

HackerDivulgation.com

DOCS

HTTP-SUITE

Es una pequeña suite que permite escanear dominios. Cuenta con scripts para: enumerar subdominios, listar los DNS, encontrar paneles de administración, escanear puertos, etc.

Proyecto: [HTTP-Suite-Github](#)

Contenido

- [Instalación](#)
- [Opciones](#)
- [Uso](#)
 - [Whois](#)
 - [Headers](#)
 - [Crawling](#)
 - [Buscar Directorios](#)
 - [Buscar panel de administración](#)
 - [Escanear puertos](#)
 - [Enumerar DNS](#)
 - [Escanear subdominios](#)
- [Referencias](#)

Instalación

Clonar el repositorio del proyecto,

```
git clone https://github.com/whoamisec75/httpsuite
```

Entrar al repositorio descargado.

```
cd httpsuite/
```

Ejecutar el archivo de instalación.

Argumento Opcional	Significado
whois	Whois Lookup
ds	Busqueda de directorios
apf	Buscador de paneles de administración
pscan	Escaner de puertos multihilo
dnsrec	Enumeración DNS
subscan	Escaner de subdominios
sub-crt	Escaner de subdominios usando el script <code>crt.sh</code>

En la sección de uso se explicará el uso que tiene cada argumento.

USO

¡¡Las siguientes pruebas se realizaron escaneando el propio dominio de HackerDivulgation.com por lo que no se interfiere con terceros. Para realizar estas mismas pruebas se puede usar el sitio VulnWeb desarrollado por Acutinex, nunca usar en sitios sin autorización!!

Whois

Se obtendrá información del dominio como: propietario del dominio, IP del servidor, dirección, país, etc.

```
httpsuite http://DOMINIO.COM --whois
```


Con este escaneo se puede además verificar si se está usando un subdominio para administración o para un panel de usuarios registrados.

```
httpsuite http://DOMINIO.COM --subscan
```

```
alex@hackerdivulgation: ~  
File Actions Edit View Help  
  
(alex@hackerdivulgation)-[~]  
$ httpsuite http://hackerdivulgation.com --subscan  
  
_/_/_/_/_/_/_/_/_/_(_)_/_/_/_/_/_/_/_/_/_(_)  
/_/_/_/_/_/_/_/_/_/_(_)/_/_/_/_/_/_/_/_/_/_/  
/_/_/_/_/_/_/_/_/_/_(_)/_/_/_/_/_/_/_/_/_/_/  
/_/_/_/_/_/_/_/_/_/_(_)/_/_/_/_/_/_/_/_/_/_/  
/_/_/_/_/_/_/_/_/_/_(_)/_/_/_/_/_/_/_/_/_/_/  
          @whoamisec  
  
:: Author   : HS Devansh Raghav  
:: Version  : 1.0  
  
[INF] Scanning Subdomains ...  
  
[RES] http://www.hackerdivulgation.com  
[RES] http://test.hackerdivulgation.com  
[RES] http://admin.hackerdivulgation.com  
[RES] http://mail.hackerdivulgation.com  
[RES] http://autoconfig.hackerdivulgation.com  
[RES] http://www.admin.hackerdivulgation.com  
[RES] http://autoconfig.admin.hackerdivulgation.com  
  
(alex@hackerdivulgation)-[~]  
$
```

REFERENCIAS

1. Proyecto publicado en Github. <https://github.com/whoamisec75/httpsuite>
2. Página para probar vulnerabilidades. <http://www.vulnweb.com/>



Este obra está bajo una [licencia de Creative Commons Reconocimiento-NoComercial-SinObraDerivada 4.0 Internacional](#).