

Actividad 02. Uso de la herramienta

Nikto

- [1. Con la información obtenida en los artículos y vídeos indicados india qué es Nikto y como se utiliza](#)
- [2. Utilizando Nikto, escanea los siguientes sitios:](#)
- [3. Genera un documento indicando las vulnerabilidades encontradas](#)

1. Con la información obtenida en los artículos y vídeos indicados india qué es Nikto y como se utiliza

Nikto es una herramienta de código abierto y gratuita, escrita en Perl, diseñada específicamente para escanear servidores web en busca de vulnerabilidades. Es una herramienta muy popular entre los profesionales de la seguridad informática debido a su capacidad para identificar una amplia gama de problemas de seguridad en los sitios web.

Nikto **sirve para:**

- **DETECCIÓN DE VULNERABILIDADES:** Busca activamente más de 6700 vulnerabilidades conocidas en servidores web, incluyendo archivos y programas peligrosos, versiones desactualizadas de software, configuraciones incorrectas, etc.
- **VERIFICACIÓN DE VERSIONES:** Identifica las versiones exactas del software del servidor web y las compara con bases de datos de vulnerabilidades conocidas para determinar si existen exploits disponibles.
- **EXPLORACIÓN DE MÚLTIPLES PUERTOS:** No sólo se limita a un puerto, sino que puede escanear múltiples puertos TCP en busca de servicios web que puedan ser vulnerables.
- **ESCANEOS DE SUBDOMINIOS:** Además del dominio principal, puede analizar subdominios para identificar posibles puntos de entrada de ataques.
- **AUTENTICACIÓN DE HOST:** Permite configurar la autenticación de host para evaluar sitios web protegidos por credenciales.

Nikto se utiliza de la siguiente manera:

- En bash: "*nikto -h IP o dominio*"

Esto iniciará un escaneo completo del sitio web o IP especificado.

Además **ofrece una gran cantidad de opciones adicionales para personalizar el escaneo:**

- **-P:** Especifica los puertos a escanear.
- **-host:** Permite escanear múltiples host en una sola ejecución.
- **-id:** Especifica un ID de prueba para limitar el alcance del escaneo.
- **-Format:** Define el formato de salida del informe (HTML, XML, CSV, etc.).
- **-Tuning:** Carga un archivo de configuración personalizado con los ajustes específicos.

Las **ADVERTENCIAS:**

- **USO ÉTICO:** Nikto es una herramienta poderosa que debe utilizarse con responsabilidad. Es importante obtener el permiso del propietario del sitio web antes de realizar el escaneo.
- **FALSOS POSITIVOS:** Nikto puede generar falsos positivos, por lo que es necesario analizar cuidadosamente los resultados del escaneo.
- **DETECCIÓN:** Los sistemas de protección contra intrusiones pueden detectar el uso de Nikto y bloquear el escaneo.

Se puede **obtener más información** de dicha herramienta en su ***página web oficial*** (en la que te da una descripción detallada de todas las opciones y funcionalidades) y en los ***tutoriales en línea*** (guías y tutoriales en línea que explican cómo utilizar Nikto de forma efectiva).

2. Utilizando Nikto, escanea los siguientes sitios:

- Instalamos Nikto:

Con el comando "*sudo apt install nikto*", pero ya nos viene instalado en la versión más reciente.

```
Archivo Acciones Editar Vista Ayuda
--nolookup Disables DNS lookups
--nossl Disables the use of SSL
--noslash Strip trailing slash from URL (e.g., '/admin/' to '/admin')
--noadv Disables nikto attempting to guess a 404 page
--option Over-ride an option in nikto.conf, can be issued multiple times
--output+ Write output to this file ('-' for auto-name)
--Pause+ Pause between tests (seconds)
--Plugins+ List of plugins to run (default: ALL)
--port+ Port to use (default: 80)
--ssl Client certificate file
--root+ Prepend root value to all requests, format is /directory
--save Save positive responses to this directory ('-' for auto-name)
--ssl Force ssl mode on port
--Tuning+ Scan tuning:
1 Interesting File / Seen in logs
2 Misconfiguration / Default File
3 Information Disclosure
4 Injection (CSS/Script/HTML)
5 Remote File Retrieval - Inside Web Root
6 Denial of Service
7 Remote File Retrieval - Server Wide
8 Command Execution / Remote Shell
9 SQL Injection
a File Upload
a Authentication Bypass
b Software Identification
c Remote Source Inclusion
d WebService
e Administrative Console
x Reverse Tuning Options (i.e., include all except specified)
--timeout+ Timeout for requests (default 10 seconds)
--Userdb+ Load only user databases, not the standard databases
all Disable standard dbs and load only user dbs
tests Disable only db tests and load odb_tests
--useragent Over-rides the default useragent
--until Run until the specified time or duration
--url+ Target host/URL (alias of -host)
--usecookies Use cookies from responses in future requests
--useproxy Use the proxy defined in nikto.conf, or argument http://server:port
--version Print plugin and database versions
--vhost+ Virtual host (for Host header)
--wcode Ignore these HTTP codes as negative responses (always), Format is '302,301'.
--wcodestring Ignore this string in response body content as negative response (always). Can be a regu
lar expression.
+ requires a value

jorgekalilinux@jorgekalilinux:~$
jorgekalilinux@jorgekalilinux:~$ sudo apt install nikto
[sudo] contraseña para jorgekalilinux:
nikto ya está en su versión más reciente (1:12.5.0+git20230814.90ff645-0kali1).
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
jorgekalilinux@jorgekalilinux:~$
```

- bWapp: <http://itsecgames.com/>

Con el comando “*sudo nikto -h http://itsecgames.com/ -o scan.html -Format html*”:

```
jorgekalilinux@jorgekalilinux:~$ sudo nikto -h http://itsecgames.com/ -o scan.html -Format html
Nikto v2.5.0
+ Target IP: 31.3.96.40
+ Target Hostname: itsecgames.com
+ Target Port: 80
+ Start Time: 2024-09-06 11:18:54 (GMT1)

+ Server: Apache
+ /: 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 X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
+ in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilitie
+ /missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 643, size: 5d7959bd3c800, mtime: grip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /dump.tar: Drupal 7 was identified via the X-generator header. See: https://www.drupal.org/project/remove_http_headers
+ /dump.tar: Drupal Link header found with value: <http://31.3.96.40/> rel="canonical",<http://31.3.96.40/> rel="shortlink". See: https://www.drupal.org/
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 19 error(s) and 6 item(s) reported on remote host
+ End Time: 2024-09-06 11:20:14 (GMT1) (620 seconds)

1 host(s) tested
jorgekalilinux@jorgekalilinux:~$
```

Nikto Report	
file:///home/jorgekaliinux/scan.html	
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec	
itsecgames.com / 31.3.96.40	
port 80	
Target IP	31.3.96.40
Target hostname	itsecgames.com
Target Port	80
HTTP Server	Apache
Site Link (Name)	http://itsecgames.com:80/
Site Link (IP)	http://31.3.96.40:80/
URI	/
HTTP Method	GET
Description	/: The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://itsecgames.com:80/ http://31.3.96.40:80/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
URI	/
HTTP Method	GET
Description	/: 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.
Test Links	http://itsecgames.com:80/ http://31.3.96.40:80/
References	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
URI	/
HTTP Method	GET
Description	/: Server may leak inodes via ETags, header found with file /, inode: e43, size: 5d7959bd3c800, mtime: gzip.
Test Links	http://itsecgames.com:80/ http://31.3.96.40:80/
References	CVE-2003-1418
URI	/dump.tar
HTTP Method	GET
Description	/dump.tar: Drupal 7 was identified via the x-generator header.
Test Links	http://itsecgames.com:80/dump.tar http://31.3.96.40:80/dump.tar
References	https://www.drupal.org/project/remove_http_headers
URI	/dump.tar
HTTP Method	GET
Description	/dump.tar: Drupal Link header found with value: <http://31.3.96.40/>; rel="canonical",<http://31.3.96.40/>; rel="shortlink".
Test Links	http://itsecgames.com:80/dump.tar

- Metasploitable2:

Con el comando “*sudo nikto -h 10.0.2.4 -o scan.html -Format html*”:

```
jorgekaliinux@jorgekaliinux:~$ sudo nikto -h 10.0.2.4 -o scan.html -Format html
[sudo] contraseña para jorgekaliinux:
Nikto v2.5.0

+ Target IP: 10.0.2.4
+ Target Hostname: 10.0.2.4
+ Target Port: 80
+ Start Time: 2024-09-06 11:27:30 (GMT1)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: 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 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/
+ /index: Incommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,http://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /3/PHPE9568f35d428-11d2-A769-00AA003ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /3/PHPE9568f35d428-11d2-A769-00AA003ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /3/PHPE9568f35d428-11d2-A769-00AA003ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /3/PHPE9568f35d428-11d2-A769-00AA003ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETAGs, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec 9 17:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /php-config.php: php-config.php file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time: 2024-09-06 11:28:07 (GMT1) (37 seconds)

+ 1 host(s) tested

jorgekaliinux@jorgekaliinux:~$ sudo nikto -h 10.0.2.4:8180 -o scan3.html -Format html
Nikto v2.5.0

+ Target IP: 10.0.2.4
+ Target Hostname: 10.0.2.4
+ Target Port: 8180
+ Start Time: 2024-09-06 11:29:41 (GMT1)
```

10.0.2.4 / 10.0.2.4 port 80	
Target IP	10.0.2.4
Target hostname	10.0.2.4
Target Port	80
HTTP Server	Apache/2.2.8 (Ubuntu) DAV/2
Site Link (Name)	http://10.0.2.4:80/
Site Link (IP)	http://10.0.2.4:80/
URI	/
HTTP Method	GET
Description	/. Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
Test Links	http://10.0.2.4:80/ http://10.0.2.4:80/
References	
URI	/
HTTP Method	GET
Description	/. The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://10.0.2.4:80/ http://10.0.2.4:80/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
URI	/
HTTP Method	GET
Description	/. 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.
Test Links	http://10.0.2.4:80/ http://10.0.2.4:80/
References	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
URI	/index
HTTP Method	GET
Description	/index: Uncommon header 'tcn' found, with contents: list.
Test Links	http://10.0.2.4:80/index http://10.0.2.4:80/index
References	
URI	/index
HTTP Method	GET
Description	/index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php.
Test Links	http://10.0.2.4:80/index http://10.0.2.4:80/index
References	http://www.wisnir.it/articles/show?id=460&id=50415 http://perhanna.ufora.com/vulnerability/87375

- Metasploitable2:8180:

Con el comando “*sudo nikto -h 10.0.2.4:8180 -o scan.html -Format html*”:

```
Archivo Acciones Editar Vista Ayuda
jorgekallinux@jorgekallinux: ~
jorgekallinux@jorgekallinux: ~
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /wp-config.php: wp-config.php file found, this file contains the credentials.
+ 8210 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time: 2024-09-06 11:28:07 (GMT) (37 seconds)
+ 1 host(s) tested
jorgekallinux@jorgekallinux: ~
jorgekallinux@jorgekallinux: ~
+ sudo nikto -h 10.0.2.4:8180 -o scan.html -Format html
+ Nikto v2.5.0
+ Target IP: 10.0.2.4
+ Target Hostname: 10.0.2.4
+ Target Port: 8180
+ Start Time: 2024-09-06 11:29:41 (GMT)
+ Server: Apache-Coyote/1.1
+ /: 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 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/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /favicon.ico: Identifies this app/server as: Apache Tomcat (possibly 5.5.26 through 8.0.15), Alfresco Community. See: https://en.wikipedia.org/wiki/Favicon
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS.
+ HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: Appears to be a default Apache Tomcat install.
+ /admin/: Cookie JSESSIONID created without the httpOnly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /admin/contextAdmin.html: Tomcat may be configured to let attackers read arbitrary files. Restrict access to /admin. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0672
+ /admin/: This might be interesting.
+ /tomcat-docs/index.html: Default Apache Tomcat documentation found. See: CWE-552
+ /manager/html-manager-howto.html: Tomcat documentation found. See: CWE-552
+ /webdav/index.html: WebDAV support is enabled.
+ /jsp-examples/: Apache Java Server Pages documentation. See: CWE-552
+ /admin/account.html: Admin login page/section found.
+ /admin/controlpanel.html: Admin login page/section found.
+ /admin/cp.html: Admin login page/section found.
+ /admin/index.html: Admin login page/section found.
+ /admin/login.html: Admin login page/section found.
+ /servlets-examples/: Tomcat servlets examples are visible.
+ /manager/html: Default account found for 'Tomcat Manager Application' at (ip 'tomcat', pw 'tomcat'). Apache Tomcat. See: CWE-16
+ /manager/html: Tomcat Manager / Host Manager interface found (pass protected).
+ /host-manager/html: Tomcat Manager / Host Manager interface found (pass protected).
+ /manager/status: Tomcat Server Status interface found (pass protected).
+ /admin/login.jsp: Tomcat Server Administration interface found.
+ 8226 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time: 2024-09-06 11:30:28 (GMT) (47 seconds)
+ 1 host(s) tested
jorgekallinux@jorgekallinux: ~
jorgekallinux@jorgekallinux: ~
```

Nikto Report	
file:///home/jorgekalilinux/scan3.html	
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec	
10.0.2.4 / 10.0.2.4 port 8180	
Target IP	10.0.2.4
Target hostname	10.0.2.4
Target Port	8180
HTTP Server	Apache-Coyote/1.1
Site Link (Name)	http://10.0.2.4:8180/
Site Link (IP)	http://10.0.2.4:8180/
URI	/
HTTP Method	GET
Description	/: The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://10.0.2.4:8180/ http://10.0.2.4:8180/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
URI	/
HTTP Method	GET
Description	/: 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.
Test Links	http://10.0.2.4:8180/ http://10.0.2.4:8180/
References	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
URI	/favicon.ico
HTTP Method	GET
Description	/favicon.ico: Identifies this app/server as: Apache Tomcat (possibly 5.5.26 through 8.0.15), Alfresco Community.
Test Links	http://10.0.2.4:8180/favicon.ico http://10.0.2.4:8180/favicon.ico
References	https://en.wikipedia.org/wiki/Favicon
URI	/
HTTP Method	OPTIONS
Description	OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS .
Test Links	http://10.0.2.4:8180/ http://10.0.2.4:8180/
References	
URI	/
HTTP Method	GET
Description	HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
Test Links	http://10.0.2.4:8180/ http://10.0.2.4:8180/
References	

- Metasploitable3:

Con el comando “*sudo nikto -h 10.0.2.9 -o scan.html -Format html*”:

```
Archivo Acciones Editar Vista Ayuda
jorgekalilinux@jorgekalilinux: ~
jorgekalilinux@jorgekalilinux: ~
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ /: Web server returns a valid response with junk HTTP methods which may cause false positives.
+ /: Appears to be a default Apache Tomcat install.
+ /admin/: Cookie JSESSIONID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /admin/context/admin/contextAdmin.html: Tomcat may be configured to let attackers read arbitrary files. Restrict access to /admin. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0672
+ /admin/: This might be interesting.
+ /tomcat-docs/index.html: Default Apache Tomcat documentation found. See: CWE-552
+ /manager/html/manager-howto.html: Tomcat documentation found. See: CWE-552
+ /manager/html/manager-howto.html: Tomcat documentation found. See: CWE-552
+ /webdav/index.html: WebDAV support is enabled.
+ /jsp-examples/: Apache Java Server Pages documentation. See: CWE-552
+ /admin/account.html: Admin login page/section found.
+ /admin/controlpanel.html: Admin login page/section found.
+ /admin/cp.html: Admin login page/section found.
+ /admin/index.html: Admin login page/section found.
+ /admin/login.html: Admin login page/section found.
+ /servlets-examples/: Tomcat servlets examples are visible.
+ /manager/html: Default account found for 'Tomcat Manager Application' at (ID 'tomcat', PW 'tomcat'). Apache Tomcat. See: CWE-16
+ /manager/html: Tomcat Manager / Host Manager interface found (pass protected).
+ /host-manager/html: Tomcat Manager / Host Manager interface found (pass protected).
+ /manager/status: Tomcat Server Status interface found (pass protected).
+ /admin/login.jsp: Tomcat Server Administration interface found.
+ 8226 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time: 2024-09-06 11:38:28 (GMT) (47 seconds)

+ 1 host(s) tested
jorgekalilinux@jorgekalilinux: ~
jorgekalilinux@jorgekalilinux: ~
+ sudo nikto -h 10.0.2.9 -o scan.html -Format html
+ Nikto v2.5.0
+ Target IP: 10.0.2.9
+ Target Hostname: 10.0.2.9
+ Target Port: 80
+ Start Time: 2024-09-06 11:38:11 (GMT)

+ Server: Microsoft-IIS/7.5
+ /: Retrieved x-powered-by header: ASP.NET.
+ /: 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 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/
+ /dp80b0v7.aspx: Retrieved x-aspnet-version header: 2.0.50727.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
+ OPTIONS: Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
+ ERROR: Error Limit (20) reached for host, giving up. Last error:
+ Scan terminated: 0 error(s) and 6 item(s) reported on remote host
+ End Time: 2024-09-06 11:41:33 (GMT) (202 seconds)

+ 1 host(s) tested
jorgekalilinux@jorgekalilinux: ~
```

10.0.2.9 / 10.0.2.9 port 80	
Target IP	10.0.2.9
Target hostname	10.0.2.9
Target Port	80
HTTP Server	Microsoft-IIS/7.5
Site Link (Name)	http://10.0.2.9:80/
Site Link (IP)	http://10.0.2.9:80/
URI	/
HTTP Method	GET
Description	/. Retrieved x-powered-by header: ASP.NET.
Test Links	http://10.0.2.9:80/
References	http://10.0.2.9:80/
URI	/
HTTP Method	GET
Description	/. The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://10.0.2.9:80/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
URI	/
HTTP Method	GET
Description	/. 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.
Test Links	http://10.0.2.9:80/
References	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
URI	/dp6bkbvt.aspx
HTTP Method	GET
Description	/.dp6bkbvt.aspx: Retrieved x-aspnet-version header: 2.0.50727.
Test Links	http://10.0.2.9:80/dp6bkbvt.aspx
References	http://10.0.2.9:80/dp6bkbvt.aspx
URI	/
HTTP Method	OPTIONS
Description	OPTIONS: Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
Test Links	http://10.0.2.9:80/
References	http://10.0.2.9:80/

- OWASP Juice Shop: <https://demo.owasp-juice.shop/#/>

Con el comando “*sudo nikto -h https://demo.owasp-juice.shop/#/ -o scan.html -Format html*”:

```
Archivo Acciones Editor Vista Ayuda
jorgekallinux@jorgekallinux:~$ sudo nikto -h https://demo.owasp-juice.shop/#/ -o scan5.html -Format html
[sudo] contraseña para jorgekallinux:
Nikto v2.5.0

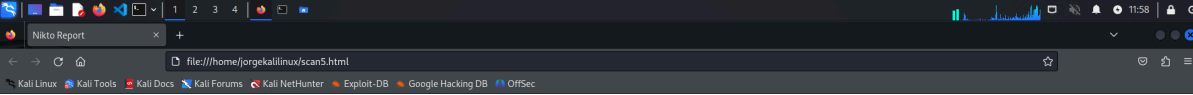
+ Multiple IPs found: 81.169.145.156, 2a01:238:20a:202:1156::
+ Target IP: 81.169.145.156
+ Target Hostname: demo.owasp-juice.shop
+ Target Port: 443

+ SSL Info: Subject: /CN=*.owasp-juice.shop
           Cipher: TLS_AES_256_GCM_SHA384
           Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=RapidSSL TLS RSA CA G1
+ Start Time: 2024-09-06 11:56:06 (GMT+1)

+ Server: Cowboy
+ /. Retrieved via header: 1.1 vegur.
+ /. Retrieved access-control-allow-origin header: *.
+ /. Uncommon header 'reporting-endpoints' found, with contents: heroku-nel=https://nel.heroku.com/reports?ts=1725620168&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=1KVeIE69X2F5iUn8Z50Bqz3zwBVWh2ofdlq7KZau7SAUX3D.
+ /. Uncommon header 'x-recruiting' found, with contents: R/jobs.
+ /. 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
+ ; Server banner changed from 'Cowboy' to 'Apache/2.4.62 (Unix)'.
+ /0xm08B8.config-: 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/
+ No CDD Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Entry '/ftp/' is returned a non-forbidden or redirect HTTP code (503). See: https://portswigger.net/kb/issues/00600000_robots-txt-file
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /. The Content-Encoding header is set to 'deflate' which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
+ /demoowasp-juiceshop.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /demo.owasp-juice.shop.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /demoowasp-juice.tar.gz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:8A000410:SSL routines::ssl/tls alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5254.
+ at /var/lib/nikto/plugins/LW2.pm line 5254.
+ Scan terminated: 20 error(s) and 15 item(s) reported on remote host
+ End Time: 2024-09-06 11:57:58 (GMT+1) (112 seconds)

+ 1 host(s) tested

jorgekallinux@jorgekallinux:~$
```



demo.owasp-juice.shop / 81.169.145.156 port 443	
Target IP	81.169.145.156
Target hostname	demo.owasp-juice.shop
Target Port	443
HTTP Server	Cowboy
Site Link (Name)	https://demo.owasp-juice.shop:443/
Site Link (IP)	https://81.169.145.156:443/
URI	/
HTTP Method	GET
Description	/. Retrieved via header: 1.1 vegur.
Test Links	https://demo.owasp-juice.shop:443/ https://81.169.145.156:443/
References	
URI	/
HTTP Method	GET
Description	/. Retrieved access-control-allow-origin header: *
Test Links	https://demo.owasp-juice.shop:443/ https://81.169.145.156:443/
References	
URI	/
HTTP Method	GET
Description	/. Uncommon header 'reporting-endpoints' found, with contents: heroku-nei=https://nei.heroku.com/reports?ts=1725620168&sid=812d0c77-0bd0-43b1-a5f1-b257503829596
Test Links	https://demo.owasp-juice.shop:443/ https://81.169.145.156:443/
References	
URI	/
HTTP Method	GET
Description	/. Uncommon header 'x-recruiting' found, with contents: /#/jobs.
Test Links	https://demo.owasp-juice.shop:443/ https://81.169.145.156:443/
References	
URI	/
HTTP Method	GET
Description	/. The site uses TLS and the Strict-Transport-Security HTTP header is not defined.
Test Links	https://demo.owasp-juice.shop:443/ https://81.169.145.156:443/
References	

3. Genera un documento indicando las vulnerabilidades encontradas

- bWapp: <http://itsecgames.com/>

Clickjacking:

- Un atacante podría engañar a los usuarios para que hagan clic en elementos ocultos dentro de un marco, lo que podría llevar a la ejecución de acciones no deseadas.

Falta de encabezado X-Content-Type-Options:

- Esta ausencia podría permitir a un navegador interpretar el contenido del sitio web de una manera no prevista, lo que podría llevar a vulnerabilidades adicionales.

Filtración de información del servidor:

- El servidor podría estar revelando información sensible sobre los archivos almacenados, lo que podría ayudar a un atacante a planificar ataques más específicos.

Identificación de la versión de Drupal:

- Se ha detectado que el sitio web utiliza Drupal 7. Conocer la versión exacta de un software permite a los atacantes buscar exploits conocidos para esa versión.

Posible falsificación de enlaces:

- Los enlaces encontrados en el sitio web podrían redirigir a los usuarios a direcciones IP en lugar de nombres de dominio, lo que podría ser utilizado para engañar a los usuarios.

Métodos HTTP permitidos:

- El servidor permite varios métodos HTTP, lo que podría abrir la puerta a ataques adicionales si no se implementan correctamente.
- Metasploitable2

Falta de seguridad en cabeceras HTTP:

- El servidor no incluye los encabezados **X-Frame-Options** y **X-Content-Type-Options**. Esto podría permitir ataques de clickjacking y renderizado incorrecto del sitio web.

Divulgación de información del servidor:

- El servidor podría estar revelando información sensible sobre los archivos almacenados.

Versión antigua de Apache:

- Se detectó que el servidor utiliza una versión obsoleta de Apache (2.2.8). Las versiones obsoletas tienen más probabilidades de contener vulnerabilidades conocidas.

Método TRACE habilitado:

- El método HTTP TRACE está activo, lo que podría ser vulnerable a ataques de Cross-Site Tracing (XST).

Información de PHP revelada:

- La función `phpinfo()` está habilitada, lo que revela información del sistema y de la configuración de PHP.

Directorios vulnerables:

- Se encontró que los directorios `/doc/`, `/test/`, `/icons/` y `/phpMyAdmin/` son accesibles y podrían contener información sensible.

Potencial existencia de wp-config.php:

- Se detectó una referencia a `#wp-config.php#`, lo que sugiere que el sitio web podría estar basado en WordPress y el archivo de configuración `wp-config.php` podría ser accesible. Este archivo contiene credenciales sensibles de la base de datos.

- Metasploitable2:8180

Falta de configuración de seguridad:

- No se encuentran los encabezados de seguridad `X-Frame-Options` y `X-Content-Type-Options`.

Exposición de información sensible:

- Revelación de la versión de Tomcat.
- Presencia de directorios y archivos por defecto.
- Posiblemente credenciales de acceso expuestas.

Métodos HTTP permitidos no seguros:

- Se permiten métodos como PUT y DELETE, que podrían permitir a atacantes modificar o eliminar archivos en el servidor.

Falta de autenticación o autorización adecuada:

- La ausencia de mecanismos de autenticación fuertes en áreas administrativas como `/admin/` y `/manager/` podría permitir a atacantes tomar el control del servidor.

Debilidad en credenciales:

- Se encontraron credenciales por defecto para Tomcat Manager (`tomcat:tomcat`).
- Metasploitable3

Falta de configuración de seguridad:

- No se encuentran los encabezados de seguridad `X-Frame-Options` y `X-Content-Type-Options`.

Exposición de información sensible:

- Revelación de la versión de ASP.NET (`x-aspnet-version`).

Métodos HTTP permitidos no seguros:

- Se permiten métodos como TRACE, que no son necesarios para el funcionamiento normal de un servidor web y pueden ser utilizados por atacantes para obtener información del sistema.

- OWASP Juice Shop: <https://demo.owasp-juice.shop/#/>

Falta de configuración de seguridad:

- No se encuentran los encabezados de seguridad `X-Frame-Options` y `X-Content-Type-Options`.
- El encabezado `Strict-Transport-Security` no está definido.

Exposición de información sensible:

- El servidor informa una versión de Apache distinta a la real (`Cowboy` cambiado a `Apache/2.4.62`).

Debilidad en el servidor:

- El servidor es vulnerable al ataque BREACH debido al uso del encabezado `Content-Encoding: deflate`.

Potencial filtrado de archivos:

- Se encontraron referencias a archivos que podrían contener información sensible:
 - [demoowasp-juiceshop.cer](#)
 - [database.cer](#)
 - [demo.owasp-juice.shop.jks](#)
 - [database.jks](#)
 - [demoowasp-juice.tar.bz2](#)

Otros hallazgos:

- El servidor responde con código 503 (Servicio no disponible) para la ruta [/ftp/](#) mencionada en el archivo robots.txt.