

RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

C U SRF: Cross USer Request Forgery

SESSION ID: HTA-W02

Amichai Shulman

CTO
Imperva



Amichai Shulman – CTO, Imperva



- ◆ Speaker at Industry Events
 - ◆ RSA, Appsec, Info Security UK, Black Hat
- ◆ Lecturer on Information Security
 - ◆ Technion - Israel Institute of Technology
- ◆ Former security consultant to banks & financial services firms
- ◆ Leads the Application Defense Center (ADC)
 - ◆ Discovered over 20 commercial application vulnerabilities
- ◆ Credited by Oracle, MS-SQL, IBM and others
Amichai Shulman one of InfoWorld's "Top 25 CTOs"



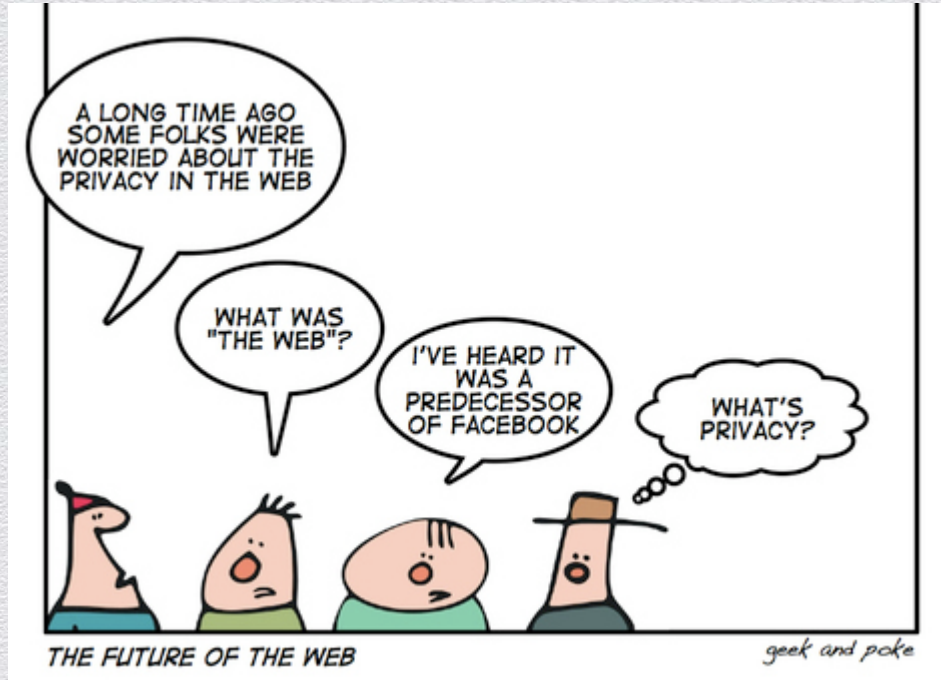


RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

The Motivation: Protecting your ID in a Hostile Online Environment

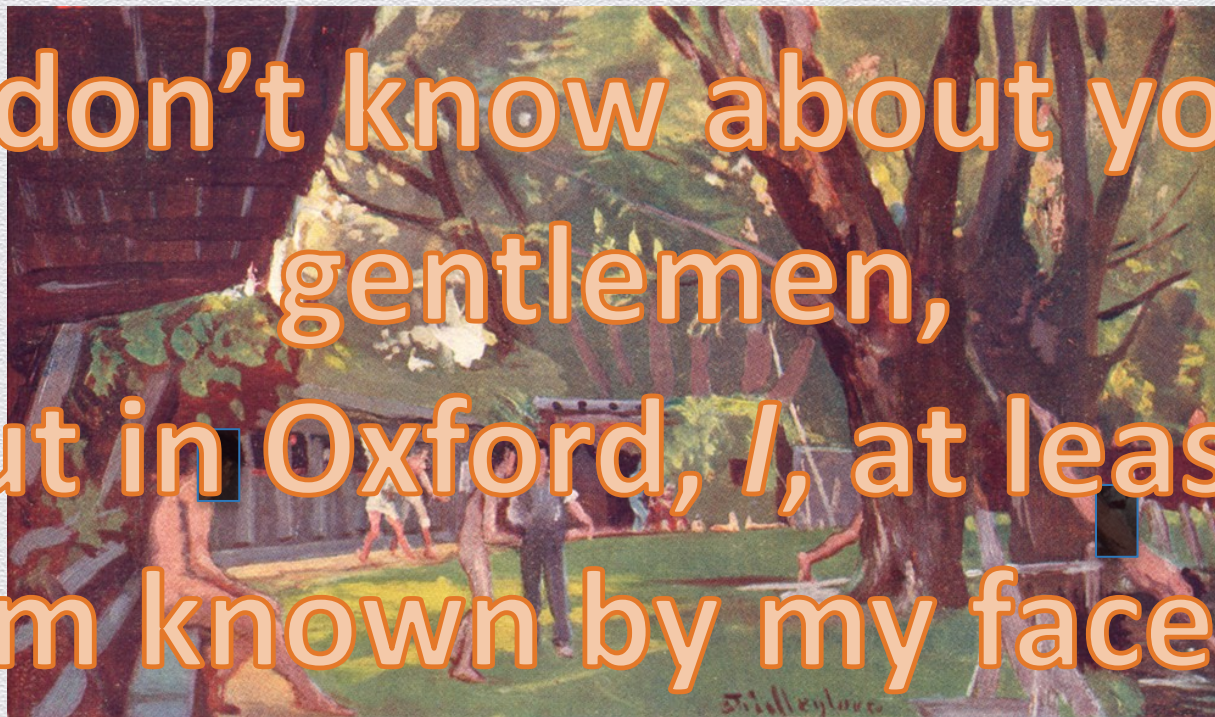
Privacy on the Web: an Uphill Battle?



<http://www.askingsmarterquestions.com/wp-content/uploads/2011/08/internet-privacy-cartoon2.jpg>

Privacy Can Be Achieved Through Anonymity

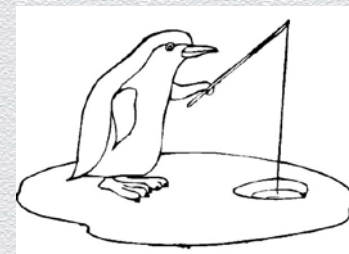
"I don't know about you, gentlemen, but in Oxford, I, at least, am known by my face."



<http://www.antiquaprintgallery.com/ekmps/shops/richben90/images/oxford-the-bathing-sheds-or-parsons-pleasure-1903-67881-p.jpg>

CUSRF Vulnerability Opens Your Social Kimono!

- ◆ CUSRF (pronounced “See You Surf”): Cross USer Request Forgery
- ◆ Web sites you visit can see your privates:
 - ◆ In real time
 - ◆ Name, Email, Work place, Title, etc.
- ◆ Potential outcomes:
 - ◆ “Ice Hole Phishing”: E.g. infect only certain roles in a specific organization.
 - ◆ Display different price
 - ◆ Disinformation



Agenda

- ◆ CSRF brief intro
- ◆ C U SRF: A close encounter with CSRF of the third kind
 - ◆ C U SRF explained
 - ◆ Vulnerable applications in the wild
 - ◆ Google Docs
 - ◆ LinkedIn.com
- ◆ Mitigations
- ◆ Summary and Conclusions



RSA[®]CONFERENCE2014

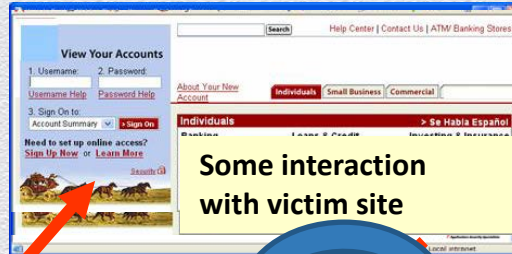
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

CSRF – Quick Intro

SOP Threat Model

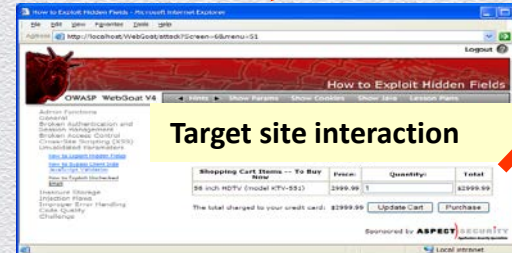
1

Attacker sets the trap on some website on the internet

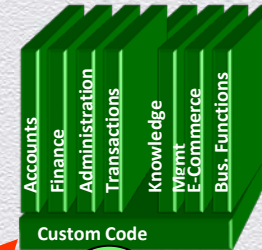


2

While logged into the victim site, victim views attacker's site



Target Application



3

Vulnerable site sees legitimate request from victim, performs the requested action and sends a response

CSRF Illustrated: “Bypassing SOP”

1

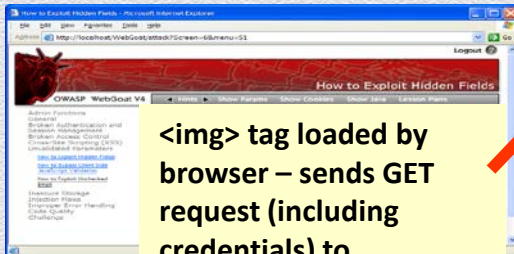
Attacker sets the trap on some website on the internet
(or simply via an e-mail)



Hidden `` tag
contains attack
against vulnerable
site

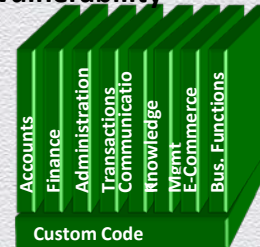
2

While logged into vulnerable site,
victim views attacker site



`` tag loaded by
browser – sends GET
request (including
credentials) to
vulnerable site

Application with CSRF
vulnerability



3

Vulnerable site sees
legitimate request from
victim and performs the
requested action

CSRF

- ◆ The “Confused Deputy” Problem
 - ◆ Web browsers automatically include access tokens with each request
 - ◆ Requests can be invoked by malicious sites from victim’s browser without user consent
- ◆ Automatically Provided Tokens: Session cookie, Basic authentication header, IP address, Client side SSL certificates, Windows domain authentication



CSRF Type I: Classic CSRF

- ◆ The “Transfer Fund” attack
- ◆ Attacker tricks the browser into issuing a “transfer funds” request to the attacker’s account
- ◆ “/transferFund.jsp?To=<attacker>&Sum=10000000”

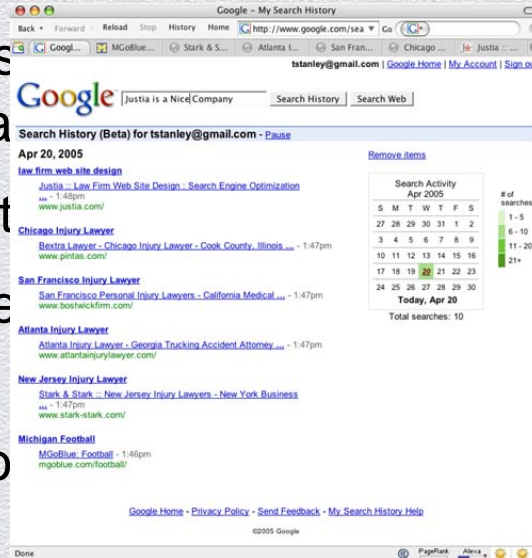
Attack Type	Used credentials	Interacts with
Classic CSRF	Victim’s	Victim’s web account

CSRF Type II: Login CSRF

- ◆ The attacker mounts a CSRF attack that logs the victim into an attacker controlled account (sink account)
- ◆ “signin.jsp?user=<attacker>&password=123456”
- ◆ Later on, the attacker is able to track the victim’s activity in the sink account
- ◆ E.g. log the victim to attacker’s controlled Google account to collect search history

CSRF Type II: Login CSRF

- ◆ The attacker mounts a CSRF attack using a link that logs the victim into an attacker controlled account
- ◆ “signin.jsp?user=<attacker@gmail.com>”
- ◆ Later on, the attacker logs into the victim’s account
- ◆ E.g. log the victim to Google search history



Attack Type	Used credentials	Interacts with
Classic CSRF	Victim's	Victim's web account
Login CSRF	Attacker's	Attacker web account

CSRF is Very Relevant



The screenshot shows the SC Magazine website. The header includes the SC Magazine logo, navigation links for SC US, SC UK, and SC AUS/NZ, and a menu with NEWS, PRODUCTS, BLOGS, RESOURCES, VIDEOS, and SC MAP. A sidebar on the left features a bar chart comparing Information Leakage (55%) and Cross-Site Scripting (53%). The main content area displays a news article titled "Google fixes flaw in Gmail password reset process" by Danielle Walker, Reporter, dated November 22, 2013. The article text discusses a security issue in Gmail's password recovery process, mentioning a blog post by Oren Hafif and a video demonstrating the exploit. A sidebar on the right shows a bar chart with percentages for various security topics: 7% for SQL Injection and 4% for HTTP Response Splitting.

SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

NEWS PRODUCTS BLOGS RESOURCES VIDEOS SC MAP

SC Magazine > News > Google fixes flaw in Gmail password reset process

Danielle Walker, Reporter
Follow @daniellewvkr

November 22, 2013

Google fixes flaw in Gmail password reset process

Google has fixed a security issue in its Gmail password recovery process which could leave users' passwords vulnerable to theft via social engineering.

According to a Thursday blog post by Oren Hafif, the white hat hacker who discovered the bug and demonstrated how to exploit it in a video, Google's security team acted swiftly, fixing the issue in 10 days.

By sending a victim a phishing email, designed to look like a password reset email from Google, an attacker could easily lead users to a malicious URL, setting the stage for exploit.

Hafif showed how a cross-site request forgery (CSRF) attack, followed by a cross-site scripting (XSS) attack, could prompt Google to actually allow users to reset their passwords under the watchful eyes of a saboteur.



RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

**C U SRF:
A Close Encounter
With CSRF of the
Third Kind**

CSRF Type III: C U SRF

- ◆ A new type of CSRF, bringing CSRF to Web 2.0 environment
- ◆ “Cross USer Request Forgery” (CUSRF, pronounced “See You Surf”) attack
- ◆ Composition of the known CSRF vulnerability types, for collaboration environment

Web 2.0: It's All About Collaboration

- ◆ “A Web 2.0 site may allow users to interact and collaborate with each other in a social media dialogue as creators of user-generated content in a virtual community” (Source: Wikipedia)



<http://conceptart.ca/>

CUSRF Explained

- ◆ The attacker forges collaboration requests on behalf of the victim
 - ◆ Similar to the “Classic CSRF”
- ◆ The collaboration target is located on an attacker controlled account
 - ◆ Similar to the “Login CSRF”
- ◆ Outcome: Attacker can reveal the victim’s social network identity.

Attack Type	Used credentials	Interacts with
Classic CSRF	Victim’s	Victim’s web account
Login CSRF	Attacker’s	Attacker’s web account
CUSRF	Victim’s	Attacker’s web account



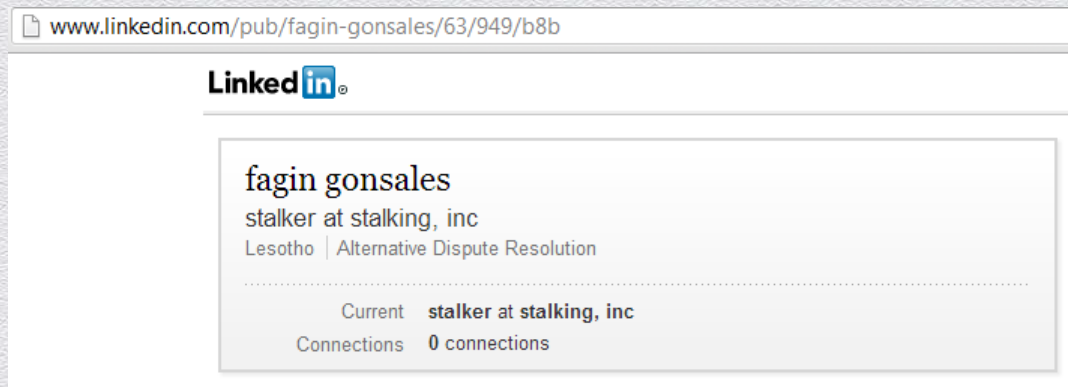
RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

C U SRF in the Wild 1: LinkedIn Profile

Attack Setup: Creating a LinkedIn Profile

- ◆ Attacker sets up a LinkedIn account



Attack Setup: Setting

- ◆ In order to view the identity of profile visitors, the attacker can either:
 - ◆ Go “Pro”
 - ◆ Make her “LinkedIn” identity available to others

What others see when you've viewed their profile

☒ Your name and headline (Recommended)

 **fagin gonsales**
stalker at stalking, inc
Lesotho

☐ Anonymous profile characteristics such as industry and title

Note: Selecting this option will disable [Profile Stats](#).

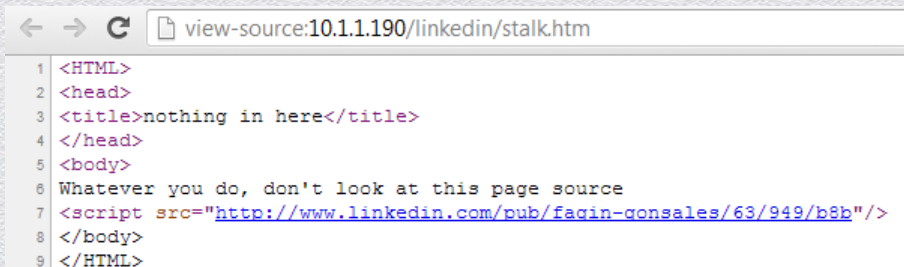
 **Someone on LinkedIn**

☐ You will be totally anonymous.

Note: Selecting this option will disable [Profile Stats](#).

Attack Setup: CSRF Page

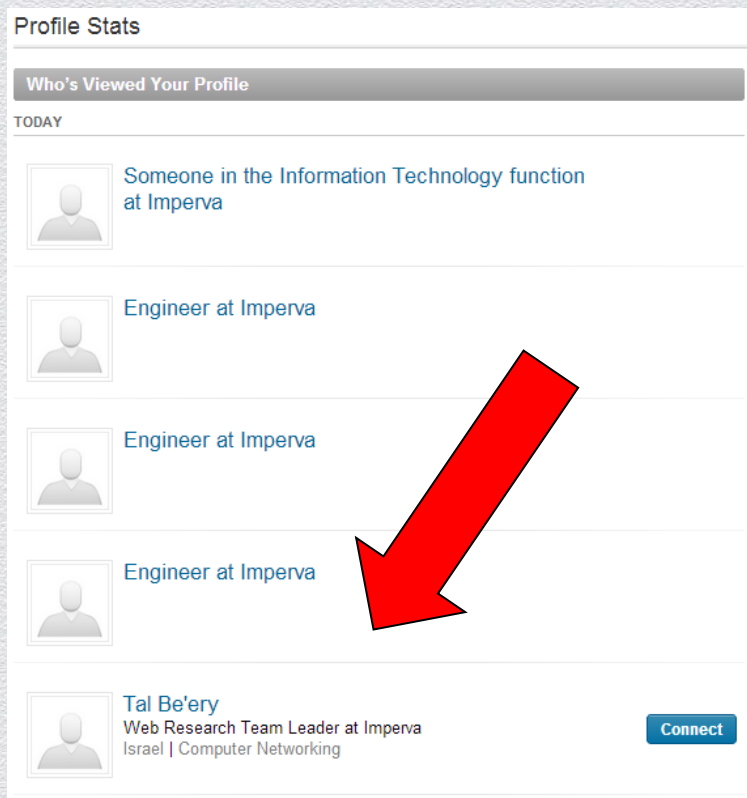
- ◆ Attacker adds an invisible CSRF link referencing the attacker's LinkedIn Profile to their online asset
- ◆ Asset can be:
 - ◆ A "watering hole" page
 - ◆ A phishing page
 - ◆ Etc.



```
1 <HTML>
2 <head>
3 <title>nothing in here</title>
4 </head>
5 <body>
6 Whatever you do, don't look at this page source
7 <script src="http://www.linkedin.com/pub/fagin-consales/63/949/b8b"/>
8 </body>
9 </HTML>
```


Launching the Attack

- ◆ When the intended target visits the CSRF page:
 - ◆ The attacker discovers his identity (“Tal Be’ery”) instantly
- ◆ Can act accordingly:
 - ◆ E.g. infect him personally with a “drive by download” infection



Resolving “Semi Anonymous Profiles”

- ◆ Victim can choose to share only “profile characteristics”
 - ◆ E.g “Engineer in Imperva”
- ◆ This is the default setting
- ◆ Sometimes that’s enough information for the attacker



Resolving “Semi Anonymous Profiles”

- ◆ In 2013, *Linkedininsights.com* had demonstrated a bypass
- ◆ LinkedIn “Red Herring” Module showed list of 10 possible “candidates” for the “Semi Anonymous Profiles”
- ◆ One was the actual person; Others were just “Red Herrings”
- ◆ The problem: “Red Herrings” were randomized, actual person was not
- ◆ Exploit: Attacker should view the “candidates” list twice and mark the overlapping item

A Smelly Red Herring

The screenshot shows two columns of LinkedIn profiles. The left column is titled 'One of these people viewed your profile' and the right column is titled 'One of these people viewed your profile'. Both columns list profiles of people at JPMorgan Chase. A red box highlights the profile of John D Warlow in the right column, and a blue arrow points from this box to the profile of John D Warlow in the left column.

Left Column: One of these people viewed your profile

- Patricia Larkin-Green
VP at JPMC
Greater Chicago Area | Banking
- Pratish Lad
FX API On-Bordering Manager at JPMorgan Chase
Houston, Texas Area | Investment Banking
- Mary Roemmela
VP, QA Architect at J P Morgan Chase
San Francisco Bay Area | Banking
- Brendan Connelly
Vice President at JPMorgan Chase
Greater Boston Area | Banking
- Trisha Lowe
Mortgage Banking/Financial Services Professional
Dallas/Fort Worth Area | Banking
- F. John Deyeso, CFP, CFA
AVP, business analyst at JPMorganChase
Greater New York City Area | Financial Services
- Trung Nguyen
AVP - JPMAC External & Public Reporting
Dallas/Fort Worth Area | Real Estate
- Amogh Ranade
Vice President: Strategy & Process Improvement Team
JPMorgan
Greater New York City Area | Banking
- John D Warlow
VP, JPMorgan Chase (LI Col Ret.)
Greater Philadelphia Area | Banking
In Common: 5 shared connections 1 shared group
- Monica Oviedo
Assistant Vice President at JP Morgan Chase
Greater New York City Area | Financial Services

Right Column: One of these people viewed your profile

- Beccy Krenelka
VP, Analytics and Reporting at JPMorgan Chase
Columbus, Ohio Area | Information Technology and Services
- Stephanie Moore
AVP at JPMorganChase
Greater New York City Area | Financial Services
- Vinny Nicosia
vp at jpmchase
Greater New York City Area | Banking
- Bryan Kunath, ITIL
Application Support Manager, VP at JP Morgan Chase
Greater Chicago Area | Financial Services
- Max Robins
Vice President at JP Morgan Chase
Greater New York City Area | Financial Services
- Tanis Schmidt
Unit Manager / Vice President at Chase
San Antonio, Texas Area | Banking
- John D Warlow
VP, JPMorgan Chase (LI Col Ret.)
Greater Philadelphia Area | Banking
In Common: 5 shared connections 1 shared group
- Vickie Adkins
Vice President at JPMorgan Chase
Columbus, Ohio Area | Information Technology and Services
- Kurt Wadenpuhl
Assistant Vice President at JPMorgan Chase
Jacksonville, Florida Area | Financial Services
- LaVeeshia Pryor
Branch Manager, VP at Chase
Lexington, Kentucky Area | Financial Services

<http://www.linkedininsights.com/useful-linkedin-hack-identify-your-anonymous-browser-by-screenshot/>

RSA[®]CONFERENCE2014

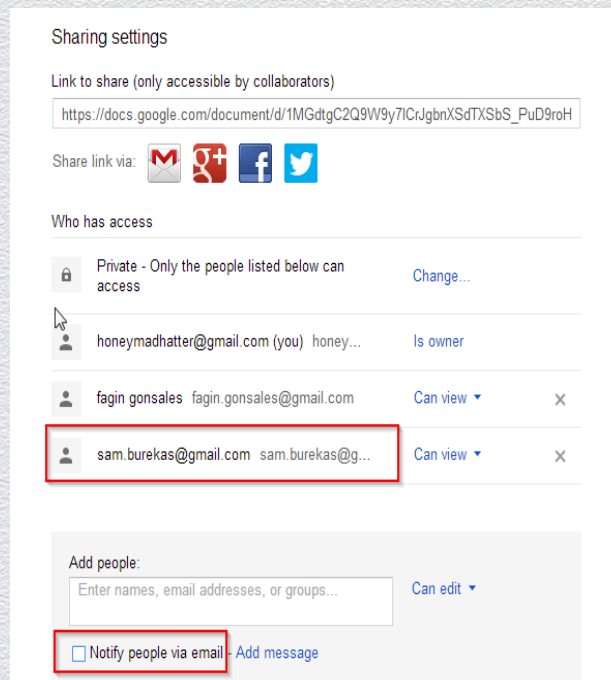
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



C U SRF in the Wild 2: Google Docs

Attack Setup: Creating a Google Doc

- ◆ Attacker (“honeymadhatter”) shares her doc with targeted account(s) (“sam.burekas”)
- ◆ Only needs to know the targets’ email
- ◆ No email is sent, as the option can be unchecked







The screenshot shows the 'Sharing settings' dialog for a Google Doc. It includes a link to share, social media sharing options, and a list of people with access. The entry for 'sam.burekas@gmail.com' is highlighted with a red box. At the bottom, the 'Notify people via email' checkbox is also highlighted with a red box and is currently unchecked.

Sharing settings

Link to share (only accessible by collaborators)

https://docs.google.com/document/d/1MGdtgC2Q9W9y7ICJgbnXSdTXSbS_PuD9roH

Share link via:    

Who has access

Access Level	People	Role	Actions
Private - Only the people listed below can access			Change...
	honeymadhatter@gmail.com (you)	honey...	Is owner
	fagin gonsales fagin.gonsales@gmail.com		Can view ×
	sam.burekas@gmail.com sam.burekas@g...		Can view ×

Add people:

[Can edit](#)

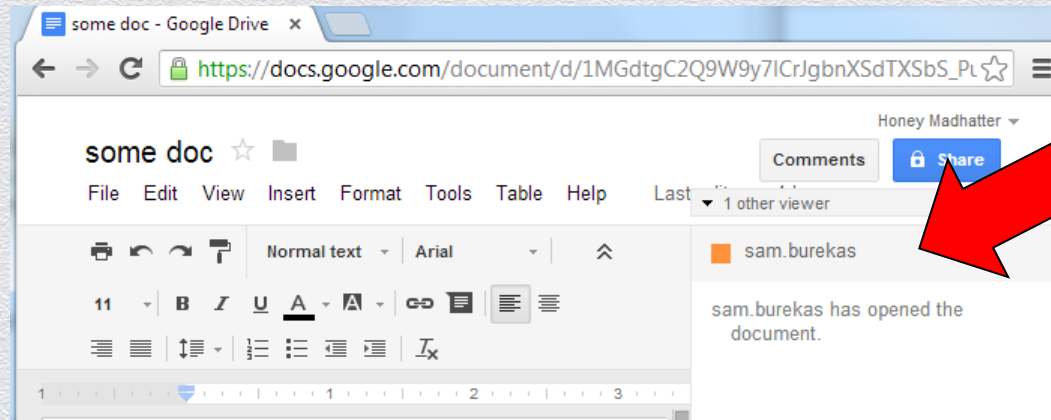
☐ Notify people via email [Add message](#)

Attack Setup: CSRF Page

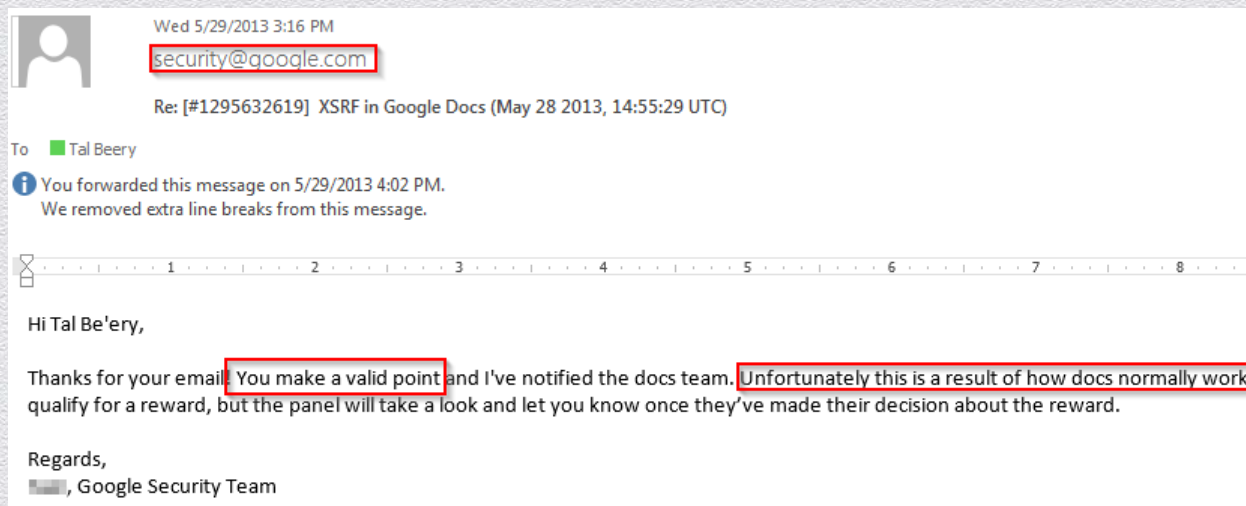
- ◆ Attacker adds an invisible CSRF link referencing to the attacker's Google Doc to their online asset
- ◆ Asset can be
 - ◆ A “watering hole” page
 - ◆ A phishing page
 - ◆ Etc.
- ◆ Invisible link example:
 - ◆ “<script src = "<https://docs.google.com/document/d/<some doc id>/edit>"></script>”

Launching the Attack

- ◆ When the intended target visits the CSRF page:
 - ◆ The attacker uncovers victim's identity (“sam.burekas”) instantly
- ◆ Can act accordingly: e.g. infect victim with malware



Google's Response



RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



Mitigations

Consumers

- ◆ Logout more!
- ◆ Use stricter privacy settings for vulnerable applications
 - ◆ Full anonymity for LinkedIn
- ◆ Use personal Anti CSRF add-ons to block cross-site requests
 - ◆ RequestPolicy
 - ◆ CsFire
 - ◆ NoScript

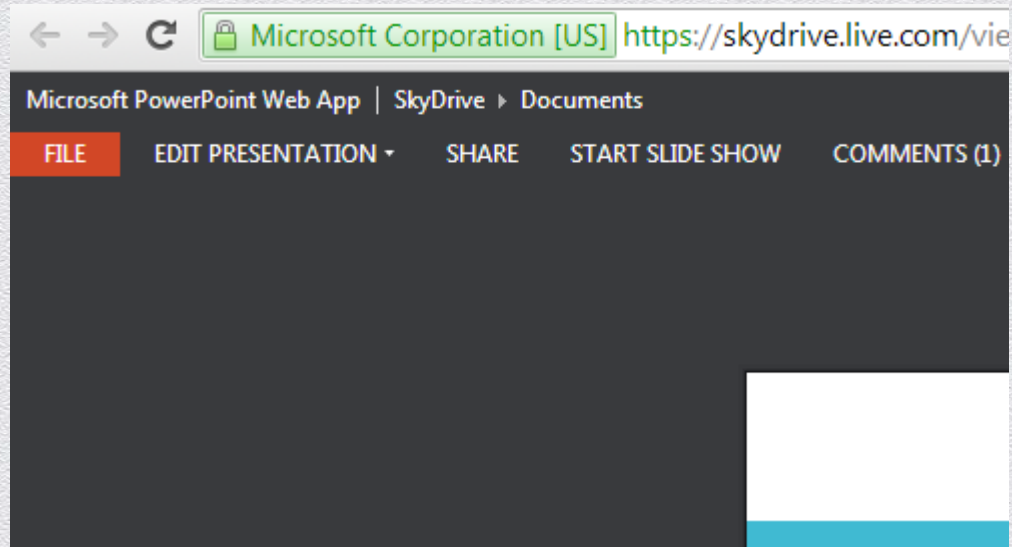
Platform Providers

- ◆ Use standard CSRF protections
 - ◆ Don't allow a collaboration based on **a single request** from **other domain**
- ◆ Other domains can be determined by HTTP headers
 - ◆ Referer
 - ◆ Origin

Platform Providers

- ◆ Single request collaboration, within same domain can be secured with a CSRF token
 - ◆ Changing, un-guessable, unique identifier appended to the request
- ◆ Libraries exist to include this functionality in the code
 - ◆ <http://anticsrf.codeplex.com/> (.NET)
 - ◆ https://www.owasp.org/index.php/Category:OWASP_CSRFGuard_Project (Java, PHP, .NET)

MS Seems to Get It Right





RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Summary & Conclusion

Summary

- ◆ CSRF vulnerabilities of various types are common within applications
- ◆ CUSRF is a new type of CSRF that affects users of collaboration platforms and applications
 - ◆ Disclosing the true identity of a victim, when accessing an attacker controlled application
- ◆ CUSRF can be used for fraud as well as “Ice Hole Phishing”

Recommendations

- ◆ Consumers
 - ◆ Review privacy settings for collaboration platforms
- ◆ Providers
 - ◆ Apply anti-CSRF mechanisms to collaboration activity

RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



**Questions?
shulman@imperva.co
m**

RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



Thank You!