if no
                                                             argument
                                                             supplied: 1-100
                                                  Separator to use between
                                                      the values: ','
                                                  Default: All Plugins,
                                                     Config Backups
                                                  Value if no argument
                                                     supplied: vp,vt,tt,cb
                                                     ,dbe,u,m
                                                  Incompatible choices (
                                                     only one of each
                                                     group/s can be used):
                                                   - vp, ap, p
                                                   - vt, at, t
      --exclude-content-based REGEXP_OR_STRING    Exclude all responses
         matching the Regexp (case insensitive)  during parts of the
         enumeration.
                                                  Both the headers and
                                                     body are checked.
```

```
                                                Regexp delimiters are
                                                 not required.
      --plugins-list LIST                       List of plugins to
         enumerate
                                                Examples: 'a1', 'a1,a2,
                                                   a3', '/tmp/a.txt'
      --plugins-detection MODE                  Use the supplied mode to
          enumerate Plugins.
                                                Default: passive
                                                Available choices: mixed
                                                   , passive, aggressive
      --plugins-version-all                     Check all the plugins
         version locations according to the choosen mode (--detection-
         mode, --plugins-detection and --plugins-version-detection)
      --plugins-version-detection MODE          Use the supplied mode to
          check plugins' versions.
                                                Default: mixed
                                                Available choices: mixed
                                                   , passive, aggressive
      --plugins-threshold THRESHOLD             Raise an error when the
         number of detected plugins via known locations reaches the
         threshold. Set to 0 to ignore the threshold.
                                                Default: 100
      --themes-list LIST                        List of themes to
         enumerate
                                                Examples: 'a1', 'a1,a2,
                                                   a3', '/tmp/a.txt'
      --themes-detection MODE                   Use the supplied mode to
          enumerate Themes, instead of the global (--detection-mode)
         mode.
                                                Available choices: mixed
                                                   , passive, aggressive
      --themes-version-all                      Check all the themes
         version locations according to the choosen mode (--detection-
         mode, --themes-detection and --themes-version-detection)
      --themes-version-detection MODE           Use the supplied mode to
          check themes versions instead of the --detection-mode or --
         themes-detection modes.
                                                Available choices: mixed
                                                   , passive, aggressive
      --themes-threshold THRESHOLD              Raise an error when the
         number of detected themes via known locations reaches the
         threshold. Set to 0 to ignore the threshold.
```

```
                                                Default: 20
        --timthumbs-list FILE-PATH              List of timthumbs'
           location to use
                                                Default: /wpscan/.wpscan
                                                   /db/timthumbs-v3.txt
        --timthumbs-detection MODE              Use the supplied mode to
            enumerate Timthumbs, instead of the global (--detection-mode)
           mode.
                                                Available choices: mixed
                                                   , passive, aggressive
        --config-backups-list FILE-PATH         List of config backups'
           filenames to use
                                                Default: /wpscan/.wpscan
                                                   /db/config_backups.
                                                   txt
        --config-backups-detection MODE         Use the supplied mode to
            enumerate Config Backups, instead of the global (--detection-
           mode) mode.
                                                Available choices: mixed
                                                   , passive, aggressive
        --db-exports-list FILE-PATH             List of DB exports'
           paths to use
                                                Default: /wpscan/.wpscan
                                                   /db/db_exports.txt
        --db-exports-detection MODE             Use the supplied mode to
            enumerate DB Exports, instead of the global (--detection-mode)
            mode.
                                                Available choices: mixed
                                                   , passive, aggressive
        --medias-detection MODE                 Use the supplied mode to
            enumerate Medias, instead of the global (--detection-mode)
           mode.
                                                Available choices: mixed
                                                   , passive, aggressive
        --users-list LIST                       List of users to check
           during the users enumeration from the Login Error Messages
                                                Examples: 'a1', 'a1,a2,
                                                   a3', '/tmp/a.txt'
        --users-detection MODE                  Use the supplied mode to
            enumerate Users, instead of the global (--detection-mode) mode
           .
                                                Available choices: mixed
                                                   , passive, aggressive
```

```
    -P, --passwords FILE-PATH                     List of passwords to use
        during the password attack.
                                                  If no --username/s
                                                     option supplied, user
                                                      enumeration will be
                                                     run.
    -U, --usernames LIST                          List of usernames to use
        during the password attack.
                                                  Examples: 'a1', 'a1,a2,
                                                     a3', '/tmp/a.txt'
        --multicall-max-passwords MAX_PWD         Maximum number of
           passwords to send by request with XMLRPC multicall
                                                  Default: 500
        --password-attack ATTACK                  Force the supplied
           attack to be used rather than automatically determining one.
                                                  Available choices: wp-
                                                     login, xmlrpc, xmlrpc
                                                     -multicall
        --login-uri URI                           The URI of the login
           page if different from /wp-login.php
        --stealthy                                Alias for --random-user-
           agent --detection-mode passive --plugins-version-detection
           passive
```

1.2 Ejemplos básicos de uso

A continuación vamos a ver algunos ejemplos básicos de uso.

Ejemplo 1

Para obtener la lista de *plugins* instalados en nuestro sitio WordPress podemos ejecutar:

```
docker run -it --rm wpscanteam/wpscan --url http://192.168.22.20  --
   enumerate p
```

Donde **192.168.22.20** será la dirección IP de la máquina donde hemos realizado la instalación de WordPress.

Ejemplo 2

Para realizar un escaneo completo de un sitio WordPress podemos ejecutar:

```
docker run -it --rm wpscanteam/wpscan --url http://192.168.22.20
```

Donde **192.168.22.20** será la dirección IP de la máquina donde hemos realizado la instalación de WordPress.

Ejemplo 3

En este ejemplo haremos uso de la API de WPScan que nos permite detectar vulnerabilidades haciendo uso de su base de datos de vulnerabilidades.

Para poder hacer uso del servicio de la API de WPScan,es necesario registrarse en su web y obtener un TOKEN.

```
docker run -it --rm wpscanteam/wpscan --url http://192.168.22.20 --api-
    token 8pIlWnF2dxbgfvyQfDAUaV3T3iafo0uO1K8OPr2KKRM
```

Donde **192.168.22.20** será la dirección IP de nuestro balanceador web.

1.3 Seguridad en WordPress

A continuación se muestran varias referencias relacionadas con la seguridad de WordPress.

- Seguridad para WordPress. Colección de artículos de Javier Casares.
- WPdanger: Guía de seguridad para WordPress. Una guía en PDF de Javier Casares
- Blog sobre administración de sistemas WordPress.

2 Referencias

- WordPress
- WPScan
- Imagen WPScan en Docker Hub
- Ebook: 21 Trucos para tener tu WordPress seguro. SiteGround.

3 Licencia