



MY EXPERIMENTS WITH TRUTH: A DIFFERENT ROUTE TO BUG HUNTING

DEVESH BHATT

WHO AM I?

- Hardcore Application Security enthusiast
- Enjoy reporting security bugs to organizations
- Member of n|u (null.co.in) Bangalore chapter
- Passionate Security Researcher at Adobe Systems



#deveshbhatt11



A Big Disclaimer..

"The views and opinions expressed here are my own only and in no way represent the views, positions or opinions - expressed or implied - of my employer (present and past) "

NEWS

China's culture of hacking cost the country \$873 million in 2011

PayPal Rewards Researcher with \$5,000 for Finding Remote Code Execution Flaw

Pakistani Student Gets \$500 Reward For Facebook Bug Bounty Program - [News]

PayPal plugs SQL injection hole, tosses \$3k to bug-hunter

Google ups bug bounty to \$20,000 per flaw

Mozilla Raises Bug Bounty To \$3000 For Security Bugs

Yahoo Japan says 22 million user IDs may have been stolen

Nir Goldshlager Finds XSS Vulnerability in Google And Twitter

Facebook Pays £24k To Hackers In 'Bug Bounty'

database attack

AMol NAik earned \$5000 after finding CSRF vulnerability in Facebook

Microsoft: Hackers obtained high-profile Xbox Live accounts

\$500 to Pakistani Hacker for Reporting Vulnerability

BUG BOUNTY PROGRAMS

RAVI VALDIYA PHOTOGRAPHY

Crowdsourcing security





Responsible Disclosure

REWARD PER BUG, \$\$\$, SWAGS AND T SHIRTS



Web Applications, products and even networks

RAVI VALDIYA PHOTOGRAPHY

HISTORY

2004



2010



2011



2012



The background consists of several geometric shapes. A large orange triangle occupies the right half of the image. On the left, there are two overlapping triangles: a light blue one on top and a darker blue one below it. The text is positioned in the white space between these blue triangles.

WHAT'S IN FOR THE
RESEARCHERS?

WHY DO BUG HUNTING..?



Normal
Resume



Resume with
HOF

Research and Learning

Google

facebook

twitter

PayPal

Etsy



mozilla

meraki.



Microsoft

Dropbox

Nokia Siemens
Networks



Adobe



NOKIA

avast!
be free

BARRACUDA
NETWORKS

MediaFire
File Hosting Made Simple

Instant recognition



\$\$\$\$



BENEFITS TO ORGANIZATIONS

Easy to manage





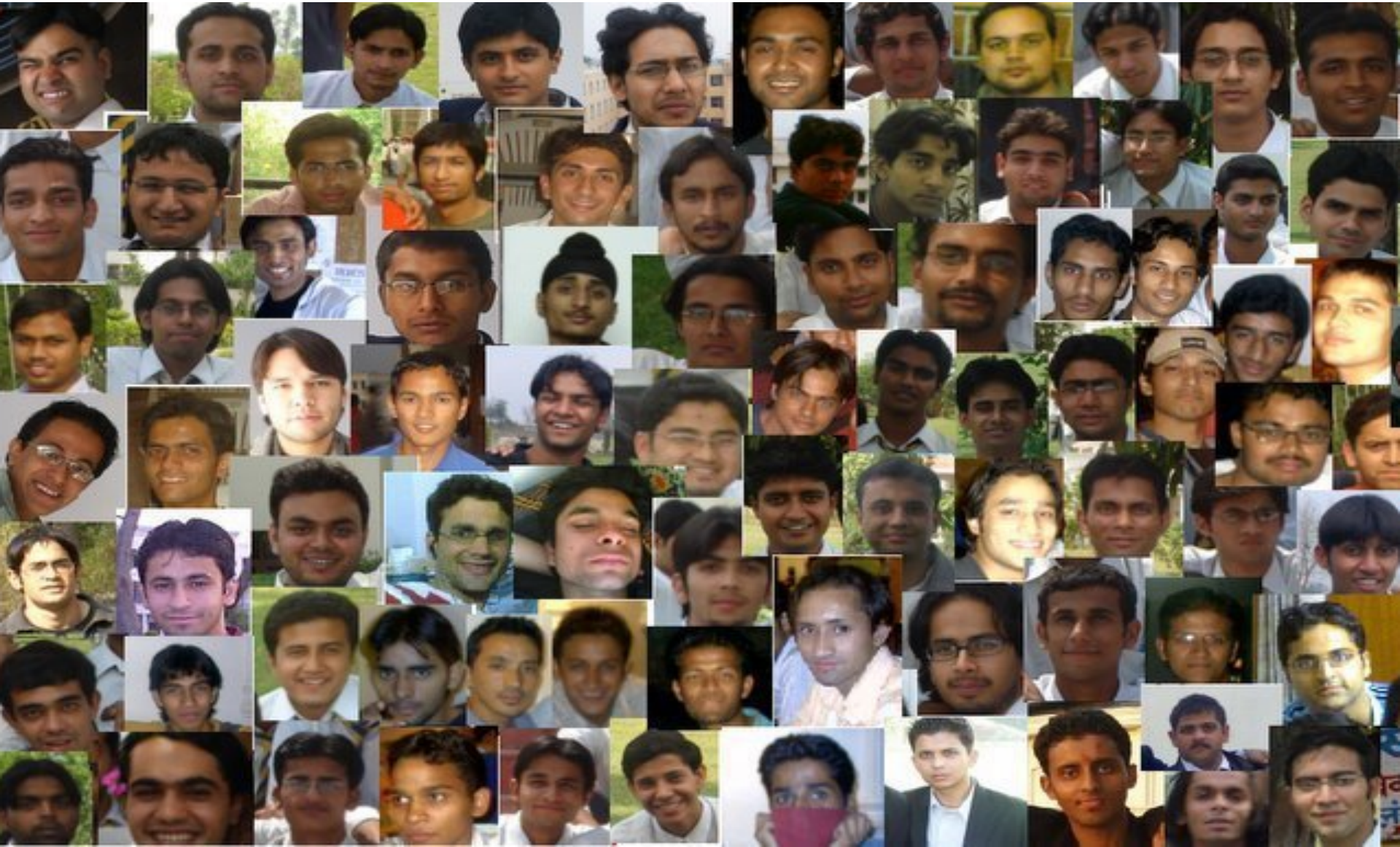
RAVI VALDTIA PHOTO

Continuous Testing

Market Your Security



Diversity in Tools, Techniques and Approach




Only Pay For Results



TRIED AND TESTED PATH

Overview

- ✓ Pick the target
 - ✓ Know the company
 - ✓ Search for the recent acquisitions
 - ✓ Less traversed sub-domains
 - ✓ Useful Information
 - ✓ Obvious Vulnerabilities
- 

Pick the target

PRODUCTS AND SERVICES (REWARD OFFERED)

BROKERS AND SECURITY COMPANIES

- Bugcrowd – <http://bgcd.co/join-th>
- Facebook – <http://www.facebook.com>
- Etsy – <http://www.etsy.com/help/>
- Google – <http://www.google.com/>
- Paypal – <https://www.paypal.com/issues>
- Mozilla – <http://www.mozilla.org/s>
- Piwik – <http://piwik.org/security/>
- Barracuda – <http://www.barracuda.com>
- Yandex – <http://company.yandex.ru>
- Gallery – <http://codex.gallery2.org>
- Qmail – <http://cr.yp.to/djbdns/guar>
- AT&T – <http://developer.att.com/detailPage.jsp?passedItemId>
need to sign up to the Developer
- Tarsnap – <https://www.tarsnap.com>
- Samsung – <https://samsungtvblog.com>
- Access – <https://www.accessnow.com>
- Avast! – <http://blog.avast.com/20>
- Hex-Rays – <http://www.hex-rays.com>
- Kaneva – <http://docs.kaneva.com>
- Mega.co.nz – <http://thenextweb.com>
- Cryptocat – <https://crypto.cat/bug>

PRODUCT AND SERVICES (HALL OF FAME ONLY)

PRODUCT AND SERVICES (HALL OF FAME + SWAG)


- HP Zero-Day Initiative (ZDI) – <http://www.zerodayinitiative.com/about/benefits/>
- Packet Storm – <http://packetstormsecurity.com/bugbounty>
- COSINC – <http://www.coseinc.com/en/index.php?rt=advisory>
- Beyond Security – <http://www.beyondsecurity.com/ssd.html>
- Exodus Intelligence – <https://www.exodusintel.com/eip/>
- iDefense – https://www.verisigninc.com/en_US/products-and-services/network-intelligence-availability/idefense/vulnerability-intelligence/index.xhtml
- White Fir Design – <https://www.whitefirdesign.com/about/wordpress-security-bug-bounty-program.html>
- Secunia – <http://secunia.com/community/research/svcrp>
- ExploitHub – <https://www.exploithub.com/request/index/developmentrequests/>
- Insight Partners – https://gvp.isightpartners.com/program_details.gvp?page=3&title=1§ion=0
- Netragard – <http://pentest.snosoft.com/netragards-eap/>

- Github – <https://help.github.com/articles/responsible-disclosure-of-security-vulnerabilities> (Reward: T-shirt and stickers)
- Engineyard – <https://www.engineyard.com/legal/responsible-disclosure-policy> (Reward: T-shirt)
- ifixit – http://www.ifixit.com/Info/Responsible_Disclosure (Reward: T-shirt)
- Dropbox – https://www.dropbox.com/special_thanks (Reward: T-shirt)
- Soundcloud – <http://help.soundcloud.com/customer/portal/articles/439715-responsible-disclosure> (Reward: T-shirt)
- Amazon – aws.amazon.com/security/vulnerability-reporting (Reward: T-shirt)

curity
-T1318
om/en-us/security/cc308589
/knowledge/articles/66234
n/dev/hall-of-fame
'security/disclosure
ecurity/whitehats
ex.php/Contributors#Security_Researchers
w-report-security-issue
ort_security.php
.it/security/hall-of-fame/
w.nokiasiemensnetworks.com/about-

m/security/
'security/acknowledgements/
tycenter/ResearchersAcknowledgement.html
m/devblog.asp?a=blog&nbid=2384
d.com/legal/responsible-disclosure-policy
'node/6657#gsc.tab=0
v/business/topics/security/incident-response-

Overview


- ✓ Pick the target
 - ✓ Know the company
 - ✓ Search for the recent acquisitions
 - ✓ Less traversed sub-domains
 - ✓ Useful Information
 - ✓ Obvious Vulnerabilities
- 

A man in a dark jacket and beanie holds a yellow sign on a busy city street. The street is decorated with large, ornate Christmas lights hanging over the road. Pedestrians are visible in the foreground, and a white van is parked in the background. The scene is set in a city with multi-story buildings and shops like 'Hickey's Pharmacy' and 'meteok' visible.

IRISH FORTUNE TELLERS
KAY x MARIE SEEN ON TV^{HEARD OR RADIO}
HANDS CARDS
CRYSTAL BALL x TEACUP
NO APP NEEDED READINGS

Know the Company


Overview

- ✓ Pick the target
 - ✓ Know the company
 - ✓ Search for the recent acquisitions
 - ✓ Less traversed sub-domains
 - ✓ Useful Information
 - ✓ Obvious Vulnerabilities
- 



Search for the recent acquisitions


Overview

- ✓ Pick the target
 - ✓ Know the company
 - ✓ Search for the recent acquisitions
 - ✓ Less traversed sub-domains
 - ✓ Useful Information
 - ✓ Obvious Vulnerabilities
- 

Less traversed sub-domains



Overview

- ✓ Pick the target
 - ✓ Know the company
 - ✓ Search for the recent acquisitions
 - ✓ Less traversed sub-domains
 - ✓ Useful Information
 - ✓ Obvious Vulnerabilities
- 

Useful Information

- Directory Indexing

- Site:xyz.com intitle:index.of

- Critical Files


- Site:xyz.com filetype:txt(xml,pdf)

- Admin Interface


- Site:xyz.com inurl:admin



Overview

- ✓ Pick the target
 - ✓ Know the company
 - ✓ Search for the recent acquisitions
 - ✓ Less traversed sub-domains
 - ✓ Useful Information
 - ✓ Obvious Vulnerabilities
- 

Obvious Vulnerabilities

- Default usernames/password
 - Sensitive information disclosure
 - Admin interfaces
 - XSS
 - Account enumeration
 - Clickjacking
- 

Google: Default

- List of mergers and Acquisitions

Invitemedia.com interesting!!

Site: invitemedia.com --www

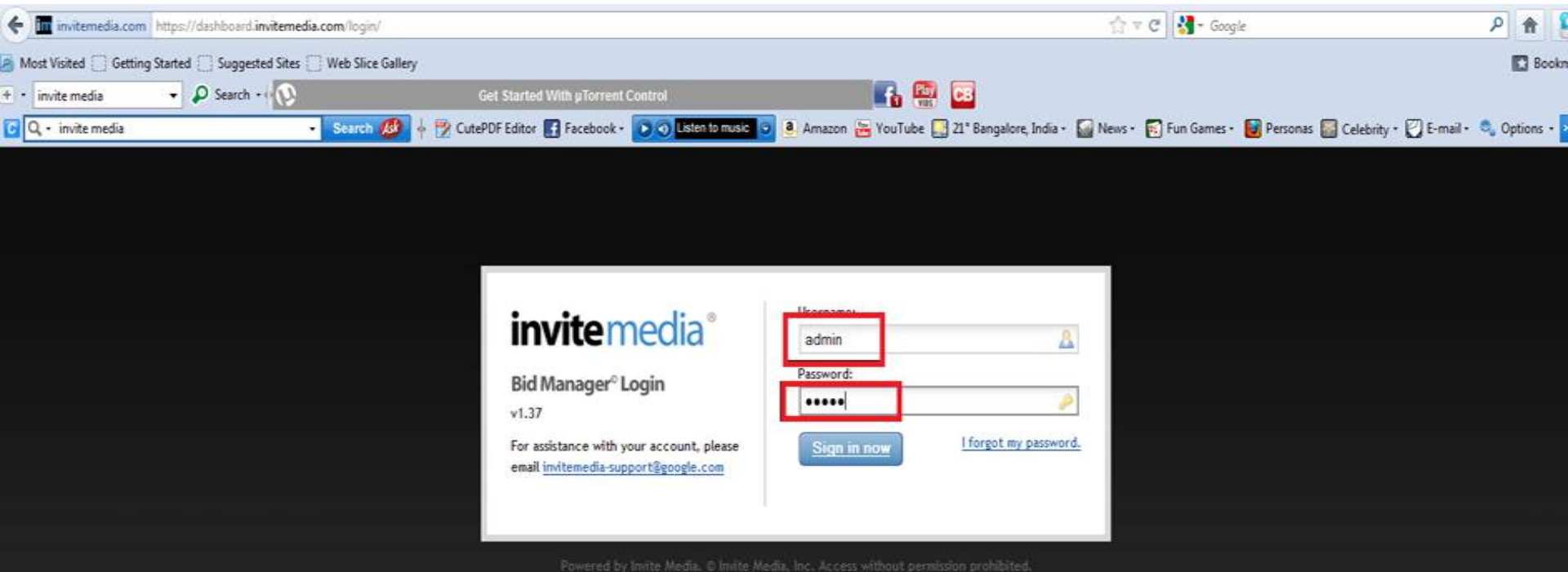
- After every search result , I excluded that search result using a minus “-” operator till I got the interesting looking URL

<https://dashborad.invitemedia.com/login>

“Bid Manager login”

Google: Default (Cont'd)

- Bypass login, SQL Injection??
- Proper input validation and parameterized queries as expected



Google: Default (Cont'd)

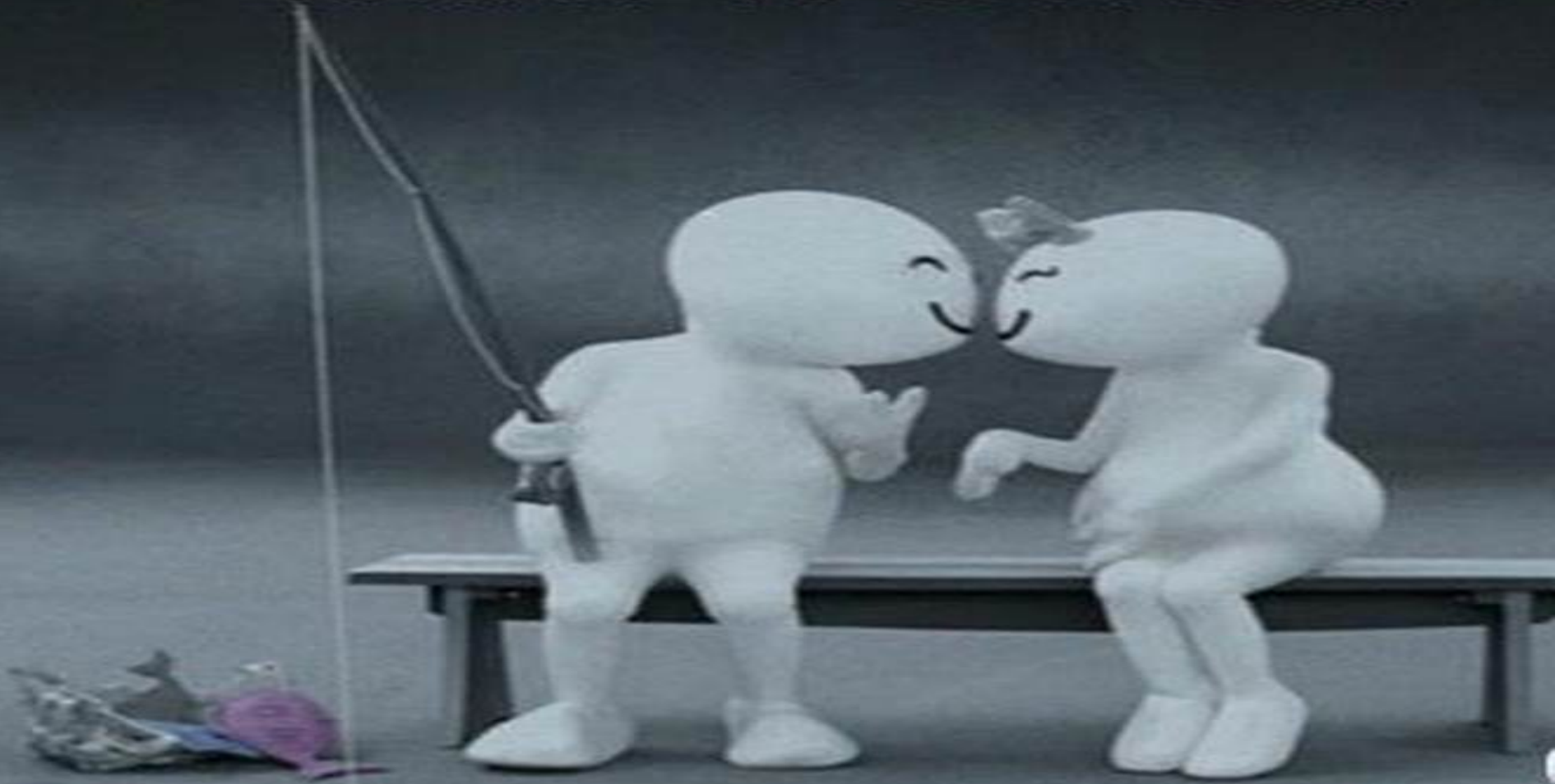
- Logged in using the default credentials

The screenshot shows a web browser window with the URL `https://dashboard.invitemedias.com/publishers/` in the address bar. The browser's toolbar includes a search bar with the text "invite media" and various icons for social media and services. Below the browser window, the dashboard interface is visible, featuring a navigation bar with tabs for Dashboard, Advertisers, Publishers, Reporting, Graphing, Inventory Availability, Tools, and Data. The "Publishers" tab is selected, and the page title is "Publishers". A "Create a New Publisher" button is located at the top left of the main content area. Below this button is a table with the following columns: ID, Actions, Name, and Impressions. The table contains several rows of publisher data, with the first six rows highlighted by a red box. The data in the table is as follows:

ID	Actions	Name	Impressions
452		411	
29		Adb	
448		Adc	
34920		AK	
42114		Aley	
32		Anc	
152		Brav	
25		Bur	
27		Bur	
5410		Can	
41		CNe	

Google: Default (Cont'd)

WHAT A CATCH!



REWARD!!

 **Google Security Team** <security@google.com>

7/11/12 ☆


to me ▾

Hello,

Congratulations! This vulnerability is eligible for a reward of \$500.

www.google.co.in/about/appsecurity/hall-of-fame/reward/			☆ ▾ ↻	goodie hall of fame	🔍 🏠 🖨 ⚙
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options					
Q4 2012	Eric "Cosmo" Taylor	@CosmoTheGod			
Q4 2012	Josip Franjkovic - RIT/ACMT	http://dc-studio.net			
Q4 2012	Mohamed Ramadan	Attack-Secure			
Q4 2012	Kamil Sevi	@kamilsevi			
Q4 2012	Bharadwaj Machiraju - HACK UR LIFE	www.tunnelshade.in			
Q4 2012	Martin Obiols	http://makensi.es			
Q3 2012	Daniel Cocking & Glenn Mangham	http://gmangham.blogspot.co.uk/			
Q3 2012	Jason Calvert	http://appsec.ws/			
Q3 2012	Devesh Bhatt				
Q3 2012	Michele Spagnuolo	http://michele.spagnuolo.me			
Q3 2012	Amir Etemadieh	@Zenofex			
Q3 2012	Shai Rod	@NightRang3r			
Q3 2012	Sam "truenui" Jay	http://truenui.blogspot.com			
Q3 2012	Andris Aftoka	Blue Coat Systems			
Q3 2012	Saket Jajodia	Dzire 2 Dzine (D2D): Logo Designing Graphic Designing 3D Modeling Animation			
Q3 2012	Takeshi Terada	Mitsui Bussan Secure Directions, Inc.			
Q3 2012	Riyaz Walikar	http://www.riyazwalikar.com			
Q3 2012	Eyvind Niklasson	http://eyvindniklasson.se/			
Q3 2012	Dmitriy Shcherbatov	http://vk.com/id133353396			
Q3 2012	João Lucas Melo Brasio	White Hat Hackers Consultoria de Segurança da Informação LTDA (Brazil)			
Q3 2012	Masato Kinugawa				
Q3 2012	Nils Juenemann	http://www.nilsjuenemann.de/			
Q3 2012	Sergey Markov				

Obvious Vulnerabilities

- Default usernames/password
 - Sensitive information disclosure
 - Admin interfaces
 - XSS
 - Account enumeration
 - Clickjacking
- 

PayPal:PII

Site:secure.paypal.com inurl:.com

Google

devesh bhatt 0 + Share

Web Images Maps More ▾ Search tools

No results found for **site:secure.paypal.com inurl:.com**.

Results for [site secure paypal com inurl com](#) (without punctuation - [Learn more](#)):

[Make payments with PayPal - it's fast, free and](#)
<https://secure.paypal.com/affil/pal/sales@seasonsla.com>
A description for this result is not available because of this site's robots.txt – learn more.

[Use PayPal.com for auction payments. Fast free](#)
<https://secure.paypal.com/affil/pal/info@yutopian.com>
A description for this result is not available because of this site's robots.txt – learn more.

[tip jar - PayPal](#)
<https://secure.paypal.com/affil/pal/paypal@bmezine.com>
A description for this result is not available because of this site's robots.txt – learn more.

<https://secure.paypal.com/affil/pal=okuth0r@yahoo.com>
A description for this result is not available because of this site's robots.txt – learn more.

<https://secure.paypal.com/affil/pal-thomash@throne...>
A description for this result is not available because of this site's robots.txt – learn more.

Information Disclosure Channel Intelligence



System Error

A system error has occurred.

If this problem persists - please notify your JIRA administrator of this problem.

Otherwise, please create a support issue on our **support system** at <http://support.atlassian.com> with the following information:

1. a description of your problem
2. cut & paste the error and system information found below
3. attach the application server log file (/usr/local/atlassian-jira-enterprise-3.13-standalone/atlassian-jira.log)


Cause:

java.lang.NullPointerException

Stack Trace: [\[hide\]](#)

```
java.lang.NullPointerException
    at com.atlassian.core.user.UserUtils.resetPassword(UserUtils.java:310)
    at com.atlassian.jira.web.action.user.ForgotPassword.doPassword(ForgotPassword.java:29)
    at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
    at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:39)
    at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:25)
    at java.lang.reflect.Method.invoke(Method.java:597)
    at webwork.util.InjectionUtils$DefaultInjectionImpl.invoke(InjectionUtils.java:61)
    at webwork.util.InjectionUtils.invoke(InjectionUtils.java:52)
    at webwork.action.ActionSupport.invokeCommand(ActionSupport.java:417)
    at webwork.action.ActionSupport.execute(ActionSupport.java:146)
    at com.atlassian.jira.action.JiraActionSupport.execute(JiraActionSupport.java:54)
    at webwork.dispatcher.GenericDispatcher.executeAction(GenericDispatcher.java:132)
    at com.atlassian.jira.web.dispatcher.JiraServletDispatcher.service(JiraServletDispatcher.java:178)
    at javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
    at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:269)
    at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:188)
    at com.atlassian.jira.web.filters.AccessLogFilter.doFilter(AccessLogFilter.java:51)
    at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:215)
    at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:188)
    at com.opensymphony.module.sitemesh.filter.PageFilter.parsePage(PageFilter.java:119)
    at com.opensymphony.module.sitemesh.filter.PageFilter.doFilter(PageFilter.java:55)
    at com.atlassian.jira.web.filters.SitemeshExcludePathFilter.doFilter(SitemeshExcludePathFilter.java:38)
    at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:215)
    at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:188)
    at com.atlassian.seraph.filter.SecurityFilter.doFilter(SecurityFilter.java:192)
    at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:215)
    at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:188)
    at com.atlassian.seraph.filter.TrustedApplicationsFilter.doFilter(TrustedApplicationsFilter.java:120)
    at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:215)
```

Obvious Vulnerabilities

- Default usernames/password
 - Sensitive information disclosure
 - Admin interfaces
 - XSS
 - Account enumeration
 - Clickjacking
- 

Apple: Admin


Site:apple.com inurl:admin

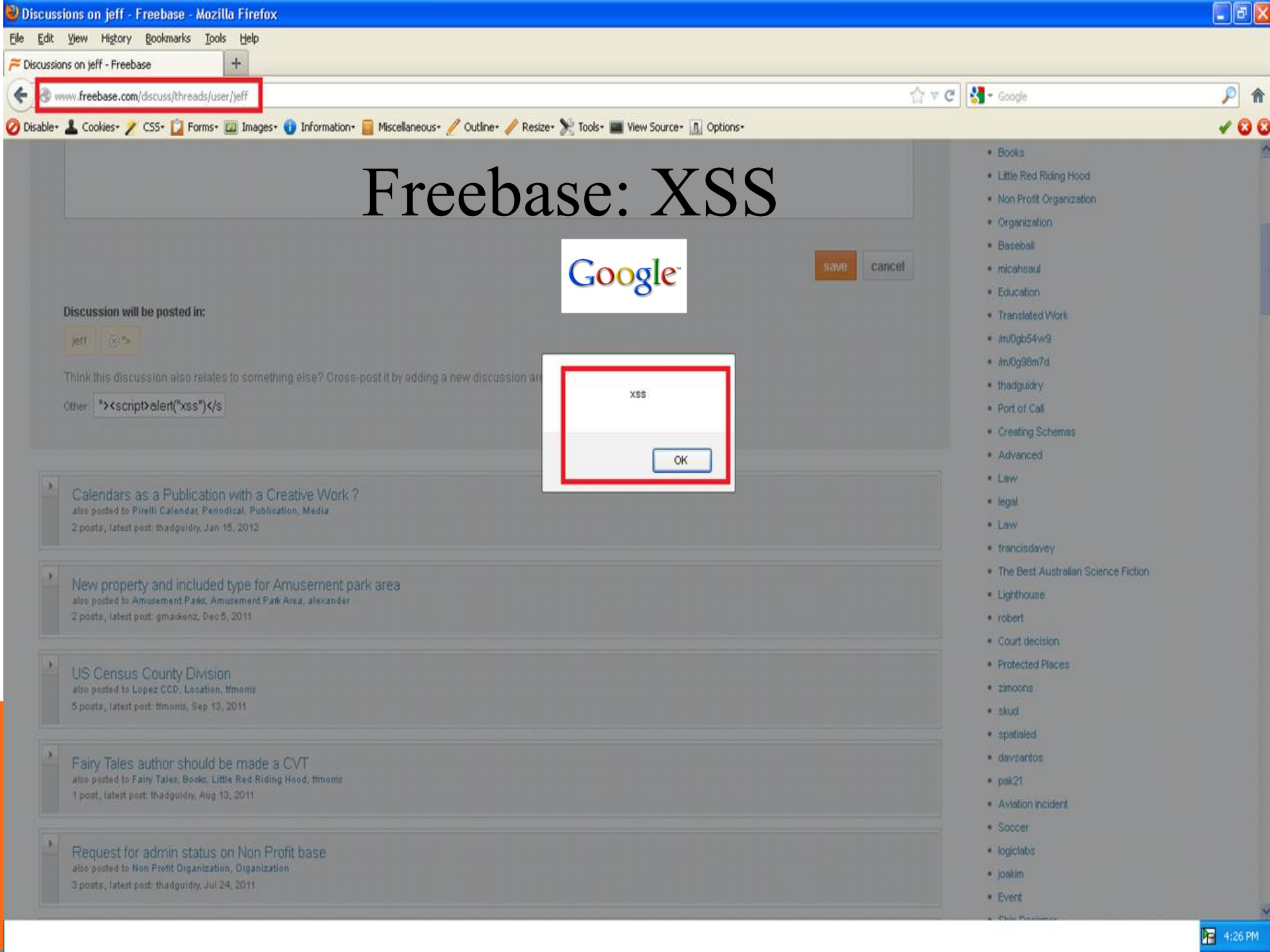


Username: Password:

The login details you provided were invalid. Did you [forget your password?](#)

Obvious Vulnerabilities

- Default usernames/password
 - Sensitive information disclosure
 - Admin interfaces
 - XSS
 - Account enumeration
 - Clickjacking
- 



Integration demo: confirmation

Redirect Url:

url https://pay01.zong.com/zongpay/test/confirmation.jsp

Params:

key	value
merchantNotified	test



Zong.com: XSS



ZAGAT

LISTS VOTE DEALS & EVENTS STORE MOBILE BLOG ZAGAT WINE

Zagat.com:XSS

XSS

OK

Google

What are you looking for? (restaurant, bar, etc.)

Advanced Search

NEW YORK CITY BLOG »



Zagat Pizza Survey Results Are Live!

1 week 1 hour ago

The 8 Best Pizza Shops in NYC

1 week 1 hour ago

Your Guide to Regional Pizza Styles

1 week 1 hour ago

INTI

some exciting news.

Read on...

XSS Channel Intelligence



https://reports.channelintelligence.com/Login/Login.asp



Username:

`';alert(String.fromCharCode(0x2014'))>`

XSS

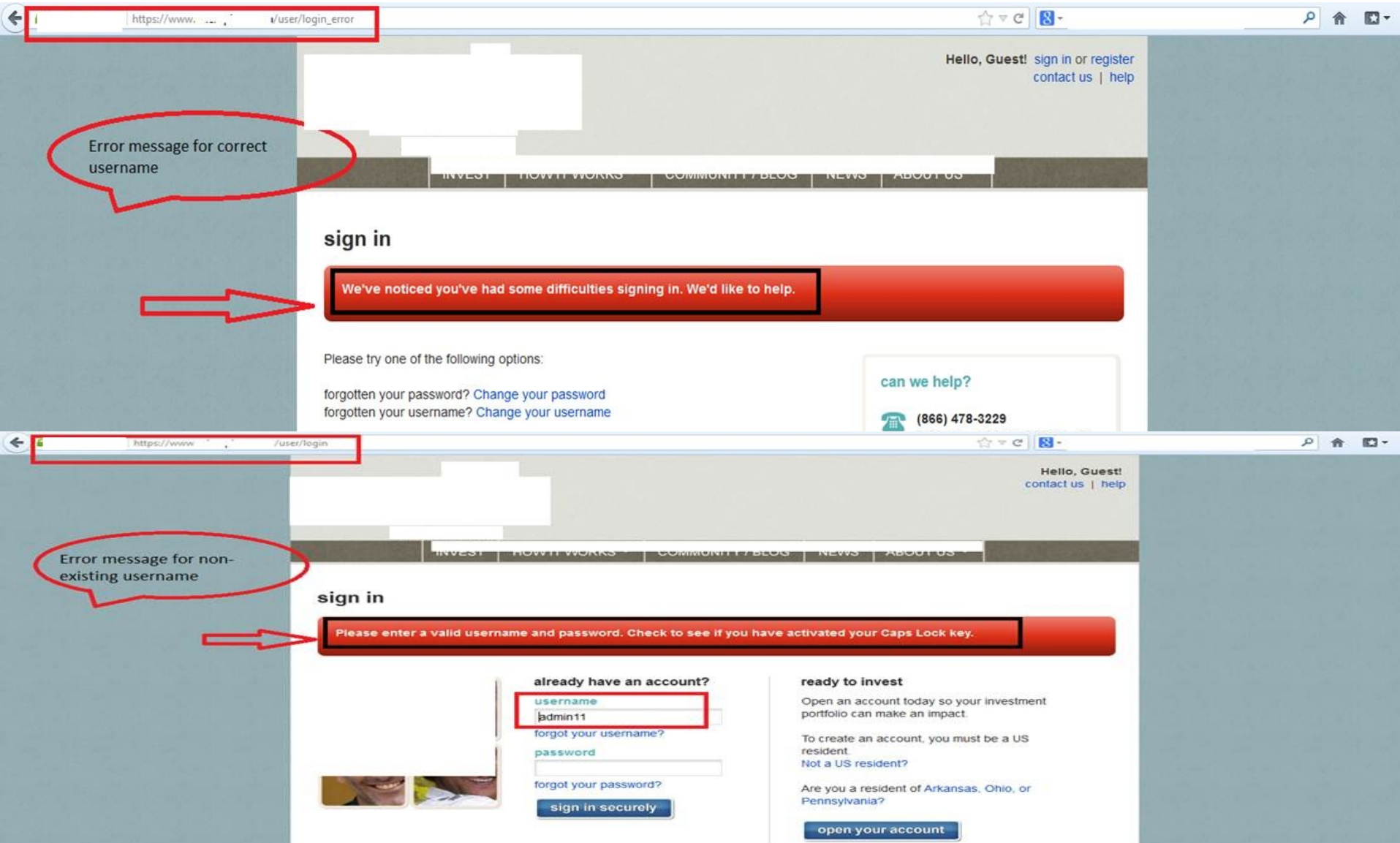
OK

h4bsi3gtmydbe4p41j1mqufsur6", "name": "shared_secret": "cqaKwo6vjJINYSq5uA7kxNrEY+2YqcWfWrWfWbGAgda=", "e54x0ndgi7nc3r4eagvssx72q0p": {"token":

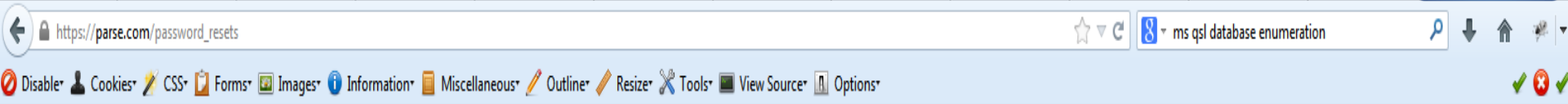
Obvious Vulnerabilities

- Default usernames/password
 - Sensitive information disclosure
 - Admin interfaces
 - XSS
-
- Account enumeration
-
- Clickjacking

Account Enumeration



Enumeration Parse.com



You're invited: The Making of the Sesame Street Apps with IDEO and Parse [Register Now](#)

Parse

[Products](#)

[Customers](#)

[Pricing](#)

[Docs](#)

[Help](#)

[Blog](#)

[Sign Up](#)

[Log In](#)

We're hiring

No user was found with that email address

Forgot Password

Enter your email below and instructions to reset your password will be emailed to you:

Email:

[Reset My Password](#)

[Parse](#)

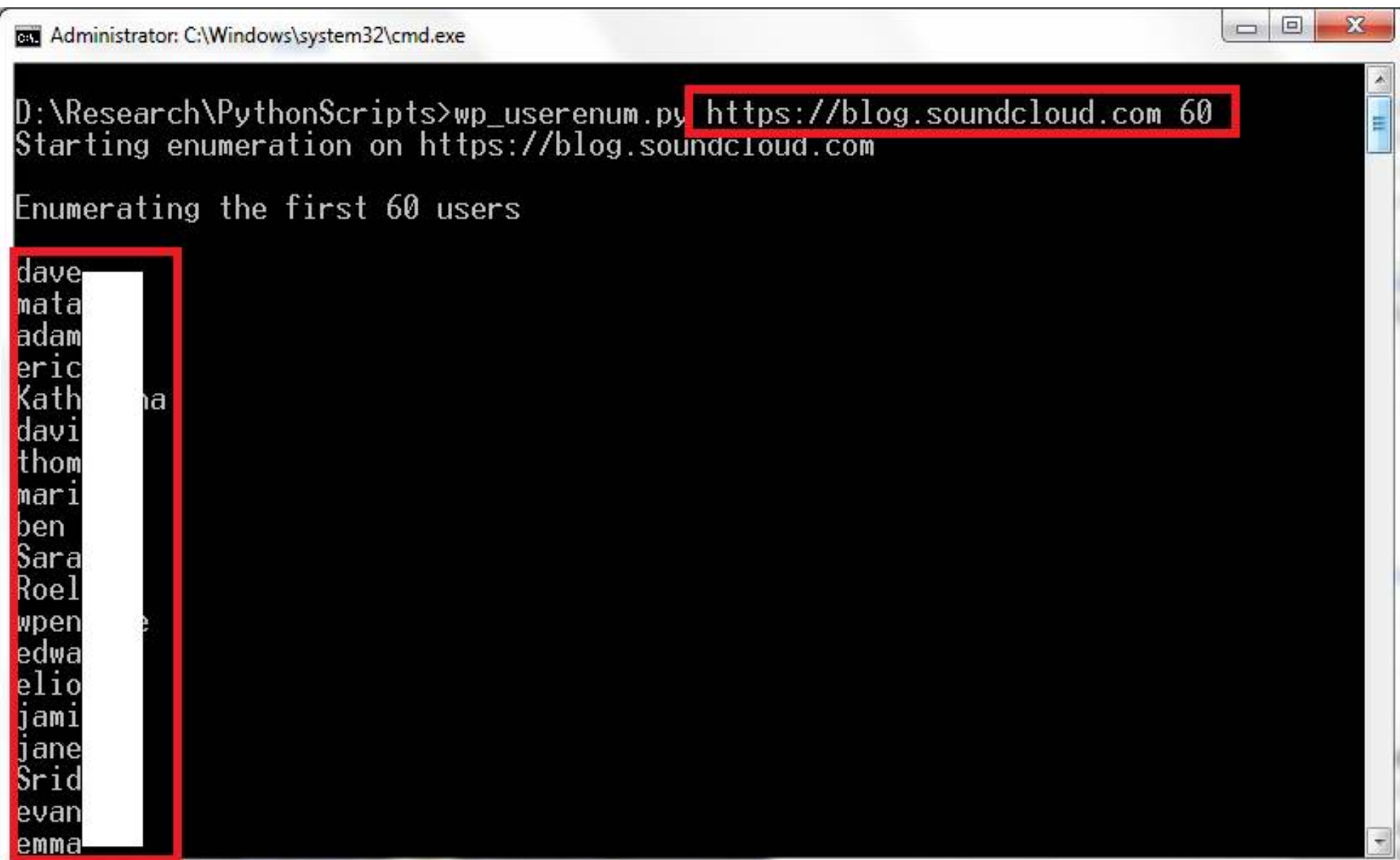
[Products](#)

[Customers](#)

[Docs](#)

[Help](#)

Soundcloud: enumeration via a "/?author=x" redirection



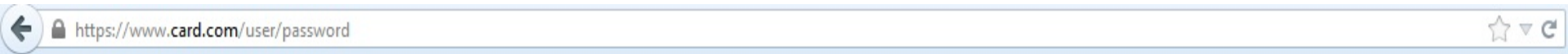
The screenshot shows a Windows command prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The command prompt displays the following text:

```
D:\Research\PythonScripts>wp_userenum.py https://blog.soundcloud.com 60
Starting enumeration on https://blog.soundcloud.com
Enumerating the first 60 users
```

The command `wp_userenum.py https://blog.soundcloud.com 60` is highlighted with a red box. Below the command, a list of names is displayed, with the first 15 names (dave, mata, adam, eric, Kath, davi, thom, mari, ben, Sara, Roel, wpen, edwa, elio, jami) highlighted by a red box. The list continues with jane, Srid, evan, and emma.

Name
dave
mata
adam
eric
Kath
davi
thom
mari
ben
Sara
Roel
wpen
edwa
elio
jami
jane
Srid
evan
emma

Enumeration card.com



CARD.com

[how it works](#)

[about](#)

[load](#)

[login](#)

[view card](#)

 Sorry, *deveshbhatt11@gmail.com* is not recognized as a user name or an e-mail address.

User account

Your email *

deveshbhatt11@gmail.com

A password reset message will be sent to your email address.

Email



Enumeration Nokia

The screenshot shows a web browser window with the address bar containing `https://inventwithnokia.nokia.com/login`. The page has a blue header with the breadcrumb `Home > My Account`. The main content area is white and contains a **Login** section with the instruction "Please enter your login details below to submit a new invention." Below this is a login form with a red border. The email input field contains the text "No active user found with that email address" and is highlighted with a black box. Below the login form is a **Reset Your Password** section with the instruction "Instructions for resetting your password will be sent to you by email. Enter your email address." Below this is a password reset form with a red border. The email input field contains the text "dds@dSD.com" and is highlighted with a black box. At the bottom, there is a link "Not Registered? Click here to register." and a green button labeled "Reset my password".

← `https://inventwithnokia.nokia.com/login` ☆ ▼ C 8

Home > My Account

Login

Please enter your login details below to submit a new invention.

No active user found with that email address

Reset Your Password

Instructions for resetting your password will be sent to you by email. Enter your email address.

dds@dSD.com

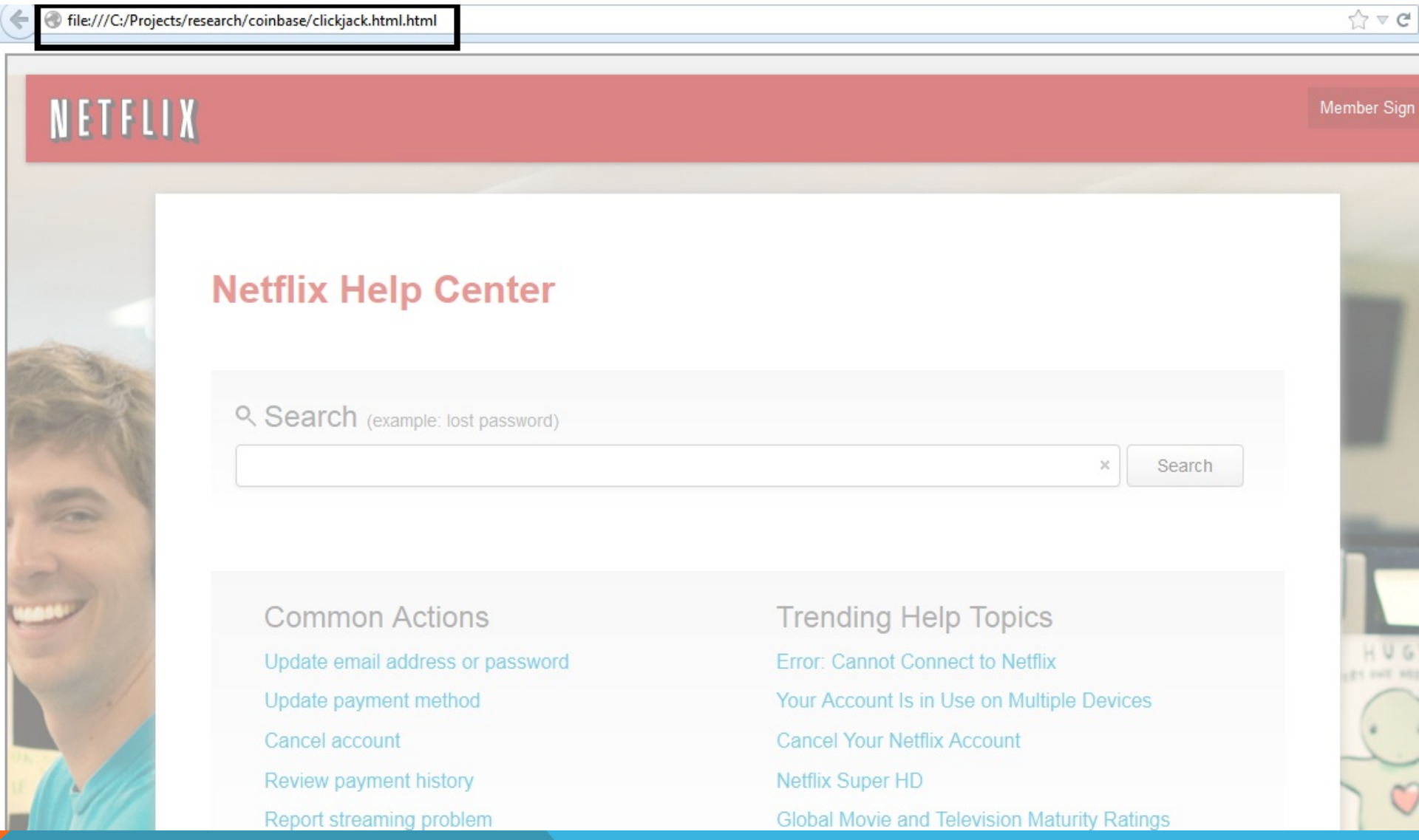
Not Registered? [Click here to register.](#)

Reset my password

Obvious Vulnerabilities

- Default usernames/password
 - Sensitive information disclosure
 - Admin interfaces
 - XSS
 - Account enumeration
-
- Clickjacking

UI Redressal/Clickjacking in Netflix



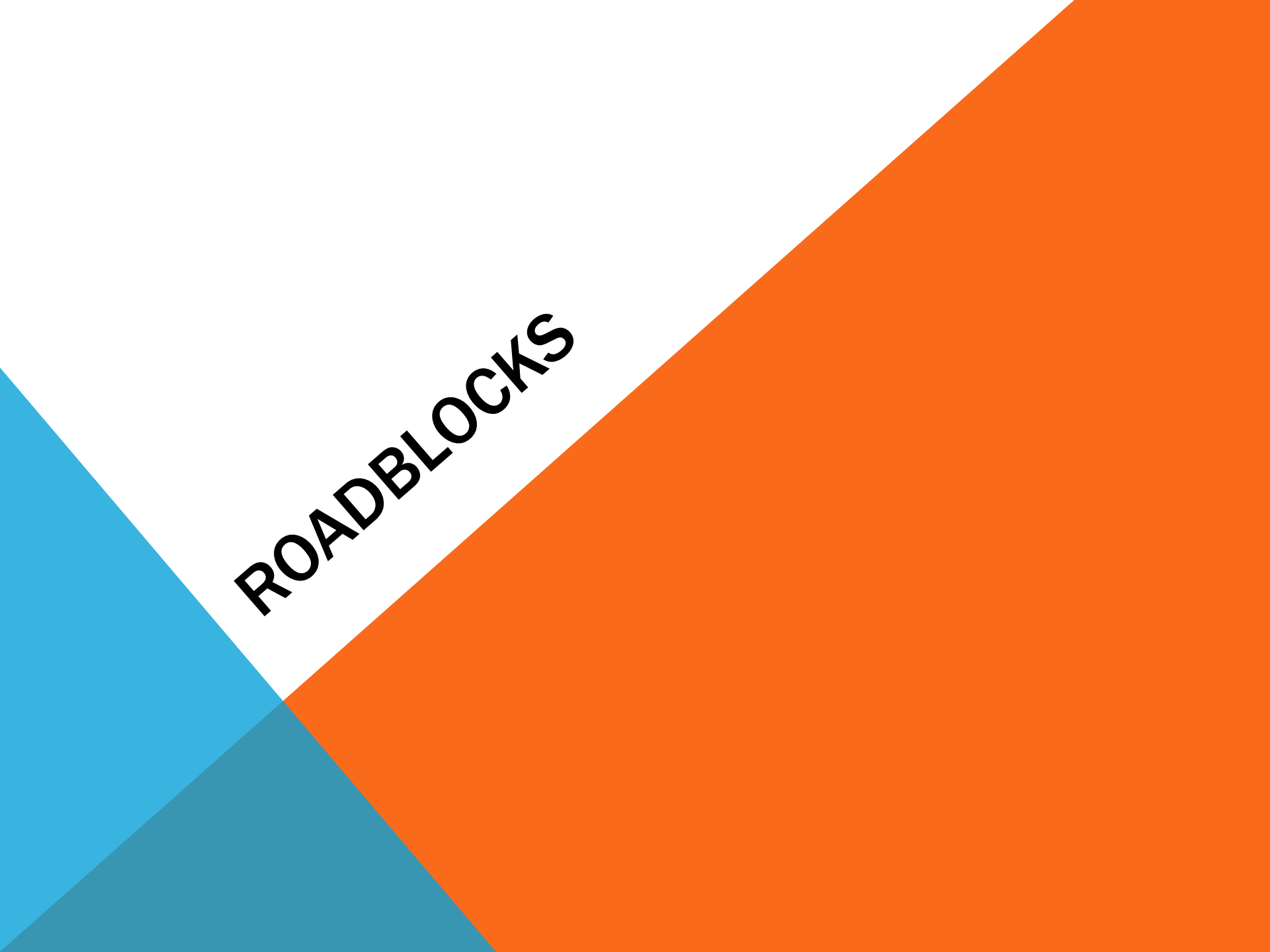
STORY SO FAR

- Facebook has paid out \$1 Million to security researchers
- Almost 70% of valid bugs are XSS
- 44% percent of all bugs are the first and only bug sent by a researcher



ARE COMPANIES WITH
BOUNTY MORE SECURE?





ROADBLOCKS

Cross border Legal Issues



D U P L I C A T E S



Fixing is
important



facebook
you



REAL
you



False positives

A young boy is riding a blue bicycle on a paved path. He is wearing a blue hoodie, a blue helmet with yellow stars, and plaid shorts. The background is a lush green field with trees. A large blue thought bubble is overlaid on the right side of the image, containing the text "Responsible Disclosure is hard to comply with".

Responsible
Disclosure is hard to
comply with



WAY FORWARD

Best model for security testing

SAVI VALDIYA PHOTOGRAPHY



Make internet a safer place



WIN – WIN SITUATION



Increase in security awareness



References

http://www.slideshare.net/michael_coates/bug-bounty-programs-for-the-web

<http://www.slideshare.net/goldshlager19/nir-goldshlager-killing-a-bug-bounty-program-twice-hack-in-the-box-2012>

<http://www.riyazwalikar.com/>

<https://www.owasp.org/images/1/14/Rose.pdf>

<http://ravivaldiyaphotography.com/>



QUESTIONS?



THANK YOU!!

