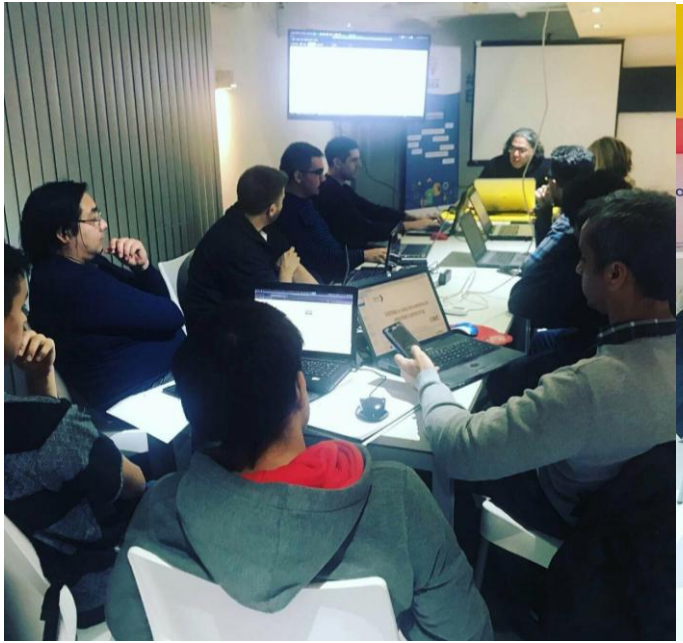
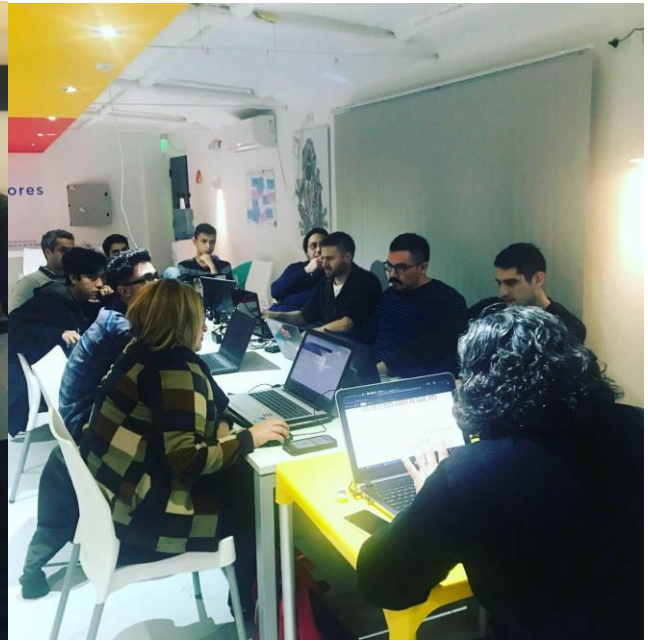
GDG Neuquén

Cybersecurity Highlights

Sobre labs:

Motivación?





Objetivo del grupo:

- **Compartir conocimiento** sobre temas de seguridad informática.
- **Pasar un buen rato,** con gente que comparte este mismo interés, “sin jerarquías”.

Sobre labs:

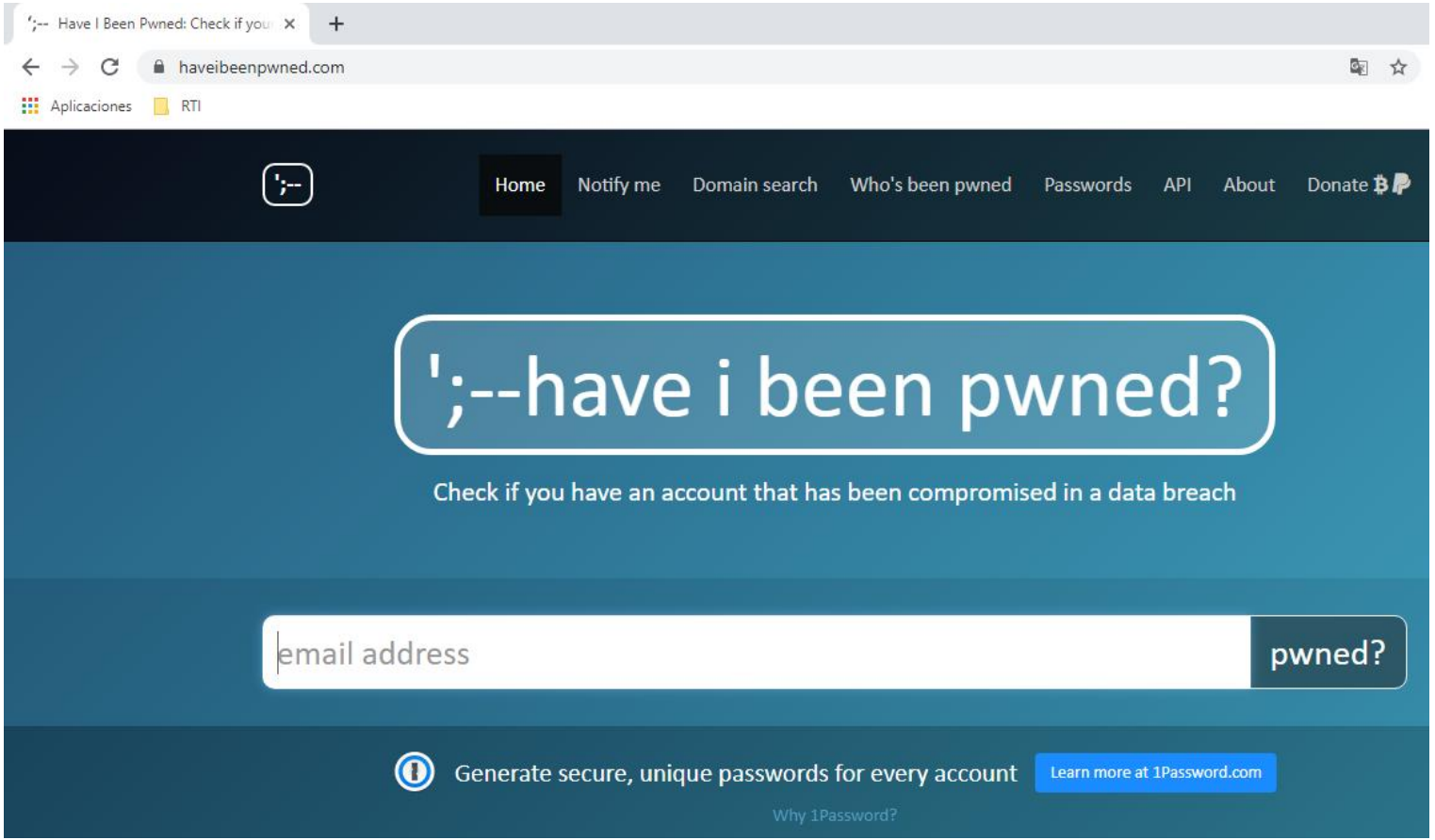
Motivación?

En la actualidad convivimos con la tecnología, **todo pasa por internet.** Luego al navegar en tan sólo 1 minuto por internet nos exponemos a:

- Nuevas variantes de **MALWARE (RANSOMWARE)**
- Ataques de **PHISHING**
- Registros de **FUGAS DE DATOS (*)**
- **WEB VULNERABLES (*)**
- **APPs MOVILES MALICIOSAS**
- **CRIPTO MINERIA MALICIOSA**
- ETC...

...entonces, ¿estas seguro en internet?

Sobre labs:


';-- Have I Been Pwned: Check if you
haveibeenpwned.com
Aplicaciones
RTI
Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
';--have i been pwned?
Check if you have an account that has been compromised in a data breach
email address
pwned?
Generate secure, unique passwords for every account
Learn more at 1Password.com
Why 1Password?

el otro día escuché una charla de desarrolladores...

quiero capturar las **cookies que cachea** el webserver y pasarlas como **parámetro al servidor** de base de datos, **¿se podrá?**

¡si se puede!

y mi amigo el desarrollador pudo...
y cualquier atacante tambien!!!...

buscando cookies en la web

intitle:index.of homedir/cache/

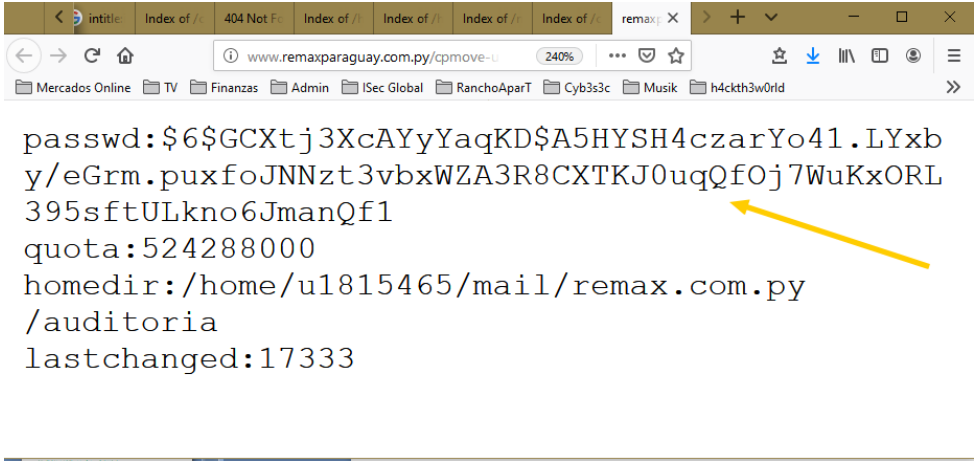
intitle:index.of homedir/tmp/

encontrando cookies en la web!!! (y otras cosas...)

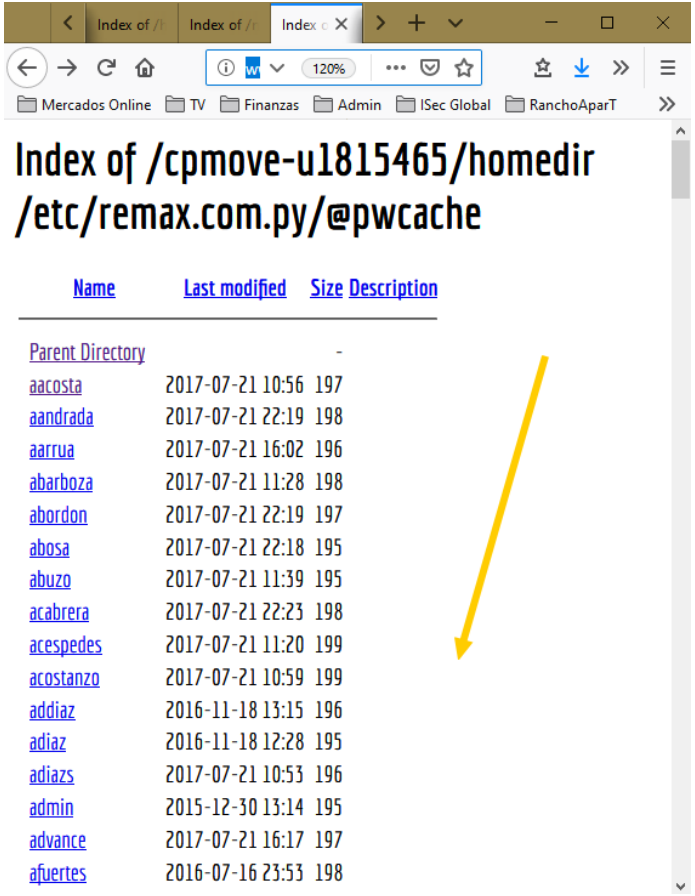
- http://adriananichifor.com/homedir/cache/
- http://tribalistasmotoclube.com.br/homedir/tmp/sendmail
- http://www.remaxparaguay.com.py/cpmove-u1815465/homedir/cache/

¿Qué? ¿Cachea Paswords?

- http://www.remaxparaguay.com.py/cpmove-u1815465/homedir/etc/remax.com.py/@pwcache/auditoria

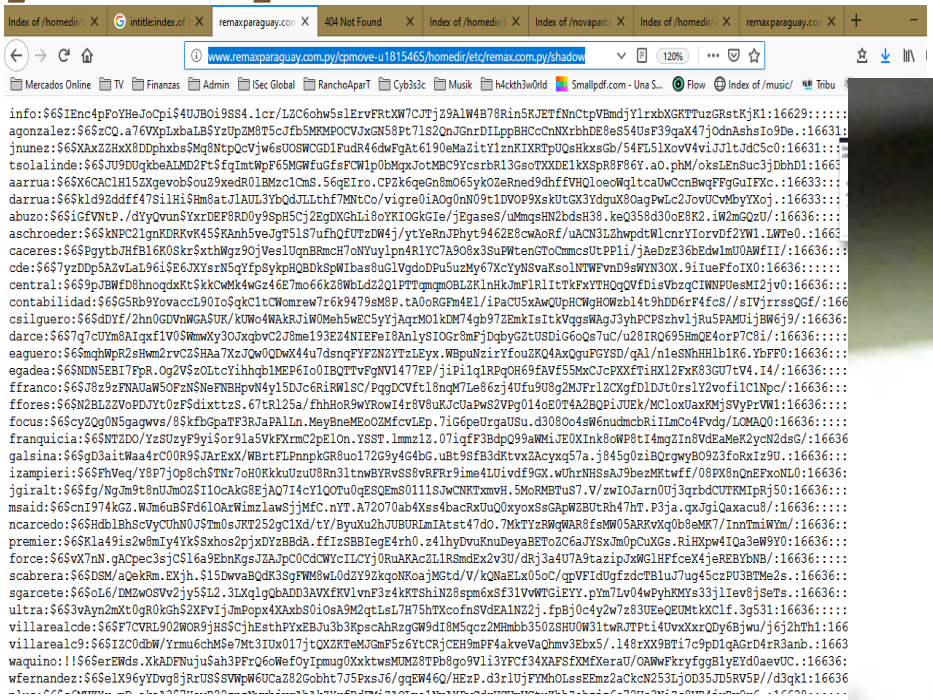


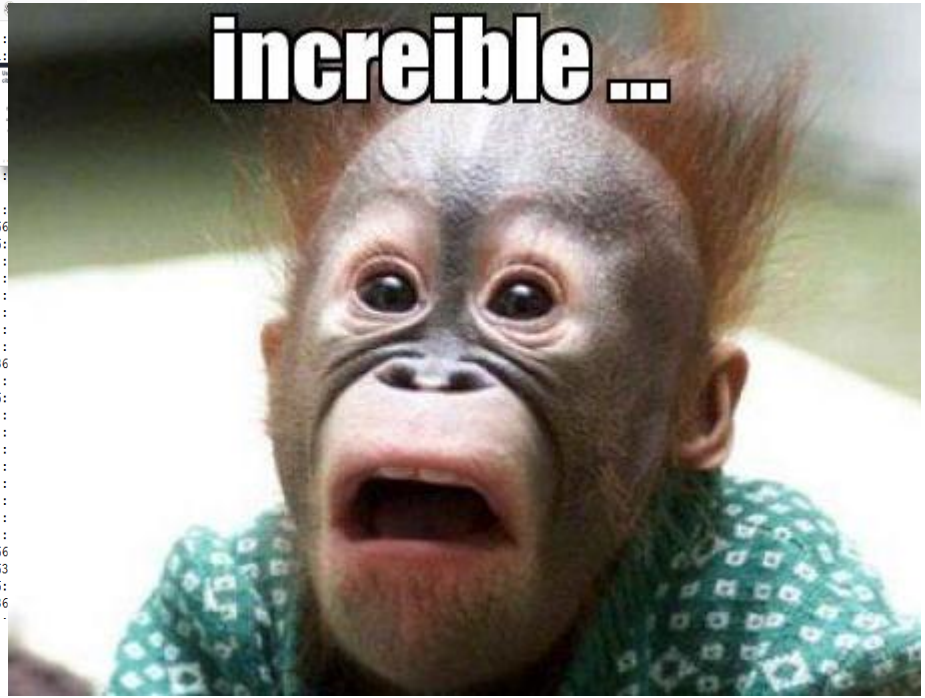
¿Queeeeeeeeeee? ¿Cachea todas las Paswords?



- http://www.remaxparaguay.com.py/cpmove-u1815465/homedir/etc/remax.com.py/@pwcache/

/etc/shadow tambien!



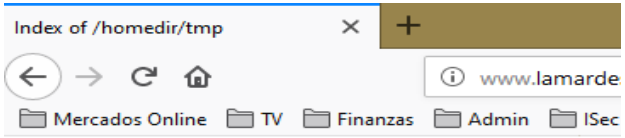


- http://www.remaxparaguay.com.py/cpmove-u1815465/homedir/etc/remax.com.py/shadow

¿Qué más un atacante podrá obtener de la cookie?

toda la codificación y base de datos →

- http://www.lamardesigngroup.com/homedir/tmp/



Index of /homedir/tmp

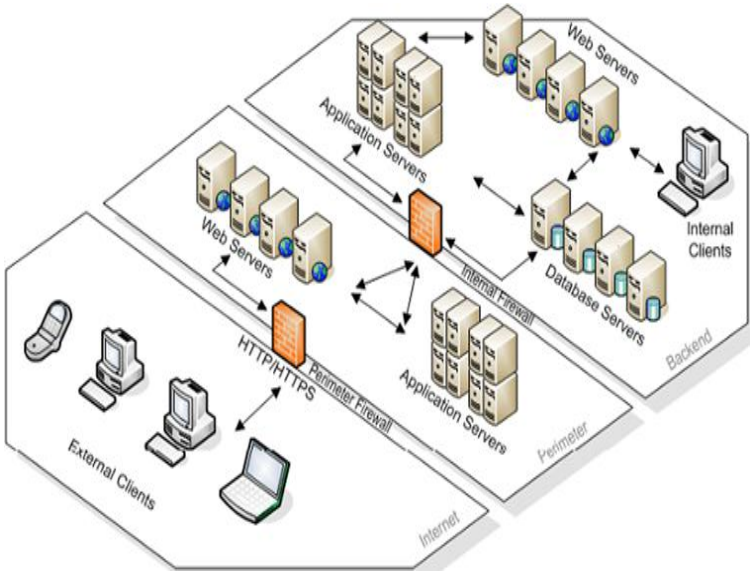
- Parent Directory
- analog/
- awstats/
- cpbandwidth/
- logaholic/
- sess_arlv540k3hgci92a0p5cn9vf1hr9h6r0
- sess_d77tdhulmmer45m65diea0nsrbat05ti
- sess_lgm5ilkdq7ojk75bngcntk0po2ki3efr
- sess_r8qobc1crfsljrob1fo6mm7jjqma6ek1
- webalizer/
- webalizerftp/

WHERE (`fp`.`ProductID` = '420' AND `fp`.`menu_order` = 105) OR (`fp`.`ProductID` = '420' AND `fp`.`menu_order` = 110) OR (`fp`.`ProductID` = '420' AND `fp`.`menu_order` = 133) OR (`fp`.`ProductID` = '420' AND `fp`.`menu_order` = 135) ORDER BY `ProductID` ASC,`menu_order` ASC";}s:32:"468f0df3e98f825236e5c565d07aceaa";a:3:{s:2:"db";s:13:"lamarde_IFPDB";s:5:"table";s:2:"fp";s:8:"sqlquery";s:18:"SELECT * FROM `fp`";}s:32:"2031e2709ca5340d547f0f90835cebc1";a:3:{s:2:"db";s:13:"lamarde_IFPDB";s:5:"table";s:2:"fp";s:8:"sqlquery";s:86:"....

SELECT * FROM `fp_backup` WHERE ProductID='420' or ProductID='425' limit 99";}}Import_message|a:2:{s:7:"message";s:143:" Your SQL query has been executed successfully ";s:11:"go_back_url";s:111:"tbl_sql.php?db=lamarde_IFPDB&table=fp_backup&token=a77e242647ed2172178598598beb8a6c&table=fp_backup";}errors|a:0:{}

algunas soluciones

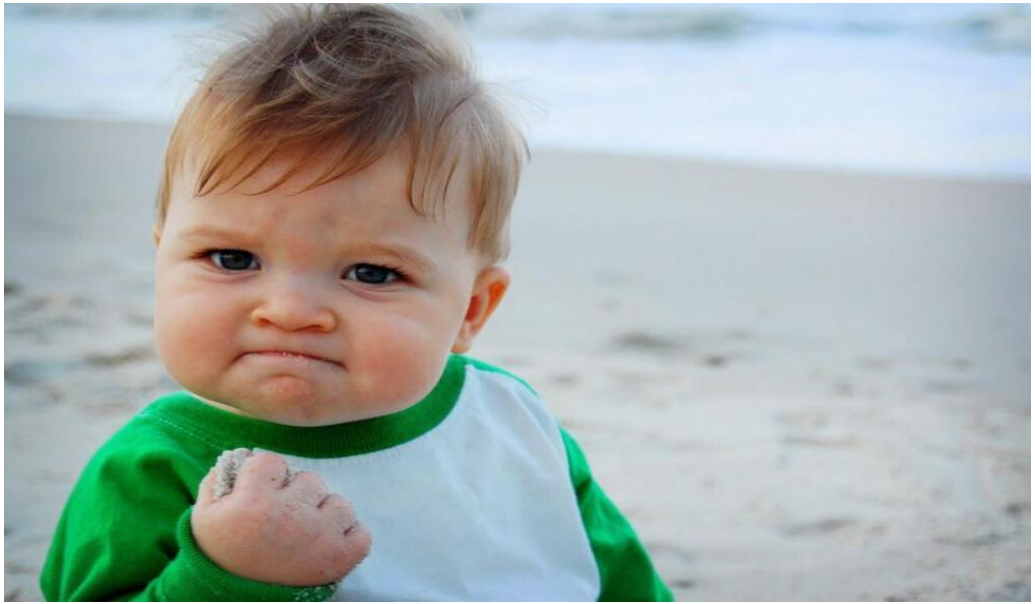
análisis de la arquitectura



análisis de la normativa

RFC, ISO, NIST, OWASP...

1. DESARROLLO
2. **TESTING**
3. PRODUCCIÓN



GDG Neuquén

eof()

r.nico.c.rti@gmail.com

christian.vila@isec-global.com