RSA CONFERENCE 2014
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

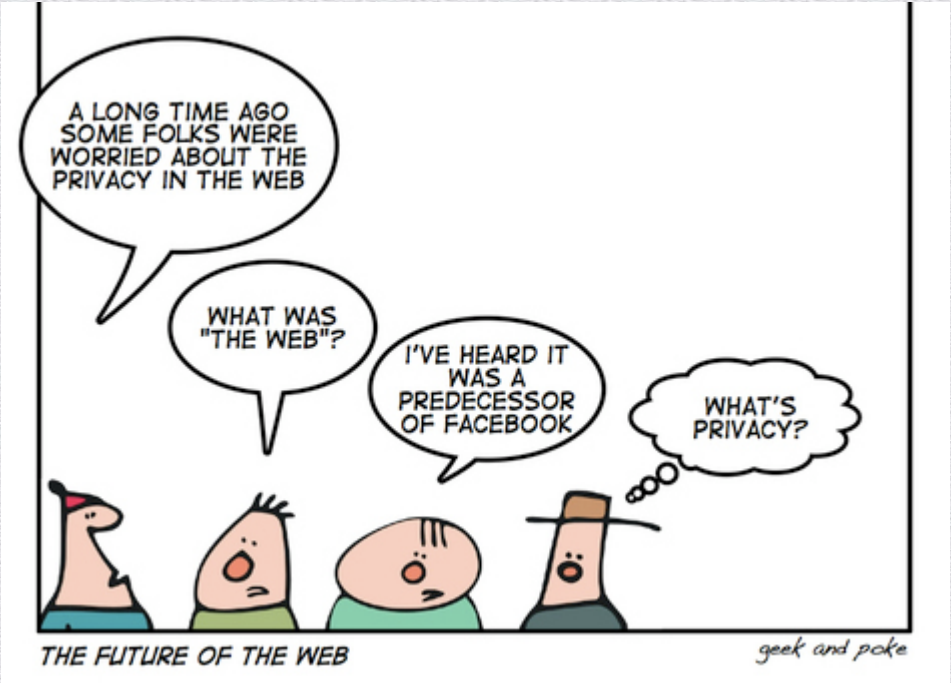
Amichai Shulman – CTO, Imperva

- 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"

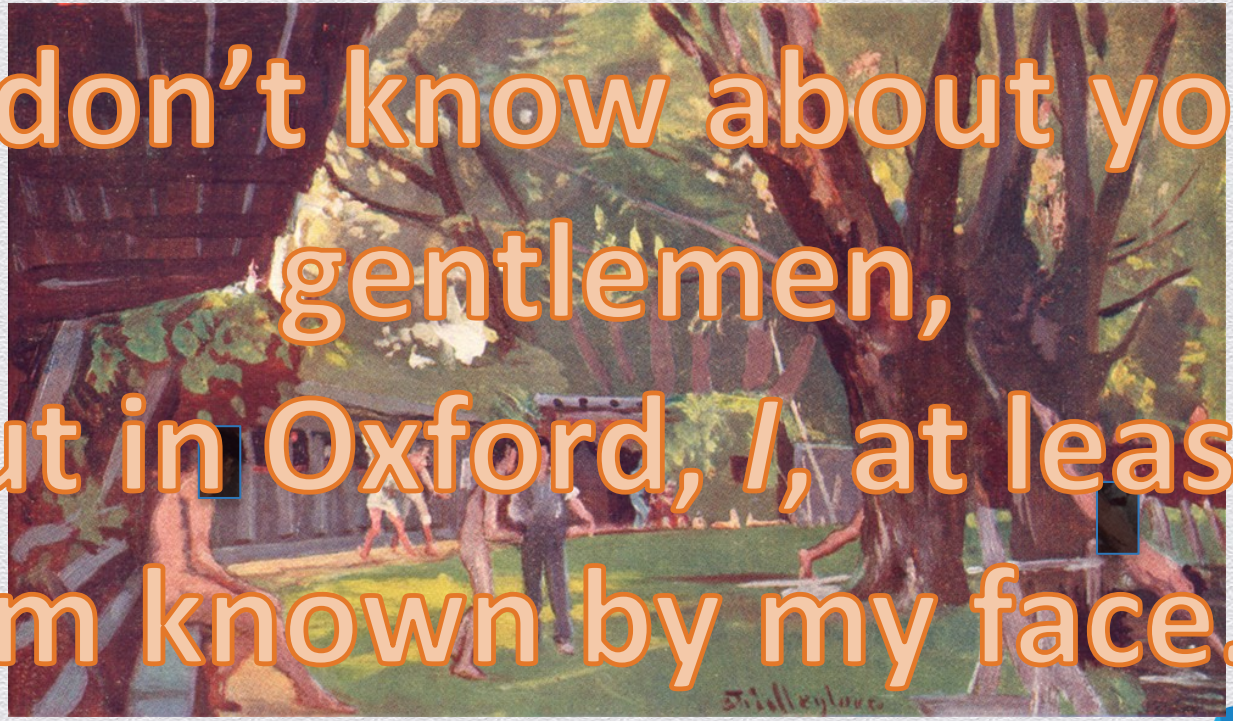
The Motivation: Protecting your ID in a Hostile Online Environment

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

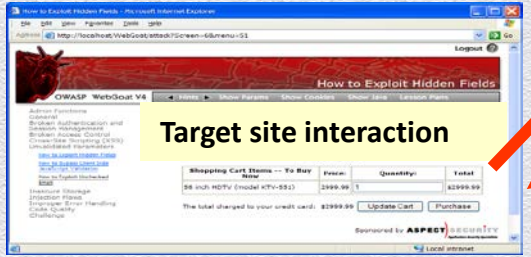
- CSRF brief intro
- C U SRF: A close encounter with CSRF of the third kind
  - C U SRF explained
  - Vulnerable applications in the wild
    - Google Docs
    - Linkedin.com
- Mitigations
- Summary and Conclusions

CSRF – Quick Intro

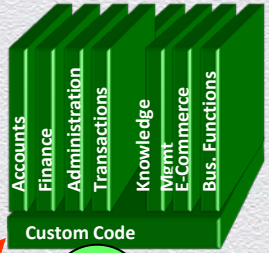
SOP Threat Model

1 Attacker sets the trap on some website on the internet

2 While logged into [illegible],
victim views atta[illegible]



Target Application



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

CSRF Illustrated: “Bypassing SOP”

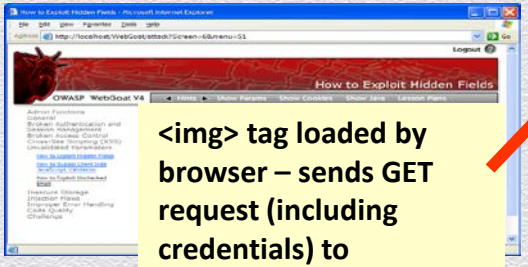
1

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

Hidden <img> tag contains attack against vulnerable site

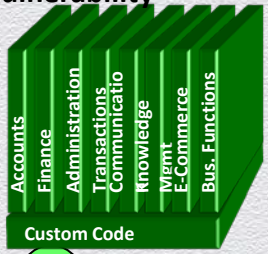
2

While logged into vulnerable site, victim views attacker site



<img> 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”

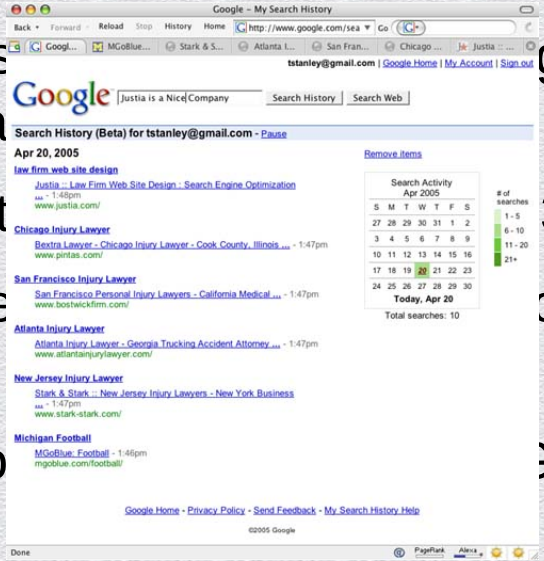
Attack Type	Used credentials	Interacts with
Classic CSRF	Victim’s	Victim’s web account

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 gs the victim into an attacker controlled a
- “signin.jsp?user=<at 3456”
- Later on, the attacke ctim’s activity in the sink account
- E.g. log the victim to Google account to collect 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

RSA CONFERENCE 2014
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

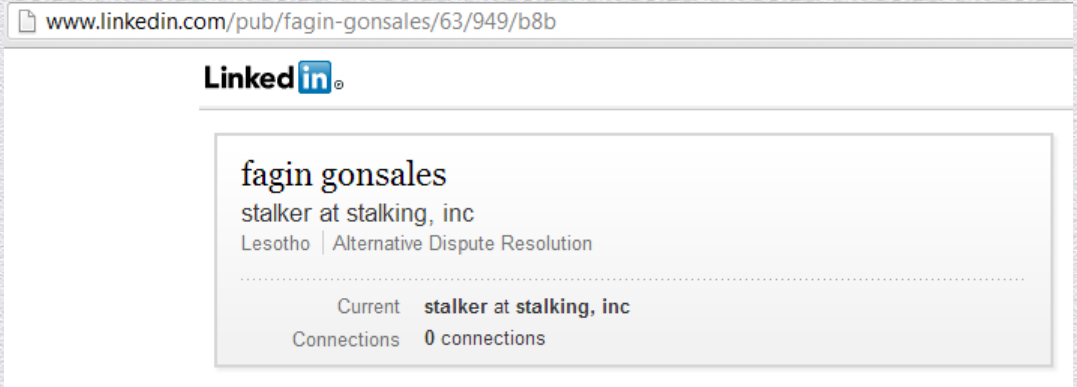
- The attacker forges collaboration requests on behalf of the victim
  - Similar to the “Classic CSRF”
- The collaboration target is located on an attacker controlled account
  - Similar to the “Login CSRF”
- Outcome: Attacker can reveal the victim’s social network identity.

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

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

Attack Setup: CSRF Page

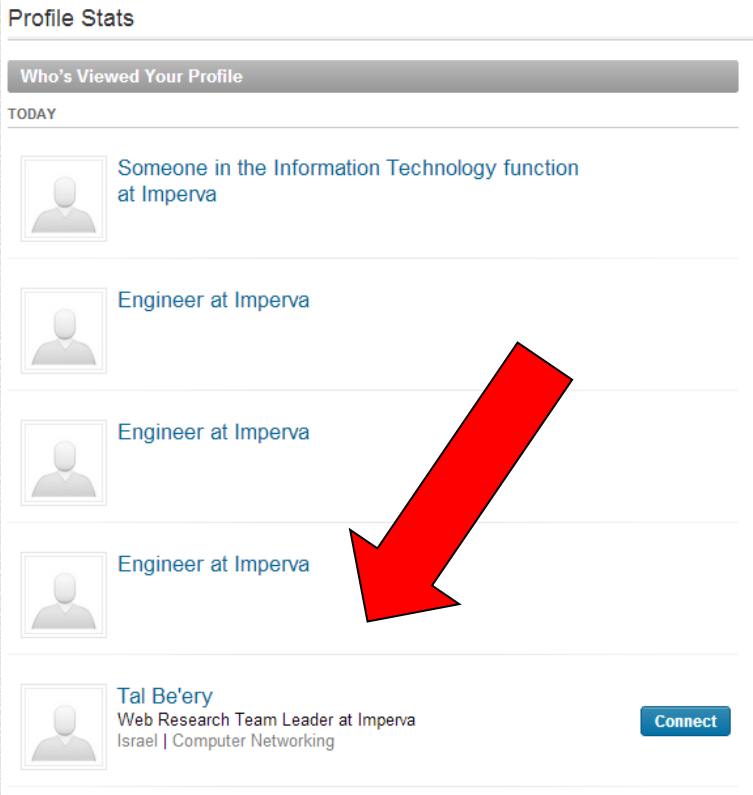
- Attacker adds an invisible CSRF link referencing the attacker's LinkedIn Profile to their online asset
- Asset can be:
  - A "watering hole" page
  - A phishing page
  - Etc.

view-source:10.1.1.190/linkedin/stalk.htm

```
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-gonsales/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

the security ledger

INTERNET OF THINGS ▾ | THREATS ▾ | PODCASTS | REPORTS | VIDEO

You are here: Home » Companies » Apple » Many Watering Holes, Targets In Hacks That Netted Facebook, Twitter and Apple

Many Watering Holes, Targets In Hacks That Netted Facebook, Twitter and Apple

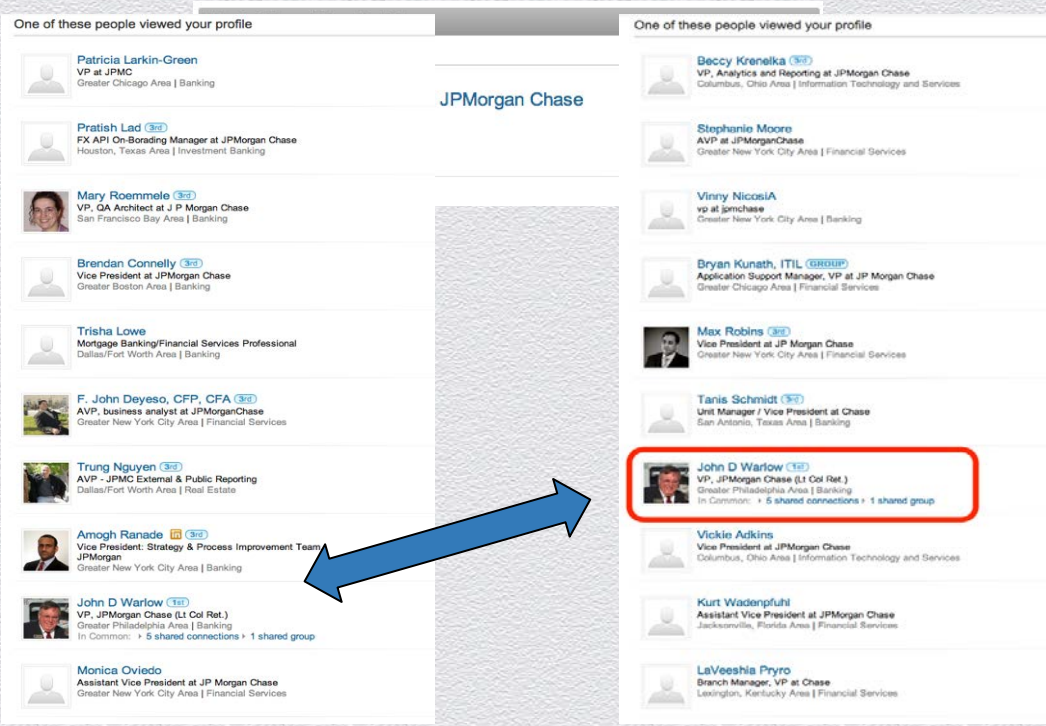
POSTED BY: PAUL ROBERTS MARCH 11, 2013 04:00 COMMENTS OFF

The attacks that compromised computer systems at Facebook, Twitter, Apple Corp. and Microsoft were part of a wide-ranging operation that relied on many “watering hole” web sites that attracted employees from prominent firms across the U.S., The Security Ledger has learned.

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

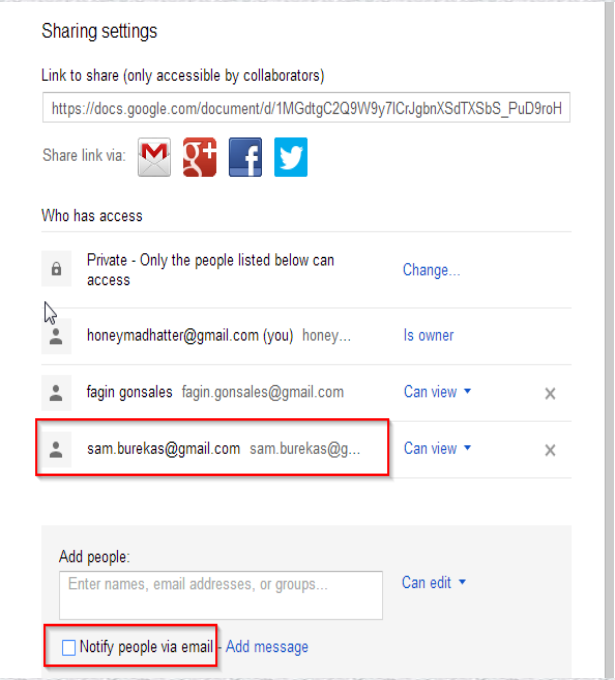


http://www.linkedinsights.com/useful-linkedin-hack-identify-your-anonymous-browser-by-screenshot/

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

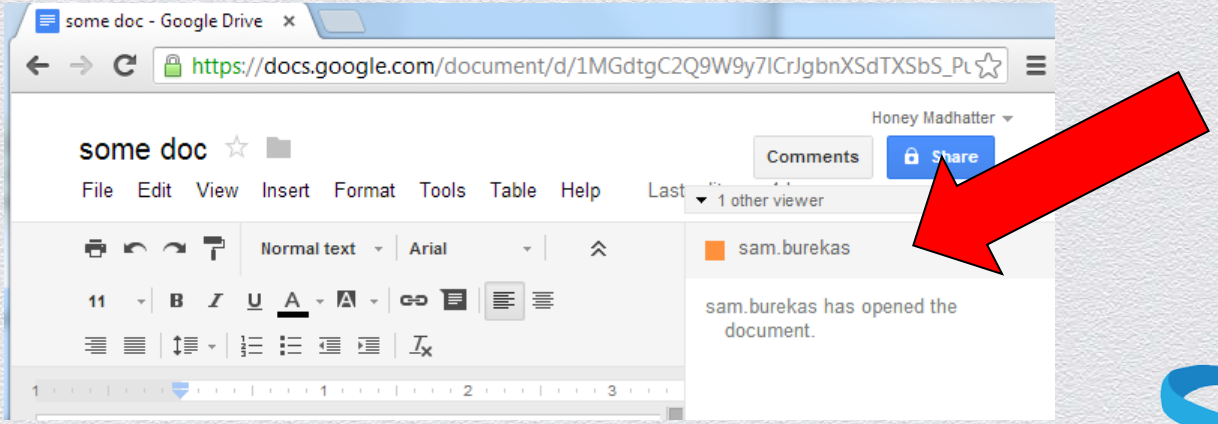


Attack Setup: CSRF Page

- 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

Wed 5/29/2013 3:16 PM

security@google.com

Re: [#1295632619] XSRF in Google Docs (May 28 2013, 14:55:29 UTC)

To Tal Beery

You forwarded this message on 5/29/2013 4:02 PM.
We removed extra line breaks from this message.

Hi Tal Be'ery,

Thanks for your email! You make a valid point and I've notified the docs team. Unfortunately this is a result of how docs normally work qualify for a reward, but the panel will take a look and let you know once they’ve made their decision about the reward.

Regards,
, Google Security Team

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

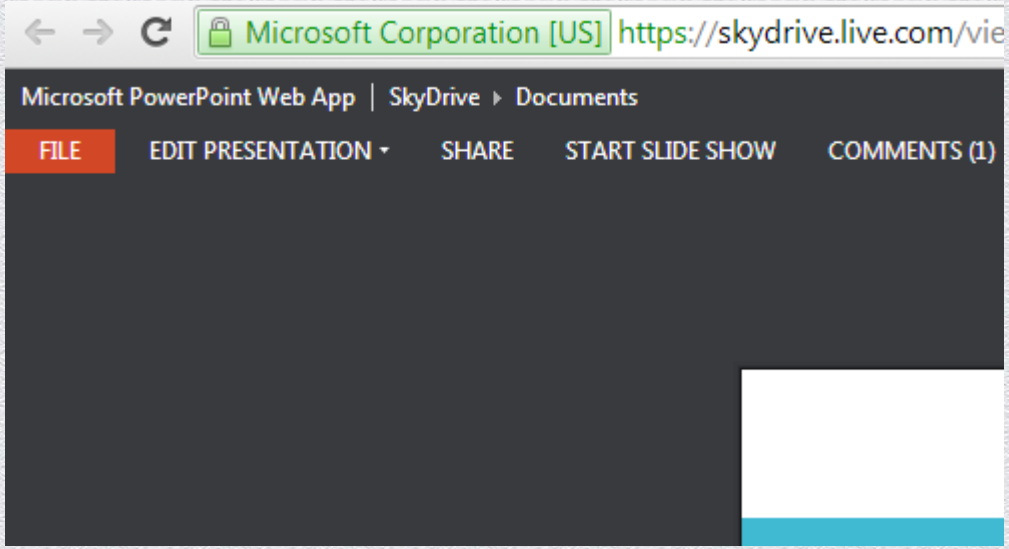
Platform Providers

- 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



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

Questions?
shulman@imperva.com

Thank You!