Errori informatici da non commettere nel mondo lavorativo!

Andrea Draghetti

UNIVERSITÀ
DEGLI STUDI
DI PALERMO

$ whoami

Phishing Analysis and Contrast @ D3Lab

Team Member @ BackBox Linux

$ Europa e Informatica

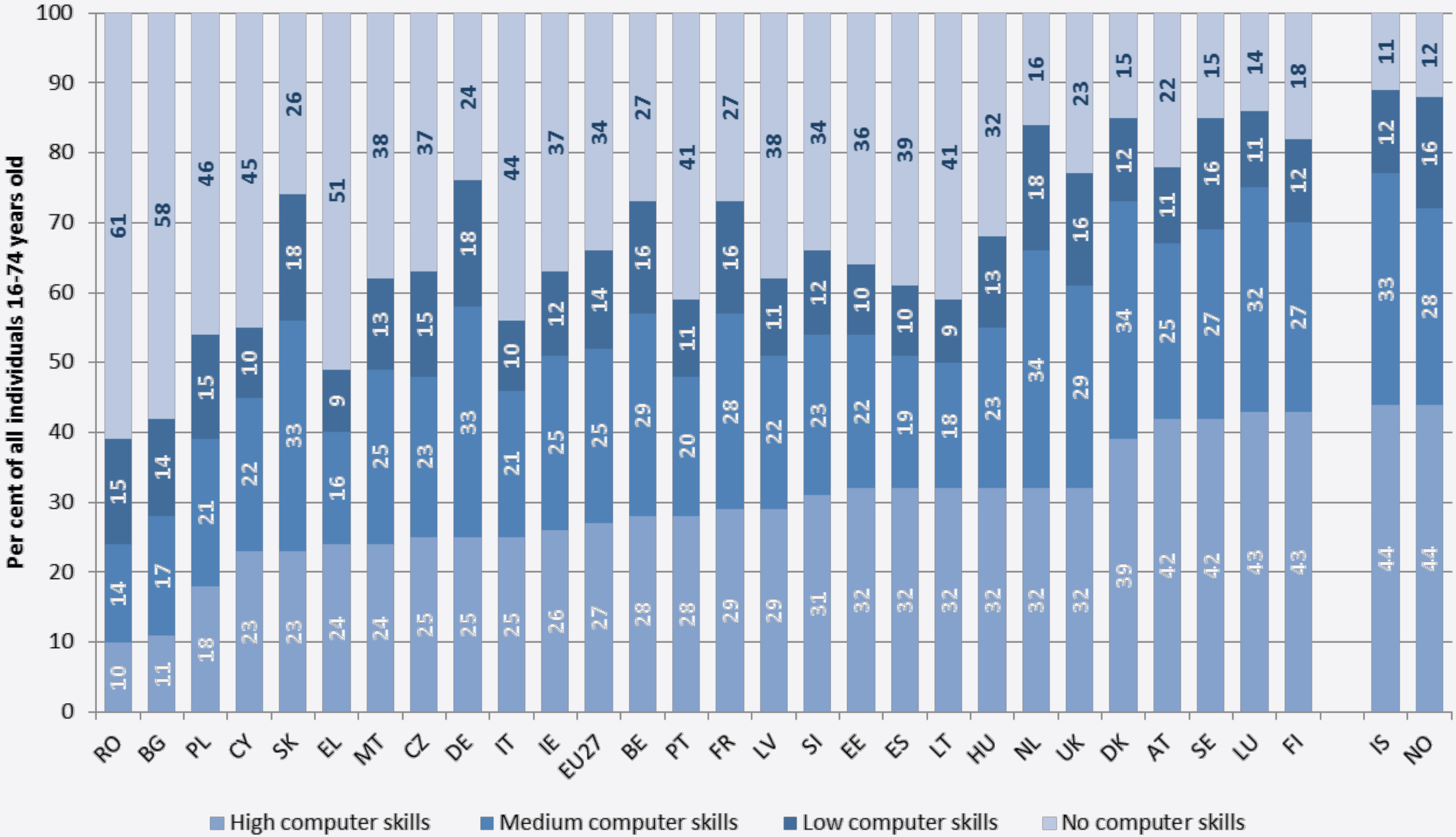
Popolazione Europea: 743 milioni

Occupanti Settore IT: 6,7 milioni

ossia il 3,1% del totale UE

Fonte: Eurostat

$ Europa e Informatica



Fonte: Eurostat

$ Cronaca

UniCredit nel mirino degli hacker, conti correnti e password al sicuro

26 Luglio 2017 126

Instagram Suffers Data Breach! Hacker Stole Contact Info of High-Profile Users

Wednesday, August 30, 2017 Swati Khandelwal

Instagram has recently suffered a possibly serious data breach with hackers gaining access to the phone numbers and email addresses for many "high-profile" users.

fin24tech

HOME NEWS COMPANIES MOBILE GADGETS OPINION CYBER SECURITY

TECH

Massive data leak could be from a credit bureau

2017-10-18 14:50 - Angelique Serrao

POST A COMMENT 0

SHARE:

Johannesburg - The sensitive private information of 30 million South Africans, contained in a massive data breach, appears to have been hacked from a credit bureau.

This is according to Australian Microsoft regional director, Tory Hunt, who exposed the leak on Twitter on Tuesday.

- READ: **Millions of South Africans' personal information may have been leaked online**

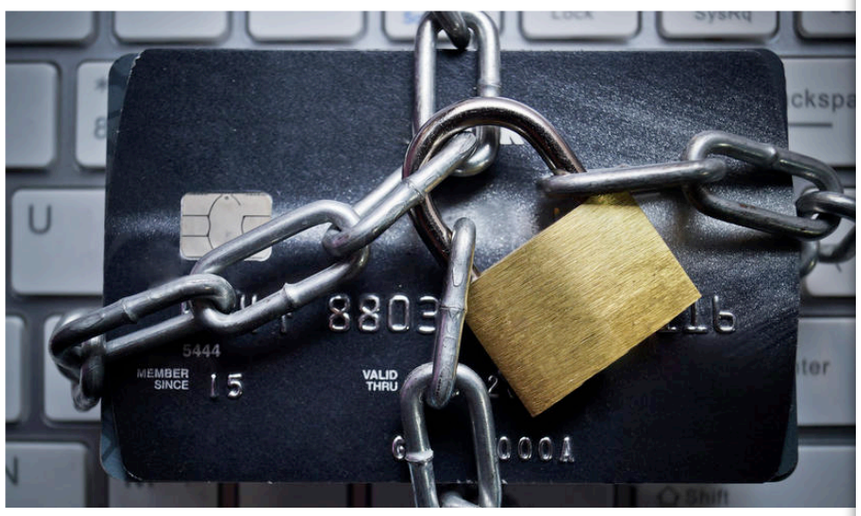
Hunt is also a security researcher and creator of the website Havelbeenpwned.com. The website allows people to check if their personal information has been compromised.

Earlier this year the site exposed the hacking of Ster-Kinekor's website, which put more than six million accounts at risk, Business Day reported.

Hunt said on Twitter on Wednesday that the data

On Finance: What you need to know about Equifax hack

By Steve Burgess, For the News Tribune on Oct 22, 2017 at 8:00 p.m.



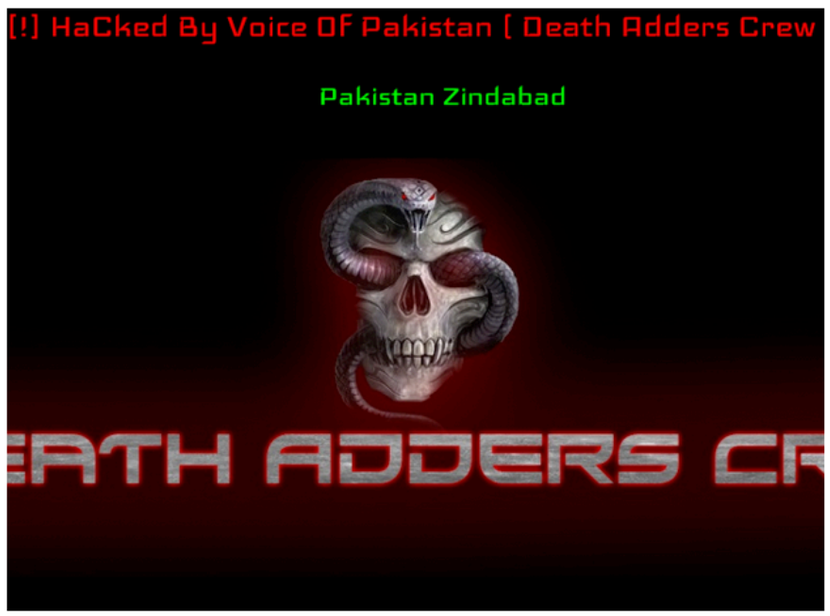
Thinkstock.com

The Equifax data breach has been making headlines since it was first announced on Sept. 7, and with good reason. The breach may have exposed personal information — including Social Security numbers, driver's license numbers and addresses — of 143 million Americans, making it one of the largest and most serious cybersecurity breaches in history. Read on for answers to some commonly asked consumer questions.

PTI website defaced by hackers

By News Desk Published: August 2, 2017

83 SHARES SHARE TWEET EMAIL



$ Aggiornamenti

Dopo 16 anni il 9,17% degli utenti usa Windows XP.

È il terzo OS più usato al mondo!

$ Aggiornamenti: cosa potevamo evitare...

$ Password: Hash ≠ Cifratura

$ Password: Hash ≠ Cifratura

Salve, mi consigliate x un sistema di login/autenticazione i classico MD5 oppure SHA512?

Ci sono poi caratteristiche particolari che non posso mettere nell'annuncio ma che prevedono API e scambio di dati con client con crittografia MD5.

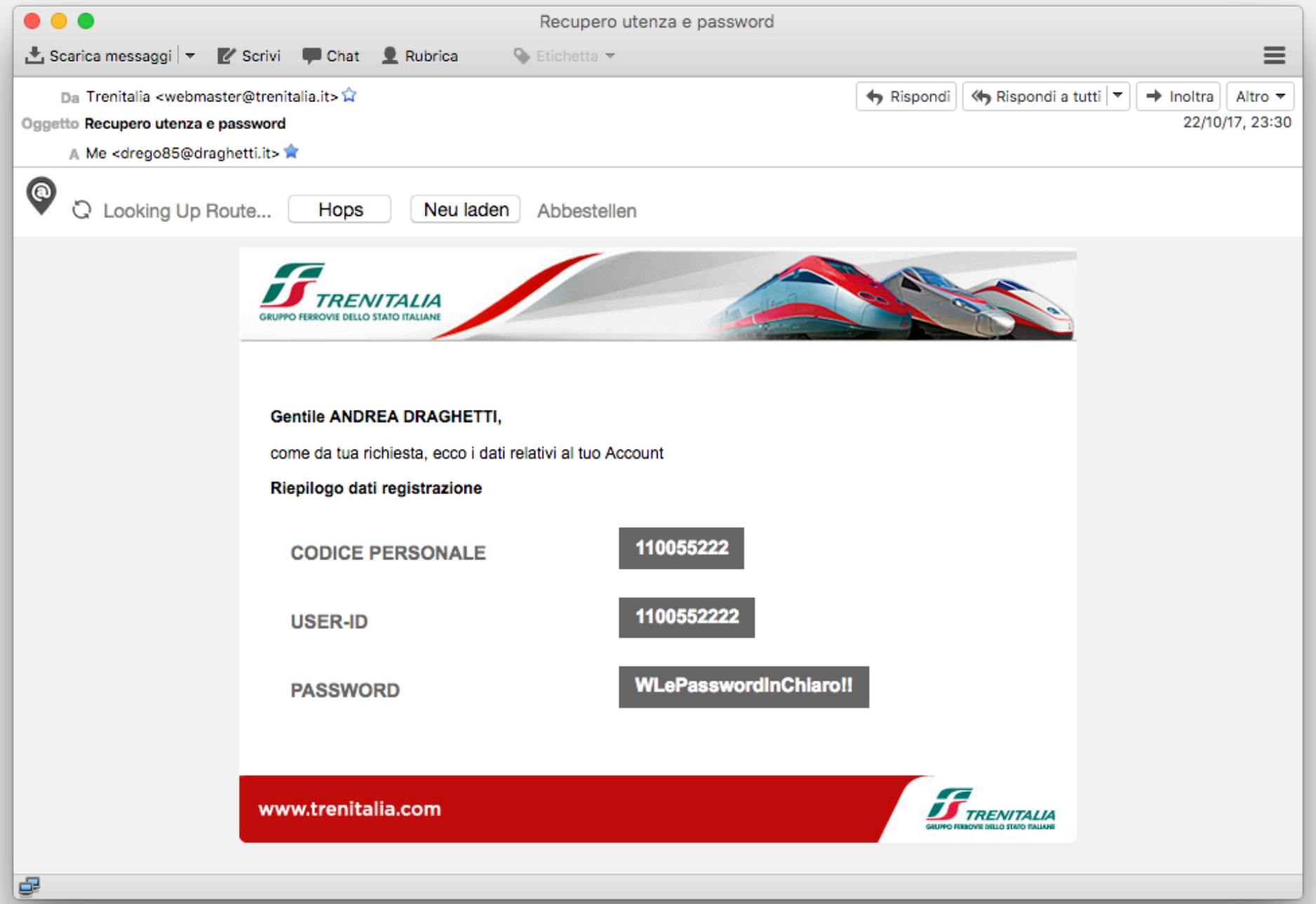
Oltre alla classica pwd in chiaro, la semplice criptazione MD5 che può generare due stesse identiche stringhe e anche la MD5 + salt. Voi che sistema utilizzate?

$ Password: Hash ≠ Cifratura

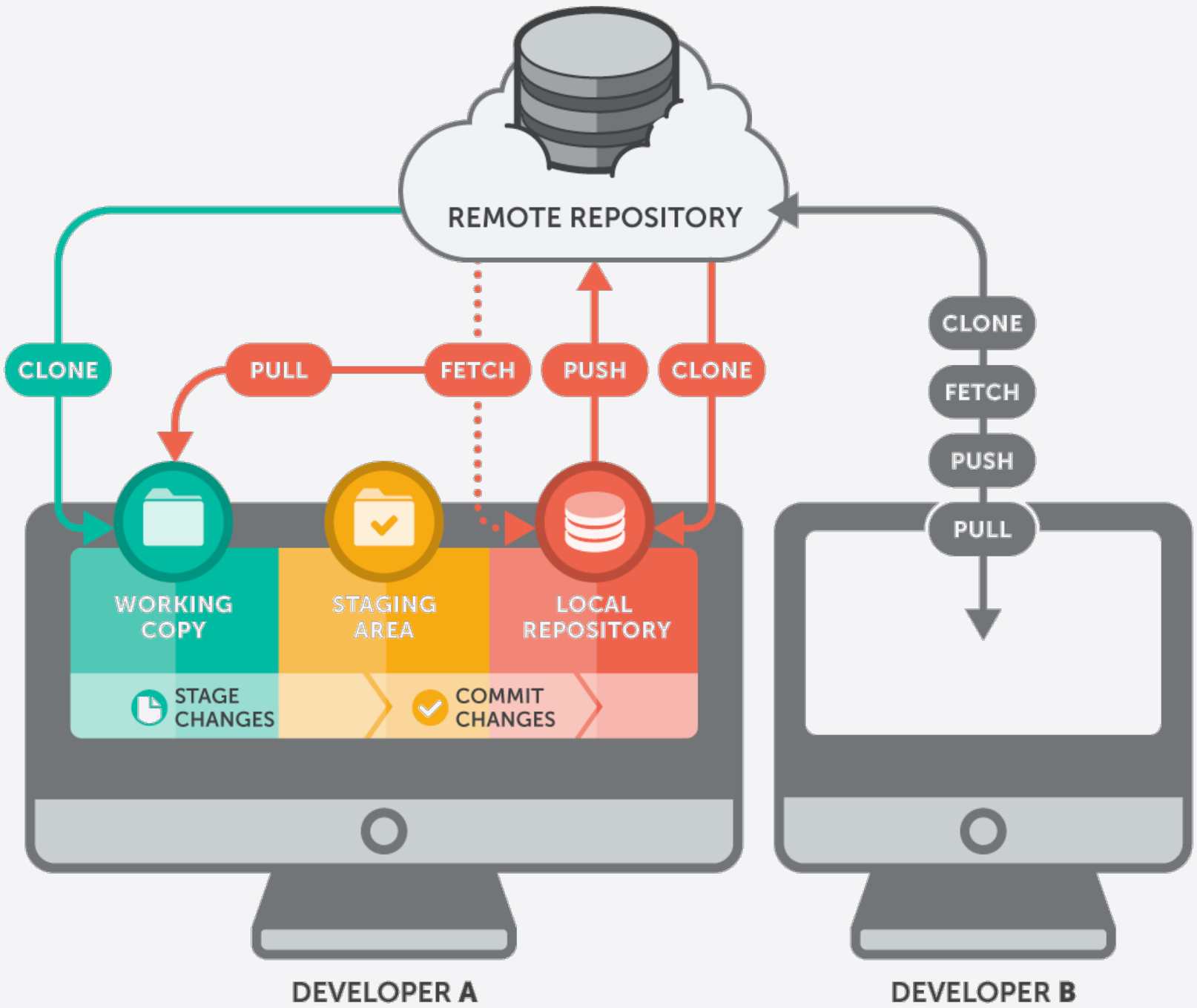
hashkiller.co.uk

- 829.726 billion unique decrypted MD5
- 312.072 billion unique decrypted SHA1

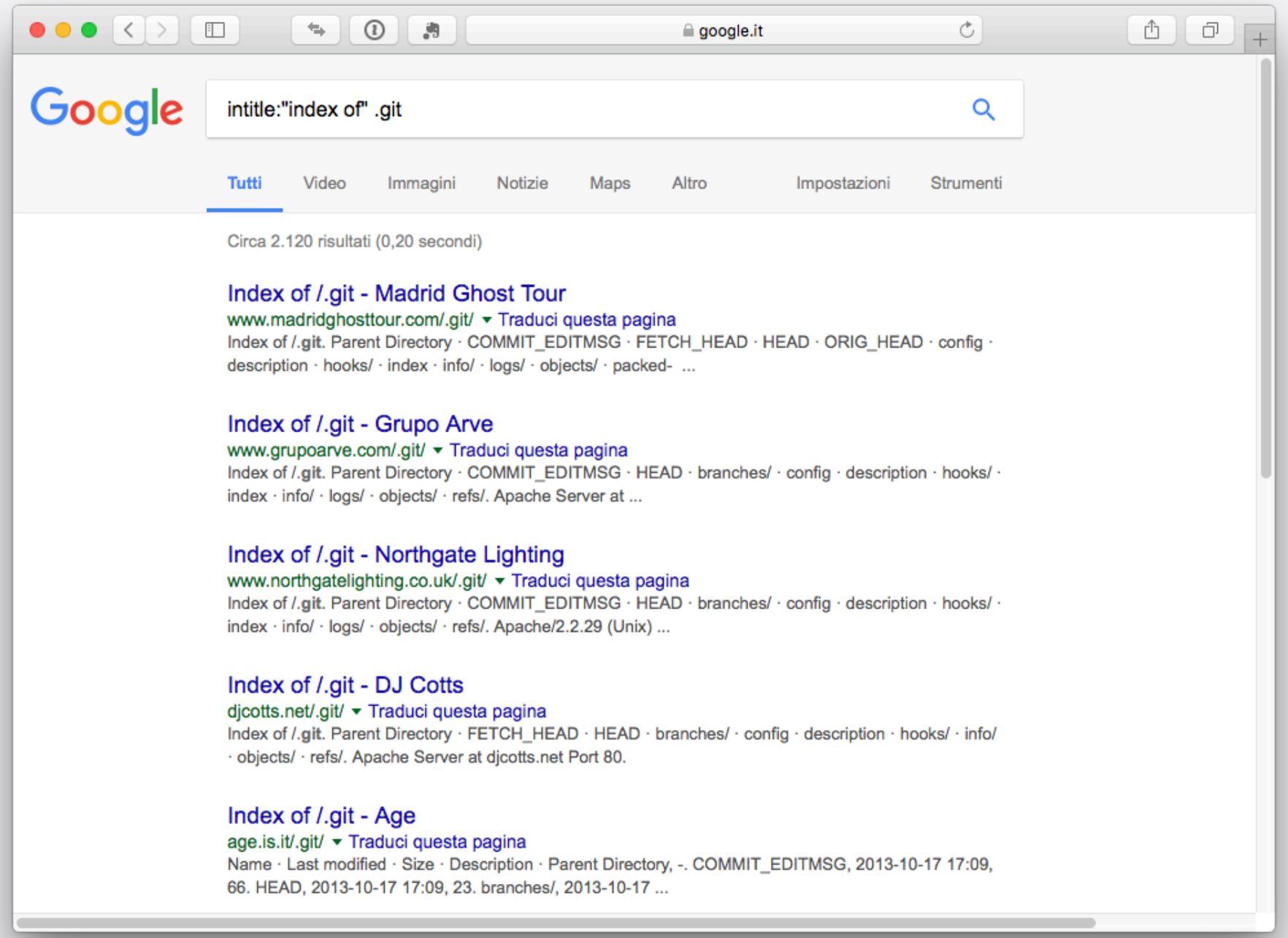
$ Password: in chiaro🤦



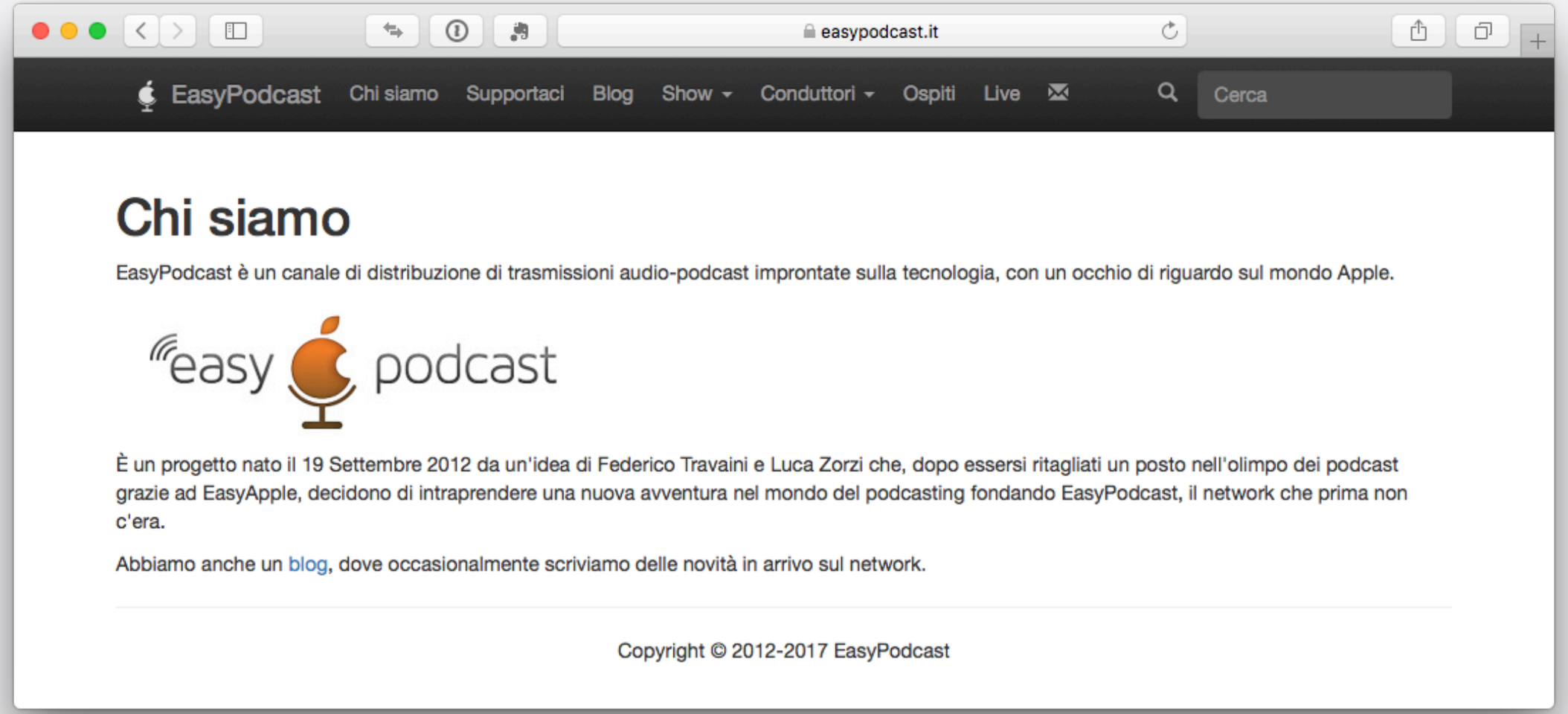
$ Git: Distributed Version Control System



$ Git: Distributed Version Control System



$ Git: Distributed Version Control System



EasyApple #297

$ Git: Distributed Version Control System

ksericpro/certis-api – constants.py — Python

Showing the top nine matches Last indexed on 20 Sep

```
1  SMTP_HOST = "smtp.gmail.com"
2  SMTP_PORT = 587
3  SMTP_USERNAME = "wheytvroot@gmail.com"
4  SMTP_PASSWORD = "wheytv54321"
```

ogstation/hongid – smtp.conf

Showing the top 14 matches Last indexed on 17 Sep 2016

```
1  # 邮件配置
2  [smtp]
3  smtp.server=smtp.gmail.com
4  smtp.port=25
5  smtp.username=mint.zhao.chiu@gmail.com
6  smtp.password=Zhaoming123
7  smtp.host=smtp.gmail.com
```

smoothpanda1981/HQ – mail.properties — INI

Showing the top nine matches Last indexed on 21 Sep 2016

```
1  smtp.host=smtp.gmail.com
2  smtp.port=587
3  smtp.username=daigouswitzerland@gmail.com
4  smtp.password=ouafah1979
```

$ Git: Distributed Version Control System

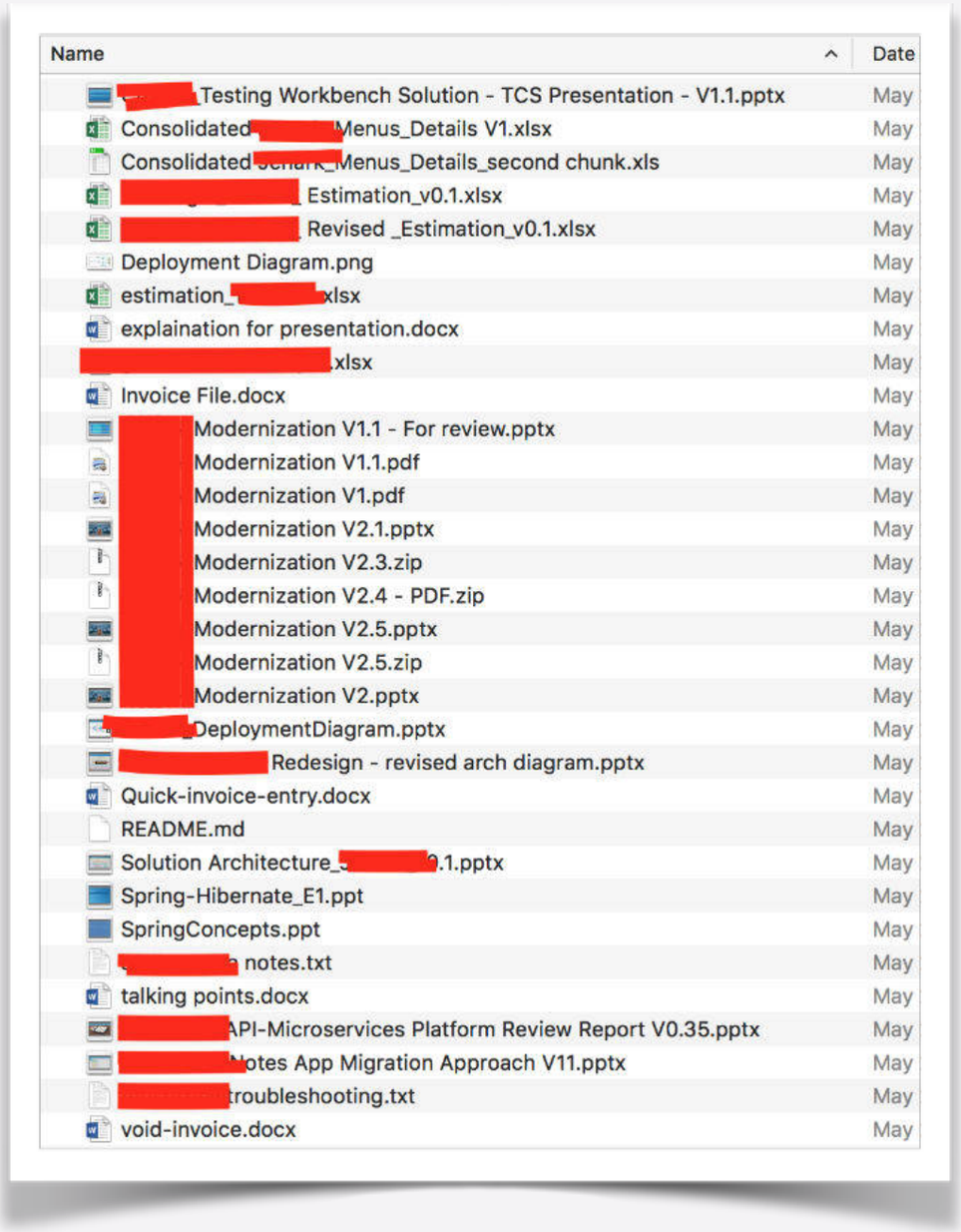
$ Git: Distributed Version Control System

53 lines (40 sloc) | 1.51 KB — Raw | Blame | History

```
#rdps for flux
//asundhar
10.26.131.101
User Name : USDEV\asundhar
Password : Portal1!

//mrazak
10.26.216.61
USDEV\morazak
Password : P@ssword239


//vpn credentails for deloitte
https://aexternal.deloittenet.deloitte.com/my.policy#
sipatra
Pa$$word79(
P@ssword239

//flux database info
10.25.112.22; Database=Flux; User Id=Flux_User; Password=1@/D20Y6m4;


#test server web site flux
https://ddisclosureanalytics.deloitte.com/flux/uploadtb
usdev\leeldridge
Portal1!
```

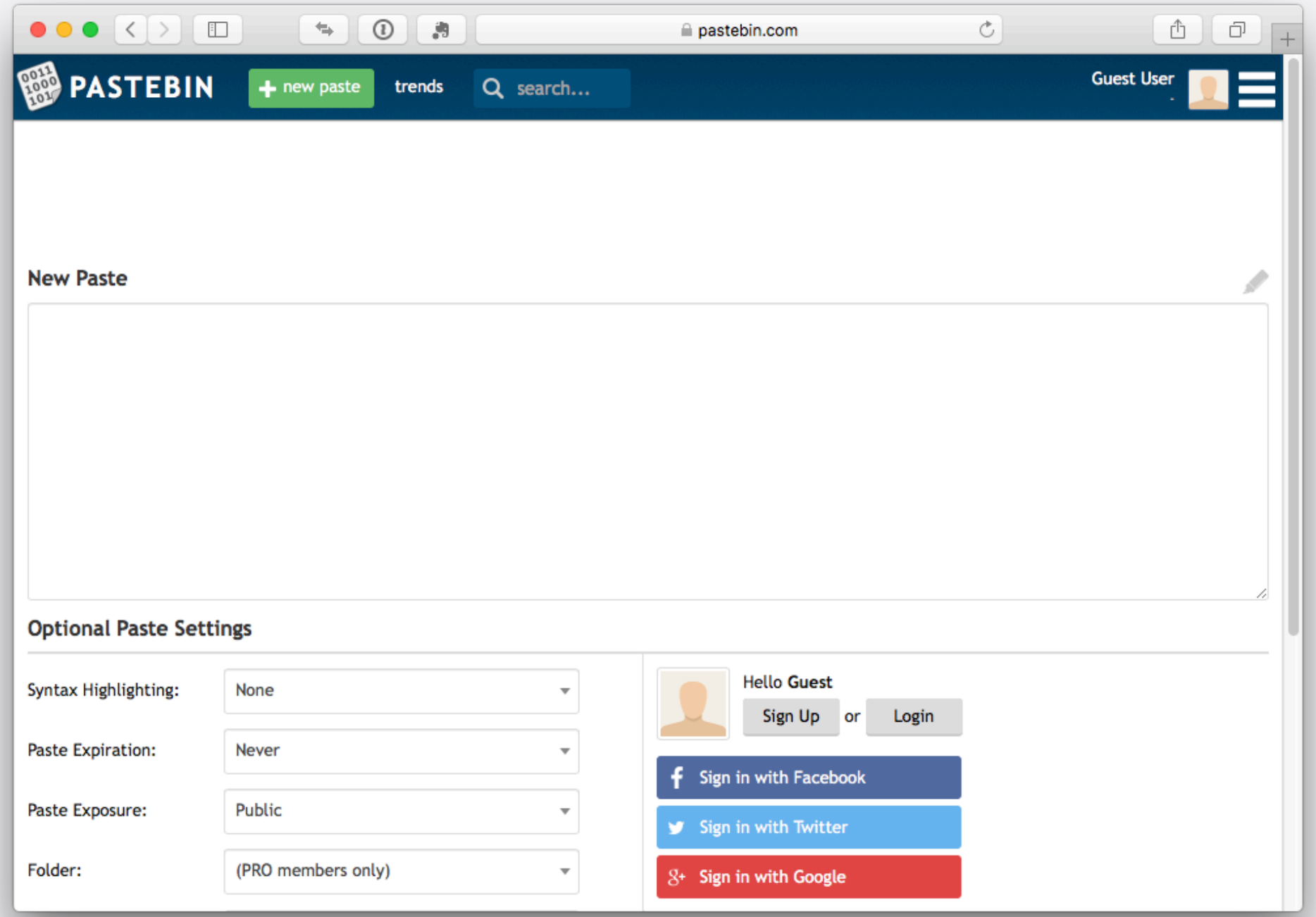
https://archive.fo/flmFv

$ Git: Distributed Version Control System

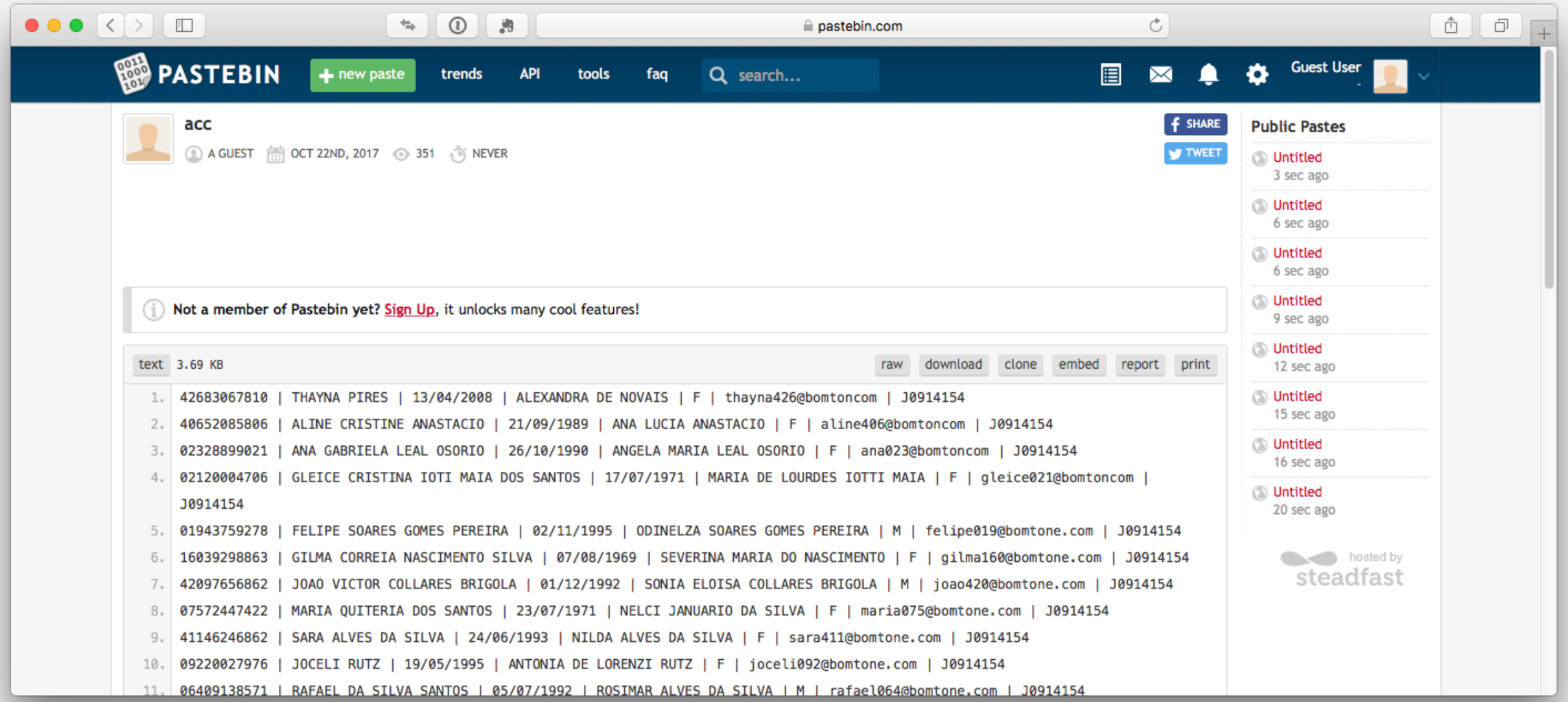


https://www.theregister.co.uk/2017/06/12/tata_bank_code_github/

$ Pastebin

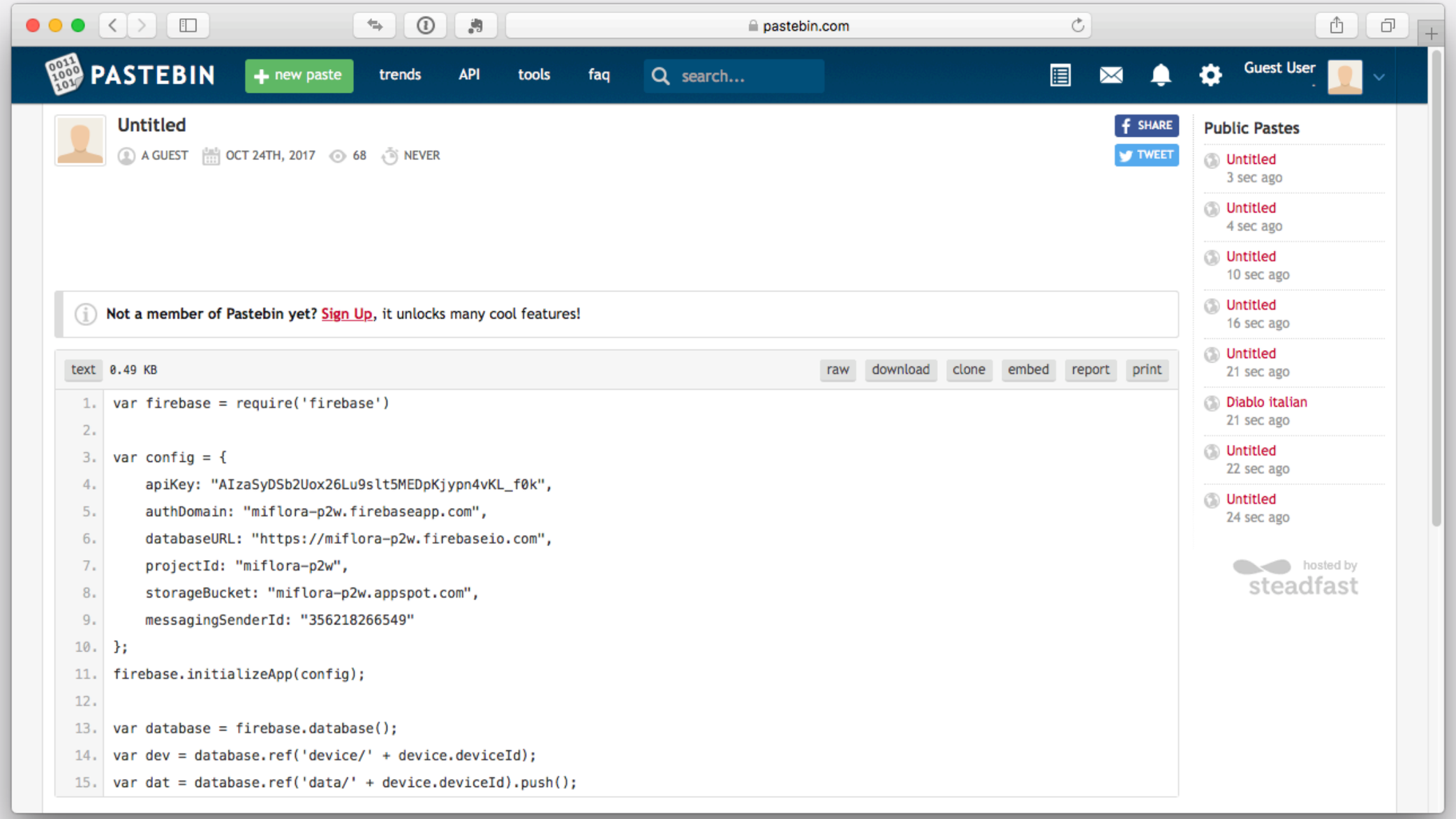

pastebin.com
PASTEBIN
+ new paste
trends
search...
Guest User
New Paste
Optional Paste Settings
Syntax Highlighting:
None
Paste Expiration:
Never
Paste Exposure:
Public
Folder:
(PRO members only)
Hello Guest
Sign Up
or
Login
Sign in with Facebook
Sign in with Twitter
Sign in with Google

$ Pastebin: Dati Sensibili



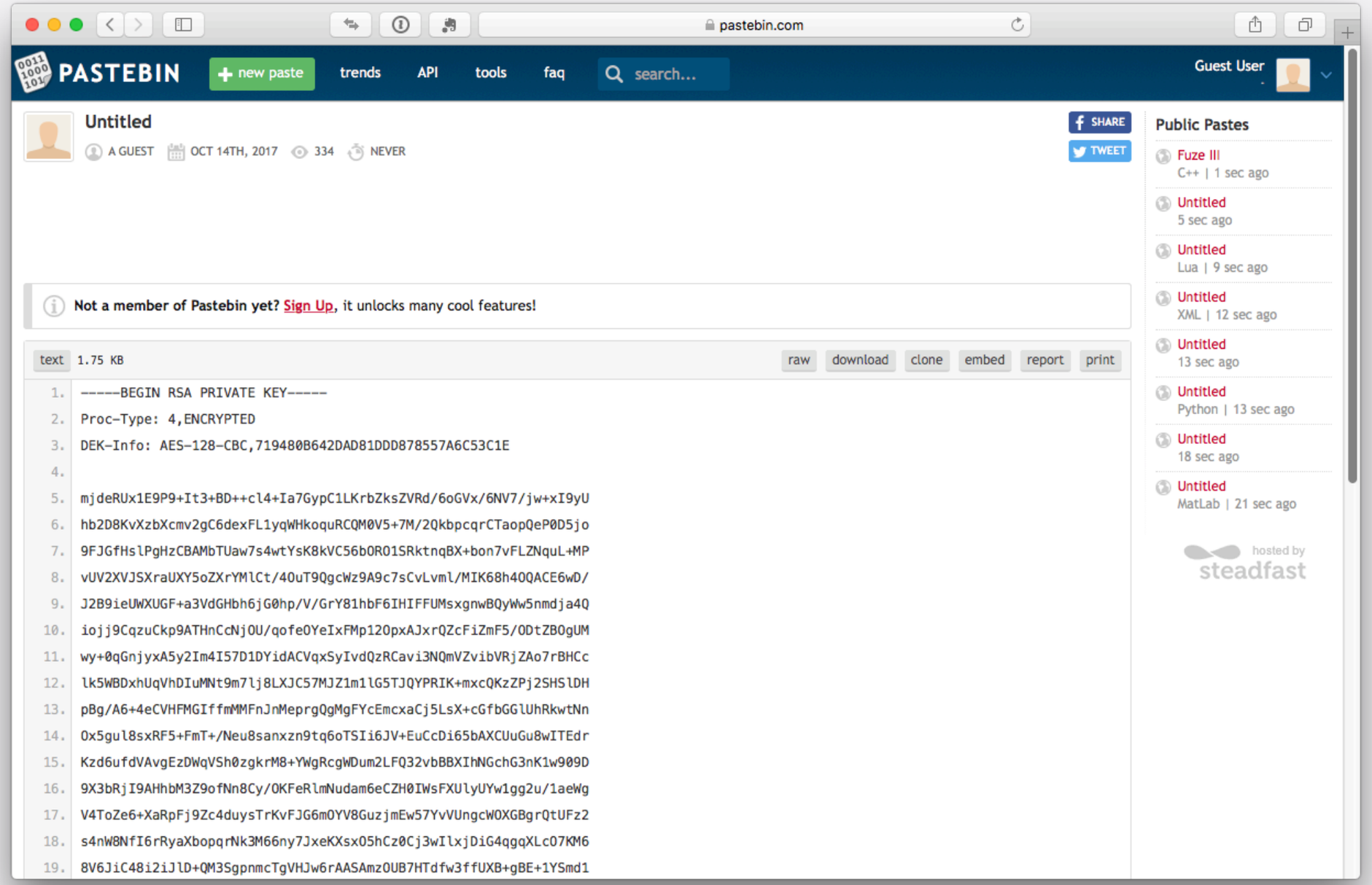
Fonte: @dumpmon

$ Pastebin: API Key



Fonte: @dumpmon

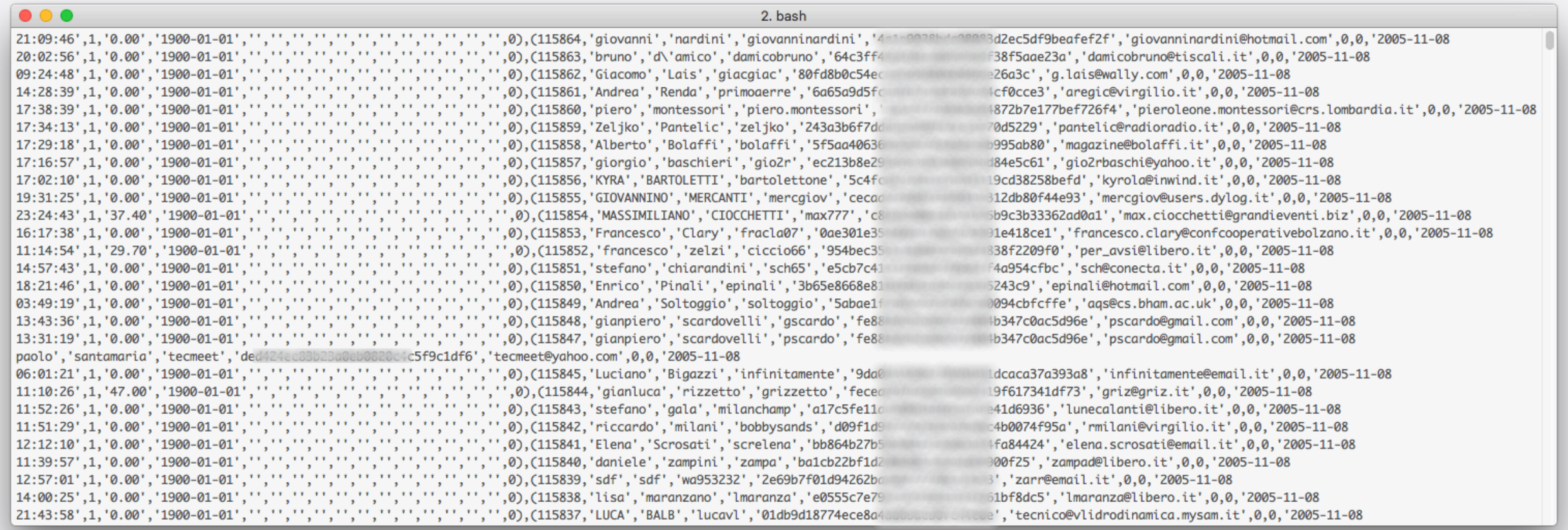
$ Pastebin: SSH Private Key



Fonte: @dumpmon

$ Backup/Dev Server Exposed

$ Backup/Dev Server Exposed



Libero Quotidiano - Fonte: Anonymous

$ Backup/Dev Server Exposed

Aeroporto di New York-Stewart - Fonte: Gestalt IT

$ Injection

OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

$ SQL Injection

SQL Injection Vulnerability in 'Yahoo! Contributors Network'

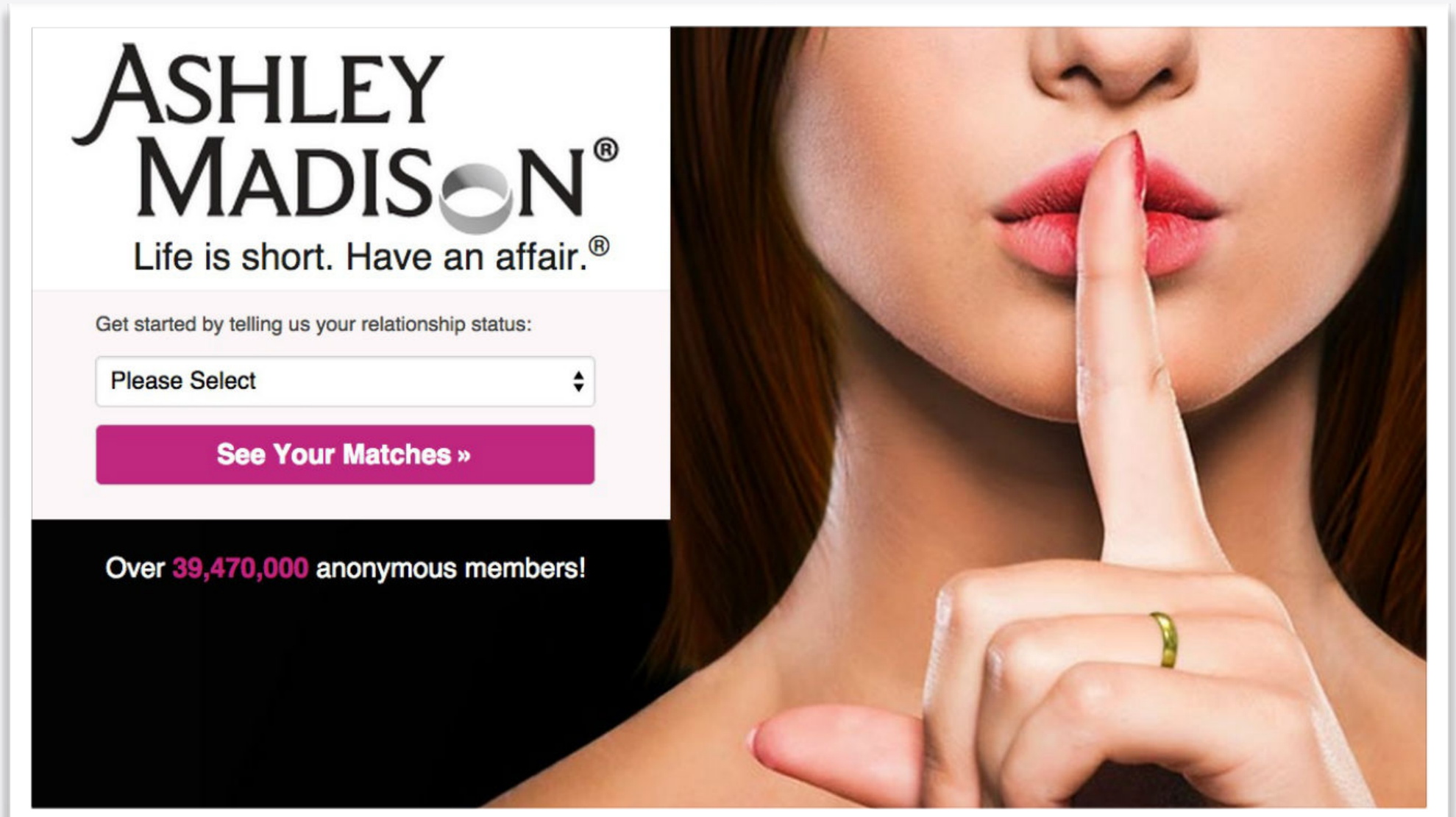
Wednesday, October 08, 2014 Mohit Kumar

Yahoo! Contributors Network (*contributor.yahoo.com*), the network of authors that generated the contents such as photographs, videos, articles and their knowledge to more than 600 million monthly visitors, was vulnerable to a Time based Blind SQL Injection vulnerability.

Behrouz Sadeghipour, a security researcher reported the ***Blind SQLi vulnerability in Yahoo!***'s website that could be exploited by hackers to steal users' and authors' database, containing their personal information.

453491 eMail e Password - Fonte: ThN

$ SQL Injection



33 milioni di eMail e Password - Fonte: Guerre di Rete

$ SQL Injection

Drupal SQL Injection Vulnerability leaves Millions of Websites Open to Hackers

Sunday, November 02, 2014 Wang Wei

Drupal™

One of the most popular content management systems, **Drupal**, is warning its users to consider their websites as compromised unless their sites were updated immediately with a security patch released on 15 October 2014.

12 milioni di siti con Drupal Vulnerabile al 2014 - Fonte: ThN

$ SQL Injection

Sony Pictures hacked and Database Leaked by LulzSec

Thursday, June 02, 2011 Mohit Kumar

Sony Pictures hacked and Database Leaked by **LulzSec**

YES ! Sony Hacked Again once more by Lulzsec. The Target is SonyPictures.com and It compromised over 1,000,000 users'personal information, including passwords, email addresses, home addresses,dates of birth, and all Sony opt-in data associated with their accounts.Also compromised all admin details of Sony Pictures(including passwords) along with 75,000 "music codes" and 3.5 million "music coupons".

1 milione di utenti coinvolti - Fonte: ThN

$ SQL Injection

Clone | Raw text | New

anagraphic_id	anagraphic_valido	anagraphic_txn_id	anagraphic_ip	anagraphici_cf	anagraphic_piva	anagraphic_data	anagraphic_nome	anagraphic_citta	anagraphic_email	anagraphic_sesso	anagraphic_cognome	anagraphic_importo	anagraphic_privacy	anagraphic_bilancio	anagraphic_indirizzo	anagraphic_mail_sent	anagraphic_confirmed	anagraphic_tipologia	anagraphic_data_nascita	anagraphic_tipo_donatore	anagraphic_privacy_public	anagraphic_ragione_sociale	anagraphic_legale_rappresentante
1	0	<blank>	<blank>	MCCMRC71a04c261k	<blank>	2017-06-23 15:29:36	nome	milano	info@casaleggio.it	M	Maiocchi	1.00	1	<blank>	via gerolamo morone 6, c/o Casaleggio associati	<blank>	<blank>	paypal	1971-01-04	persona_fisica	<blank>	<blank>	<blank>
3	0	<blank>	<blank>	MCCMRC71a04c261k	<blank>	2017-06-23 15:30:52	nome	milano	info@casaleggio.it	M	Maiocchi	1.00	1	<blank>	via gerolamo morone 6, c/o Casaleggio associati	<blank>	<blank>	paypal	1971-01-04	persona_fisica	<blank>	<blank>	<blank>
4	0	<blank>	<blank>	MCCMRC71a04c261k	<blank>	2017-06-23 15:31:35	nome	milano	info@casaleggio.it	M	Maiocchi	1.00	1	<blank>	via gerolamo morone 6, c/o Casaleggio associati	<blank>	<blank>	paypal	1971-01-04	persona_fisica	1	<blank>	<blank>
5	0	<blank>	<blank>	MCCMRC71a04c261k	<blank>	2017-06-23 15:32:05	nome	milano	info@casaleggio.it	M	Maiocchi	100.00	1	<blank>	via gerolamo morone 6, c/o Casaleggio associati	<blank>	<blank>	paypal	1971-01-04	persona_fisica	1	<blank>	<blank>
6	0	<blank>	<blank>	MCCMRC71a04c261k	<blank>	2017-06-23 15:54:49	nome	milano	info@casaleggio.it	M	Maiocchi	100.00	1	<blank>	via gerolamo morone 6, c/o Casaleggio associati	<blank>	<blank>	paypal	1971-01-04	azienda	1	<blank>	<blank>
7	0	<blank>	<blank>	MCCMRC71a04c261k	asasd	2017-06-23 16:02:21	Marco	milano	info@casaleggio.it	M	Maiocchi	20.00	1	1	via gerolamo morone 6, c/o Casaleggio associati	<blank>	<blank>	paypal	1971-01-04	azienda	<blank>	<blank>	legalizzamelo
8	0	<blank>	<blank>	<blank>	asdas	2017-06-23 16:04:36	marco	milano	info@casaleggio.it	<blank>	maiocchi	12.34	1	1	via gerolamo morone 6, c/o Casaleggio associati	<blank>	<blank>	paypal	<blank>	azienda	1	rag	sasssss leg
9	0	<blank>	<blank>	MCCMRC71a04c261k	<blank>	2017-06-23 17:01:33	marcolino	milano	info@casaleggio.it	M	maiocchi	0.00	1	<blank>	via gerolamo morone 6, c/o Casaleggio associati	<blank>	<blank>	bonifico	1971-01-04	persona_fisica	<blank>	<blank>	<blank>

Rousseau - Movimento 5 Stelle

$ Front End e Back End

$ Front End e Back End: SSL Self Signed


```
GET https://camp.tim.it/widgetCamp/loginDca.do HTTP/1.1
Accept: */*
User-Widget: iPhone
Accept-Language: it-it
Client-Device-Id: [redacted]-2D36-408B-947A-[redacted]E
Password: 1[redacted]85
User-Name: 36[redacted]55
User-Agent: Mozilla/5.0 (iPhone; U; CPU like Mac OS X; en) AppleWebKit/420+
Mobile/1A543 FileDownloader/3.0
Connection: keep-alive
Widget-Version: 4.0
Cookie: dtCookie=DAAE8E1CF89E171A12[redacted]aW1Nb2JpbGVBcHB8MQ; J
n8dHLKSQGEfgShhF9hybykx0_[redacted]m!1875506470!-1320192397
Host: camp.tim.it
```

$ Q&A

@AndreaDraghetti