

The leaky web: Owning your favorite CEOs

Cesar Cerrudo
CTO at IOActive Labs



Introduction

- Every minute Internet is being more widely used
 - Almost everything we use has a web site on Internet and we have an account on it
 - E-commerce
 - Media streaming
 - Cell phones, computers, tablets, etc.
 - Sports accessories
 - Airlines, Hotels, Car rentals companies
 - Video game consoles
 - Social media
 - Online news, etc..
 - A huge amount of data about us is just one click away



Getting data about someone

- How?
 - Looking on known places
 - Google
 - Social media
 - Etc.
 - Abusing authentication related mechanisms
 - Works on 90% (aprox.) of web sites
 - We just need someone's email address



Getting data about someone

- Authentication

- User name

- Email address used in most web sites
 - Few websites uses specific usernames and not email addresses
 - But email address sometimes used on “Forgot username or password”

- Issues on most websites

- In user registration if email address already exists the web site will tell you
 - In “Forgot password?” if the email address doesn’t exist then the web site will tell you
 - If it exists the web site will tell you and it could leak more information too



Getting data about someone

- Is it a serious problem?
- Warning
 - This is not something personal or intentional against companies that could be mentioned neither against the employees
 - Most web sites have these kind of issues, only some of them show too much data





[Your Account](#) |

E-mail Address Already in Use

You indicated you are a new customer, but an account already exists with the e-mail **[redacted]@[redacted].com**

Are you a returning customer?



We found your email address: **[redacted]@[redacted].com**

What do you want to do next?

- I need to create a new password
- I know my password and want to login

Continue



Register with eBay

Tell us about yourself All fields are required

First name Last name

Street address

ZIP / Postal code City, State

Country / Region

Email address

Your email address is already registered with eBay. Did you forget your user ID?

You've entered an email address that is already registered with Netflix. If you already are or previously were a member please click 'Member Sign In'.

Start Your 1 Month Free Trial

[Free trial offer details](#)



Email

Confirm Email

LGNSFID01: We can't find a match for that email address. Be sure that you entered it again. This is the email you provided when you set up your account online.

Further help call the Web Assistance Center at 1-866-755-0451 (Mon.-Fri.)

AT&T Online Account Verification

Verify Your Email Address


Your online account security is very important to us. Please enter the contact information for your AT&T U-verse or AT&T Email for verification. This is the contact information provided when you set up your online account.

Contact Email Address



Sign up or Log in

Another user is already using this email

 Become a Nike member

FIRST NAME*

LAST NAME*

EMAIL*
EMAIL ADDRESS IS ALREADY TAKEN

❌

SCREEN NAME*

PASSWORD*

CONFIRM PAS*


LinkedIn®

Home What is LinkedIn? Join Today

❌ The email address, ██████████@██████████.com, is already registered.

Over 150 million professionals use LinkedIn to exchange information, ideas and opportunities

Full Name*



Email Address*

❌ An account with this email address already exists. Please [sign in](#) to that account, or, if you want to create a new account, enter a different email address.

Register 

E-mail Address: ❗

Requested username is unavailable. Please enter username and password to create your account.

Form 

Email: ❗ This email already exists.

h Email:

The Washington Post

FREE access to this article and other exclusive content!

Sign In Now

ORACLE MyProfile Create User

Please provide the following information to create your Oracle

Your Oracle.com account gives you access to a variety of online services. Your Oracle.com account gives you access to a variety of online services. PartnerNetwork. If you are registering for one of these services

on this computer.

Now

Free Membership

E-MAIL ADDRESS:

This e-mail address is already registered with us. [Click here to Sign In](#) or [Click here to be sent your password.](#)

PASSWORD:

CONFIRM PASSWORD:

Become a Free Member Now

New User Registration

*Indicates required field

Create Your Account

x* E-mail

Username already exists. Please login or enter another Username

NYTimes.com

Already have an account? Log

THE WALL STREET JOURNAL.

ACCOUNT IDENTIFIED

The following user name was located for the email

[redacted]@oracle.com

E-Mail Address

That e-mail address is already associated with an account. Try again or log in »



YOU ABOVE
jetBlue
Plan a trip

priceline.com
flights | hotels | rental cars | vacation packages | cruises | tours
Create Your Priceline
An account already exists with the information you provided.
Please select a sign-in question.

DIRECTV Sign In
What is DIRECTV? TV Packages Premium
Sign In or Create A
What is your email address? Sign in with usern
[redacted]@[redacted].com
Do you have a
 No, I am a D
 Yes, I have a
Sign In
Forgot Password
Security Question
Your high school mascot?
Answer

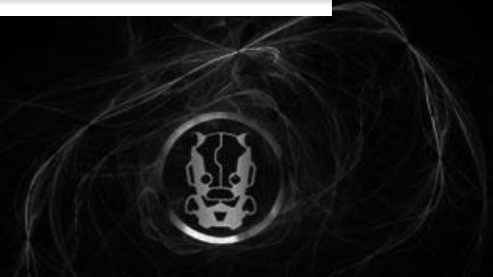
TRUEBLUE
Title cannot be blank.
First name cannot be blank.
Last name cannot be blank.
Street address 1 cannot be blank.
City cannot be blank.
State/Province cannot be blank.
Zip/Postal code cannot be blank.
Phone number cannot be blank.
Your email: '[redacted]@[redacted].com' is already in use.

spg Starwood Preferred Guest | **FOUR POINTS** BY SHERATON
Find & Book
Forgot Username and Password

Please enter the required information below in order to verify your identity and change your usernam

Starwood Preferred Guest Member Number [redacted] 8280
Reminder Question
City you were born in?
Answer

Google accounts
Create an Account
If you already have a Google Account, you can [sign](#)
Required information for Google account
Your current email address: [redacted]@[redacted].com
There's already a Google Account associated with this email address. Please sign in; or, if you forgot your password, [reset it](#) now.
[?]
e.g. myname@example.com. This will be used to sign-in to your account.



LOST USERNAME OR PASSWORD?

LOST USERNAME OR PASSWORD?

Please enter your email which you first registered with.

• There is no user with this email.

Email:

Send Email



xHamster

just porn, no bullshit

BTW, your mobile devices can [watch porn](#) t

Video

Live Cams

Pictures

Stories

Games

[Fresh PornVideos](#) • [Top Rated](#) • [Recommended for Me](#) • [My Favorite Videos](#) • [My Videos](#) • [M](#)

This email already exist!

Sign Up

New Member? Just fill out the account information below.

Email Address:

XVIDEOS

ACCOUNT CREATION

Create an account

Errors : Your password is too short, Please give your name, Please give your firstname, This account already exist, Bad Captcha

Email, (your login)



What could we get?

- Demo



What could we get?

- Websites used
 - Social media, news and magazines, E-commerce, Media streaming , Porn, etc.
 - GPS watches
 - Airlines
 - Car rental companies
 - Hotels
 - Video game consoles
 - Etc.
- Websites identified can be hacked to get more information about victim



How can be used?

- Penetration tests
 - Gather information about people for performing specific attacks later.
- Social engineering, phishing, DoS, identity theft, fraud, etc.



Choosing a victim

- Victim

- Any person

- For this experiment I chose C-Level executives (Fortune 500)

- Devices (Smartphone, notebook, desktop PC, tablet)
 - Travel (Airlines, Hotels, Car rentals)
 - Social media (twitter, linkedin, facebook, etc.)
 - Sports (GPS watches)
 - Movies and music (media streaming)
 - Buy (Amazon, Ebay, etc.)
 - Play (Sony Playstation, Nintendo Wii, etc.)
 - News



Starting the experiment

- With the victim email we can start
 - Websites accounts are “silently enumerated”
 - Websites forced to leak if the email is used in an existing account
 - Other information could be leaked too: usernames, air miles program number, hotel rewards program number, emails, secret questions, etc.



The experiment

- 840 C-Level executives corporate email addresses tried in 30 websites(automated, no CAPTCHA, no user registration)
 - 250 social media websites accounts(42 facebook, 127 twitter, 17 myspace, 41 plaxo.com, 6 naymz.com, 17 linkedin.com)
 - 241 news websites accounts (58 wsj.com, 28 washingtonpost.com, 5 gartner.com, 14 economist.com, 52 nytimes.com, 80 marketwatch.com, 4 bloomberg.com)
 - 35 media streaming websites accounts (13 hulu.com, 22 netflix.com)
 - 43 hotel websites accounts (29 accorhotels.com, 14 starwoodhotels.com)
 - 23 airlines websites accounts (ua2go.com)
 - 38 GPS watches websites accounts (nikeplus.com, garmin.com)
 - 176 Google, 11 Skype, 29 orbitz.com, 76 Dropbox.com and 8 sonyentertainmentnetwork.com accounts



The experiment

- The list of websites used by victims and leaked info allow to build a detailed profile
 - Weakest websites can be hacked
 - To get user passwords
 - Not uncommon (important site was found allowing anyone to retrieve any user pass)
 - Find XSS for exploiting victims
 - Spear phishing attacks become easier
 - Send emails and wait for the fish



The experiment

- Emails could be sent
 - Emails identical to the ones usually sent by previously identified websites
 - Just a IMG tag (`src=http://attackersite/img.jpg`) to collect data when image displayed
 - Get browser, OS, device, etc. information.
 - If emails are evil then high probability of ownage



The experiment

- 100% automated
 - Check websites to identify accounts
 - Send emails to collect info and/or attack victims
- Few sites have CAPTCHA and send e-mail notifications
 - We just avoid them when targeting dozen of emails or if just few emails then manual work could be fine
 - Hire CAPTCHA bypass services



Conclusions

- Website data leaking is a world wide problem
- It's very easy to gather data about most people
 - No need of special skills to do it, just need an email address
- While Internet use grows more, less privacy we have and more possibilities of being attacked
- C-level executives should use corporate email address just for email
 - Companies should implement special security programs and policies to protect executives



Fin

- Questions?
- Gracias.
- E-mail: ccerrudo@ioactive.com
- twitter: [@cesarcer](https://twitter.com/cesarcer)

