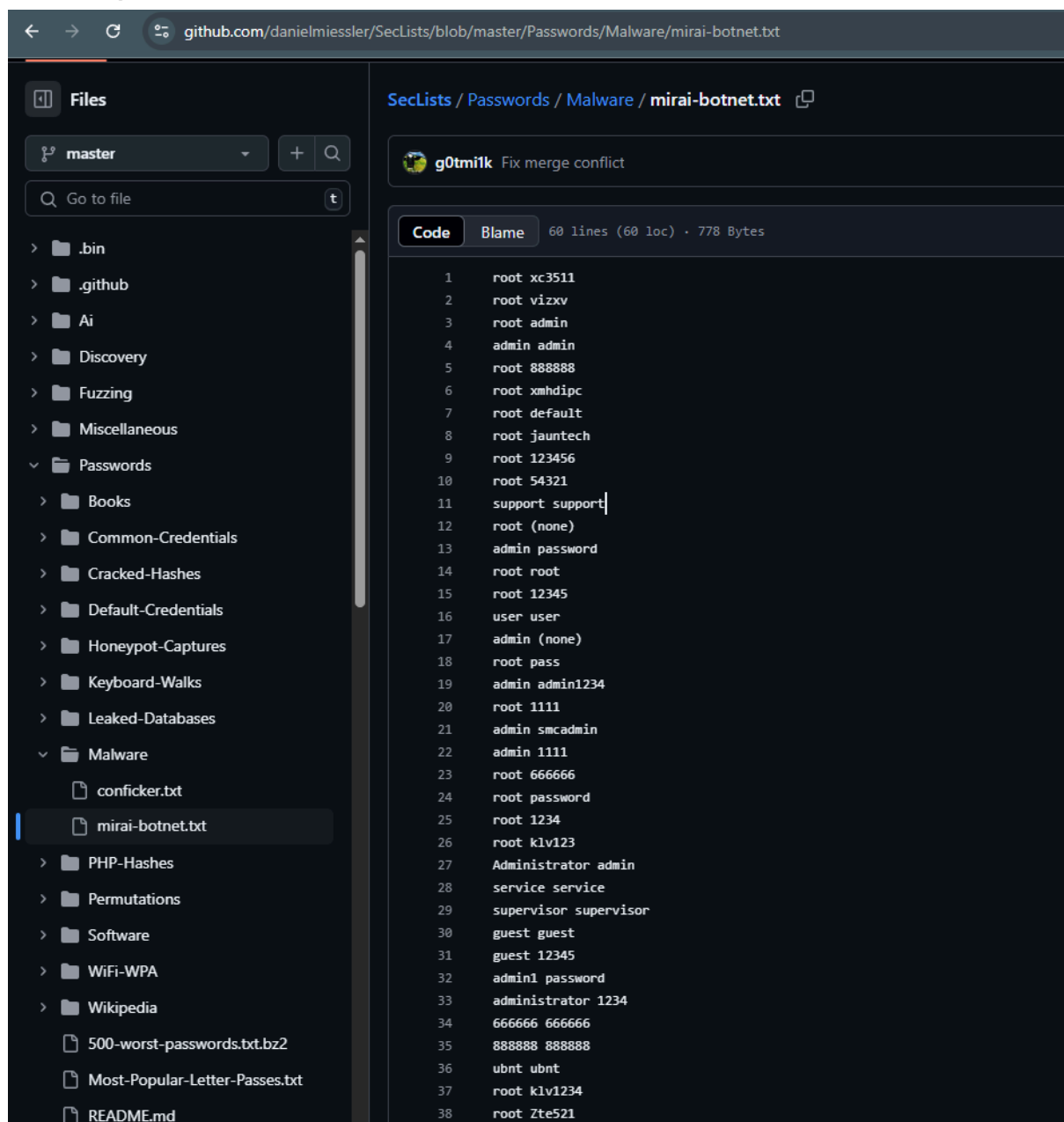


4. Neste exercício iremos estudar o impacto do uso de funções de hash sem salt para o armazenamento de senhas.

a) Considere a lista de usuários e senhas usados pelo código malicioso Mirai para fazer força bruta em dispositivos IoT (<https://github.com/danielmiessler/SecLists/blob/master/Passwords/Malware/mirai-botnet.txt>). Escolha 10 senhas (segunda coluna).



The screenshot shows a GitHub web interface for the repository `danielmiessler/SecLists`. The file `Passwords/Malware/mirai-botnet.txt` is selected in the left sidebar. The main content area displays the file's contents, which is a list of 38 lines of usernames and passwords separated by a space. The interface includes a file explorer on the left, a breadcrumb trail at the top, and a commit message from `g0tmilk` at the top right.

Line	Username	Password
1	root	xc3511
2	root	vizxv
3	root	admin
4	admin	admin
5	root	888888
6	root	xmhdipc
7	root	default
8	root	jauntech
9	root	123456
10	root	54321
11	support	support
12	root	(none)
13	admin	password
14	root	root
15	root	12345
16	user	user
17	admin	(none)
18	root	pass
19	admin	admin1234
20	root	1111
21	admin	smcadmin
22	admin	1111
23	root	666666
24	root	password
25	root	1234
26	root	klv123
27	Administrator	admin
28	service	service
29	supervisor	supervisor
30	guest	guest
31	guest	12345
32	admin1	password
33	administrator	1234
34	666666	666666
35	888888	888888
36	ubnt	ubnt
37	root	klv1234
38	root	Zte521

pass

54321

tech

1234

guest

xmhdipc

meinsm

hi3518

support

Zte521

b) Use o OpenSSL ou qualquer ferramenta online para calcular o MD5 e o SHA-1 de cada uma das senhas. Dicas: use <https://www.md5hashgenerator.com> ou o seguinte comando: "echo -n "SENHA" | openssl dgst -md5". Verifique se o valor de hash gerado pelo OpenSSL realmente é o valor correto.

Your String	pass
MD5 Hash	1a1dc91c907325c69271ddf0c944bc72
SHA1 Hash	9d4e1e23bd5b727046a9e3b4b7db57bd8d6ee684

Your String	54321
MD5 Hash	c42af6b8160c554530855b8fec5ad50
SHA1 Hash	0c3fd7f50369b5fdd7aac22f5f6ed03e713560b7

Your String	tech
MD5 Hash	d9f9133fb120cd6096870bc2b496805b
SHA1 Hash	c95ee47689a0aaec70c3eb950244657722c69b1f

Your String	1234
MD5 Hash	81dc9bdb52d04dc20036dbd8313ed055
SHA1 Hash	7110eda4d09e062aa5e4a390b0a572ac0d2c0220

Your String	guest
--------------------	-------

MD5 Hash	084e0343a0486ff05530df6c705c8bb4
SHA1 Hash	35675e68f4b5af7b995d9205ad0fc43842f16450
Your String	xmhdipc
MD5 Hash	726927827f6c51a8995b49185ca8bc8e
SHA1 Hash	068767b389590dbb57dd3c5b7bc66971afcdf17d
Your String	meinsm
MD5 Hash	f985a3b18830f3566cdd29c242b53561
SHA1 Hash	ce7987ef8225cc1a2699a07901f59de7f09bdfed
Your String	hi3518
MD5 Hash	bdfde4de898d679633fd1cf16af79242

SHA1 Hash	180a4def3cfd00b29905c73a437ced125211f233
------------------	--

Your String	support
--------------------	---------

MD5 Hash	434990c8a25d2be94863561ae98bd682
-----------------	----------------------------------

SHA1 Hash	5bdcd3c0d4d24ae3e71b3b452a024c6324c7e4bb
------------------	--

Your String	Zte521
--------------------	--------

MD5 Hash	0ec3772a8336ecddd6b6c61f01c05244
-----------------	----------------------------------


SHA1 Hash	8df2ae0668218b74822da6e7de4d18b678230bd6
------------------	--

c) Faça buscas no Google usando como parâmetro o valor de hash obtido. A busca retorna resultados? Se sim, discuta os resultados.

Google


1a1dc91c907325c69271ddf0c944bc72

Todas Shopping Imagens Vídeos Notícias Maps Vídeos curtos Mais Ferramentas

 MD5 Center
<https://md5.gromweb.com> › md5... › Traduzir esta página


MD5 reverse for 1a1dc91c907325c69271ddf0c944bc72

The MD5 hash **1a1dc91c907325c69271ddf0c944bc72** was successfully reversed into the string pass. Feel free to provide some other MD5 hashes you would like to try ...

 Md5Calc.com
<https://md5calc.com> › hash › pass › Traduzir esta página


1a1dc91c907325c69271ddf0c94...

MD5 hash for "pass" is "1a1dc91c907325c69271ddf0c944bc72". Free online md5 hash calculator. Calculate md5 hash from string.

 MD5Hashing
<https://md5hashing.net> › ... › Blame website's content


1a1dc91c907325c69271ddf0c94...

2 de nov. de 2015 — MD5 (128 bit). The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically ...

 HackerDna
<https://hackerdna.com> › tools › 1a... › Traduzir esta página


Tools / MD5 Reverse: pass

The HackerDNA Toolbox. Quickly hash or reverse your text with MD5. The clear text value of **1a1dc91c907325c69271ddf0c944bc72** is pass.

 Dovecot docs
<https://doc.dovecot.org> › passwo... › Traduzir esta página

Password databases (passdb) — Dovecot documentation


{PLAIN}plaintext-password or {PLAIN-MD5}**1a1dc91c907325c69271ddf0c944bc72**. Dovecot authenticates users against password databases. It can also be used to ...

 GitHub
<https://github.com> › blob › frien... › Traduzir esta página

Google

c42af6b8160c554530855b8fec5ad50

Todas Shopping Imagens Vídeos Notícias Maps Vídeos curtos Mais Ferramentas


 Pastebin
<https://pastebin.com> › ... › Traduzir esta página

cc3a0280e4fc14159308998965...

29 de out. de 2017 — **Pastebin.com** is the number one paste tool since 2002. Pastebin is a website where you can store text online for a set period of time.


Google

Todas Shopping Imagens Vídeos Notícias Maps Vídeos curtos Mais

 **HackerDna**
<https://hackerdna.com> › tools › d... Traduzir esta página


Tools / MD5 Reverse: tech

Easy to Use: Simply input your string, and the tool will **instantly reverse or generate the hash**.
 Versatile: Use it for CTF resolutions, data integrity checks, ...

 **GitHub**
<https://github.com> › GLPI › blob Traduzir esta página

GLPI/install/mysql/glpi-0.85.5-empty.sql at master


GLPI de AGRO RURAL. Contribute to agrorural/GLPI development by creating an account on GitHub.

 **GLPI Project**
<https://forum.glpi-project.org> › vi... Traduzir esta página

[solved] Security hole? / English support / Forum GLPI-Project


24 de mar. de 2011 — Anyone can access to <http://yourhost/glpi/files/> without authentication. This folder is totally open. The problem is that all log files, dumps, ...

Elimination des users GLPI TECH NORMAL et POST-ONLY 10 de out. de 2011
 ne r'arrive plus a me connecter a glpi / Utilisation GLPI ... 2 de ago. de 2018
 Mais resultados de forum.glpi-project.org

 **GitHub**
<https://github.com> › blob › john.... Traduzir esta página

keybrute/keylists/john.lst.keys at master

A wordlist-based encryption key brute force targeting weak key choice/derivation -
 keybrute/keylists/john.lst.keys at master · unicornsasfuel/keybrute.

 **perturb.org**
<https://www.perturb.org> › content Traduzir esta página


Cryptographic hashes for tech - Perturb.org

Hashes for "tech" ; base64: dGVjaA== ; md4: 46413bdc3563753241b19e429b3ff77b ; md5:
d9f9133fb120cd6096870bc2b496805b ; sha1: ...

Google

Todas Imagens Vídeos Shopping Notícias Maps Vídeos curtos Ferramentas Mais

Dica: Limitar esta pesquisa aos resultados em **português (Brasil)**. Saiba mais sobre como filtrar por idioma

 **SHA-1 Center**
<https://sha1.gromweb.com> › hash... Traduzir esta página

What is a SHA-1 hash? - GromWeb

The SHA-1 hash **7110eda4d09e062aa5e4a390b0a572ac0d2c0220** was successfully reversed into the string 1234.

Ao buscar os valores de hash no Google, vários deles apareceram com resultados, e em muitos casos dava até pra ver a senha original em sites de

consulta de hash. Isso mostra como usar só MD5 ou SHA-1, sem nenhum tipo de proteção como um salt, deixa as senhas bem vulneráveis. Mesmo sem ver a senha direto, qualquer pessoa consegue usar esses bancos de dados públicos pra descobrir o que tá por trás do hash. Por isso é importante usar algoritmos mais seguros como bcrypt ou Argon2, que já incluem mecanismos melhores para proteger a senha.

Mas não adianta só colocar salt, a senha também precisa ser forte. Isso quer dizer que ela tem que ter letras maiúsculas e minúsculas, números, símbolos e um tamanho mínimo. Senha simples tipo “1234” ou “admin” não adianta nada. E o salt também precisa ser bem feito, se for um número sequencial ou algo previsível, perde totalmente o sentido de proteção. Então o ideal é sempre combinar uma senha forte com um bom algoritmo e um salt aleatório e único pra cada usuário.

d) Tente melhorar/filtrar os resultados obtidos usando como exemplo diretivas/dorks

(<https://www.avg.com/pt/signal/google-dorks>) de busca do Google presentes na Google Hacking Database

(<https://www.exploit-db.com/google-hacking-database>). Por exemplo, uma diretiva interessante seria buscar por hashes somente em arquivos .txt. Uma outra diretiva seria buscar por hashes em um determinado domínio e assim por diante. Use a sua criatividade aqui!

Exemplo de busca por hashes MD5 em arquivos .txt

filetype:txt intext:"1a1dc91c907325c69271ddf0c944bc72"

Todas Shopping Imagens Vídeos Notícias Maps Vídeos curtos : Mais



Dovecot docs

https://doc.dovecot.org/_sources · Traduzir esta página

virtual_users.rst.txt

... **1a1dc91c907325c69271ddf0c944bc72** . UNIX UIDs ----- The most important thing you need to understand is that ****Dovecot doesn't access the users' mails as ...**



GitHub

<https://github.com/blob/master> · Traduzir esta página

passwdMd5.txt - vieyang/md5F2F

... **1A1DC91C907325C69271DDF0C944BC72** 0196F6C4F97DF3F48D570C23E46501AE
8A88344A8786439FEF8C7BDD49E69E31 413C8E4AC31A519DDBF6F0EC8048848A ...



GitHub

<https://github.com/blob/master> · Traduzir esta página

php-malware-analysis/webshells/wso_in_depth/passwords ...

... **1a1dc91c907325c69271ddf0c944bc72** pass 6f238b53828dd00ada713972805cf1a3 pass0elpasso
43ae7930b90b7e345aad5267cc2f94a9 pass=nhzgrf ...



University of Notre Dame

<https://www3.nd.edu/static/h...> · Traduzir esta página

hashes.txt

... **1a1dc91c907325c69271ddf0c944bc72** 99c8ef576f385bc322564d5694df6fc2
327401d00875b45314447b206550b2b7 c0cdd82ce092b01267bdd88a8bfb1f4 ...



Packet Storm

<http://www2.packetstormsecurity.org> · Traduzir esta página

jobberbase20subscribe-sql.txt

You can use this script to verify if YOUR OWN instance is vulnerable. \$ bash verify.sh
<http://localhost/jobberbase/> admin:**1a1dc91c907325c69271ddf0c944bc72** ...



perlwatch.net


<https://perlwatch.net/VirtualUsers> · Traduzir esta página

<https://perlwatch.net/docs/cheatdocs/dovecot/wiki/>

Buscar por hashes em pastas expostas


intitle:"index of" "md5"

Todas Imagens Vídeos Shopping Vídeos curtos Notícias Web : Mais Ferramentas ▾

 kpe.io
http://files.kpe.io › md5 · Traduzir esta página ⋮


Index of /md5

Index of /**md5** ; [], **md5**-1.8.5.tar.gz, 2004-12-04 18:31, 8.8K.

 Centro Universitário CESMAC
https://cesmac.edu.br › common · Traduzir esta página ⋮


Index of /common/js/plugins/md5

Index of /common/js/plugins/**md5**. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -, [], **md5**.min.js, 2023-08-18 14:48, 3.8K.

 dlib C++ Library
http://dlib.net › dlib › md5 · Traduzir esta página ⋮


Index of /dlib/md5

Index of /dlib/**md5**. Name Last modified Size Description · Parent Directory - md5_kernel_1.cpp.html 2022-05-08 07:30 81K md5_kernel_1.h.html 2022-05-08 07:30 ...

 Prefeitura Municipal de São Luís - MA
https://www.semus.saoluis.ma.gov.br › ... · Traduzir esta página ⋮


Index of /inversor/node_modules/md5.js

Index of /inversor/node_modules/**md5**.js. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -, [], LICENSE, 1985-10-26 05:15, 1.1K.

 Literacy Empowerment Foundation
https://www.lefbbooks.org › content · Traduzir esta página ⋮

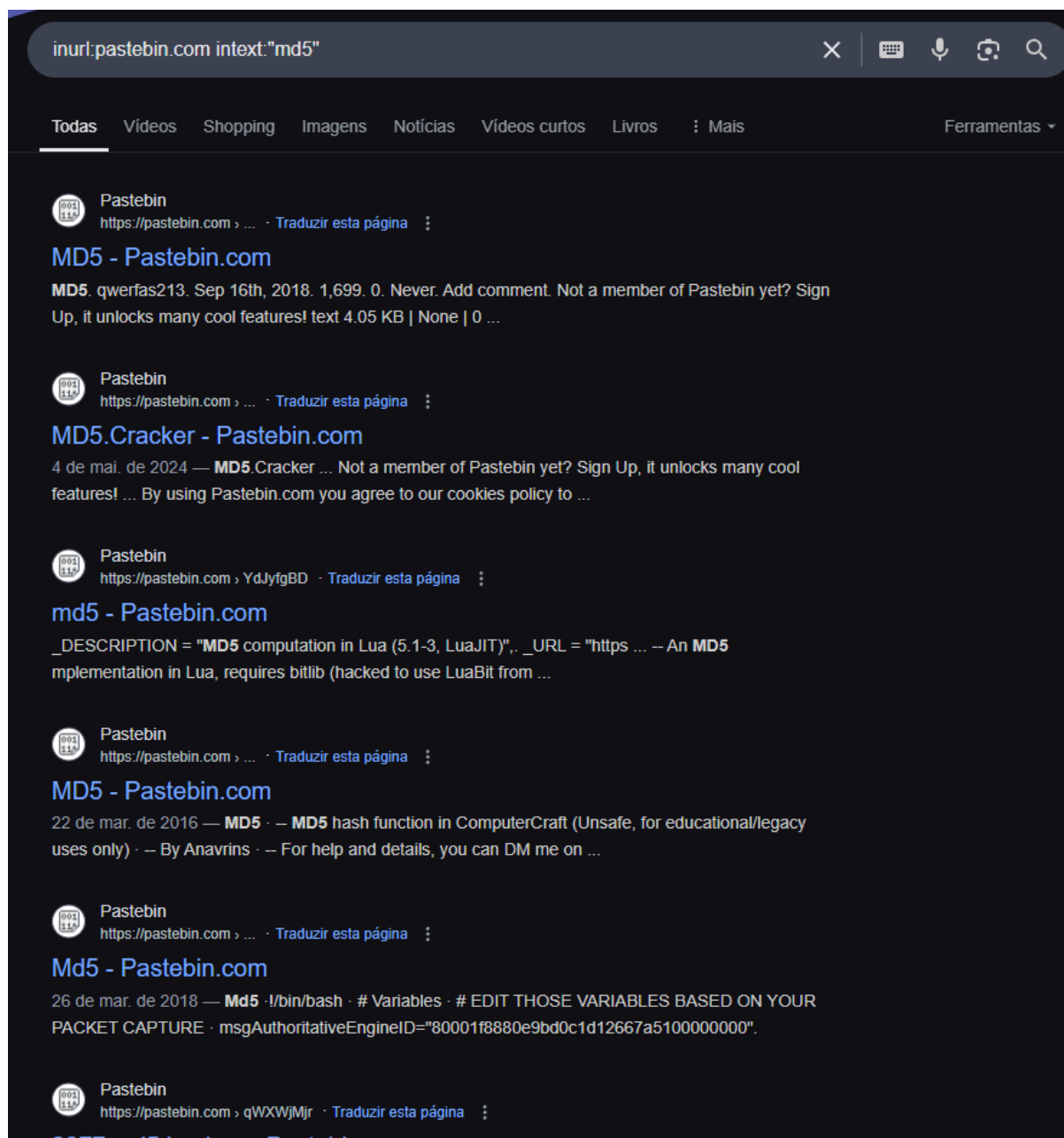
Index of /content/vendors/md5

Index of /content/vendors/**md5**. Name · Last modified · Size · Description · Parent Directory, -, **md5**-min.js, 2019-02-28 11:03, 5.2K. **md5**.js, 2019-02-28 11:03 ...

 wware.org
http://libs.wware.org › md5 · Traduzir esta página ⋮

Index of /md5/ - WWARE

Procurar por senhas em sites que listam dumps



Dork de busca por listas de credenciais em CSV

filetype:csv intext:password

Lookout
https://www.lookout.com › Uploads › csv › App_IOCs
[here](#)
... **password**,311e4c2b1d4b90664c56d8caa0d32035dde68cc6 All
Passwords,com.mobilesoft.security.**password**,8716359ca3b4b7ed707e94b280e6e1e4c106035a All...

New Zealand Information Security Manual
https://nzism.gcsb.govt.nz › csv › Section
<https://nzism.gcsb.govt.nz/ism-document/csv/Section...>
01., "Confidential, Top Secret, Secret", Must, 1868, "Agencies MUST: ensure that passwords are changed at least every 90 days; prevent system users from changing ...

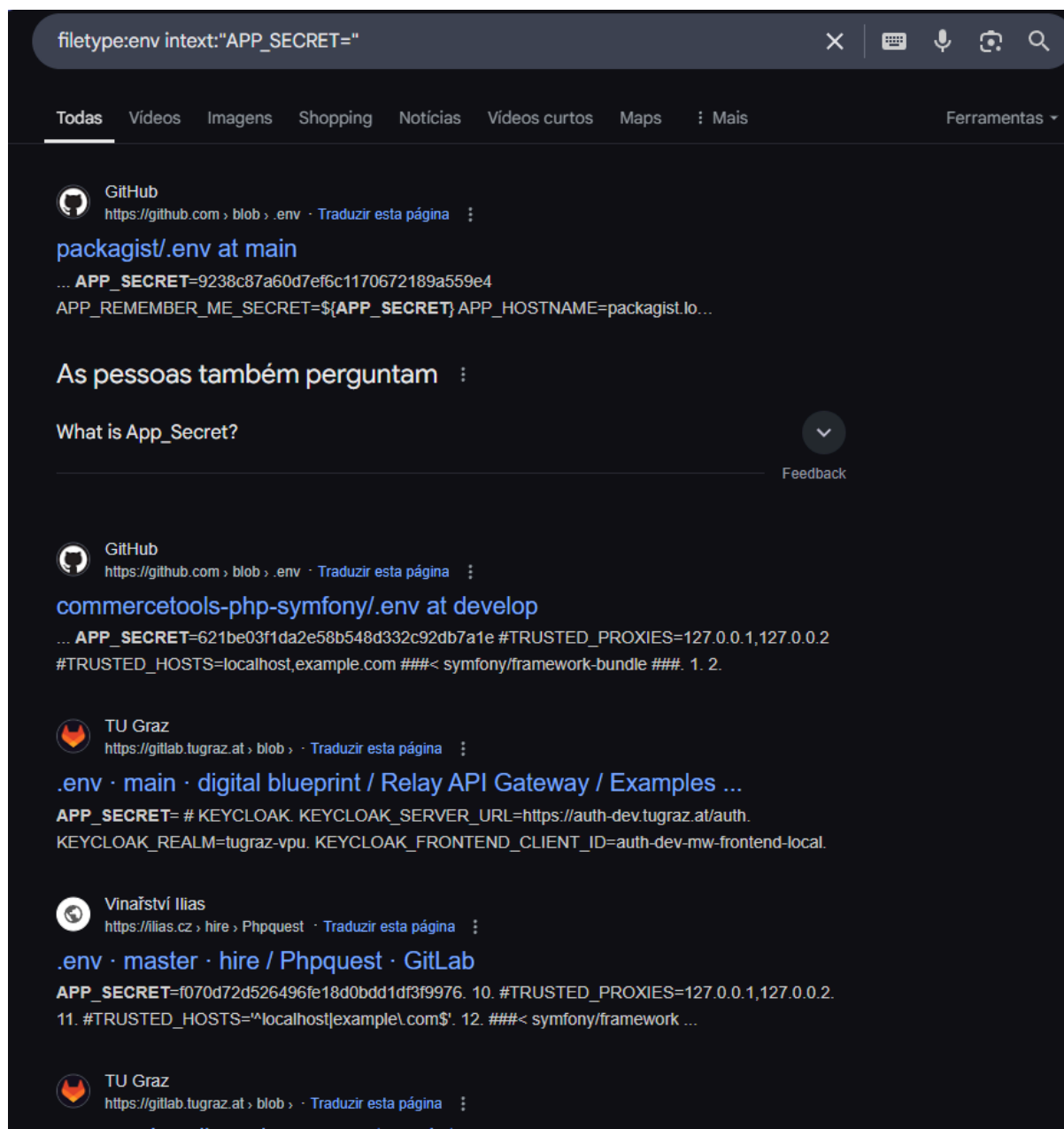
Wear.t.mx
https://wear.t.mx › frontend › Magento › luma › es_MX
[en_US.csv](#)
Leading and trailing spaces will be ignored." "Minimum of different classes of characters in **password** is %1. Classes of characters: Lower Case, Upper Case, ...

WordPress Trac
https://core.trac.wordpress.org › ticket
<https://core.trac.wordpress.org/ticket/9710?format=csv>
... **Password**"" nag, Basically, When someone logs in with a auto-generated **password** (Fresh install, Or **password** reset) they're greeted with a message asking ...

Enpass
https://dl.enpass.io › docs › CSV_Templates_Logins
[Login](#)
"Title","Username","Email","**Password**","Website","TOTP Secret Key","Custom Field 1","Custom Field 2","Note","Tags" "Twitter","SSmithpaul","s.smithpaul ...

NetApp
https://docs.netapp.com › us-en › install-fc › media › M...
<https://docs.netapp.com/us-en/ontap-metrocluster/i...>
... **password**,,,,, , Management ports,,,,, ,Name,Port,IP address,Network mask,Default gateway Node 1,,,,, Node 2,,,,, Node 3,,,,, Node 4,,,,, , LIFs and ...

Buscar por arquivos de config com senhas expostas



Usando dorks do Google, é possível refinar bastante as buscas por informações sensíveis como senhas e hashes. Por exemplo, conseguimos procurar diretamente por arquivos .txt ou .csv contendo hashes MD5 ou SHA-1, ou até restringir a busca para sites específicos. Isso mostra como dados mal protegidos podem ser facilmente localizados por qualquer pessoa com acesso à internet, sem nem precisar de ferramentas avançadas. Por isso, além de proteger as senhas com algoritmos seguros e salt, é essencial evitar expor arquivos sensíveis publicamente na web.