SOPHOS

HACK &BEERS

RastLeak: Leak Information as a Service

Nacho Brihuega Rodríguez (N4xh4ck5)

1. Whoami
2. Hacking con buscadores
3. Fuga de info -Metadatos
4. Ciberfraude
5. RastLeak

1. Whoami
2. Hacking con buscadores
3. Fuga de info -Metadatos
4. Ciberfraude
5. RastLeak

Whoami

- Security Consultant – Tiger Team SIA
- Máster de Seguridad Informática en Universidad de la Rioja (UNIR)
- Grado en Ingeniería en Tecnologías de la Telecomunicación, especialidad en ingeniería telemática.
- Coautor en el blog “Follow the White Rabbit” – fwhibbit.es
- Info de contacto:
  - **Linkedin**: https://es.linkedin.com/in/ignacio-brihuega-rodr%25C3%25ADguez-b89564a6
  - **Twitter**: twitter.com/@nachoo_91

HACK &BEERS

Disclamer

- La información que se va a mostrar es de carácter público.
- Se ofuscará la mayor parte de las ocasiones para no mostrar el origen de la información.
- Las técnicas demostradas son para fines académicos, no me hago responsable de su uso para otro fin.
- Hack&Learn&Share

HACK
&BEERS

Hacking con buscadores

Deja que Google haga el trabajo sucio!!!

Google bing

EXPLOIT DATABASE

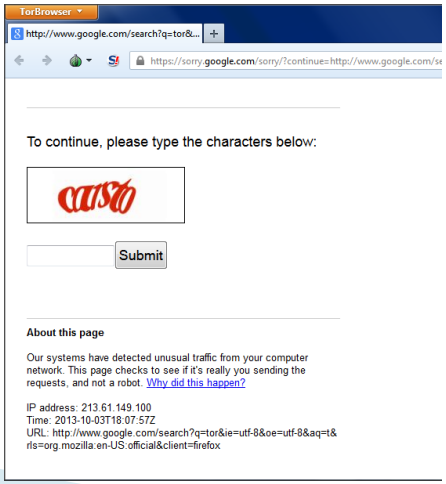
Footprinting de un pentesting web
Scaning pasivo
Búsqueda de fuga de información
Búsqueda de dominios
Reputación: Abuso de marca
Cyberfraude: phishing, cyber/typosquating,

HACK &BEERS

Hacking con buscadores

Herramientas semiautomáticas insuficientes

Surge la necesidad de personalizar búsquedas avanzadas pero está el captcha de Google



HACK &BEERS

Hacking con buscadores

Dorks

Google & Bing

- site: sitio web
- inurl: Aparece en la url – exclusivo de Google
- intitle: título
- intext: Aparezca en el texto
- filetype/ext: extensión.
- info: información
- cache: cacheado
- ip – sólo en Bing
- link: enlaces contenido sitio web
- Domain: listar subdominios. De Bing

Operadores lógicos

Or: |

And: +

Comillas: “”

?:Puede estar o no

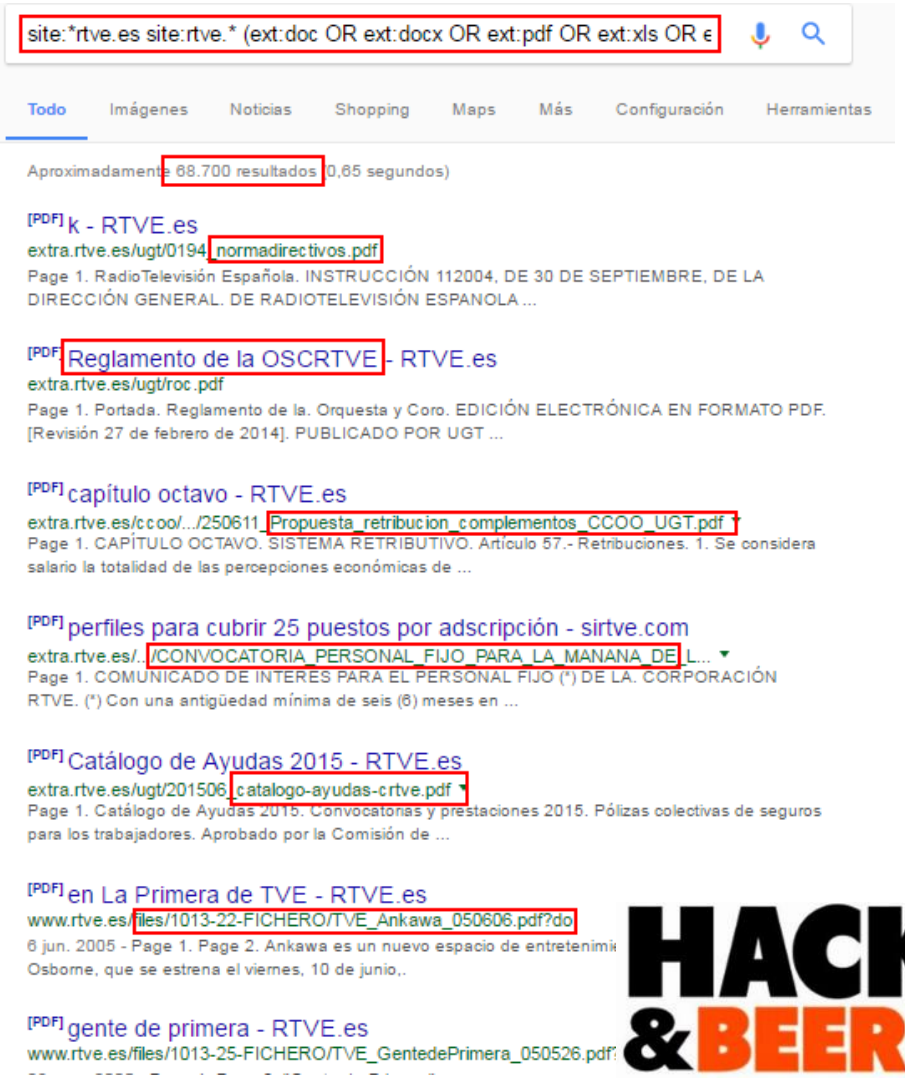
*: comodín

-: operador negativo

HACK &BEERS

Hacking con buscadores & Fuga de información

site:*rtve.es site:rtve.* (ext:pdf OR ext:doc OR ext:docx OR ext:xls OR ext:ppt)



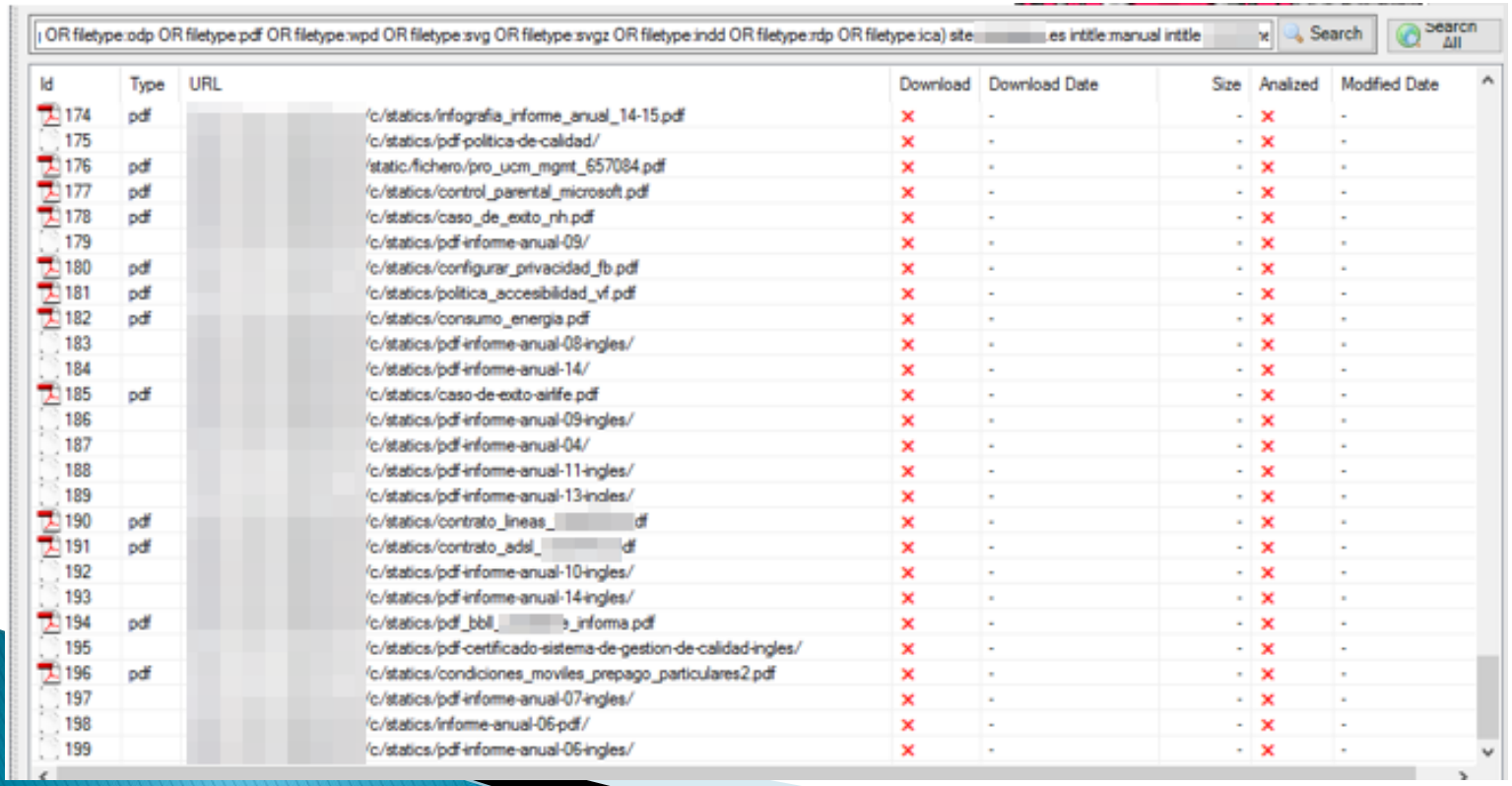
Hacking con buscadores & Fuga de información

intext:rtve intitle:rtve -site:rtve.es -site:www.rtve.es (ext:pdf OR ext:doc OR ext:docx OR ext:xls OR ext:ppt)

Hacking con buscadores & Fuga información&metadatos

Leak information – Metadatos -> FOCA

Usuarios del directorio activo, software, versiones, SSOO, rutas de carpetas, fechas y tiempo de creación, modificación,…



OR filetype:odp OR filetype:pdf OR filetype:wpd OR filetype:svg OR filetype:svgz OR filetype:indd OR filetype:rdp OR filetype:ica) site: .es intitle:manual intitle: Search Search All

Id	Type	URL	Download	Download Date	Size	Analized	Modified Date
174	pdf	/c/statics/infografia_informe_anual_14-15.pdf	✗	-	-	✗	-
175		/c/statics/pdf-politica-de-calidad/	✗	-	-	✗	-
176	pdf	/static/fichero/pro_ucm_mgmt_657084.pdf	✗	-	-	✗	-
177	pdf	/c/statics/control_parental_microsoft.pdf	✗	-	-	✗	-
178	pdf	/c/statics/caso_de_exito_nh.pdf	✗	-	-	✗	-
179		/c/statics/pdf-informe-anual-09/	✗	-	-	✗	-
180	pdf	/c/statics/configurar_privacidad_fb.pdf	✗	-	-	✗	-
181	pdf	/c/statics/politica_accesibilidad_vf.pdf	✗	-	-	✗	-
182	pdf	/c/statics/consumo_energia.pdf	✗	-	-	✗	-
183		/c/statics/pdf-informe-anual-08-ingles/	✗	-	-	✗	-
184		/c/statics/pdf-informe-anual-14/	✗	-	-	✗	-
185	pdf	/c/statics/caso-de-exito-airlife.pdf	✗	-	-	✗	-
186		/c/statics/pdf-informe-anual-09-ingles/	✗	-	-	✗	-
187		/c/statics/pdf-informe-anual-04/	✗	-	-	✗	-
188		/c/statics/pdf-informe-anual-11-ingles/	✗	-	-	✗	-
189		/c/statics/pdf-informe-anual-13-ingles/	✗	-	-	✗	-
190	pdf	/c/statics/contrato_lineas_ df	✗	-	-	✗	-
191	pdf	/c/statics/contrato_adsl_ df	✗	-	-	✗	-
192		/c/statics/pdf-informe-anual-10-ingles/	✗	-	-	✗	-
193		/c/statics/pdf-informe-anual-14-ingles/	✗	-	-	✗	-
194	pdf	/c/statics/pdf_bbll_ _informa.pdf	✗	-	-	✗	-
195		/c/statics/pdf-certificado-sistema-de-gestion-de-calidad-ingles/	✗	-	-	✗	-
196	pdf	/c/statics/condiciones_moviles_prepago_particulares2.pdf	✗	-	-	✗	-
197		/c/statics/pdf-informe-anual-07-ingles/	✗	-	-	✗	-
198		/c/statics/informe-anual-06-pdf/	✗	-	-	✗	-
199		/c/statics/pdf-informe-anual-06-ingles/	✗	-	-	✗	-

HACK & BEERS

Hacking con buscadores & Fuga de información

Leak sensitive Information

Búsqueda de metalocalizaciones de archivos que desvelan usuarios, carpetas, impresoras y SSOO.

ext:pdf intitle: c users – Listar info de Windows 7

ext:pdf intitle:"c documents and settings" – Listar info de Windows XP

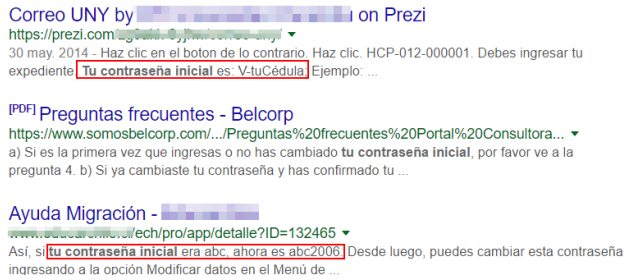
También para Linux:

ext:pdf "file home"

Hacking con buscadores & Fuga de información

Leak sensitive Information – Usuarios y contraseñas por defecto

Búsqueda de políticas de nombre de usuarios y contraseñas



"user name consists of the" password
"usuario esta formado por" contraseña

"tu contraseña inicial"-- 659 resultados!!!
"su contraseña inicial" -- 4.320 resultados!!!
"your initial password"-- 129.000 resultados!!!

HACK & BEERS

Hacking con buscadores & Fuga de información

Leak sensitive Information – Política de contraseñas

Reutilización de contraseñas → Normativas!!!

"your password is the same"
"your password is the same" site:edu
"tu contraseña es la misma que"
"tu contraseña es la misma"

Acceder al área de clientes Fibra / ADSL -
https://ayuda. es/particulares/adsl-y-fibra/mi-adsl/1894...
. **tu contraseña es la misma** para tu área de clientes y para tu app Mi . No recuerdo mi contraseña. Si has olvidado tu contraseña clica en la opción ...

Ranking de Notas - puedes ingresar a un simulador
.cl
Tu contraseña es la misma que utilizaste para el proceso de Inscripción PSU INGRESAR. Recuperar contraseña de acceso

Corporation Online Courses Traducir esta página
edu
... login on the left side of this page using your full FCSL email as your login ID. **Your password is the same** one utilized to login to the FCSL network and email.

- Login Traducir esta página
edu/Login.aspx
*Your password is the same as your JagMail or USAonline/Sakai password. For USA Health System employees: *If you do not already have a USA online/Sakai account ...

Moodle @ Mac Traducir esta página
edu/my
Your password is the same one you use to access your MacMurray email. Site News. Subscribe to the Site News forum below for updates on scheduled Moodle downtime, ...

Login :. Traducir esta página
edu/ balance
Home > . Please log in with your UMass Lowell email address, .. **Your password is the same** as your email password. Email: Password: UCard, ...

How to use the Zone
/finaid/PDFdocs/1011/How to use the Zon... - Archivo PDF
How to use the Zone to check your Financial Aid Information . **Your password is the same** password used for your Zone login. FYI: If you can't find your Financial Aid

Home - Traducir esta página
edu/ /default.aspx
In tandem with our new website, Queens College has launched its intranet, ... **Your password is the same** password you adopted for your QC Username account.

YOU Portal Login Traducir esta página
.edu
Enter your Username and Password. U sername: P assword: .. **Your password is the same** as the password you use to access your WesternU e-mail account.

HACK & BEERS

Hacking con buscadores & Fuga de información

Leak sensitive Information as Pentesting

Descubrir ficheros indexados – Extraer metadatos -> obtener usuarios (DA) y/o direcciones de correo -> Conocer políticas de contraseña y de bloqueo -> Enumerar usuarios ->Política de contraseña débiles

¿Acceso a la parte privada?

Todo empezó con un fichero indexado….

HACK &BEERS

Hacking con buscadores & Ciberfraude

site:pastebin.com intext:username intext:password intext:"@TARGET.com"

site:pastebin.com intext:"@TARGET.com"

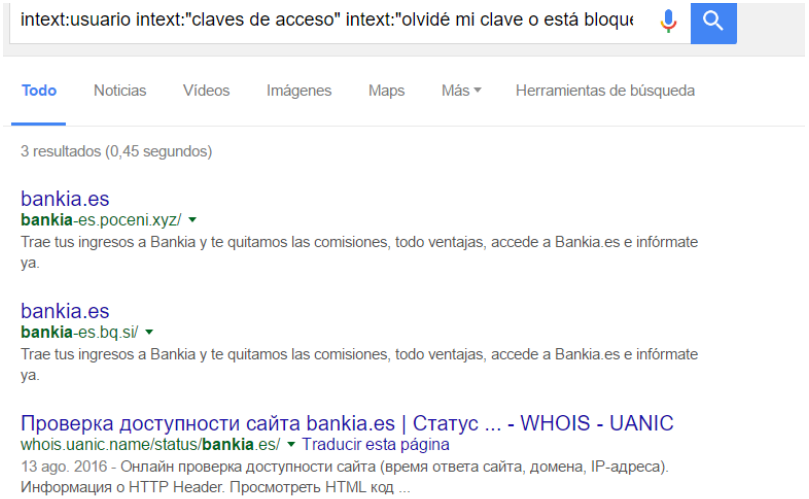
Búsqueda de usuarios y contraseñas de BBDD que fueron comprometidas

Pastebin for everywhere!!!

Hacking con buscadores & Ciberfraude

Dorks-phishing

```
intext:usuario intext:"claves de acceso"
intext:"olvidé mi clave o está bloqueada"
intitle:bankia -site:www.bankia.es
```

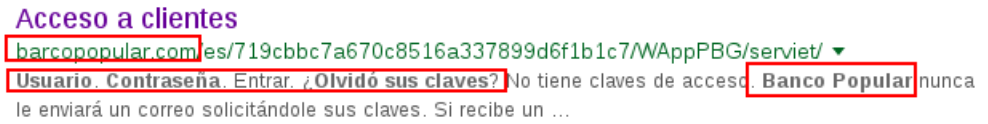


HACK & BEERS

Hacking con buscadores & Ciberfraude

Phishing- dorks

intext:"Intoduzca sus datos de identificación y su Clave de acceso" intitle:santander intext:"acceso particulares" inurl:php -site:*.gruposantander.es



intext:Usuario intext:Contraseña intext:"¿Olvidó sus claves?" intext:"banco popular" -site:*.bancopopular.es

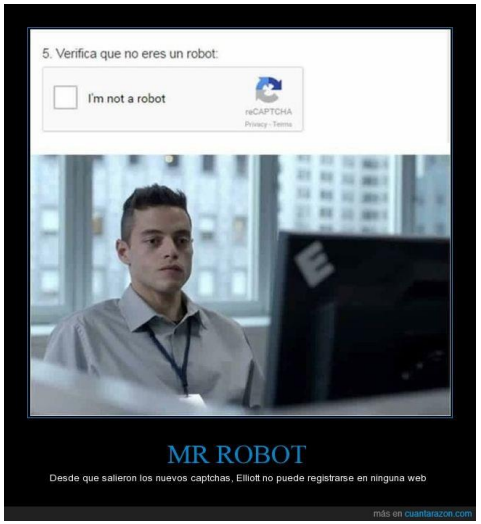
HACK & BEERS

1. Whoami
2. Hacking con buscadores
3. Fuga de info - Metadatos
4. Ciberfraude
5. RastLeak

RastLeak

Herramienta para automatizar las búsquedas manuales de un pentester con objeto de identificar ficheros indexados en Internet dando la opción de su descarga y extracción de metadatos.

Google



Demo time!!!

TRABAJO FUTURO

- Automatización de correos “comprometidos” en pastes.
- Añadir screenshots de los dominios ¬¬ “archive.org”
- Posibilidar cambiar de IP mediante TORibio -> evitar parcialmente captcha Google.
- Categorizar todos los metadatos extraídos en plan “La FOCA”
- ~~¿Pagar API de Google?~~

HACK &BEERS

Ruegos Y Preguntas

Muchas gracias