Práctica:

RECOPILACION DE INFORMACION

Adrián Armesto García

Objetivo:

https://hackerone.com/av?type=team

Azbuka Vkusa

- ***.av.ru**
- ***.azbukavkusa.ru**
- **jobazbuka.ru**
- **CIDR 195.19.210.0/24**

Herramientas

- **Gospider**
- **Amass**
- **EyeWitness**
- **Nmap**
- **Httpx**
- **Dirsearch**
- **Wappalyzer**
- **Wafw00f**
- **Spoofcheck**
- **Subzy**
- **Nuclei**

Análisis

av.ru

Lista de subdominios encontrados: **amass -src -v -d av.ru -cidr 195.19.210.0/24 -oA av.ru_amass** (Archivo adjunto)

Eliminados de la lista los que están fuera de scope.

Comprobación del estado de los dominios con **httpx -list av.ru_list.txt**:

- Mail.av.ru (Failed)

Utilización de EyeWitness para la lista: **./EyeWitness.py --web -f av.ru_list.txt -d av.ru** (Archivos adjuntos)

Dominios con login:

- drive.av.ru
- sentry.av.ru
- 365.av.ru
- admin-booking.av.ru
- booking.av.ru
- ums.av.ru
- lms.av.ru
- dpdd-zabbix.av.ru (Utiliza zabbix, monitorización de redes)
- zabbix.av.ru
- portal.av.ru

Dominios sin WAF: **waf00f -DOMAIN-**

- Images.av.ru
- dev-unsubscribe.av.ru
- soap-siebel.av.ru
- dpdd-zabbix.av.ru
- zabbix.av.ru
- employee-rest.av.ru

Escaner de puertos por medio de nmap: **sudo nmap -sV -sC -A -Pn -O -iL av.ru_list.txt -oA av.ru_nmap** (Archivo adjunto)

Escaneo de vulnerabilidades con nuclei: **nuclei -list av.ru_list.txt -o av.ru_nuclei** (Archivo adjunto)

142.250.184.179 / **drive.av.ru** / mad07s23-in-f19.1e100.net

- 80/443 Google drive

185.18.52.208 / **dpdd-zabbix.av.ru** / kvmnl01-19956-1.fornex.org

- PHP 5.4.16
- puerto 80 y 443, ngingx 1.16.1
- puerto 22, openSSH 7.4, vulnerable CVE-2018-15473
- puerto 5432, PostgreSQL
- puerto 9102, jetdirect (para impresoras)

No se encontraron vulnerabilidades de DMARC o subdomain takeover, por medio de **spoofcheck** y **subzy**. (**python3 spoofcheck.py -DOMAIN- / subzy -targets av.ru_list.txt**)

No se encontraron directorios de interés por medio de **dirsearch** (Archivo adjunto)

python3 dirsearch.py -i 200 -t 10 --format=csv -l av.ru_list.txt -o av.ru_dirsearch

azbukavkusa.ru

Lista de subdominios encontrados: **amass -src -v -d azbukavkusa.ru -cidr 195.19.210.0/24 -oA azbukavkusa.ru_amass** (Archivo adjunto)

Comprobación del estado de los dominios con **httpx -list azbukavkusa.ru_list.txt**:

- http://av.azbukavkusa.ru [FAILED]
- http://wc.azbukavkusa.ru [FAILED]
- http://mail1.azbukavkusa.ru [FAILED]
- http://mail2.azbukavkusa.ru [FAILED]

Resultados de EyeWitness: **./EyeWitness.py --web -f azbukavkusa.ru_list.txt -d azbukavkusa.ru** (Archivo adjunto)

Escaner de puertos de nmap: **sudo nmap -sV -sC -A -Pn -O -iL azbukavkusa.ru_list.txt -oA azbukavkusa.ru_nmap** (Archivo adjunto)

- **autodiscover.azbukavkusa.ru / mail-service.azbukavkusa.ru**
  Puertos 80/443 Microsoft IIS httpd 7.5
  Puerto 465 Microsoft Exchange smtpd
  Puerto 993 Microsoft Exchange 2007-2010 imapd

Escaneo de vulnerabilidades con nuclei: **nuclei -list azbukavkusa.ru_list.txt -o azbukavkusa.ru_nuclei** (Archivo adjunto)

Dominios sin WAF: **waf00f -DOMAIN-**

- cavist.azbukavkusa.ru
- lyncdiscover.sip.azbukavkusa.ru
- pool01.azbukavkusa.ru
- autodiscover.azbukavkusa.ru
- meet.azbukavkusa.ru
- mail-service.azbukavkusa.ru
- owa.azbukavkusa.ru
- lyncdiscover.azbukavkusa.ru
- sip.azbukavkusa.ru
- join.azbukavkusa.ru
- owa-test.azbukavkusa.ru

No se encontraron posibles vulnerabilidades por medio de **nuclei**, **spoofcheck** y **subzy**.

No se encontraron directorios de interés por medio de **dirsearch** (Archivo adjunto) **python3 dirsearch.py -i 200 -t 10 --format=csv -l azbukavkusa_list2.txt -o azbukavkusa.ru_dirsearch**

jobazbuka.ru

No se encontraron subdominios por medio de **amass:** : **amass -src -v -d jobazbuka.ru -cidr 195.19.210.0/24 -oA jobazbuka.ru_amass**

Nmap: nmap -sV -sC -A -Pn -O -oA jobazbuka.ru_nmap jobazbuka.ru Solo muestra los puertos 80/443 con nginx.

Por medio de **dirsearch**(**python3 dirsearch.py -i 200 -t 10 --format=csv -u https://jobazbuka.ru -o jobazbuka.ru_dirsearch**), se encontró una api, para la cual requiere login y la función de registro está prohibida > **https://jobazbuka.ru/api/#main-content**.

El dominio no posee **WAF**.

No se encontraron vulnerabilidades (**subzy, nuclei, spoofcheck**).

Correos Corporativos

Adquiridos de los dominios o de documentos/web encontrados por medio de Google dorks.

welcome@azbukavkusa.ru

resume@azbukavkusa.ru Centro de selección y formación

smironov@azbukavkusa.ru Gerente sénior de cuentas clave

ibashkireva@azbukavkusa.ru Gerente de ventas al por mayor Enotec

nkozlov@azbukavkusa.ru Jefe del departamento de ventas corporativas

elomakova@azbukavkusa.ru Vicepresidenta de asuntos comerciales

spashentsev@azbukavkusa.ru Vicepresidente de Comercio

oegorova@azbukavkusa.ru Jefe del departamento de MTO

ebonadykov@azbukavkusa.ru Jefe de producción agrícola

dmlebedev@azbukavkusa.ru Vicepresidente de comercio electrónico

akudlay@azbukavkusa.ru Vicepresidente de Seguridad

okz@azbukavkusa.ru Jefe del Departamento de Compras y Licitaciones

eustinova@azbukavkusa.ru Coordinador del Departamento de Desarrollo

ylosev@azbukavkusa.ru Vicepresidente de Desarrollo

pmershiev@azbukavkusa.ru Jefe del Departamento de Desarrollo de Azbuka Vkusa y AB Daily Supermarkets

akrachkevich@azbukavkusa.ru Gerente de Desarrollo de Moscú

ndarbaidze@azbukavkusa.ru Jefe del departamento de subarrendamiento

vmukhin@azbukavkusa.ru Gerente de Desarrollo de San Petersburgo

yletuchaya@azbukavkusa.ru Gerente de subarrendamiento

rverholantsev@azbukavkusa.ru Jefe del Departamento de Seguridad de la Información

reklama@azbukavkusa.ru Publicidad en supermercados

marketing@azbukavkusa.ru

vkhomyakov@azbukavkusa.ru Director de División San Petersburgo

oknyazeva@azbukavkusa.ru Director comercial San Petersburgo

gbykovskaya@azbukavkusa.ru Responsable de producción culinaria San Petersburgo

obrailko@azbukavkusa.ru Jefe de servicios técnicos de la división San Petersburgo

mpavlova@azbukavkusa.ru Jefe del Departamento de Recursos Humanos San Petersburgo

Gerentes de categorías de productos:

lanokhina@azbukavkusa.ru

ekovaleva@azbukavkusa.ru

opereborova@azbukavkusa.ru

dbabkin@azbukavkusa.ru

parsentev@azbukavkusa.ru

mtarasova@azbukavkusa.ru

ndmitruk@azbukavkusa.ru

yulebed@azbukavkusa.ru Directora de relaciones públicas

asobolnikova@azbukavkusa.ru Subdirector de relaciones públicas

aleksmorozov@azbukavkusa.ru

bug@azbukavkusa.ru

achursin@azbukavkusa.ru

abelyakova@azbukavkusa.ru

supermarkets@azbukavkusa.ru

emarchenko@azbukavkusa.ru

oberko@azbukavkusa.ru

vlubnina@azbukavkusa.ru

aptitsyn@azbukavkusa.ru

nkozina@azbukavkusa.ru