



Errori informatici da non commettere nel mondo lavorativo!

Andrea Draghetti



UNIVERSITÀ
DEGLI STUDI
DI PALERMO



Phishing Analysis and Contrast @ D3Lab

Team Member @ BackBox Linux



\$ Europa e Informatica

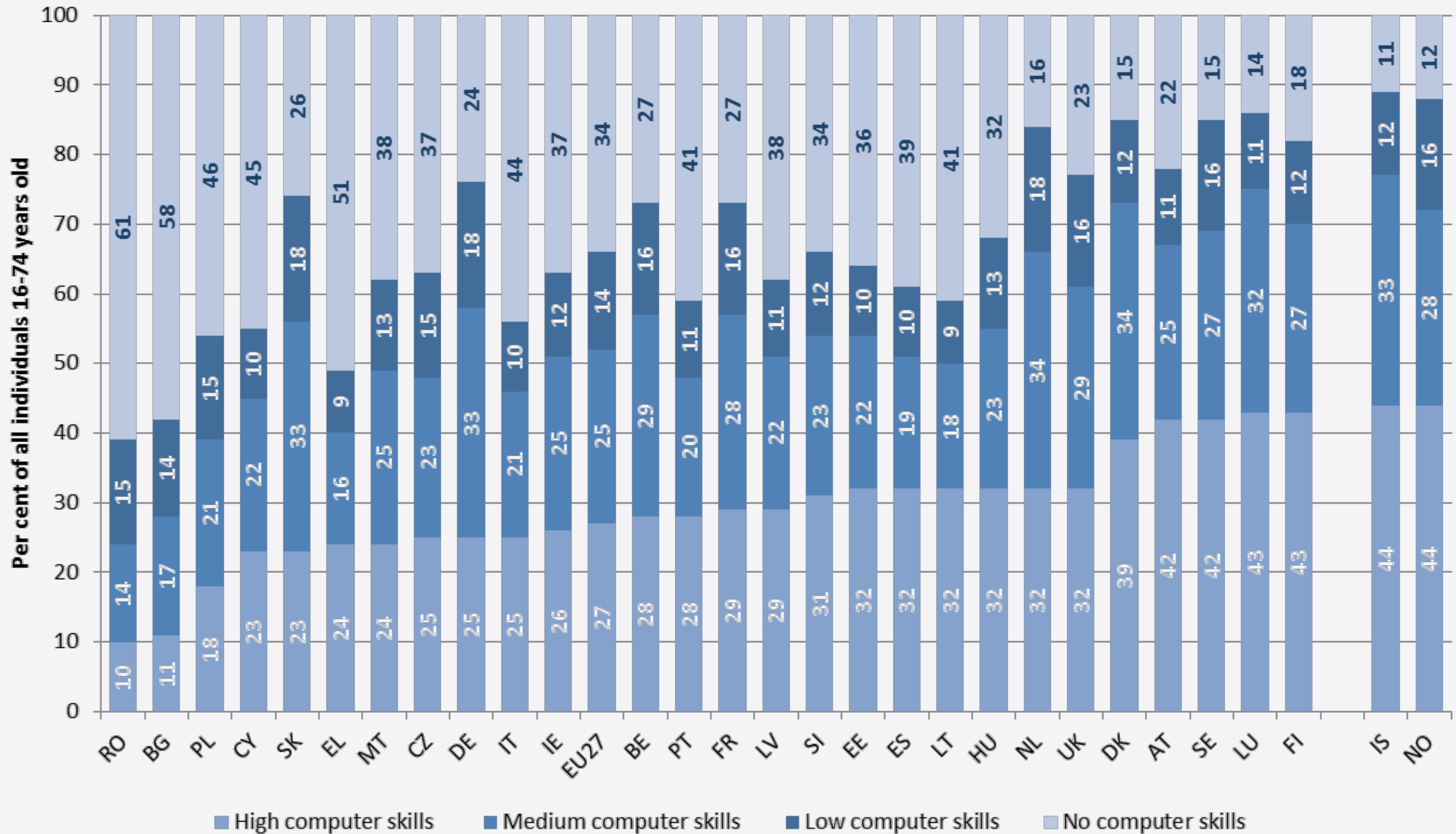
Popolazione Europea: 743 milioni

Occupanti Settore IT: 6,7 milioni
ossia il 3,1% del totale UE

Fonte: Eurostat



\$ Europa e Informatica



Fonte: Eurostat

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

26 Luglio 2017 126



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: f t g+ e

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 Havebeenpwned.com. The website allows people to check if their personal information has been compromised.

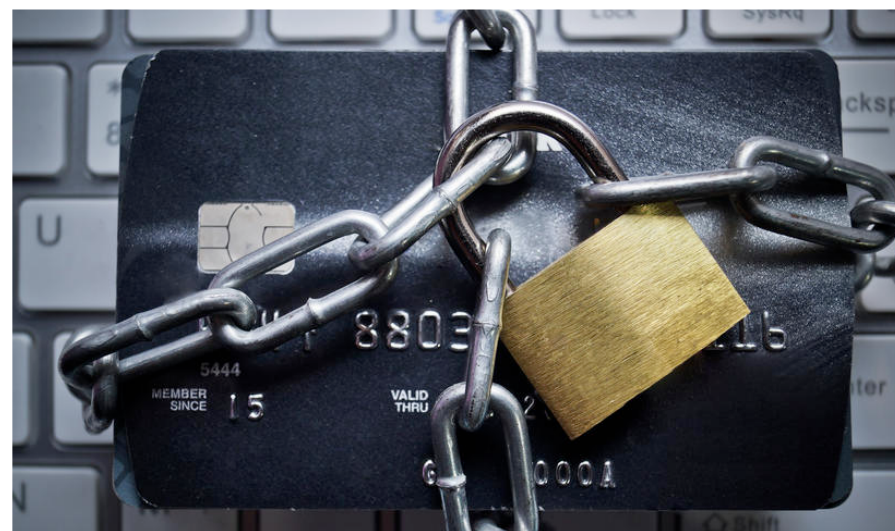
Earlier this year the site exposed the hacking of Ster-Kinekor's website, which put more than six million accounts at risk, Business Day reported.

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.

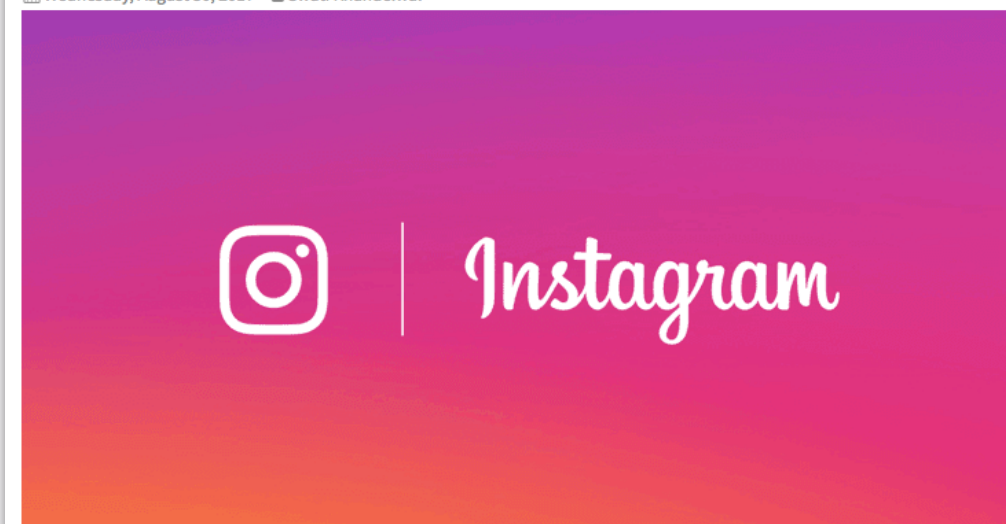


Thinkstock.com

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.

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.

PTI website defaced by hackers

By News Desk Published: August 2, 2017

83 SHARES f SHARE t TWEET e EMAIL

[!] HaCked By Voice OF Pakistan [Death Adders Crew

Pakistan Zindabad



DEATH ADDERS CREW

\$ Aggiornamenti



Dopo 16 anni il 9,17% degli utenti usa Windows XP.
È il terzo OS più usato al mondo!

\$ Aggiornamenti: cosa potevamo evitare...

WannaCry
Ransomware Attack



Data Breach
EQUIFAX

Here's How to Protect Yourself

\$ Password: Hash $\neq$ Cifratura



\$ Password: Hash $\neq$ Cifratura

Salve, mi consigliate x un sistema di login/autenticazione il 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.

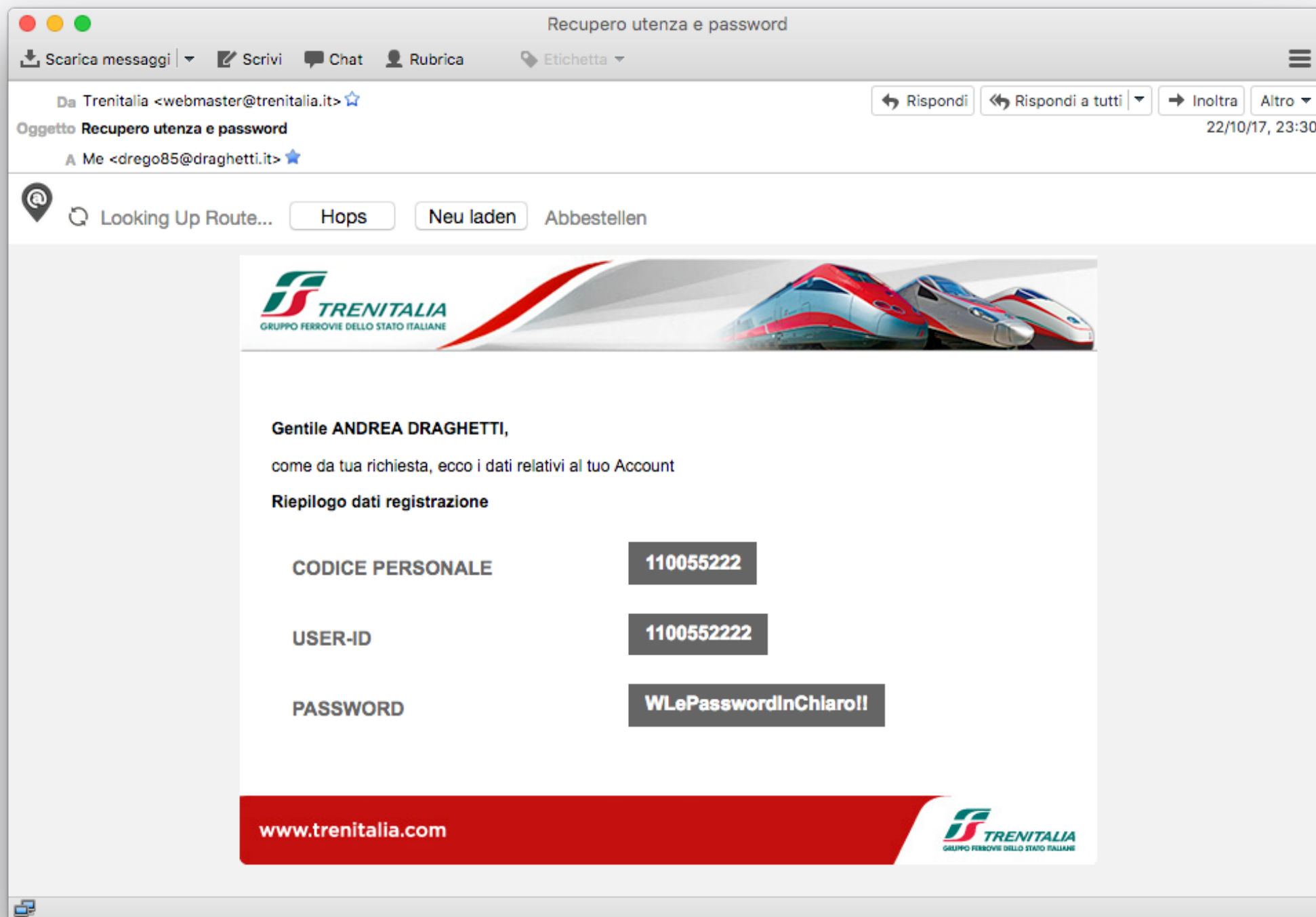
Oltre alla classica pwd in chiaro, la semplice criptazione MD5 che può generare due stesse identiche stringhe e anche la MD5 + salt. Voi che sistema utilizzate?

\$ Password: Hash $\neq$ Cifratura

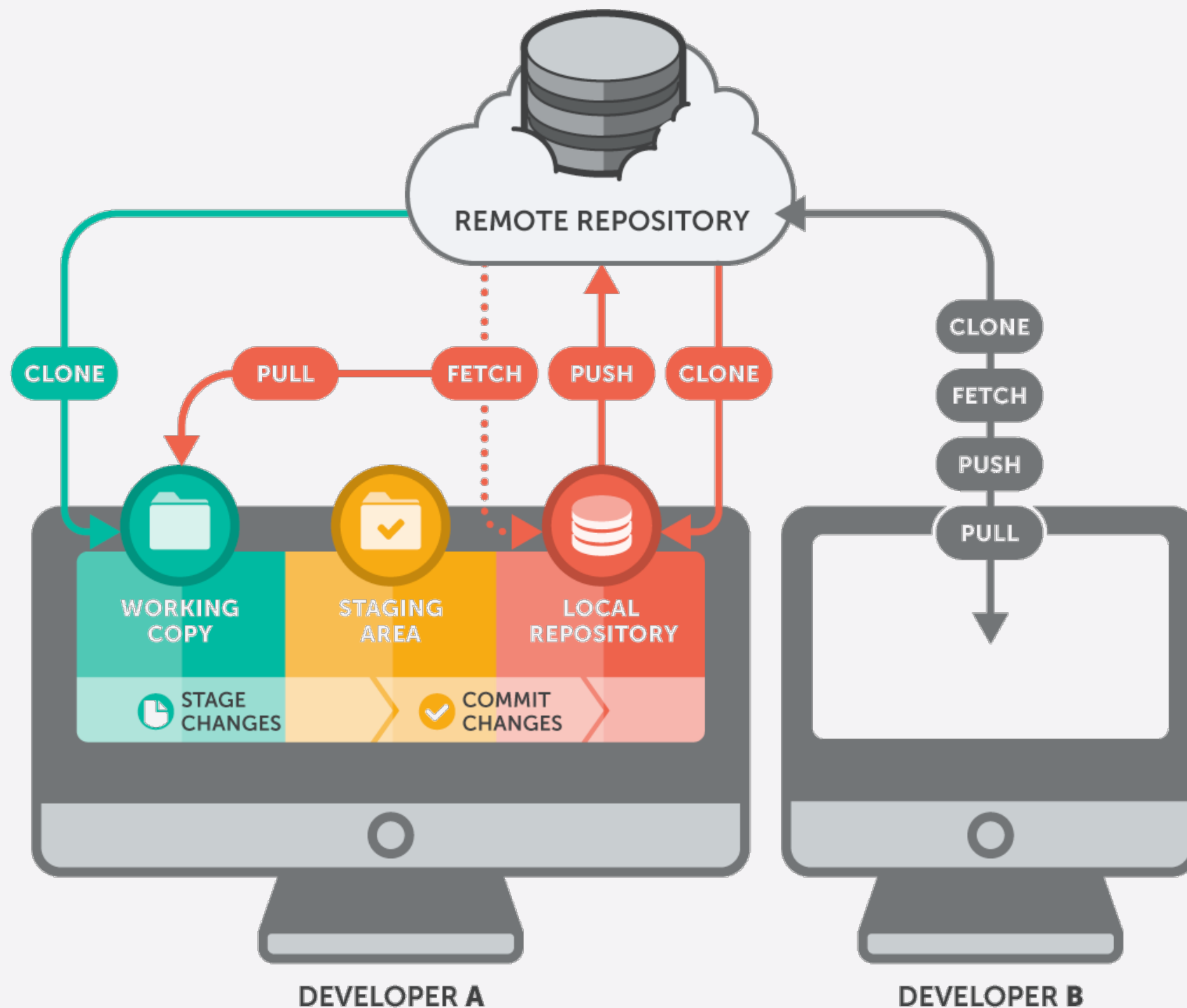
hashkiller.co.uk

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

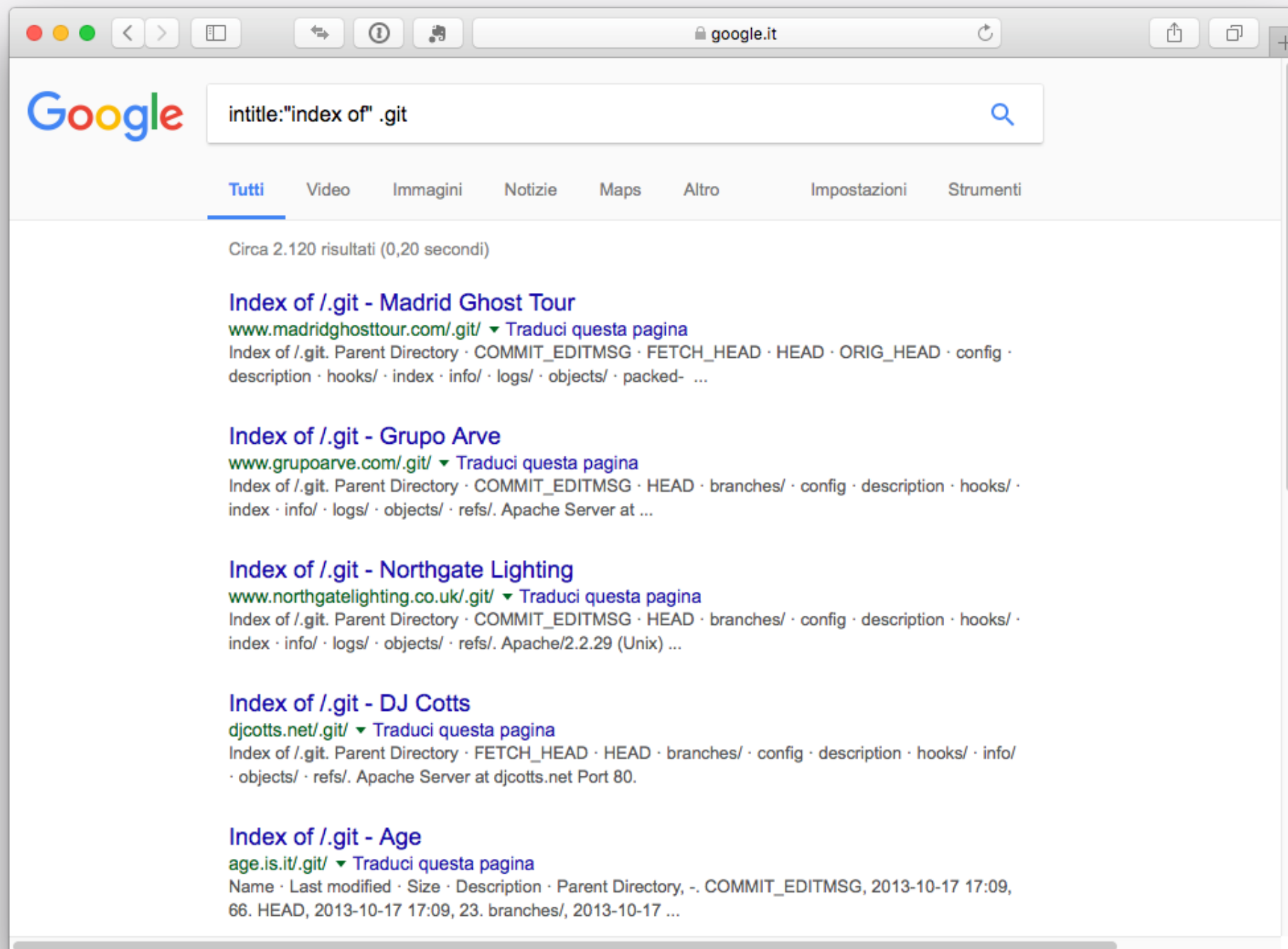
\$ Password: in chiaro 🧐



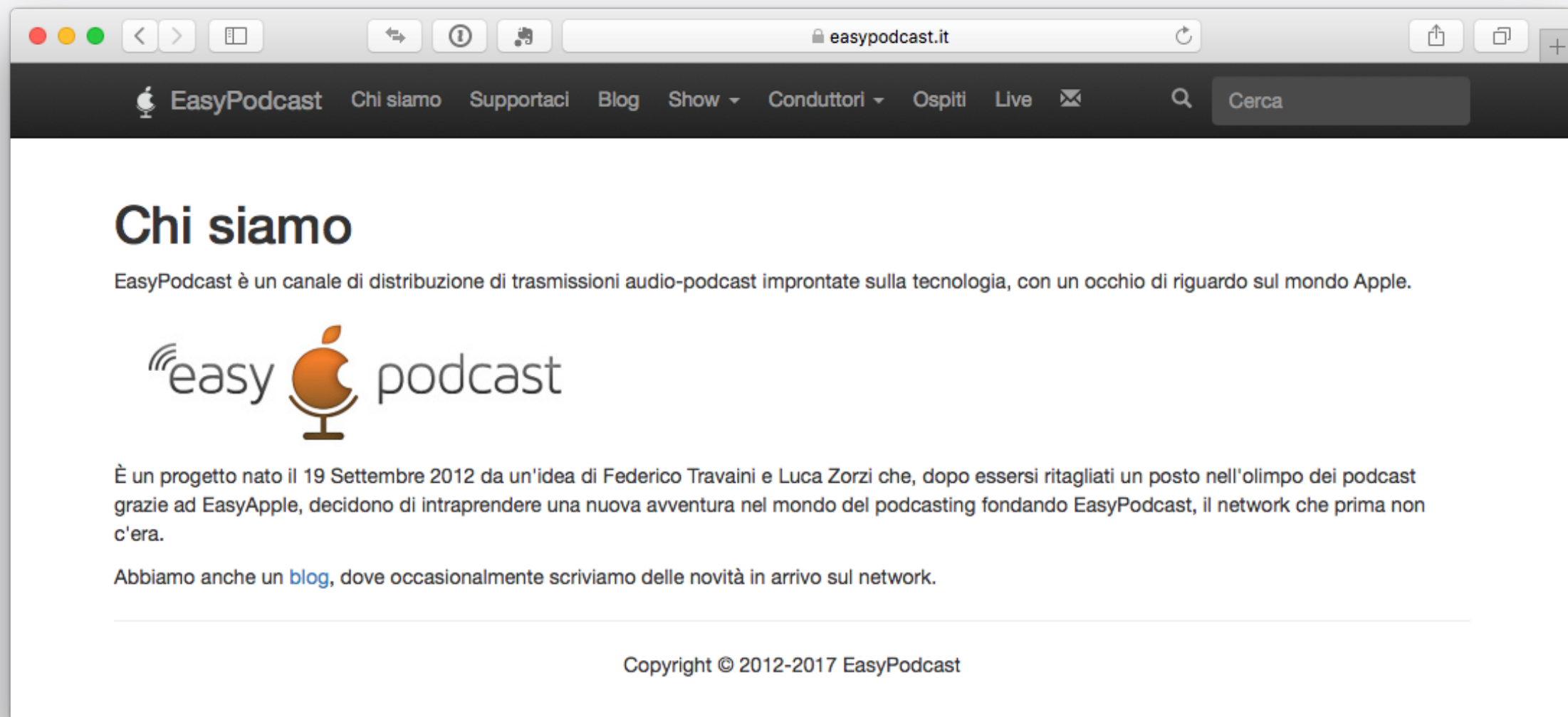
\$ Git: Distributed Version Control System



\$ 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 = "wheytrvroot@gmail.com"
4 SMTP_PASSWORD = "wheytrv54321"
```



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

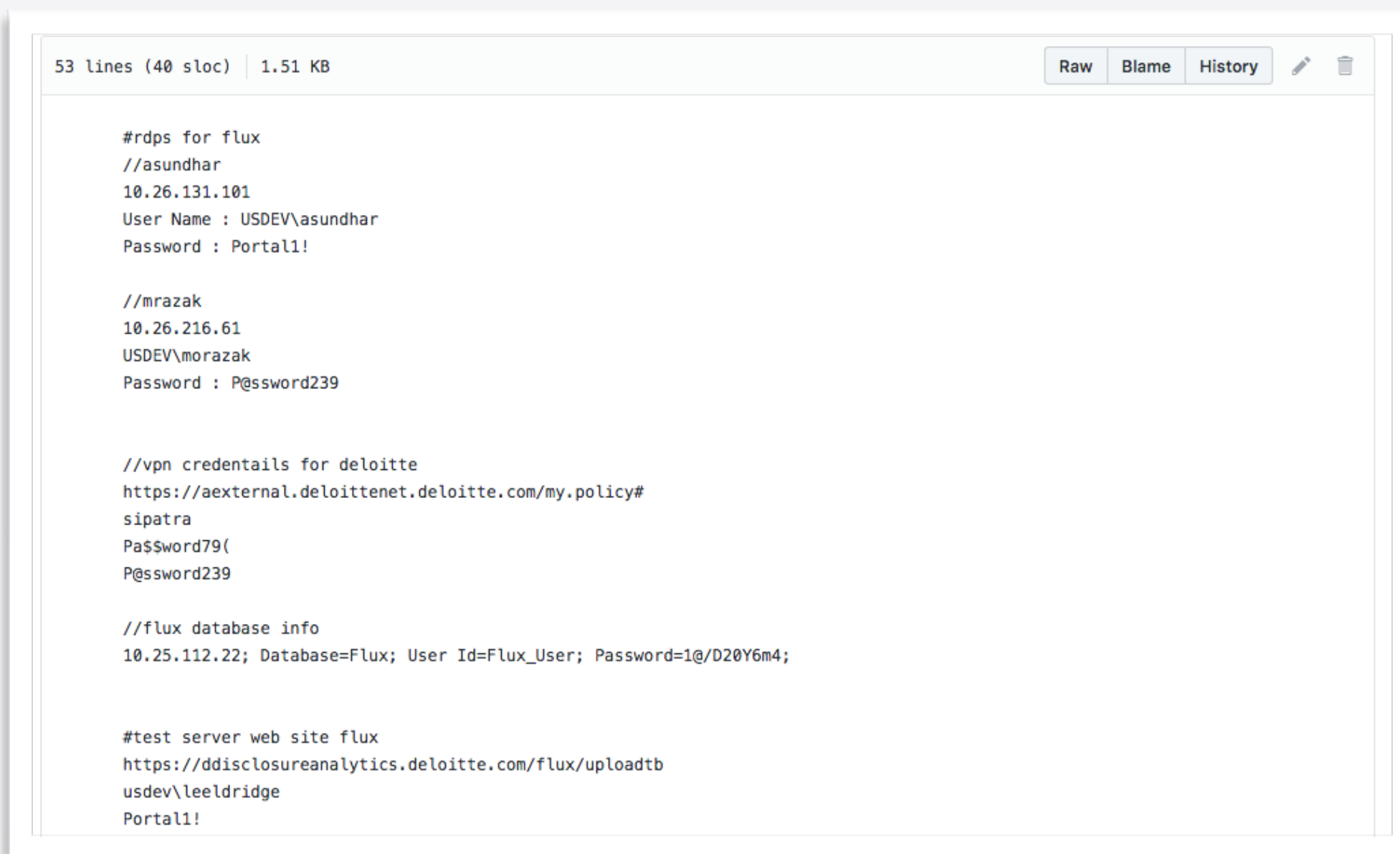


Heisenberg/PGP – [sekring.pgp](#)

Showing the top nine matches Last indexed on 26 Jan

```
1 -----BEGIN PGP PRIVATE KEY BLOCK-----
2 103400200380217398135249222006548204073328106072688005529063811770138810014207803500686
3 182100490423522711275647777363298400494886618062703278193884830249058310514357715806847
4 -----END PGP PRIVATE KEY BLOCK-----
```

\$ Git: Distributed Version Control System



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

//mrarak
10.26.216.61
USDEV\morarak
Password : P@ssword239

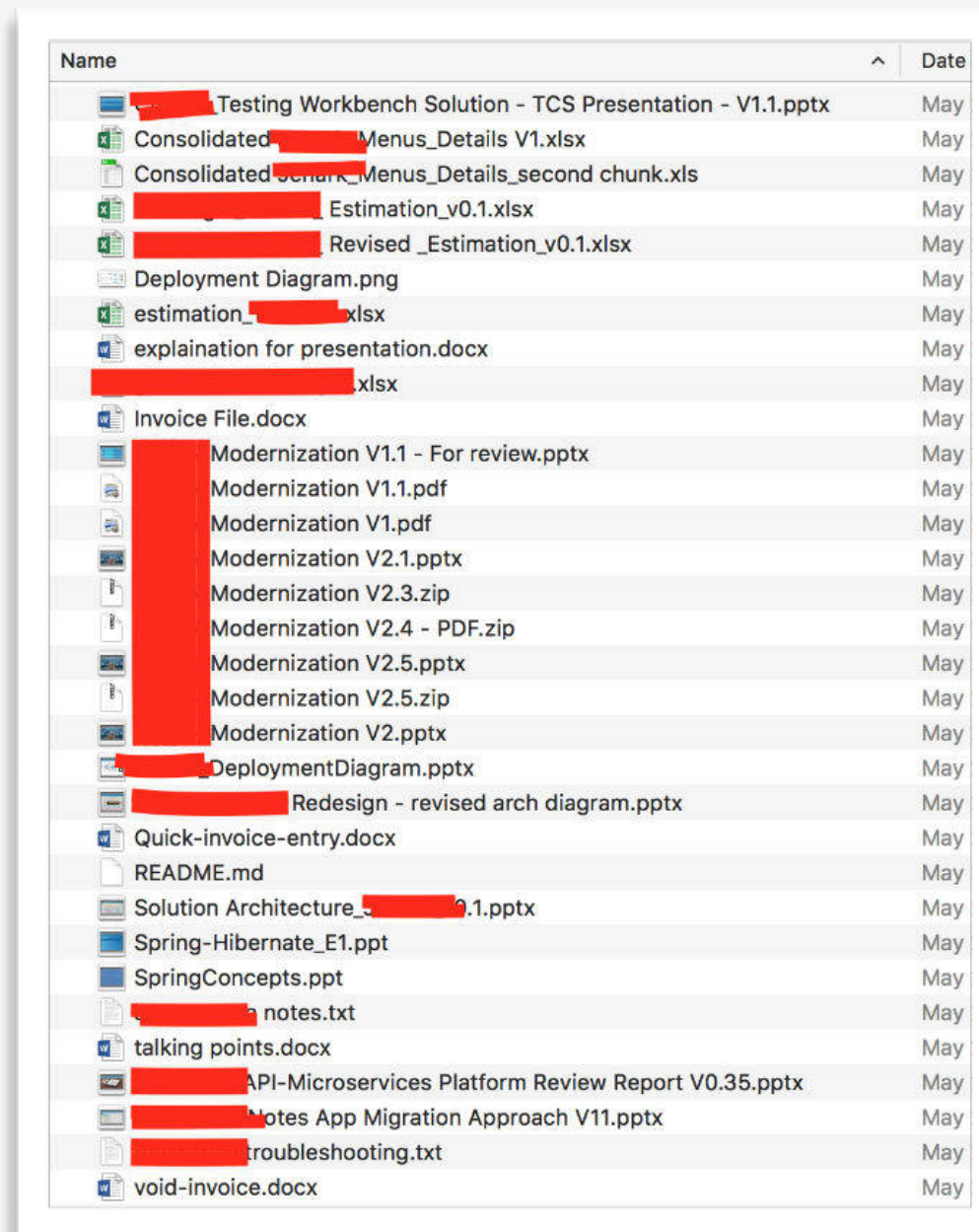
//vpn credentails for deloitte
https://aexternal.deloittenet.deloitte.com/my.policy#
sipatra
Pa$$word79(
P@ssword239

//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



Name	Date
Testing Workbench Solution - TCS Presentation - V1.1.pptx	May
Consolidated Menus_Details V1.xlsx	May
Consolidated Menus_Details_second chunk.xls	May
Estimation_v0.1.xlsx	May
Revised _Estimation_v0.1.xlsx	May
Deployment Diagram.png	May
estimation_ .xlsx	May
explanation for presentation.docx	May
.xlsx	May
Invoice File.docx	May
Modernization V1.1 - For review.pptx	May
Modernization V1.1.pdf	May
Modernization V1.pdf	May
Modernization V2.1.pptx	May
Modernization V2.3.zip	May
Modernization V2.4 - PDF.zip	May
Modernization V2.5.pptx	May
Modernization V2.5.zip	May
Modernization V2.pptx	May
DeploymentDiagram.pptx	May
Redesign - revised arch diagram.pptx	May
Quick-invoice-entry.docx	May
README.md	May
Solution Architecture_ .1.pptx	May
Spring-Hibernate_E1.ppt	May
SpringConcepts.ppt	May
notes.txt	May
talking points.docx	May
API-Microservices Platform Review Report V0.35.pptx	May
Notes App Migration Approach V11.pptx	May
troubleshooting.txt	May
void-invoice.docx	May

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

\$ Pastebin

The screenshot shows the Pastebin website interface. At the top, there's a dark blue header with the 'PASTEBIN' logo, a '+ new paste' button, a 'trends' link, a search bar, and a 'Guest User' profile. Below the header, the main content area is titled 'New Paste' and features a large text input field. Underneath the input field is the 'Optional Paste Settings' section, which includes four dropdown menus: 'Syntax Highlighting' (set to 'None'), 'Paste Expiration' (set to 'Never'), 'Paste Exposure' (set to 'Public'), and 'Folder' (set to '(PRO members only)'). To the right of these settings, there's a user profile section with a 'Hello Guest' message, 'Sign Up' and 'Login' buttons, and three social login buttons: 'Sign in with Facebook', 'Sign in with Twitter', and 'Sign in with Google'.

0011
1000
101

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

The screenshot shows a web browser window with the URL `pastebin.com`. The page header includes the Pastebin logo, a '+ new paste' button, and navigation links for 'trends', 'API', 'tools', and 'faq'. A search bar is also present. The user is logged in as 'Guest User'.

The main content area displays a paste titled 'acc' by a guest user, dated 'OCT 22ND, 2017', with 351 views and a 'NEVER' expiration. A notification banner asks if the user is a member, with a 'Sign Up' link.

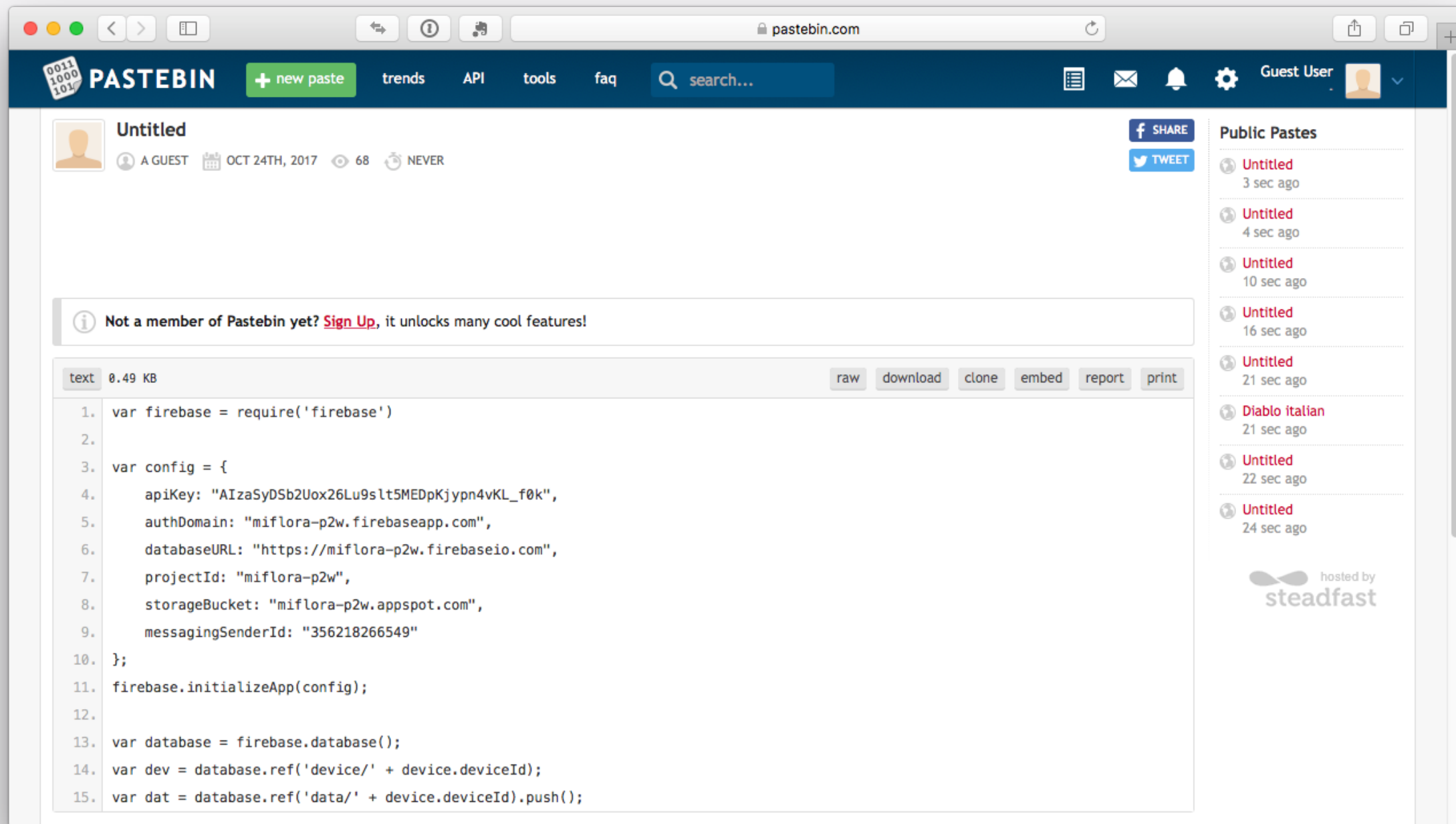
The paste content is a text file (3.69 KB) containing a list of 11 entries, each with a unique ID, a name, a date of birth, a gender, and an email address. The entries are as follows:

ID	Name	Date of Birth	Gender	Email
42683067810	THAYNA PIRES	13/04/2008	F	thayna426@bomtoncom
40652085806	ALINE CRISTINE ANASTACIO	21/09/1989	F	aline406@bomtoncom
02328899021	ANA GABRIELA LEAL OSORIO	26/10/1990	F	ana023@bomtoncom
02120004706	GLEICE CRISTINA IOTTI MAIA DOS SANTOS	17/07/1971	F	gleice021@bomtoncom
01943759278	FELIPE SOARES GOMES PEREIRA	02/11/1995	M	felipe019@bomtone.com
16039298863	GILMA CORREIA NASCIMENTO SILVA	07/08/1969	F	gilma160@bomtone.com
42097656862	JOAO VICTOR COLLARES BRIGOLA	01/12/1992	M	joao420@bomtone.com
07572447422	MARIA QUITERIA DOS SANTOS	23/07/1971	F	maria075@bomtone.com
41146246862	SARA ALVES DA SILVA	24/06/1993	F	sara411@bomtone.com
09220027976	JOCELI RUTZ	19/05/1995	F	joceli092@bomtone.com
06409138571	RAFAEL DA SILVA SANTOS	05/07/1992	M	rafael064@bomtone.com

On the right side, there is a 'Public Pastes' section showing a list of recent pastes, all titled 'Untitled', with timestamps ranging from 3 seconds ago to 20 seconds ago. At the bottom right, there is a 'hosted by steadfast' logo.

Fonte: @dumpmon

\$ Pastebin: API Key

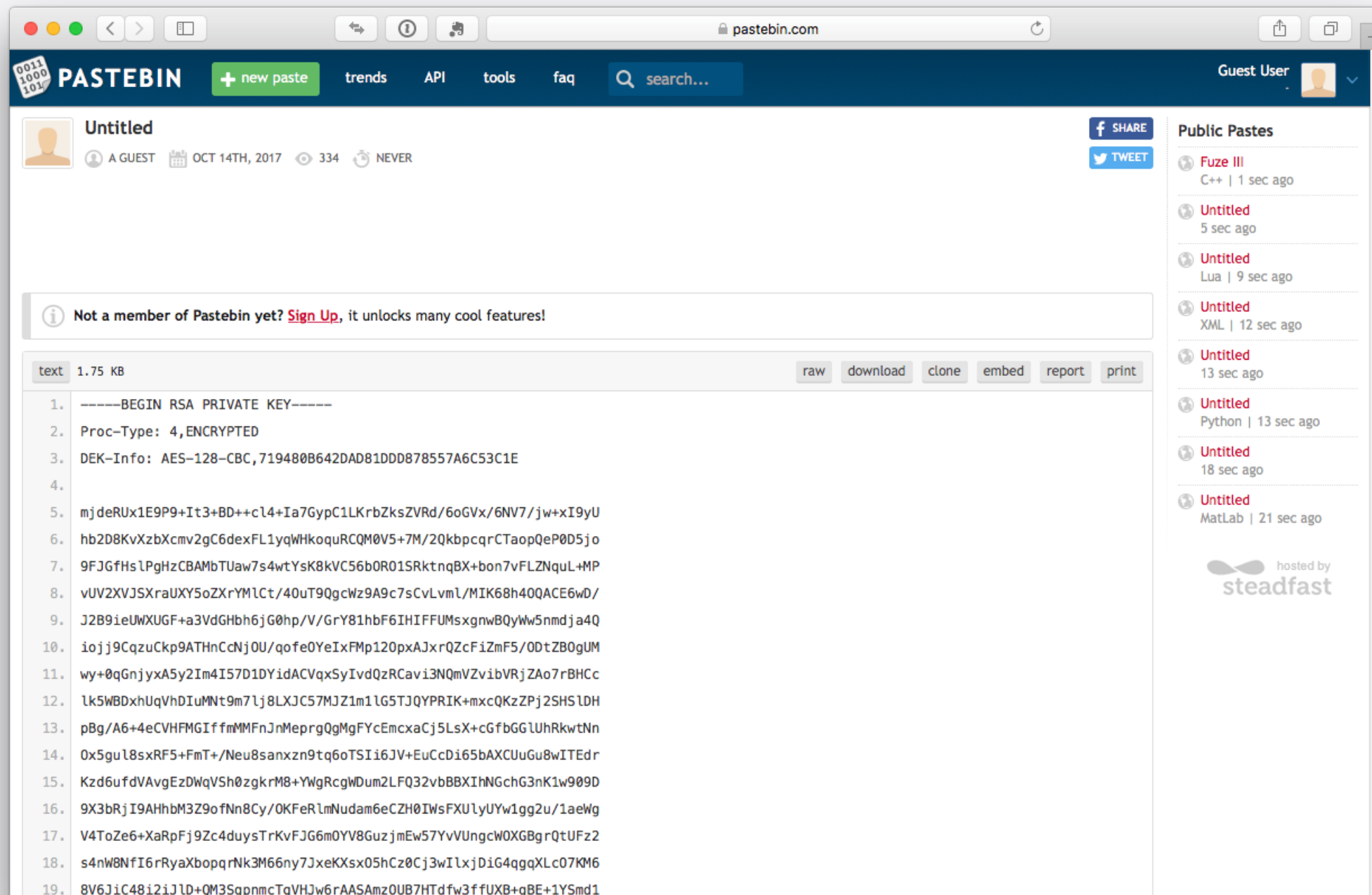


The screenshot shows a web browser window at pastebin.com. The page displays a paste titled "Untitled" by a guest user, dated October 24th, 2017, with 68 views and never expires. The code is a JavaScript snippet for initializing Firebase. A notification banner asks if the user is a member. The right sidebar shows a list of public pastes, mostly titled "Untitled".

```
1. var firebase = require('firebase')
2.
3. var config = {
4.   apiKey: "AIzaSyDSb2Uox26Lu9slt5MEDpKjypn4vKL_f0k",
5.   authDomain: "miflora-p2w.firebaseio.com",
6.   databaseURL: "https://miflora-p2w.firebaseio.com",
7.   projectId: "miflora-p2w",
8.   storageBucket: "miflora-p2w.appspot.com",
9.   messagingSenderId: "356218266549"
10. };
11. firebase.initializeApp(config);
12.
13. var database = firebase.database();
14. var dev = database.ref('device/' + device.deviceId);
15. var dat = database.ref('data/' + device.deviceId).push();
```

Fonte: @dumpmon

\$ Pastebin: SSH Private Key



The screenshot shows a web browser window at pastebin.com. The page displays a pasted SSH private key. The key is titled "Untitled" and was posted by a guest user on October 14th, 2017, at 3:34 PM. The key is 1.75 KB in size. The key text is as follows:

```
1. -----BEGIN RSA PRIVATE KEY-----
2. Proc-Type: 4, ENCRYPTED
3. DEK-Info: AES-128-CBC, 719480B642DAD81DDD878557A6C53C1E
4.
5. mjdeRUx1E9P9+It3+BD++c14+Ia7GypC1LKrbZksZVRd/6oGVx/6NV7/jw+XI9yU
6. hb2D8KvXzbXcmv2gC6dexFL1yqWHkoquRCQM0V5+7M/2QkbpqqrCTaopQeP0D5jo
7. 9FJGfHs1PgHzCBAMbTUaw7s4wtYsK8kVC56b0R01SRktngBX+bon7vFLZNQuL+MP
8. vUV2XVJSXraUXY5oZXrYMLct/40uT9QgcWz9A9c7sCvLvm1/MIK68h40QACE6wD/
9. J2B9ieUWXUGF+a3VdGHbh6jG0hp/V/GrY81hbF6IHIFUMsxgnwBQyWw5nmdja4Q
10. iojj9CqzuCkp9ATHnCcnj0U/qofe0YeIXFmp120pxAJxrQZcFiZmF5/0DtZB0gUM
11. wy+0qGnjyxA5y2Im4I57D1DYidACVqxSyIvdQzRCavi3NqmVZvibVRjZAo7rBHCc
12. lk5WBDxhUqVhDIuMnt9m7lj8LXJC57MJZ1m1lG5TJQYPRIK+mxkQKzZPj2SHS1DH
13. pBg/A6+4eCVHFMGIffmMMFnJnMeprgQgMgFYcEmcxaCj5LsX+cGfbGG1UhrKwtNn
14. 0x5gu18sxRF5+FmT+/Neu8sanxzn9tq6oTSIi6JV+EuCcDi65bAXCUuGu8wITEdr
15. Kzd6ufdVAvgEzDwqVSh0zgkrM8+YwGRcgWDum2LFQ32vbBBXIhNGchG3nK1w909D
16. 9X3bRjI9AHhbM3Z9ofNn8Cy/0KFeRlMnDam6eCZH0IWsFXUlyUYw1gg2u/1aewg
17. V4ToZe6+XaRpfj9Zc4duysTrKvFJG6m0YV8GuzjmEw57YvVUngcW0XGBgrQtUFz2
18. s4nW8NfI6rRyaXbopqrNk3M66ny7JxeKXsx05hCz0Cj3wIlxjDiG4qgqXLc07KM6
19. 8V6JiC48i2iJlD+QM3SgpnmcTgVHJw6rAASAmz0UB7HTdfw3ffUXB+gBE+1YSmd1
```

The page also includes a sidebar with "Public Pastes" and a "Steadfast" logo at the bottom right.

Fonte: @dumpmon

\$ Backup/Dev Server Exposed



\$ Backup/Dev Server Exposed

[illegible]

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

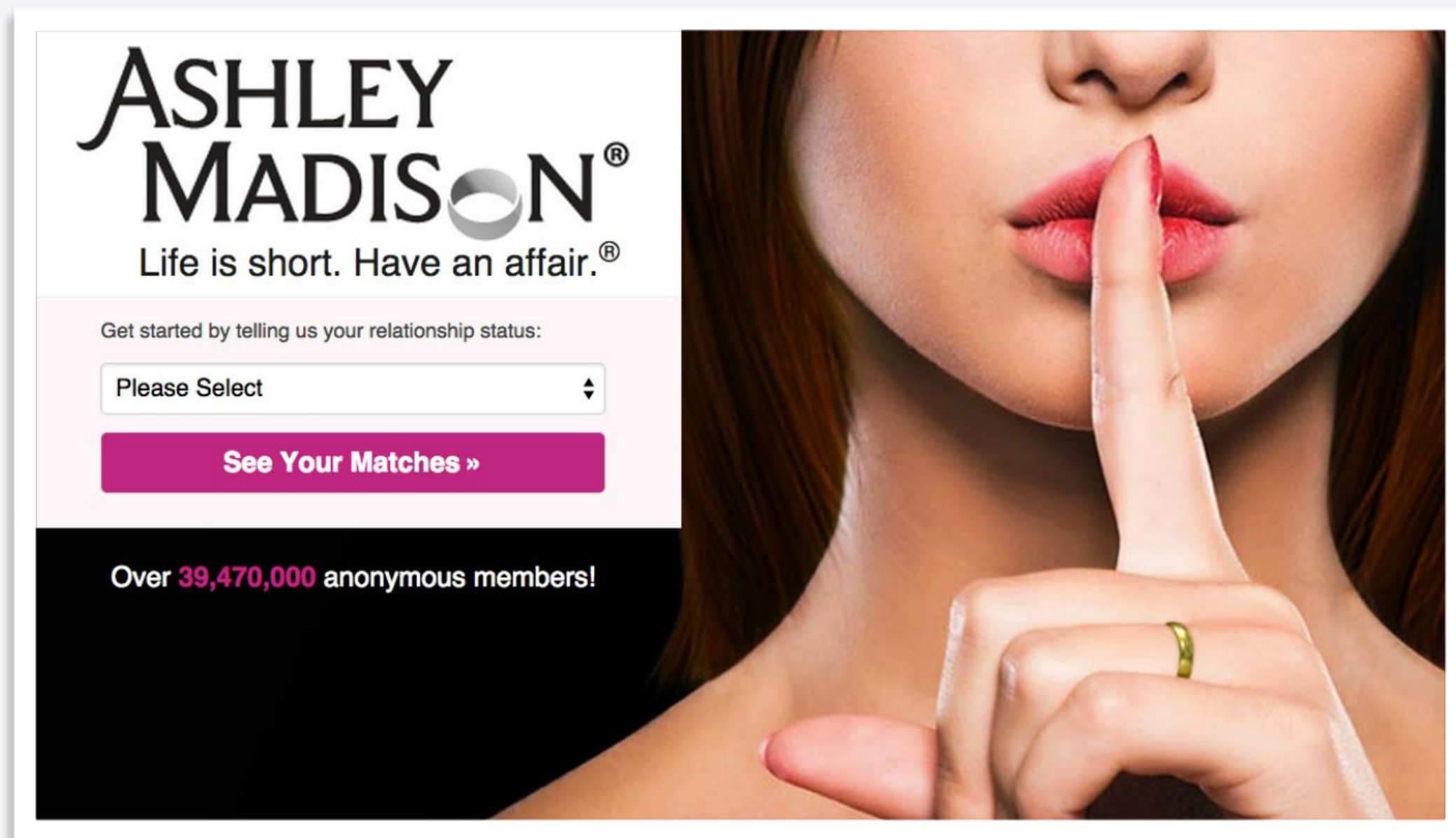


Yahoo! Contributors Network (contributor.yahoo.com), the network of authors that generated the contents such as photographs, videos, articles and their knowledge to more than 600 million monthly visitors, was vulnerable to a Time based Blind SQL Injection vulnerability.

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



DrupalTM

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

CloneRaw textNew

	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>	<blank>	via gerolamo morone 6, c/o Casaleggio associati	<blank>	<blank>	paypal	1971-	01-04	persona_fisica	<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>	<blank>	via gerolamo morone 6, c/o Casaleggio associati	<blank>	<blank>	paypal	1971-	01-04	persona_fisica	<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>	<blank>	via gerolamo morone 6, c/o Casaleggio associati	<blank>	<blank>	paypal	1971-	01-04	persona_fisica	<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>	<blank>	via gerolamo morone 6, c/o Casaleggio associati	<blank>	<blank>	paypal	1971-	01-04	persona_fisica	<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>	<blank>	via gerolamo morone 6, c/o Casaleggio associati	<blank>	<blank>	paypal	1971-	01-04	azienda	<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	<blank>	via gerolamo morone 6, c/o Casaleggio associati	<blank>	<blank>	paypal	1971-	01-04	azienda	<blank>	<blank>
8	0	<blank>	<blank>	<blank>	asdas	2017-06-23 16:04:36	marco	milano	info@casaleggio.it	<blank>	maiocchi	12.34	1	1	<blank>	via gerolamo morone 6, c/o Casaleggio associati	<blank>	<blank>	paypal		<blank>	<blank>	<blank>	<blank>
9	0	<blank>	<blank>	MCCMRC71a04c261k	<blank>	2017-06-23 17:01:33	marcolino	milano	info@casaleggio.it	M	maiocchi	0.00	1	<blank>	<blank>	via gerolamo morone 6, c/o Casaleggio associati	<blank>	<blank>	bonifico	1971-	01-04	persona_fisica	<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: 85F7A230-2D36-408B-947A-802AF48AD87E
Password: 17071085
User-Name: 3668104855
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=DAAE8E1CF89E171A12F28B87E48CE888|TX1UaW1Nb2JpbGVBcHB8B8MQ; J
n8dHLKSQGEfgShhF9hybykx0_AWm5P8GVTBqQpRwE4Zym!1875506470!-1320192397
Host: camp.tim.it
```

