



UNIVERSIDAD DE TALCA
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

Seguridad Informática

Laboratorio 3

Erik Regla
ereglal09@alumnos.utm.cl

7 de junio de 2020

Índice

1. Actividades	3
1.1. Actividad 1	3
1.1.1. filetype:sql “# dumping data for table” “‘PASSWORD‘ varchar”	3
1.1.2. text:pwd inurl:(service authors administrators users) “# -FrontPage-”	3
1.1.3. inurl:/admin/login.asp	4
1.1.4. allintitle:“Outlook Web Access Logon”	4
1.1.5. intitle:index.of “Apache/*” “server at”	5
1.1.6. “SquirrelMail version 1.4.4” inurl:src ext:php	5
1.1.7. camera linksys inurl:main.cgi	6
1.1.8. inurl:“ViewerFrame?Mode=”	6
1.1.9. inurl:“inurl:webarch/mainframe.cgi”	6
1.1.10. intitle:“network print server” filetype:shtm	7
1.1.11. “phone * * *” “address *” “e-mail” intitle: “curriculum vitae” . .	7
1.1.12. “robots.txt” “disallow:” filetype:txt	8
1.1.13. allintitle:restricted filetype:doc site:gov	8
1.1.14. index.of.dcim	9
2. En el informe de laboratorio deberá investigar a lo menos 2 comandos que no se encuentren en el listado de la actividad, entregando detalles de los resultados obtenidos y explicando cada uno de los componentes del comando.	9
2.0.1. filetype:log “usuario” “email”	9
2.0.2. filetype:pem certificate	10

1. Actividades

1.1. Actividad 1

Para esta actividad deberá explicar la estructura y la función que cumple cada uno de los comandos expuestos a continuación y además mostrar a lo menos 3 resultados diferentes de cada uno.

1.1.1. filetype:sql "# dumping data for table" “‘PASSWORD’ varchar”

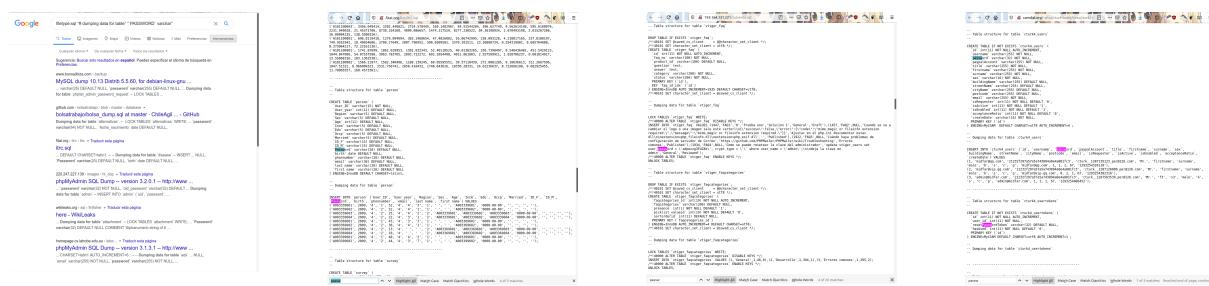


Figura 1: Archivos de tipo sql, los cuales tengan dentro del texto # dumping data for table y ‘PASSWORD’ varchar, típicos de los dumps. Intenta buscar dumps con contraseñas por si alguno la volcó y dejó disponible.

1.1.2. text:pwd inurl:(service | authors | administrators | users) “# -FrontPage-”

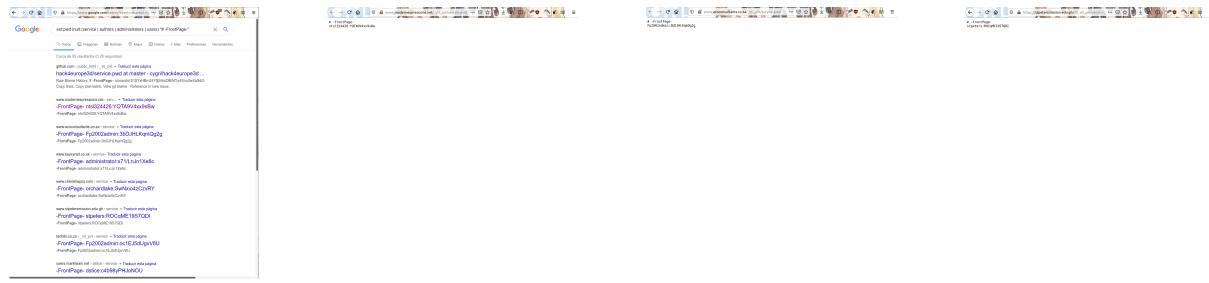


Figura 2: Sitios con el texto *pwd* que presenten match en la url (*service|authors|administrators|users*) y que poseean *-FrontPage-* en su resultado. Sirve para encontrar accesos en desarrollos hechos con FrontPage o Dreamweaver.

1.1.3. inurl:/admin/login.asp

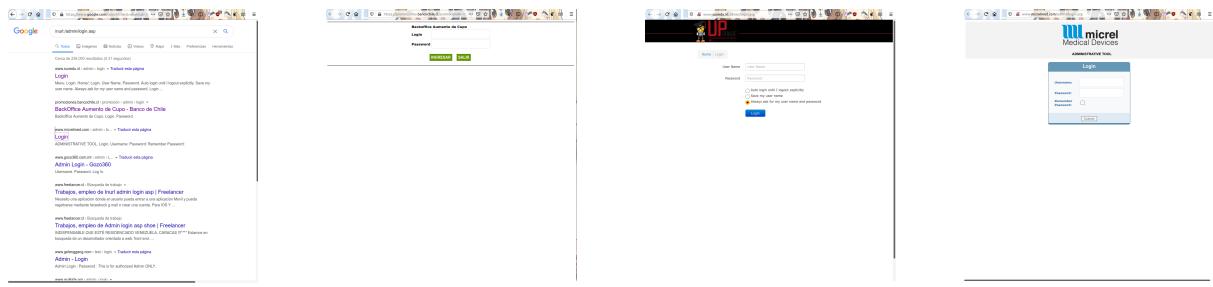


Figura 3: URLs que encajen con `/admin/login.asp`. Esas url suelen ser dejadas por desarrollos en ASP y rara vez cuentan con algun mecanismo de protección contra ataques de fuerza bruta, volviéndolas un buen objetivo para este tipo de ataques.

1.1.4. allintitle:“Outlook Web Access Logon”

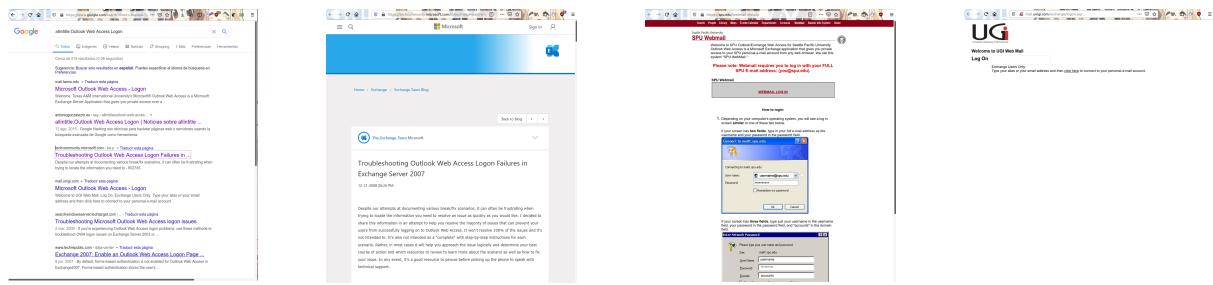


Figura 4: Sitios que tengan *Outlook Web Access Logon* en su título. Antiguamente utilizado para encontrar puntos de acceso para servidores Outlook, pero google restringe su uso como también hay cada vez menos servidores utilizando este servicio. Un ejemplo de un comando que ha envejecido mal en el tiempo.

1.1.5. intitle:index.of “Apache/*” “server at”

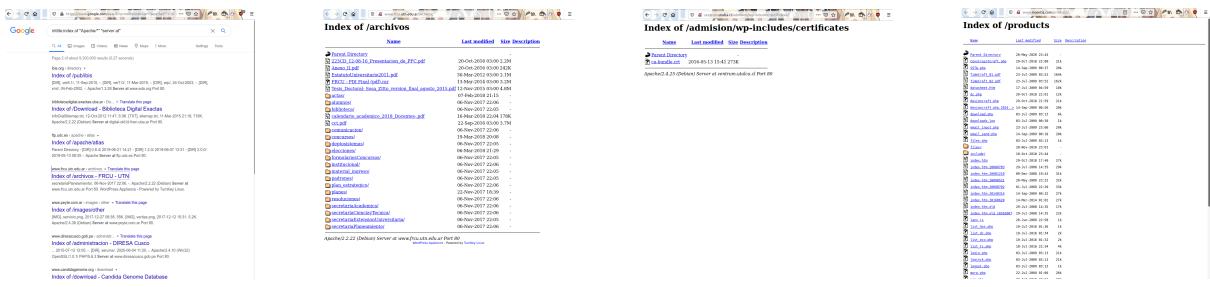


Figura 5: Sitios que tengan match *(index.of)?(.*)Apache/*(.*)(server at)* en su título. Ese título es el título que tiene por defecto el webroot en los servidores Apache, que muchos olvidan desactivar. El hecho que esté activo da la oportunidad de explorar el sistema de archivos local que está montado en el mismo lo cual puede filtrar documentos.

1.1.6. “SquirrelMail version 1.4.4” inurl:src ext:php



Figura 6: Sitios que tengan match *SquirrelMail version 1.4.4*. Exactamente la misma idea de buscar puntos de entrada a servidores outlook, pero esta vez con SquirrelMail.

1.1.7. camera linksys inurl:main.cgi

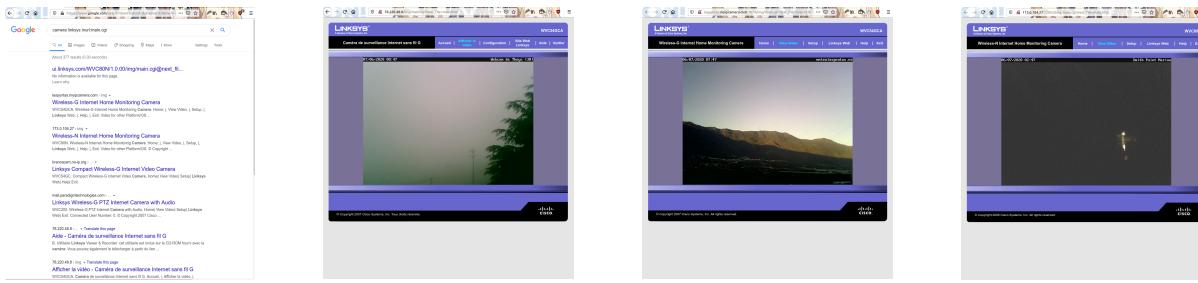


Figura 7: Sitios que tengan match *camera linksys inurl:main.cgi*. Muchas cámaras lynksys son configuradas para acceder a internet directamente en modo puente y a la gente se les olvida ponerles protección, permitiendo ver lo que transmiten.

1.1.8. inurl:“ViewerFrame?Mode=”

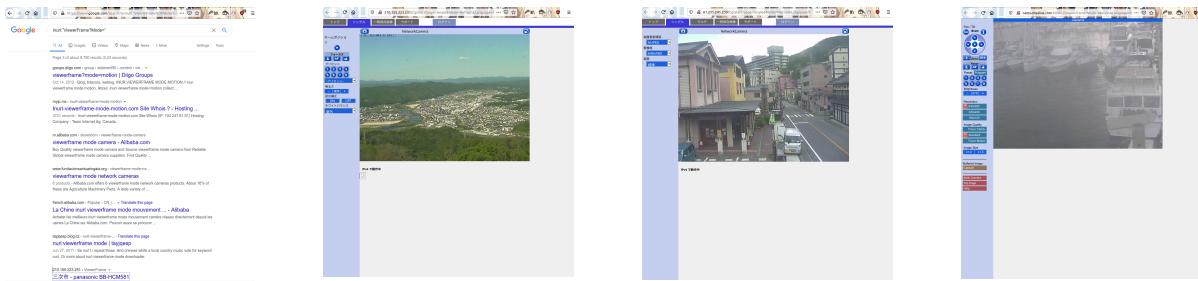


Figura 8: Sitios que tengan match “*ViewerFrame?Mode=*” en su URL. Misma idea de las camaras lynksys anterior pero en este caso apuntando a un tipo de interfaz en específico.

1.1.9. inurl:“inurl:webarch/mainframe.cgi”

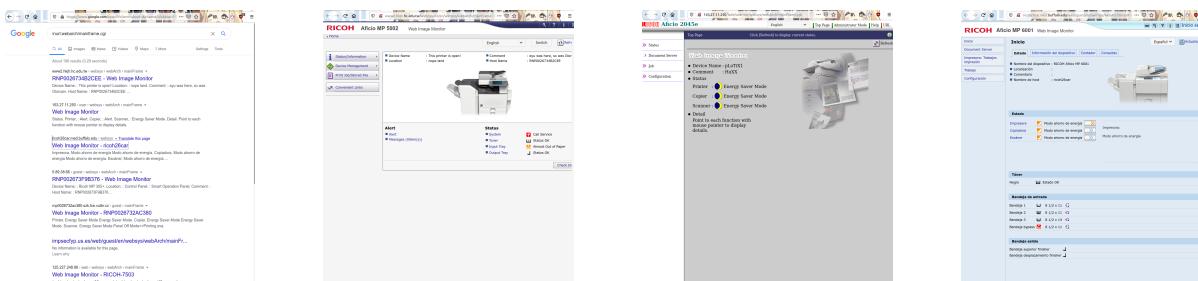


Figura 9: Sitios que tengan match “*inurl:webarch/mainframe.cgi*” en su URL. En este caso apunta a impresoras de la marca Ricoh expuestas directamente a internet.

1.1.10. intitle:“network print server” filetype:shtm

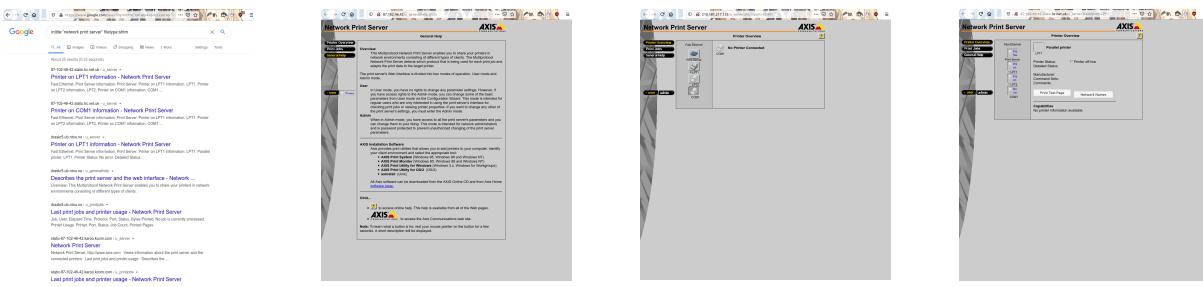


Figura 10: Sitios que tengan match “*network print server*” en su título y que sean del tipo shtm. Busca impresoras expuestas a internet operando con el servicio de Axis Print System.

1.1.11. “phone * * *” “address *” “e-mail” intitle: “curriculum vitae”

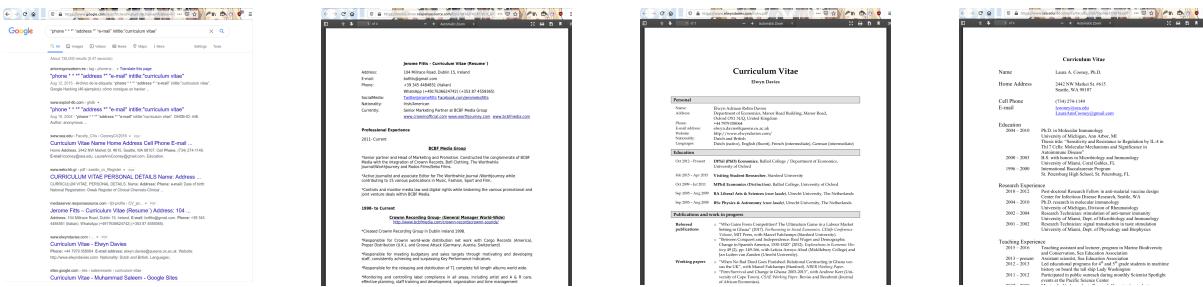


Figura 11: Sitios que tengan match $((\text{phone}|\text{address}| \text{e-mail}).+)^*$ en su contenido y que en su título indique *curriculum vitae*. Busca curriculums en inglés, puede ser útil para realizar doxxing.

1.1.12. “*robots.txt*” “*disallow:*” *filetype:txt*

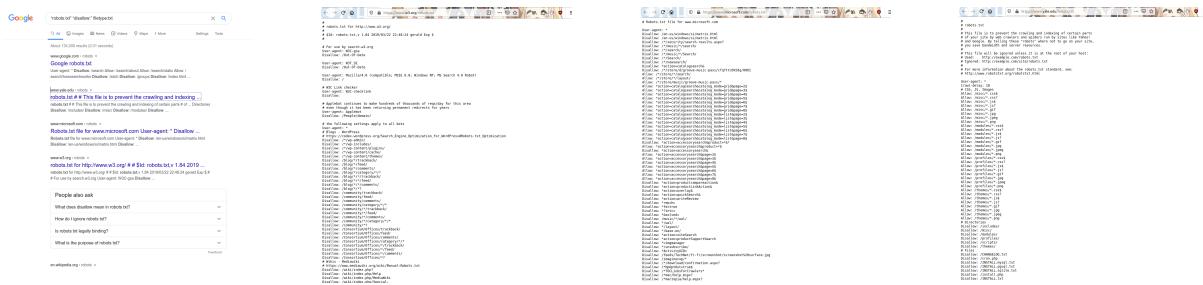


Figura 12: Archivos de texto que tengan match en su contenido con (*robots.txt|disallow:*). Sirve para encontrar sitios que tengan declarado contenido que no desea que sea indexado por un buscador. Ahora esto se respeta en la práctica solo por voluntad de quien lo implementa, además que sirve para ver contenido de interés y sus rutas que podrían no estar presentes en una búsqueda.

1.1.13. *allintitle:restricted filetype:doc site:gov*

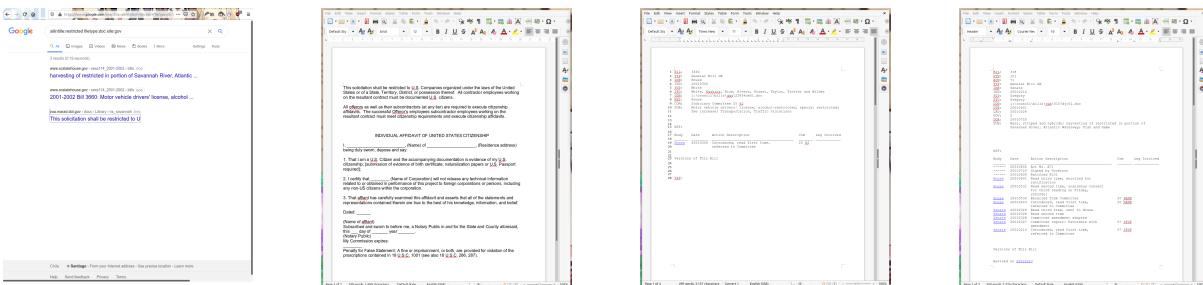


Figura 13: Archivos .doc cuyo título contenga *restricted* y que sean de un sitio del gobierno estadounidense. Lo que dice en el esquema, para nosotros poca utilizad tiene ya que este comando está regulado por google.

1.1.14. index.of.dcim

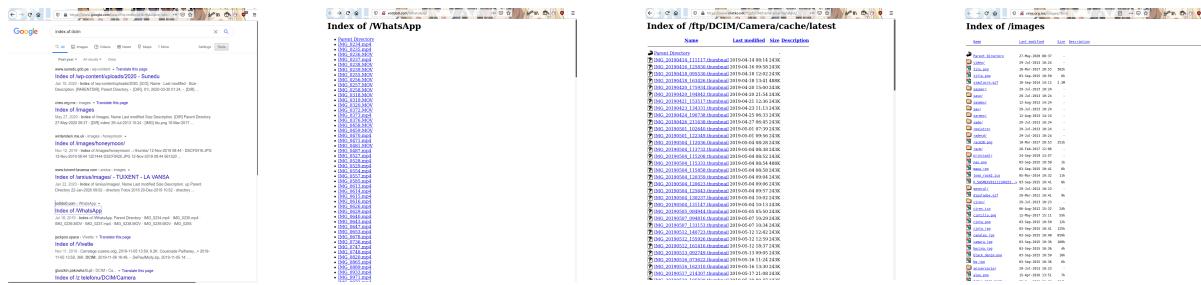


Figura 14: Entradas que contengan *index.of.dcim*. Este esquema es típico de servidores expuestos o bien indexes de apache que no han sido cerrados y que contienen archivos de imágenes

- 2. En el informe de laboratorio deberá investigar a lo menos 2 comandos que no se encuentren en el listado de la actividad, entregando detalles de los resultados obtenidos y explicando cada uno de los componentes del comando.**

2.0.1. filetype:log “usuario” “email”



Figura 15: Archivos .log que con match *usuario|email* en su contenido. Muchos logs son almacenados bajo esa extensión, lo cual resulta útil cuando los desarrolladores filtran información innecesaria en estos o bien los dejan expuestos. No solo pueden filtrar información personal, también información respecto a la infraestructura

2.0.2. filetype:pem certificate

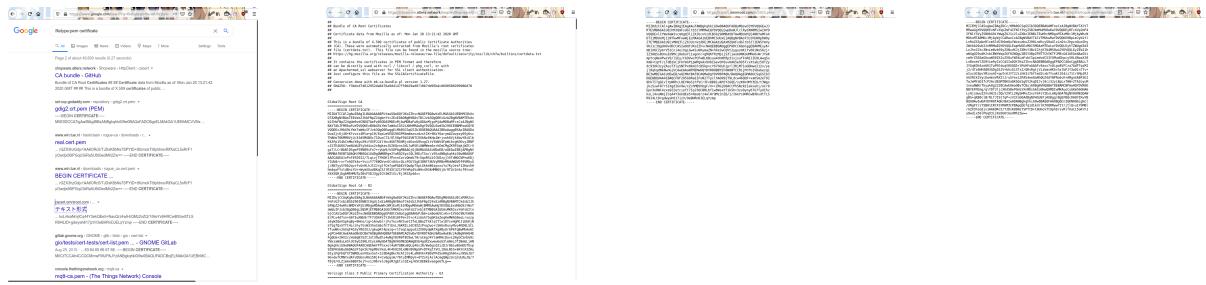


Figura 16: Archivos .pem que con el texto certificate. Usado para encontrar certificados los cuales podrían contener desde solo llaves públicas hasta definiciones completas, útil en caso de necesitar forzar el acceso a un servidor ssh o realizar spoofing.

Referencias

- [1] Moz - The Ultimate Guide to the Google Search Parameters. *WebSite*. the-ultimate-guide-to-the-google-search-parameters.
- [2] Refine web searches *Google Search Help*. <https://support.google.com/websearch/answer/2466433?hl=en>.
- [3] Mi repositorio (donde están alojadas las imágenes en mejor calidad) *Github Repository*. [https://github.com/KukyNekoi/UTAL/tree/master/ComputerScience/\(2020-1\)-Information-Security/Laboratorio](https://github.com/KukyNekoi/UTAL/tree/master/ComputerScience/(2020-1)-Information-Security/Laboratorio)