



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**



Disclaimer



- 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



Hacking con buscadores

Deja que Google haga el trabajo sucio!!!



Footprinting de un pentesting web

Scanning pasivo

Búsqueda de fuga de información

Búsqueda de dominios

Reputación: Abuso de marca

Cyberfraude: phishing, cyber/typosquatting,

**HACK
& BEERS**

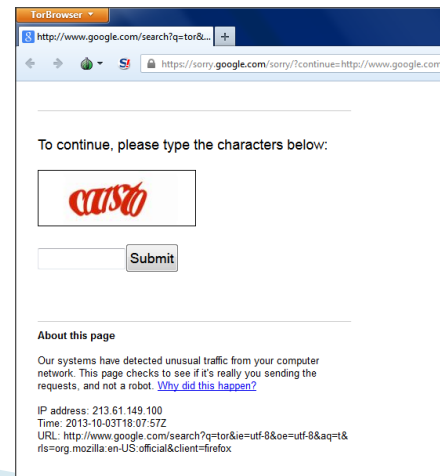
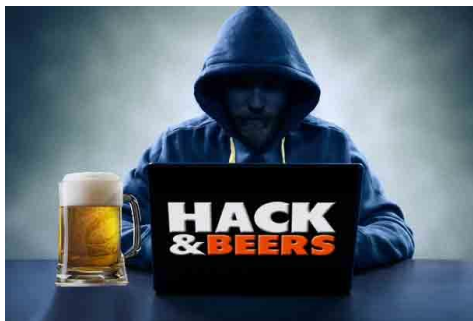


Hacking con buscadores

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



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)

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

Todo Imágenes Noticias Shopping Maps Más Configuración Herramientas

Aproximadamente 68.700 resultados (0,65 segundos)

[PDF] k - RTVE.es
extra.rtve.es/ugt/0194/normadirectivos.pdf
Page 1. RadioTelevisión Española. INSTRUCCIÓN 112004, DE 30 DE SEPTIEMBRE, DE LA DIRECCIÓN GENERAL. DE RADIOTELEVISIÓN ESPAÑOLA ...

[PDF] Reglamento de la OSCRTVE - RTVE.es
extra.rtve.es/ugt/roc.pdf
Page 1. Portada. Reglamento de la. Orquesta y Coro. EDICIÓN ELECTRÓNICA EN FORMATO PDF. [Revisión 27 de febrero de 2014]. PUBLICADO POR UGT ...

[PDF] capítulo octavo - RTVE.es
extra.rtve.es/ccool.../250611/Propuesta_retribucion_complementos_CCOO_UGT.pdf
Page 1. CAPÍTULO OCTAVO. SISTEMA RETRIBUTIVO. Artículo 57.- Retribuciones. 1. Se considera salario la totalidad de las percepciones económicas de ...

[PDF] perfiles para cubrir 25 puestos por adscripción - sirtve.com
extra.rtve.es/.../CONVOCATORIA_PERSONAL_FIJO_PARA_LA_MANANA_DE_L...
Page 1. COMUNICADO DE INTERES PARA EL PERSONAL FIJO (*) DE LA. CORPORACIÓN RTVE. (*) Con una antigüedad mínima de seis (6) meses en ...

[PDF] Catálogo de Ayudas 2015 - RTVE.es
extra.rtve.es/ugt/201506/catalogo-ayudas-crtve.pdf
Page 1. Catálogo de Ayudas 2015. Convocatorias y prestaciones 2015. Pólizas colectivas de seguros para los trabajadores. Aprobado por la Comisión de ...

[PDF] en La Primera de TVE - RTVE.es
www.rtve.es/files/1013-22-FICHERO/TVE_Ankawa_050606.pdf?do
6 jun. 2005 - Page 1. Page 2. Ankawa es un nuevo espacio de entretenimi
Osborne, que se estrena el viernes, 10 de junio,.

[PDF] gente de primera - RTVE.es
www.rtve.es/files/1013-25-FICHERO/TVE_GentedePrimera_050526.pdf?

**HACK
& BEERS**



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)

intext:rtve intitle:rtve -site:www.rtve.es -site:rtve.es (ext:pdf OR ext:doc (

Todo Noticias Vídeos Maps Imágenes Más Configuración Herramientas

Aproximadamente 1.050 resultados (0,52 segundos)

[PDF] 2.225 PROFESIONALES DE RTVE EXIGEN INDEPENDENCIA Y ...
www.infolibre.es/uploads/documentos/2017/02/16/tve_7bd3a402.pdf
16 feb. 2017 - Los Consejos de Informativos de RTVE (TVE, RNE, Interactivos) hemos recogido. 2.225 firmas de profesionales de la Corporación en apoyo al ...

[PDF] TESIS DOCTORAL LA TRANSFORMACIÓN DE RTVE DESDE LA V...
www.tesisenred.net/bitstream/handle/10803/117461/ammf1de1.pdf?sequence=1...y
Bajo la dirección del Catedrático D. José Manuel Pérez Torero. Mayo de 2012. LA TRANSFORMACIÓN DE RTVE DESDE LA VIII. LEGISLATURA: Legislación ...

[PDF] @ RTVE.ES - IMIM
https://intranet.imim.cat/esdeveniments/22394/fitxers/17571/download
3 Noviembre, 2014. @ RTVE.ES. 4 min. TMV: 539300. TVD: 406000. UUD: 5603000. UUM: www.rtve.es/noticias. TARIFA: PAÍS: URL: 5393 €. España ...

[PDF] EL RÉGIMEN JURÍDICO DE LA NUEVA CORPORACIÓN RTVE
e-spacio.uned.es/ez/eserv/bibliuned:revistaDFD-2009-1-5060/Documento.pdf
de AM Ruiz de Apodaca Espinosa - 2009 - Citado por 2 - Artículos relacionados
Administración. b) El Director General de RTVE. c) Los Consejos Asesores. B. ... Obligaciones derivadas de la condición de servicio público para RTVE. B. El.

[PDF] La crisis de RTVE - E-Prints Complutense
eprints.ucm.es/8052/1/rtve2.pdf
de S López-Pavillard - 1992 - Citado por 3 - Artículos relacionados
Santiago.lopez@rtve.es. Junio de 1992. Índice. 1. La televisión pública en Europa. 2. Organización, control y financiación de RTVE. 3. Cronología de una crisis.

[PDF] La documentación audiovisual en RTVE
https://revistas.ucm.es/index.php/DCIN/article/download/.../19961
de SL Pavillard - 1995 - Citado por 8 - Artículos relacionados
prestación a terceros de los fondos audiovisuales de RTVE, es la primera ... Radiotelevisión Española, sobre la Documentación en RTVE y sus sociedades..



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									
Id	Type	URL	Download	Download Date	Size	Analyzed	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_rh.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-airife.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_addl_ df	×	-	-	×	-		
192		/c/statics/pdf-informe-anual-10-ingles/	×	-	-	×	-		
193		/c/statics/pdf-informe-anual-14-ingles/	×	-	-	×	-		
194	pdf	/c/statics/pdf_bbil_ a_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/	×	-	-	×	-		



Hacking con buscadores & Fuga de información

Leak sensitive Information

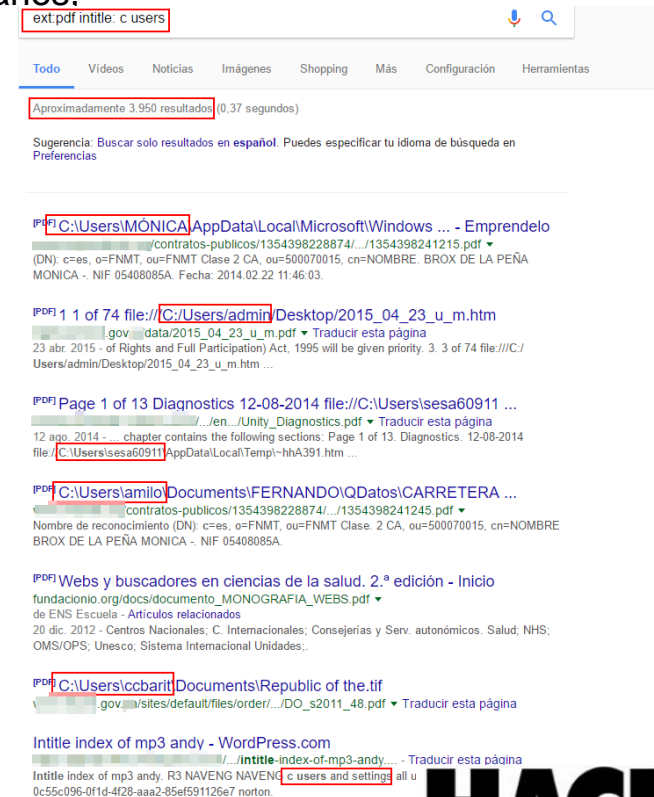
Búsqueda de metalocalizaciones de archivos que desvelan usuarios, carpetas, impresoras y SSOO.

`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

Correo UNY by [redacted] on Prezi

<https://prezi.com/AgGdH-6j/mi-correo-uny/>

30 may. 2014 - Haz clic en el botón de lo contrario. Haz clic. HCP-012-000001. Debes ingresar tu expediente. **Tu contraseña inicial es: V-tuCédula** Ejemplo: ...

[PDF] Preguntas frecuentes - Belcorp

<https://www.somosbelcorp.com/.../Preguntas%20frecuentes%20Portal%20Consultora...>

a) Si es la primera vez que ingresas o no has cambiado **tu contraseña inicial**, por favor ve a la pregunta 4. b) Si ya cambiaste tu contraseña y has confirmado tu ...

Ayuda Migración - [redacted]

www.educacion.mec.gov.ve/ech/pro/app/detalle?ID=132465

Así, si **tu contraseña inicial era abc, ahora es abc2008**. Desde luego, puedes cambiar esta contraseña ingresando a la opción Modificar datos en el Menú de ...

“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!!!

Ayuda - Biblioteca Central - Universidad Tecnológica de Panamá

[/modulos/catalogo/ayuda.faces;jsessionid...](#)

Si existe, **tu contraseña inicial es 12345**, debes cambiar de contraseña. Si no existe, Regístrate. Presentate por nuestra biblioteca para autenticar tus datos.

Biblioteca Central - Universidad Tecnológica de Panamá

[/modulos/catalogo/ayuda/catalogos.faces](#)

Si ya existes **tu contraseña inicial es 12345** es necesario que la cambies. 2. Si no existes es necesario que te registres en la opción “Regístrate” del portal ...

MANUAL DE USO DEL OPAC - [redacted]

[absysnet_Docs/Manual_opac1.pdf](#) - Archivo PDF

Tu contraseña inicial está formada por los ocho primeros caracteres de tu documento de **identidad**. A continuación, pulsa el botón Conectar. 2

Cómo obtengo el usuario y contraseña de Alquilerdeviviendas.es

www.alquilerdeviviendas.es/acceso_alquileres.php

... puedes enviarnos tus datos de contacto y te enviaremos un usuario y el código de cliente que será **tu contraseña inicial** para que tú mismo puedas insertar las ...

contraseña - Microsoft Community

answers.microsoft.com/es-es/outlook_com/forum/oemail-oapps...

... de 30 a 72 días para generar nuevamente el cambio, en ocasiones debe realizar un tercer cambio para que reconozca **tu contraseña inicial** ...

Archivo de Categoría de "03. Registro e ingreso" | Facto

<https://www.facto.cl/manuales/manual-para-usuarios/registro-e-ingreso>

Cambiar **tu contraseña inicial** después de ingresar. Si quieres cambiar la contraseña inicial por otra más fácil de recordar, ...

PLATAFORMA MOODLE - [redacted]

[/plataforma-moodle](#)

Tu contraseña inicial es como tu usuario, tu DNI con 0 delante salvo que ya hayas utilizado alguna vez la plataforma Moodle de la Conselleria d

**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 - [redacted]

<https://ayuda.cablemodems.com/particulares/adsl-y-fibra/mi-adsl/1894...>

tu contraseña es la misma para tu área de clientes y para tu app Mi [redacted]. No recuerdo mi contraseña. Si has olvidado tu contraseña clicla en la opción ...

Ranking de Notas - puedes ingresar a un simulador

[\[redacted\].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

[\[redacted\].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

[\[redacted\].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

[\[redacted\].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 :: [redacted] Traducir esta página

[\[redacted\].edu/balance](#)

Home > [redacted]. 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 [redacted]

[\[redacted\].finaid/PDFdocs/1011/How to use the Zone... 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 - [redacted] Traducir esta página

[\[redacted\].edu/default.aspx](#)

In tandem with our new website, Queens College has launched its intranet, [redacted]. **Your password is the same** password you adopted for your QC Username account

YOU Portal Login Traducir esta página

[\[redacted\].edu](#)

Enter your Username and Password. U username: Password: **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?**

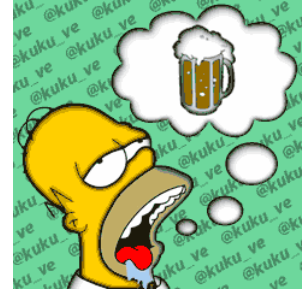
Todo empezó con un fichero indexado....



**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!!!**



**HACK
& BEERS**



Hacking con buscadores & Ciberfraude

Dorks-phishing

intext:usuario intext:"claves de acceso" intext:"olvidé mi clave o está bloqueada"

Todo Noticias Videos Imágenes Maps Más ▾ Herramientas de búsqueda

3 resultados (0,45 segundos)

bankia.es

bankia-es.poceni.xyz/ ▾

Trae tus ingresos a Bankia y te quitamos las comisiones, todo ventajas, accede a Bankia.es e infórmate ya.

bankia.es

bankia-es.bq.si/ ▾

Trae tus ingresos a Bankia y te quitamos las comisiones, todo ventajas, accede a Bankia.es e infórmate ya.

Проверка доступности сайта bankia.es | Статус ... - WHOIS - UANIC

whois.uanic.name/status/bankia.es/ ▾ Traducir esta página

13 ago. 2016 - Онлайн проверка доступности сайта (время ответа сайта, домена, IP-адреса).

Информация о HTTP Header. Просмотреть HTML код ...

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

bankia-es.bq.si

Utilizamos cookies propias y de terceros para mejorar nuestros servicios y mostrarle publicidad relacionada con sus preferencias mediante el análisis de sus hábitos de navegación. Si continúa navegando, consideramos que acepta su uso. Para obtener más información, o bien conocer cómo cambiar la configuración, consulte nuestra política de cookies.

Particulares Banca personal Banca privada Empresas Pymes y Autónomos

Atención al cliente ▾ Oficinas y cajeros Español ▾ Q

Hazte cliente Acceso clientes

Bankia CUENTAS Y TARJETAS AHORRO E INVERSIÓN FINANCIACIÓN SEGUROS

Te quitamos las principales comisiones:

- De administración y mantenimiento
- De tu tarjeta de débito ON
- De transferencias realizadas en los canales online

Abre ahora tu Cuenta_ON

Saber más Contratar

bankia-es.poceni.xyz

Utilizamos cookies propias y de terceros para mejorar nuestros servicios y mostrarle publicidad relacionada con sus preferencias mediante el análisis de sus hábitos de navegación. Si continúa navegando, consideramos que acepta su uso. Para obtener más información, o bien conocer cómo cambiar la configuración, consulte nuestra política de cookies.

Particulares Banca personal Banca privada Empresas Pymes y Autónomos

Atención al cliente ▾ Oficinas y cajeros Español ▾ Q

Hazte cliente Acceso clientes

Bankia CUENTAS Y TARJETAS AHORRO E INVERSIÓN FINANCIACIÓN SEGUROS

Te quitamos las principales comisiones:

- De administración y mantenimiento
- De tu tarjeta de débito ON
- De transferencias realizadas en los canales online

Abre ahora tu Cuenta_ON

Saber más Contratar

Usuario

NIF / NIE / Pasaporte

Clave de acceso

Entrar

Olvidé mi clave o está bloqueada >

Solicita las claves de acceso para operar online

Solicitar claves

HACK & BEERS



Hacking con buscadores & Ciberfraude

Phishing- dorks

de identificación y su clave de acceso" intitle:santander inurl:php -site:*.gruposantander.es

Todo Noticias Imágenes Vídeos Maps Más Configuración Herramientas

3 resultados (0,38 segundos)



Un recordatorio de privacidad de Google

RECORDARME MÁS TARDE

LEER

Santander particulares acceso clientes - Yulia Sverchkova

yuliasverchkova.com/hbwssvreengihl/Santander-particulares-acceso-clientes.php

Este sitio puede dañar tu ordenador.

CUENTA + de recibos. Política de Cookies. Acceso a Clientes BS Online. Enlaces Introduzca sus datos de identificación y su Clave de acceso con el teclado de ...

Banco santander particulares acceso clientes

azeus.com/bdvl7jp1zb/banco-santander-particulares-acceso-clientes.php

Beneficios Cuenta Cambia tu Hipoteca al Santander · Particulares; Atención al cliente Introduzca sus datos de identificación y su Clave de acceso con el ...

Banco santander particulares acceso clientes - Sice

mmadero.sice.com.mx/portal/lib/Pearl/7banco-santander-particulares-acceso-clientes.ph

Más de 270 oficinas para otras operaciones. NetBanco Particulares. Introduzca sus datos de identificación y su Clave de acceso con el teclado de su ordenador ...

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

Acceso a clientes

barcopopular.com.es/719cbbc7a670c8516a337899d6f1b1c7/WAppPBG/serviet/

Usuario. Contraseña. Entrar. ¿Olvidó sus claves? No tiene claves de acceso. Banco Popular nunca le enviará un correo solicitándole sus claves. Si recibe un ...

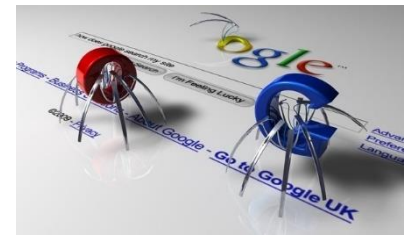
intext:Usuario intext:Contraseña intext:"¿Olvidó sus claves?" intext:"banco popular" -site:*.bancopopular.es

**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.



Demo time!!!

**HACK
& BEERS**



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?~~



Ruegos Y Preguntas



Muchas gracias

