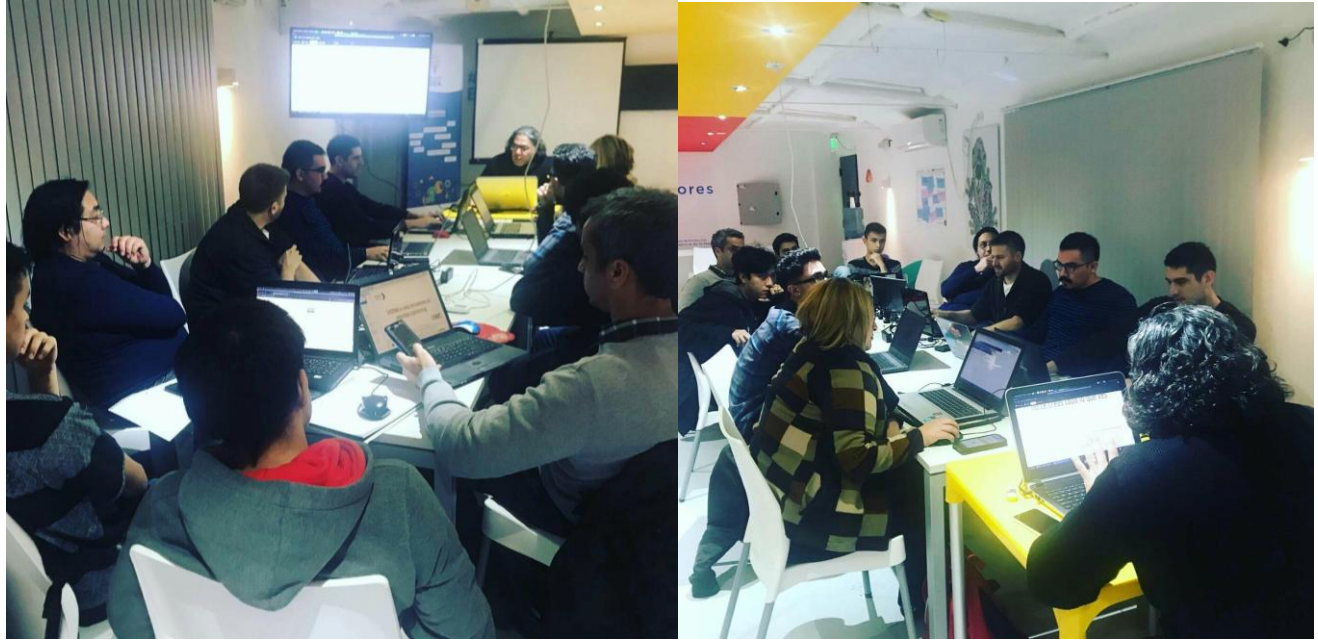


GDG
Neuquén



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:

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...

Motivación?

...entonces, ¿estas seguro en internet?

Sobre labs:

The image shows a browser window with the URL `haveibeenpwned.com`. The page features a dark blue header with a navigation menu: Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main content area has a large white rounded rectangle containing the text `';--have i been pwned?`. Below this is a subtitle: `Check if you have an account that has been compromised in a data breach`. A search input field is present with the placeholder text `email address` and a button labeled `pwned?`. At the bottom, there is a 1Password advertisement: `Generate secure, unique passwords for every account` with a `Learn more at 1Password.com` button. The footer text reads `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/

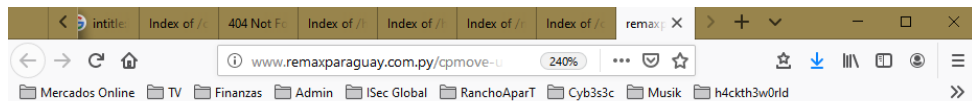
intitle:index.of homedir/tmp/

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 Passwords?

- <http://www.remamaxparaguay.com.py/cpmove-u1815465/homedir/etc/remax.com.py/@pwwcache/auditoria>



```
passwd:$6$GCXtj3XcAYyYaqKD$A5HYSH4czarYo41.LYxb  
y/eGrm.puxfoJNNzt3vbxWZA3R8CXTKJ0uqQfOj7WuKxORL  
395sftULkno6JmanQf1  
quota:524288000  
homedir:/home/u1815465/mail/remax.com.py  
/auditoria  
lastchanged:17333
```



¿Queeeeeeeeeee? ¿Cachea todas las Passwords?

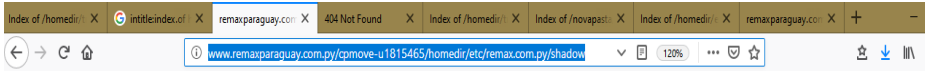


- <http://www.remamaxparaguay.com.py/cpmove-u1815465/homedir/etc/remax.com.py/@pwcache/>

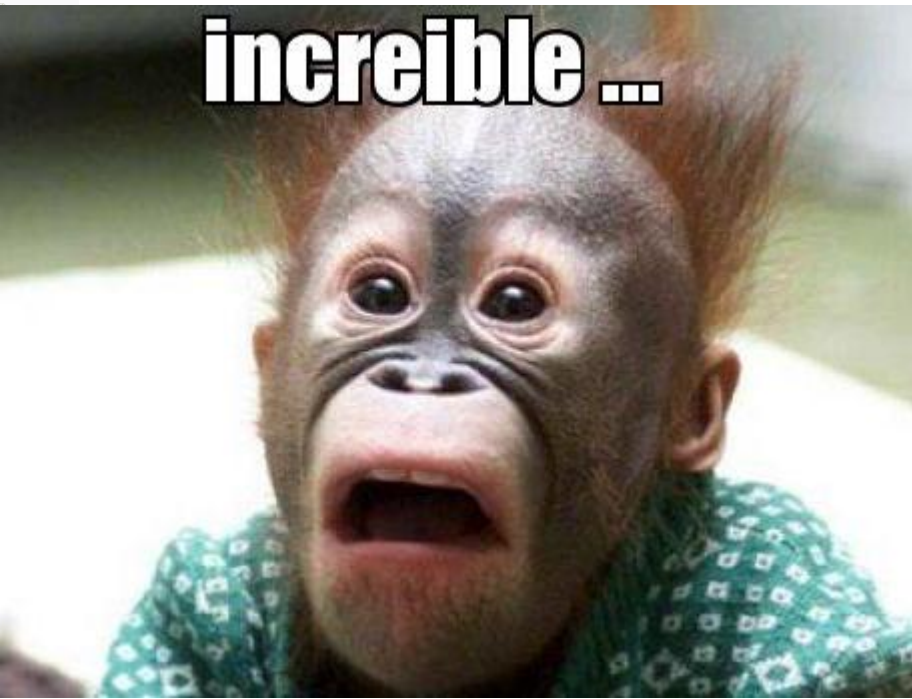
Index of /cpmove-u1815465/homedir/etc/remax.com.py/@pwcache

Name	Last modified	Size	Description
Parent Directory		-	
aacosta	2017-07-21 10:56	197	
aandrada	2017-07-21 22:19	198	
aarrua	2017-07-21 16:02	196	
abarboza	2017-07-21 11:28	198	
abardon	2017-07-21 22:19	197	
abosa	2017-07-21 22:18	195	
abuzo	2017-07-21 11:39	195	
acabrera	2017-07-21 22:23	198	
acespedes	2017-07-21 11:20	199	
acostanzo	2017-07-21 10:59	199	
addiaz	2016-11-18 13:15	196	
adiaz	2016-11-18 12:28	195	
adiasz	2017-07-21 10:53	196	
admin	2015-12-30 13:14	195	
advance	2017-07-21 16:17	197	
afuertes	2016-07-16 23:53	198	

/etc/shadow tambien!



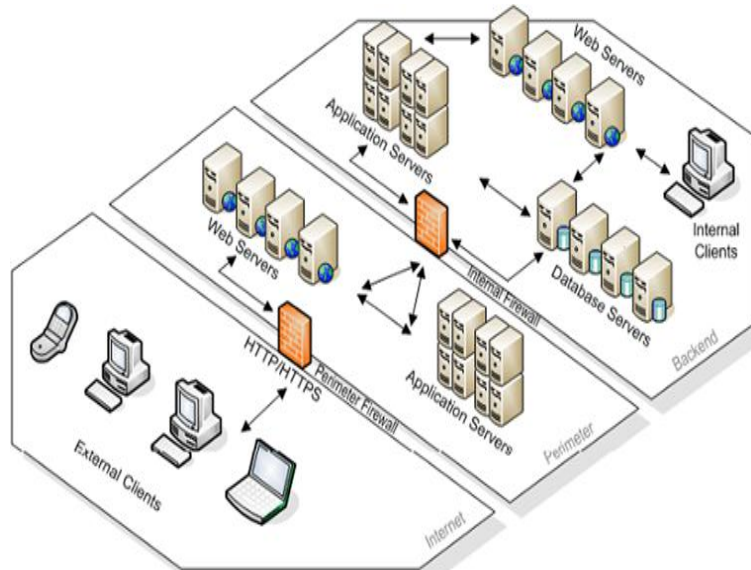
```
info:$6$IEnc4pFoYHeJocPi54UJ0i9S84.1cz/LZC6ohw5e1rVFRtXW7CJTj29AlN4B78Rin5KJETFNncPtVmdjYlrxhXGKTuzGRstKjR1:16629:.....
agonzalez:$6$8cQ.476XWqLxhLaLBSyUp2M8T5o3fB5M8MPCOVJxGN58Pt7182QnJgrNDlPpBHCcCNkRhh8E8s54UsF93qaX47jodnAsheIo9de.:16631:
jmunez:$6$XaZ2Hx28Dhpxh5Mq8NtpcVjw6S0WGGC01PdR46dFgAt6190eMaZitYlznKIXRTPQshKxsCb/54F5L1Xov74vUjL1JdC5c0:16631:
tsolalinde:$6$J9UDUqkbeALMD2Ft5EqmtWpF65MGWfuf8FCW1p0bMgXJotMBC9YcstrbR13GsoTXKDE1KXSp8F86Y.a0.pn/oksLenSsc3jDbbhd1:1665
aarraa:$6$X6CACLIH5ZgevoB5Sou29xedR01EMzCm3s.56gE1ro.CPZk6qen0m065yK0ZeRned9dhfFVHQloeeWglTcaUWcCnBwqFfgGuIFXc.:16633:
darrua:$6$Kld92ddff4781lH18m8aFJLAUL3YbQJLLCh7MNTco/vigro1A0g0nN09tLDVOP9XkUtGX3YdguX80agPwLc2JovUQWMyYXoj.:16633:
abuzo:$6$icfVntP./dyYQvunYxRDEP8RD0y98p5Cj2EgDXGhLi80YKIOGkGeI/yJgasesU/mqmsHN2bdsH38.keQ358d30oE8K2.iWmGozU/:16636:
aschroeder:$6$KNPc2lgnKDRVr455KAnh5veJgT57ufnQfUTzDw4Yj/ytYerJPhyt9462E8cwoRoE/uACN3L2hwpdTlWcnrIorvdF2YW1.LWTe0.:1663
acceres:$6$PgYtYbJHf816R08zr5XthWg290jVes1UqnBmrcH7oNyUlpn4R1YC7A908x3SuPwtenGtoCmcsutP1i/jAeDz836bdwIm00AWFII/:16636:
cde:$6$7yzDp5AZvLaL96iSE6JXyZr5yqfSykHQBDkSpWbas8uGlVgdoPu5uZMy67XcYnNSvaoKlNtWfWd9SvWYN3OX.9iUteFfoIX0:16636:
central:$6$9pJWfD8h0nqdxKt5kkCwMK4Gz467m066k28WbLd22Q1PTTmqm0BL2KlnhJmFlR1ItKfXyTHQqVFDIsVbzqCIWNPoesMI2jv0:16636:
contabilidad:$6$S5R9YovaccL9Io5gKlCtWmowr7rk9479sM8P.ta0oRGPfM4e1/1PaCU5AwOUpHCWgHwzB14tE8DD6r4fFcs//s/vjrrsGqf/:166
csilguero:$6$8dyf/2hx0GDVnWAGASUR/XUw04WAKR19WMeH5WEC5YjAgtrM01kM74gb972EmIsItkVqgsWAgJ3yhPCF82hvljru5PAMU1jBw6j9:16636:
darce:$6$7q7yUM8AIqxv1FV0MmWY30XqxbwC2J8me19324NIEFeI8AnlyIOGRgmjDqyGzTUSDI66Qo57uc/02IR695hmQ4orP708i/:16636:
eguerro:$6$SmhWpR28Hm2rvc2SHha7XaJw00W44UdsngPYE2NZYTzEyx.WBpuNzIrfouZ2KQ4XQgPVGSD/qal/nlaSHHh186.YhPFO:16636:
egadea:$6$MND5EB17FpR.Og2V5z0LctYihhqb1MEP610IB0T7VfVgNV1477EP/jiP1q1Rq0G69fAV55MxcJexPKxfiH1K1F8K3GU7tV4.I4/:16636:
franco:$6$58z9zFNAUaW50FzN5NEFNBpwn4j5DjC6RiRw18C/PqgDCVft18nqM7E8z6j40fu9U8g2MfJr2CXGfDLDTorsIY2vof1CINp0/:16636:
fiores:$6$N2BLZ0V0DUYt0zrF5dixktz8.67rKl25a/fhhR9wRRow14r8V8uKcUaPwS2Vp0140eU7A2BQ6JUeK/MCl0uXaXRMjSVYpZrW1:16636:
focus:$6$cy2Qg0N5gagwvs/8Kf8dSpaTFR30aPa1Ln.Mey8neMe0o2MfcvEP.71G6peUrgaU8u.d3080o4sW6nundmcbR11Im804Fvdg/LOMQ0:16636:
francuicia:$6$N2TD0/7z8Uzyf9y15or1A5vFXKrmc2PE1on.YST.lmm2L.07iqfF3Bdp099aWmiJEOXInk8Wp8T14mgZln80eAmeZ2ndsg/:16636
galsaina:$6$9D3aitWaa4rC00R95JArEXX/WbrTFlPnqKGR8uo172G9y4G4gb.u8t98FB3drtvxZcyxq57a.j845g0zi0rQwYB0923f0RxtZ9U.:16636:
izampieri:$6$8hVeq/y8P7j0p8chTnr70hKkUkuUwU8Rn1tWbYRvS8VFRFr9ime4L0iVdf9GX.wUhrNHSaJ9bez2Mrtwff/08PX8nQNEFxoNL0:16636:
jgiralt:$6$Gf/NgJm9t8nUjm0Z8110cAkc8EjAq714Y1Q0u0gESQeS001118JwCNKTxmVh.5MoRMBTus7./w/zl0JarnOUj3qrbdCTMUFMRj50:16636:
msaid:$6$cnI974Kz2.Wm6ub8Fp610A8rWimzLawsjJmfc.nYt.A72070ab4Xs4bacRkUo0uXyoxSgSgWZBtR4h7T.P3ja.qxJgiQaxcau8/:16636:
ncardeo:$6$Hdb1BhsCvYUcNU0J5Tm0sKJ2T52Q1Xk/ty/ByuXu2HUBURlM1Atst47D.7MkYtZRWQWAR8fsm05ARkVxq0b9eMK7/IntmYmW/:16636:
premier:$6$K1a49is26mYiYK8Sxhos2pJvDz2BbdA.fFz8BB1eagF4rh0.z41hyDvuRknuDeyAbeT0c6aJYskJm0pCuXGs.RHXpW41Qa3eW9Y0:16636:
force:$6$9v7n.n.aQcPe3cjYK16a9EbnKjsZJqJ0c0CWYILCvJ0RuAKacZ1LRSmdeX2v3U/dRj3a4U7A9tazipJwXG1Hfoc4XjE8EBYm2n.:16636:
scabrera:$6$S8m.gAqEkm.EYjh.jS15DwaBQ383GfSMwM0d2Y92kqonKoaJMGct/V/kQNaELX05oc/qpVFIudfzgcTBlUj7uq45czPUB3Tma2e.:16636:
sgarcea:$6$06L/DMZMOSVv2jy5SL2.3lXq1qGbAd283AVXKRVlVf3z4kKtShiN28sp6x5f31vVWTGIEYV.pYmL704wYhRMy8s3j1Iev8j8eT.:16636:
ultra:$6$93vAyN2Mx0Kgr0KghS2XFYjJmPopX4Aax8010sA9M2qtLsL7H75hYXcofnsVdEALN2Zj.fpbj0c4y2w7283UEQeUMtKXCl.3g531:16636:
villarealce:$6$F7CVRL902W0R9jH8ScJhstChFXEB3u36p3pcahRzggw9d18MSqcz2MHmb350ZSHU0W31tWRUPT14UwXxrOdy6BjwU/j6j2hTh:166
villarealce9:$6$Z0d0bW/Ymuc6hM9eCt3IUX017tQXZRTeM0Gmf56tCrjCEH9mPF4kveYaQmw3Ebx5/.148:XX9BT17c9pdlAgRd4r3anb.:1663
waquino:11866erEdgs.XkADFNuJuh3PF9Q6wF0YImug0XkxtwsmMUM28Tpb9go9Vli3YFCF34XAFSFXMEXeraU/OAWMkryfgyBlYeyD0aevOc.:16636:
wferandez:$6$eIX96yYdvG9jRtUS5VNWpW6UCA282GobhtJ5PxsJ6/ggEW4Q0/HzP.d3r1UjFYMh0LssEemZ2Ckcn253J0D35JDR5V5P//d3qk1:16636
```



● <http://www.remamapraguay.com.py/cpmove-u1815465/homedir/etc/remax.com.py/shadow>

algunas soluciones

análisis de la arquitectura



análisis de la normativa

RFC, ISO, NIST, OWASP...

1. DESARROLLO
2. TESTING
3. PRODUCCIÓN



`eof()`

`r.nico.c.rti@gmail.com`

`christian.vila@isec-global.com`