Práctica recopilación de información

Realizado por Yesurún González Román

Contacto: yesurn_g@hotmail.com

Técnicas de recopilación de información sobre la cadena de hoteles Hilton

Informe destinado a Keepcoding

06/06/2021

ÍNDICE

1.Introducción

a) Tratamiento del documento

Este Informe tiene como propósito aportar a Keepcoding, documentación sobre fallos de seguridad en la aplicación WebGoat.

La información que se presenta a continuación es confidencial y no debe ser modificada o distribuida a entidades o personas ajenas a la empresa Keepcoding.

b) Información del documento

En esta seccíon se detalla a las partes involucradas del proyecto, y las fases de desarrollo del mismo:

Cliete: Keepcoding

Autor: Yesurún González Román

Proyecto: Recolección de información sensible perteneciente a los dominios de Hilton

2. Ámbito y alcance

a) Breve resumen

Hilton es una de las compañias registradas en hackerone que permite análisis de ciberseguridad sobre sí misma. Se puede encontrar información detallada en este enlace: https://hackerone.com/hilton?type=team

Realización de pruebas de seguridad sobre los dominios:

*.hilton.com

*hilton.io

En hackerone, Hilton detalla sobre que superficie están interesados en recibir información sobre vulnerabilidades

In Scope

The main Hilton website (hilton.com and www.hilton.com) is included within the scope of the VDP. Finders may create a Hilton Honors account (https://www.hilton.com/en/hilton-honors/join/) for the purpose of assessing authentication functionality. The Hilton Honors program is a free sign up that only requires basic information. **Please prepend the string "Test-Hackerone" to the First and Last name fields for all HHonors accounts created for the purposes of security testing.**
In addition, the following Fully Qualified Domain Names (FQDNs) are in scope for the VDP:

- *.hilton.com (all hilton.com subdomains)
- hilton.io
- *.hilton.io (all hilton.io subdomains)

The following IP ranges are also in scope for the VDP:

- 167.187.0.0/16
- 192.251.123.0/24
- 192.251.124.0/24
- 192.251.125.0/24
- 192.251.126.0/24
- 82.196.42.196/28
- 203.79.37.2/29
- 62.216.152.46/29
- 121.200.237.36/29

También se mencionan varios rangos de ip, pero al no poder abarcarlo, he decidido tratar las IPs a las que están direccionados los subdominios (son diferentes).

Y tambíen muestra el tipo de vulnerabilidades que no quiere que se traten:

Out of Scope

Booking of reservations is considered an out-of-scope activity. In addition, the following vulnerabilities are considered out of scope:

- Clickjacking on pages with no sensitive actions.
- Unauthenticated/logout/login CSRF.
- Attacks requiring MITM or physical access to a user's device.
- Previously known vulnerable libraries without a working Proof of Concept.
- Comma Separated Values (CSV) injection without demonstrating a vulnerability.
- Missing development best practices.
- Missing best practices in SSL/TLS configuration.
- Conflict with industry policies and standards.
- Any activity that could lead to the disruption of a Hilton service (for example, DoS attacks).
- Content spoofing and text injection issues without showing an attack vector/without being able to modify HTML/CSS.
- Rate-limiting issues on endpoints that do not disclose PII or other relevant information.
- Reports originating only from automated tools or scanners (e.g., Burp, nmap, etc.).

b) Footprinting

A través de métodos que implican transparencia de certificados, web scrapping, información de dns, es posible almacenar más de 1700 subdominios.
Para una revisión mas detallada, estos subdominios se encuentran en el archivo amass_results.txt.
De los 1706 subdominios, 163 redireccionan a otro dominio y el resto se dirigen a 335 direcciones IP.
Los 163 subdominios CNAME se pueden encontrar en el archivo hilton_subdomain_cname.txt.
A su vez las 335 direcciones IP se encuentran en el archivo hilton_subdomain_ips.txt
De los 163 subdominios, hay 114 que redireccionnan a enlaces que dan fallo del tipo 404 o 403.
Los enlaces están almacenados en el archivo hilton_aquatone_cname.txt. **Estos dominios podrían ser susceptibles a subdomain takeover**.

c) Fingerprinting

De las 335 direcciones IP hay 127 que tienen fácil reconocimiento para averiguar si tienen puertos abiertos. Estas 127 direcciones IP se encuentran en el archivo hilton_subdomain_hosts.gnmap y hilton_subdomain_hosts.nmap (este último alberga más información sobre los puertos, certificados, organizaciones y demás.
Cabe destacar que no he detectado vulnerabilidades a través de escáneres.

d) Osint

He recopilado la suma de 646 correos pertenecientes a Hilton. Los correos se encuentran en el archivo hilton_correos.txt.
También, he recopilado los nombres de 73 personas que trabajan en Hilton. Los nombres se encuentran en el archivo hilton_nombres.txt.
Hilton es una compañía internacional de hoteles que recoge registros de correo de sus clientes interesados. **En internet se puede encontrar una inmensidad de correos con contraseña en claro que permiten suplantar su identidad.**
Hay que destacar que el dominio **hilton.com tiene errores de configuración en su implementación de certificado SSL, manteniendolo en categoría B**

3. Descripción del proceso

a) Reconocimiento de superficie de ataque

Para hallar todos los posibles subdominios he utilizado amass con el siguiente comando:
amass enum -d hilton.io,hilton.com > amass_results.txt

Una vez obtenidos estos subdominios, he empleado massdns para obtener más información.

- Con este comando; **massdns -r resolvers amass_results.txt -o S | grep ". A "| cut -d " " -f3| sort | uniq > hilton_subdomain_ips.txt**, obtengo todas las IP que tienen estos subdominios.
- Con este otro comando; **massdns -r resolvers amass_results.txt -o S | grep "CNAME"| cut -d " " -f3| sort | uniq > hilton_subdomain_cname.txt**, obtengo los dominios potencialmentes susceptibles de subdomain takeover.

Las IPs que contiene el archivo resolvers son 8.8.8.8 y 8.8.4.4

Gracias a Aquatone he podido obtener los enlaces con mayor peligro de subdomain takeover. Para ello he utilizado este comando: cat **hilton_subdomain_cname.txt | ./aquatone -http-timeout 5000 | grep 40 | cut -d " " -f1 > hilton_aquatone_cname.txt .**

b) Selección de zonas más vulnerables

Para identificar los servidores activos, he utilizado nmap sobre los puertos más comunes, y obtenido información sobre ellos. He tenido que usar este comando: **sudo nmap -sS -Pn -sV -sC -PS22,443,80,8080 --open --reason -oA hilton_subdomain_hosts -iL hilton_subdomain_ips.txt** .
Después he utilizado nikto en tres diferentes IPs con el puerto 80 abierto, pero no encontró ninguna vulnerabilidad.
Comandos:
nikto -h 134.213.238.16

nikto -h 146.20.26.85

nikto -h 167.187.100.29

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 134.213.238.16
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          134.213.238.16
+ Target Hostname:    134.213.238.16
+ Target Port:        80
+ Start Time:         2021-06-06 13:37:55 (GMT-4)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'x-cache-txt' found, with contents: NO:Not Cacheable
+ Uncommon header 'x-cache' found, with contents: MISS
+ Uncommon header 'x-country-code' found, with contents: ES
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 47, size: 5627defcf057b, mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS

+ 7915 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2021-06-06 13:44:39 (GMT-4) (404 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 146.20.26.85
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          146.20.26.85
+ Target Hostname:    146.20.26.85
+ Target Port:        80
+ Start Time:         2021-06-06 14:47:13 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ 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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 167.187.100.29
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          167.187.100.29
+ Target Hostname:    167.187.100.29
+ Target Port:        80
+ Start Time:         2021-06-06 15:07:28 (GMT-4)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ 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
+ Root page / redirects to: https://167.187.100.29/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated:  20 error(s) and 2 item(s) reported on remote host
+ End Time:           2021-06-06 15:17:39 (GMT-4) (611 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

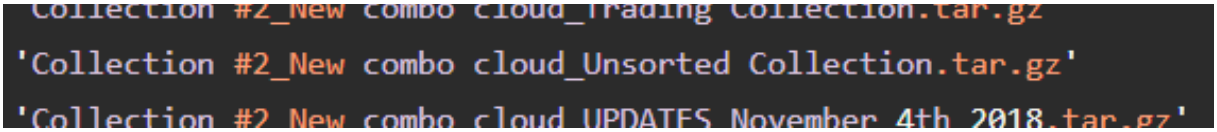
c) Incorporación de información OSINT

La herramienta que más información me ha aportado ha sido Foca. Usando web scrapping y búsqueda de archivos con los motores Google, Bing y Duckduckgo, obtuve más de 300 archivos pertenecientes a Hilton. De aquí se obtuvo los datos para crear los archivos hilton_correos.txt y hilton_nombres.txt.
Por otro lado spiderfoot no conseguía emails ni nombres de la compañía. Sin embargo, con este comando; **spiderfoot -s hilton.com -t AFFILIATE_EMAILADDR -f -x -q |grep Email| cut -d " " -f47 >> hilton_mails**, obtuve correos de clientes. Como cada vez que lo ejecutaba daba un resultado diferente, lo usé varias veces y luego utilicé este comando: **cat hilton_mails |sort| uniq > hilton_mails**.
Aun así, con Inteligence x se obtienen mejores resultados visitando su web.

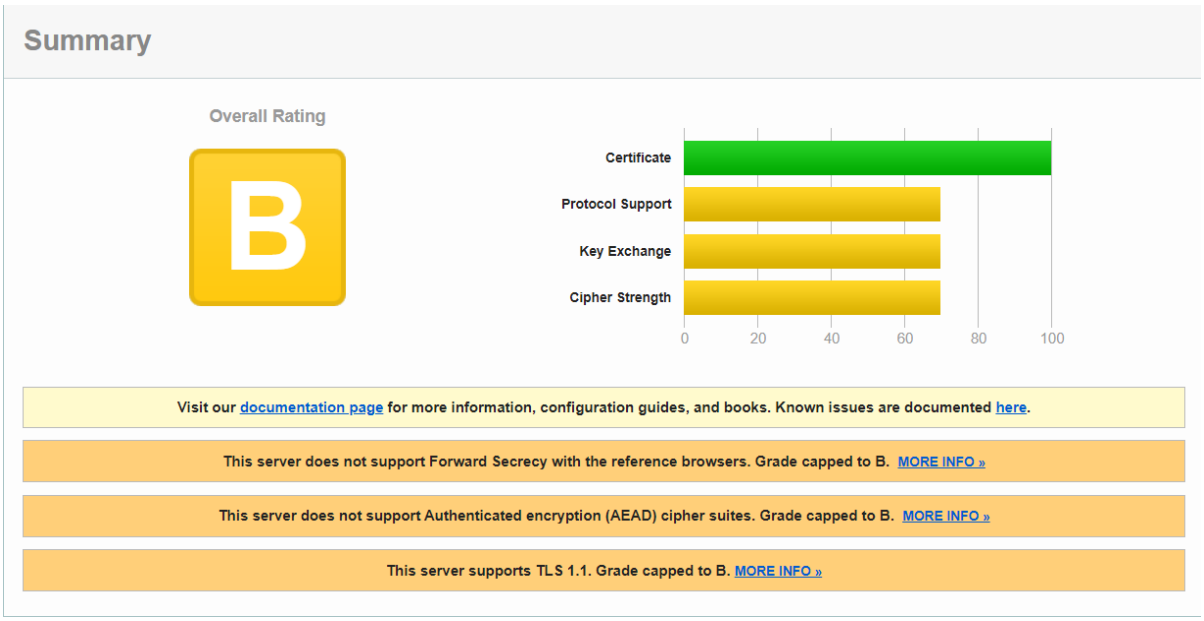
Collection #2-#5 & Antipublic/Collection #2_New combo cloud_Unsorted Collection.tar.gz/Collection #2_New combo cloud_Unsorted Collect

```
hakim_razor09@yahoo.com:0917348828
psprabhakarsingh@gmail.com:9955248025
marie_calumpang@yahoo.com:maemae
blairelrod@hotmail.com:wh16oe88
anjo1rich@yahoo.com:246824
martinsalcedo26@yahoo.com:asawako
ylanasoumaiseu@hotmail.com:ilana987454
samnbaiden@hotmail.com:whateva1
```

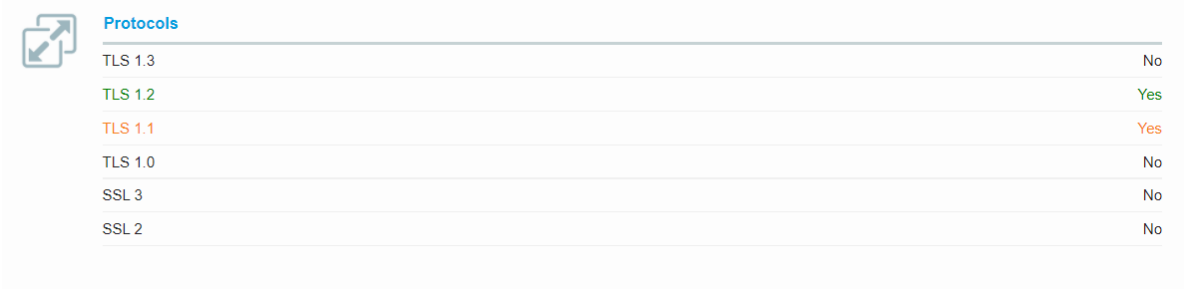
Buscando esta collección o cualquier otra en google se puede obtener los correos y contraseñas sin coste.



Visitando la web ssllabs.com se descubre el grado de seguridad en su certificado SSL



TLS 1.1 está obsoleto y debería estar deshabilitado



También se debría reemplazar los algoritmos de encriptación por otros más seguros.