

Hackito Ergo Sum

Killing a bounty program

By : Itzhak (Zuk) Avraham; Nir Goldshlager;

2012

2012

whoami | presentation

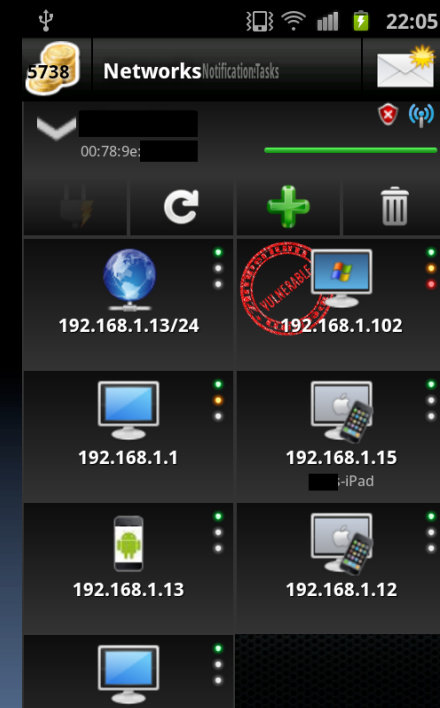
Itzhak Avraham (Zuk)
Founder & CEO

Twitter: [@ihackbanme](https://twitter.com/ihackbanme)

Blog : <http://imthezuk.blogspot.com>

zuk@zimperium.com

root



whoami | presentation

Nir Goldshlager

Senior Web Applications Researcher

Twitter: @nirgoldshlager

Blog : <http://nirgoldshlager.com>

root

Overview

Know your
enemy

Agenda

Weak spots

demos

Reasons for bug bounty

- ✓ Money
- ✓ Fame

The Facebook logo, consisting of the word "facebook" in white lowercase letters on a blue rectangular background.The Google logo, featuring the word "Google" in its multi-colored font.

Reasons for bug bounty

- ✓ Money
- ✓ Fame
- ✓ Okay, mostly fame, they don't pay much :P

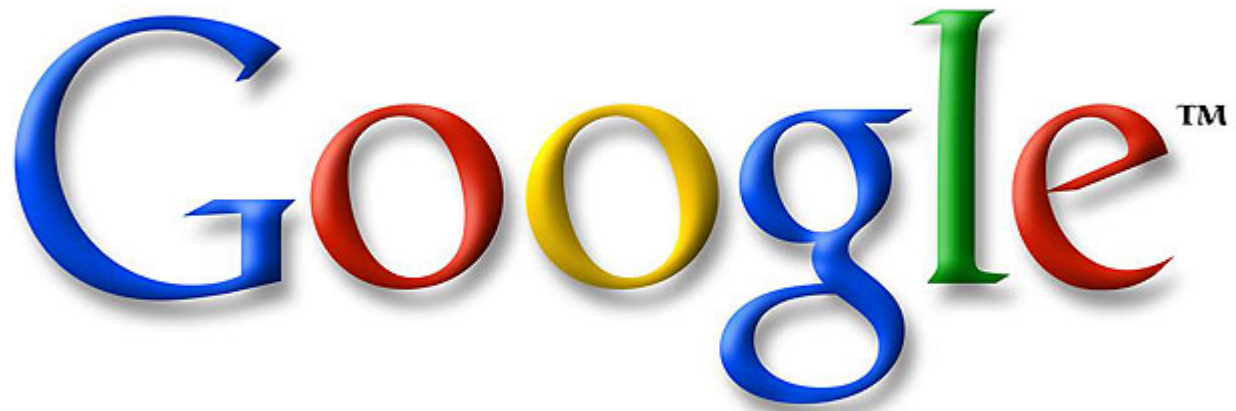
The Facebook logo, consisting of the word "facebook" in white lowercase letters on a blue rectangular background.The Google logo, featuring the word "Google" in its multi-colored font.

Bug bounty programs

- ✓ 1995 – Netscape
- ✓ 2004 – Firefox
- ✓ 2005 – ZDI
- ✓ 2007 – Pwn2own
- ✓ 2010 – Google
- ✓ 2011 – Facebook

The Facebook logo, consisting of the word "facebook" in white lowercase letters on a blue rectangular background.The Google logo, featuring the word "Google" in its multi-colored font.

Know your enemy

The Google logo is displayed in its classic multi-colored font. The letters are 'G' (blue), 'o' (red), 'o' (yellow), 'g' (blue), 'l' (green), and 'e' (red). A small 'TM' trademark symbol is located to the upper right of the 'e'. The logo is centered within a white rectangular area.

Know your enemy

- Nope. Your enemies might be :
 - Masato Kinugawa
 - Neal Poole
 - Nils Juenemann
 - Szymon Gruszecki
 - Wladimir Palant
 - ...



Know your enemy

- Nope. Your enemies might be :

- Masato Kinugawa
- Neal Poole
- Nils Juenemann
- Szymon Gruszecki
- Wladimir Palant
- ...
- ...
- ???
- TIME!



Learn your target Overview

- Spy on their blogs
 - New bugs – new ideas to detect different vulnerabilities.
- Learn the company
 - Unchecked services
 - Successful acquisitions
 - Untested/Less secured web applications
 - Multi vector
 - Unknown vectors / logical techniques
 - Repetitive of weak spots



Google Overview

- Learn the company
 - Successful acquisitions
 - http://en.wikipedia.org/wiki/List_of_acquisitions_by_Google
 - New services – Knol(???), Friends Connect
 - Subdomains
 - Learn all the functions of the application you are going to test
 - Multi vector
 - Unknown vectors / logical techniques
 - Repetitive of weak spots



Google Overview

- Successful acquisitions
http://en.wikipedia.org/wiki/List_of_acquisitions_by_Google
- More than 1 acquisition per week since 2010!



Google Overview

- Approach
 - Logical / mixed issues



XSS for fun and ... profit?

- XSS is not just for account hijacking
- Trusted website, runs malicious javascript...
 - Client Side Exploit anyone?

Google Overview

- Convention
 - Calender
 - Google.com/calendar
 - Friends Connect
 - google.com/friendconnect
 - Knol
 - Google.com/knol
 - Analytics
 - Google.com/analytics
 - Blogger
 - Google.com/blogger



Google Support Overview

- Convention
 - Knol
 - Google.com/knol
 - No
 - Friends Connect
 - Support.google.com/friendconnect
 - Calendar
 - Support.google.com/calendar
 - Analytics
 - Support.google.com/analytics
 - Blogger
 - Support.google.com/blogger
 - Admob
 - Support.google.com/admob



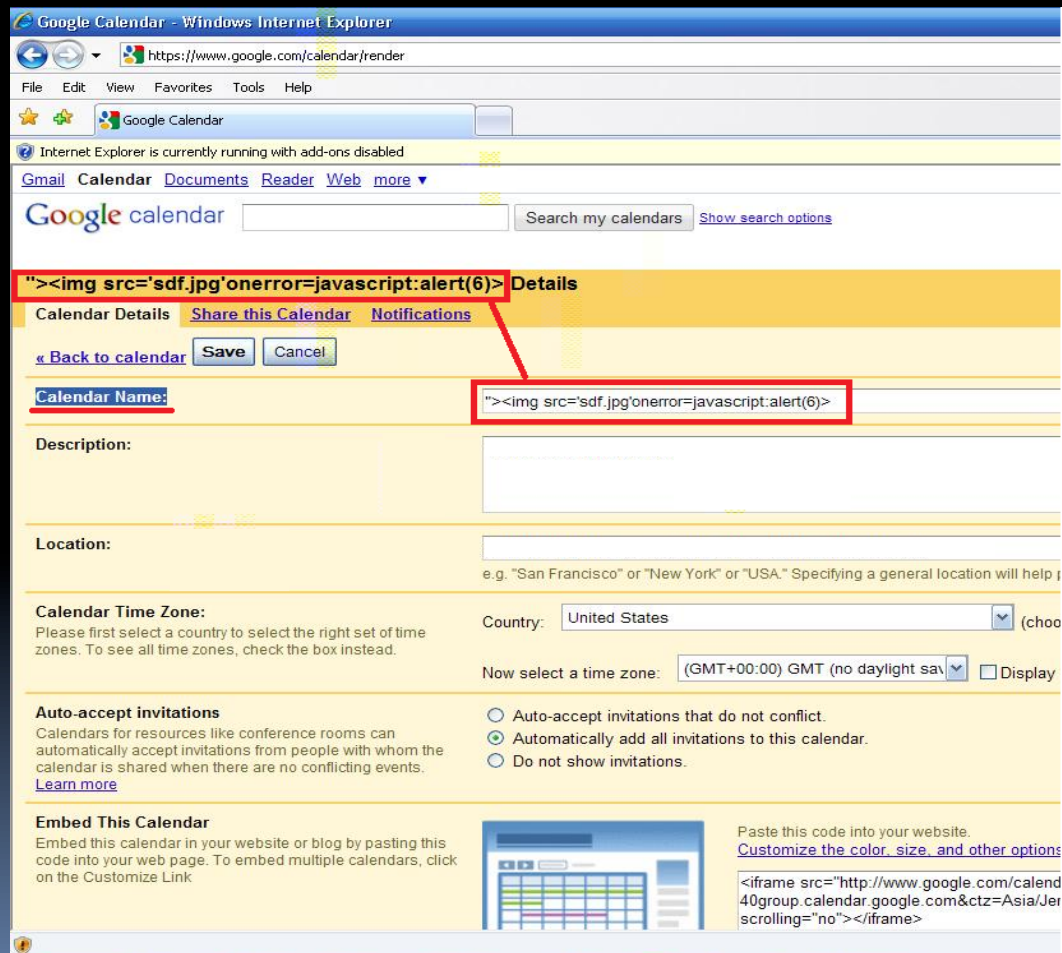
Google Calendar Stored XSS



Google calendar

Stored XSS (Error based)

- Calendar name field is vulnerable



Google Calendar Error based

- On delete of the calendar, XSS popped out.
- We need to find a way to trigger it for REMOTE users.

Google Calendar Error based

- How can one see our calendar name?

Google Calendar Error based

- Let's share our malicious calendar with the target (!!)
- Approve is not needed for sharing calendars
- Ohh hello.



Google Calendar Error based

- Let's share our malicious calendar with the target (!!)
- Approve is not needed for sharing calendars

Details

[Calendar Details](#) **Share this Calendar** [Notifications](#)

[« Back to calendar](#) [Save](#) [Cancel](#)

☐ **Make this calendar public** [Learn more](#)
This calendar will appear in public Google search results.

☐ Share only my free/busy information (Hide details)

Share with specific people

Person	Permission Settings	Remove
<input type="text"/>	Make changes AND manage sharing ▼	Add Person

Google Calendar Error based

- user must delete his calendar.

Google Calendar Error based

- user must delete his calendar.
- Let's FORCE our target to DELETE!

Google Calendar Error based

- Calendar SPAM !!!



Google Calendar Error based

- Let's share again

Details

[Calendar Details](#) [Share this Calendar](#) [Notifications](#)

[« Back to calendar](#) [Save](#) [Cancel](#)

☐ **Make this calendar public** [Learn more](#)
This calendar will appear in public Google search results.

☐ Share only my free/busy information (Hide details)

Share with specific people

Person	Permission Settings	Remove
<input type="text"/>	Make changes AND manage sharing ▼	Add Person

Google Calendar Error based

- And again

Details

[Calendar Details](#) [Share this Calendar](#) [Notifications](#)

[« Back to calendar](#) [Save](#) [Cancel](#)

☐ **Make this calendar public** [Learn more](#)
This calendar will appear in public Google search results.

☐ Share only my free/busy information (Hide details)

Share with specific people

Person	Permission Settings	Remove
<input type="text"/>	Make changes AND manage sharing ▼	Add Person

Google Calendar Error based

- And again ...

Details

[Calendar Details](#) [Share this Calendar](#) [Notifications](#)


[« Back to calendar](#) [Save](#) [Cancel](#)

☐ **Make this calendar public** [Learn more](#)
This calendar will appear in public Google search results.

☐ Share only my free/busy information (Hide details)

Share with specific people

Person	Permission Settings	Remove
<input type="text"/>	Make changes AND manage sharing ▼	Add Person

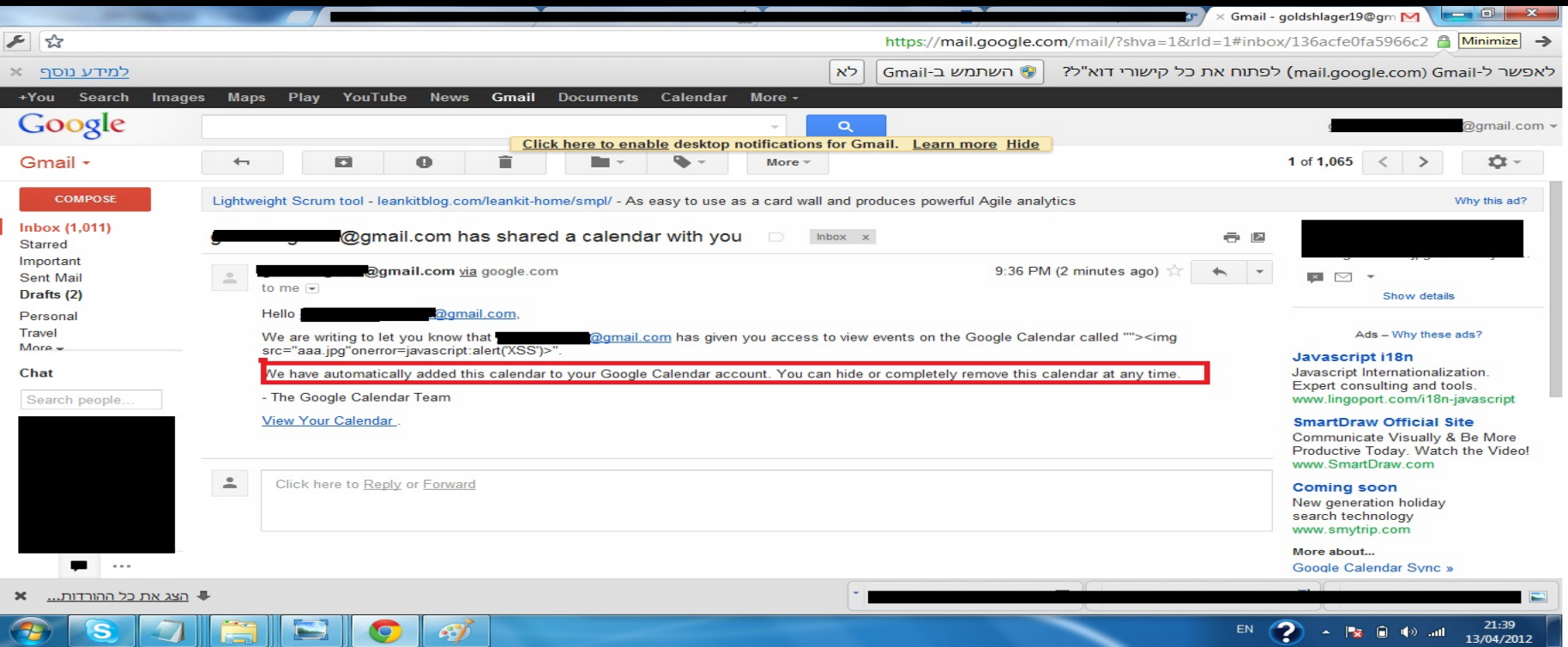


Google Calendar Error based

- No sharing limit
- User gets email for each share

Google Calendar Error based

- User gets email for each share

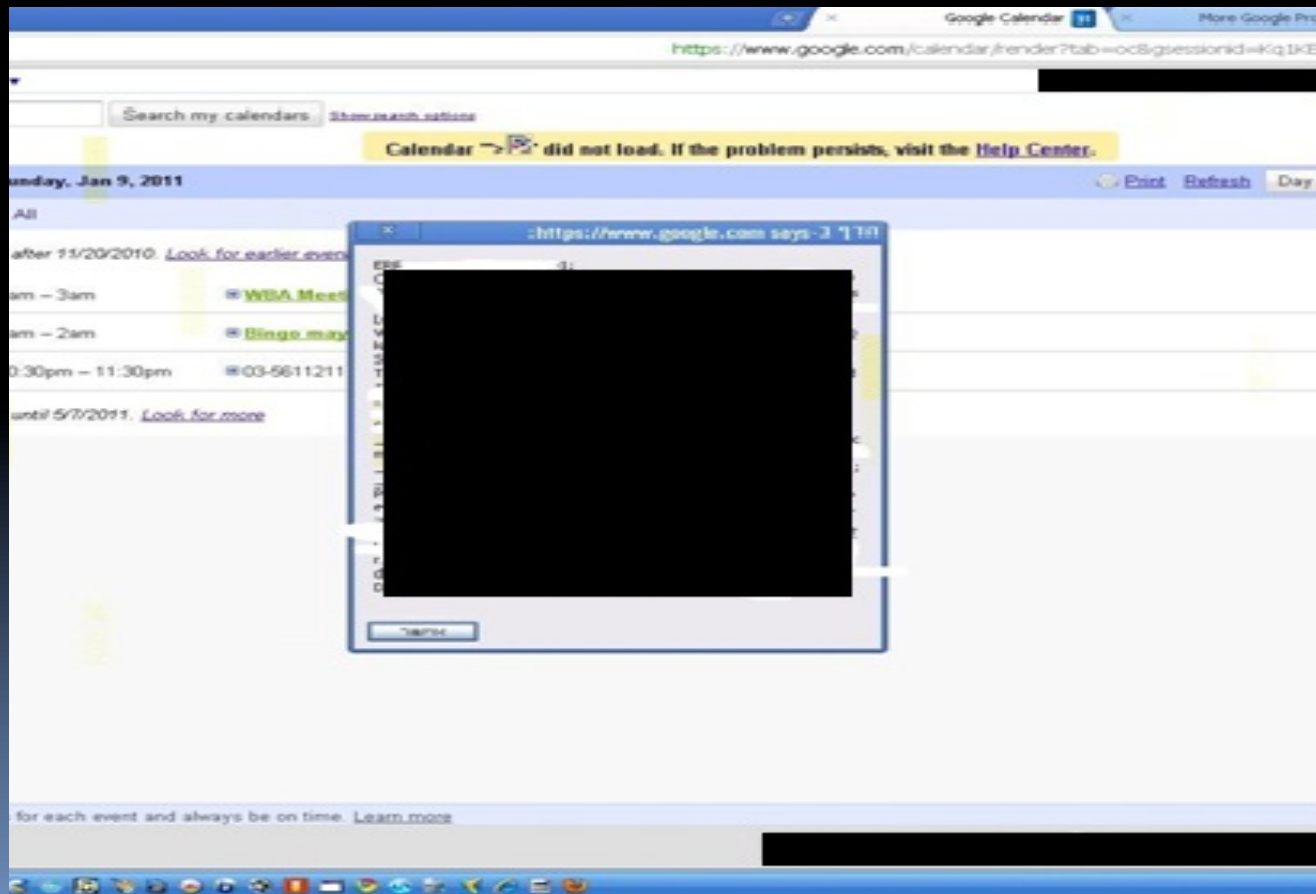


Google Calendar Error based

- After Calendar delete :
 - Achievement Unlocked.

Google Calendar Error based

- After Calendar delete :
 - Achievement Unlocked.



Google FeedBurner Stored XSS



Google Feedburner Unsubscribe XSS

- 1. Victim perform subscribe to malicious feedburner
 - Well it doesn't have to be malicious
 - Feed title is vulnerable

Google Feedburner Unsubscribe XSS

- Feed title is vulnerable

The screenshot shows the Google Feedburner 'Edit Feed Details' interface. The 'Feed Title' field contains the malicious payload: `">`. Below the form, the 'Feed Stats Dashboard' is visible, showing a line graph of feed statistics and a summary of 0 subscribers and 0 reach.

Google feedburner

">

[Edit Feed Details...](#) | [Delete Feed...](#) | [Transfer Feed...](#)

You should not change "Original Feed" unless you move your original feed to a new domain or a new location on your existing server. Also, changing "Feed Address" will require you to update your feed subscribers with your new address; the previous feed address will no longer work.

Feed Title: (Helps you identify your feed)

Original Feed: (Feed published on your site)

Feed Address: (Your FeedBurner feed)

[Save Feed Details](#) or [cancel and do not make these changes](#)

Analyze | **Optimize** | **Publicize** | **Monetize** | **Troubleshoot** | [My Feeds](#)

VIEW

Feed Stats

- Subscribers
- Item Use
- Map Overlay
- Uncommon Uses
- Export: Excel • CSV

SERVICES

- [Configure Stats](#)

Feed Stats Dashboard Show stats for **last 7 days**

1

Feb 28, 2012 Mar 6, 2012 Mar 13, 2012 Mar 20, 2012

Earn money from all that traffic up there! Your posts pay off with relevant ads from AdSense.

Tuesday, February 28 – Wednesday, March 28

- 0 subscribers (on average)
- 0 reach (on average)

Google Feedburner Unsubscribe XSS

- When the victim will decide to unsubscribe the malicious feedburner a stored xss will be run on his client.

Google Feedburner Unsubscribe XSS

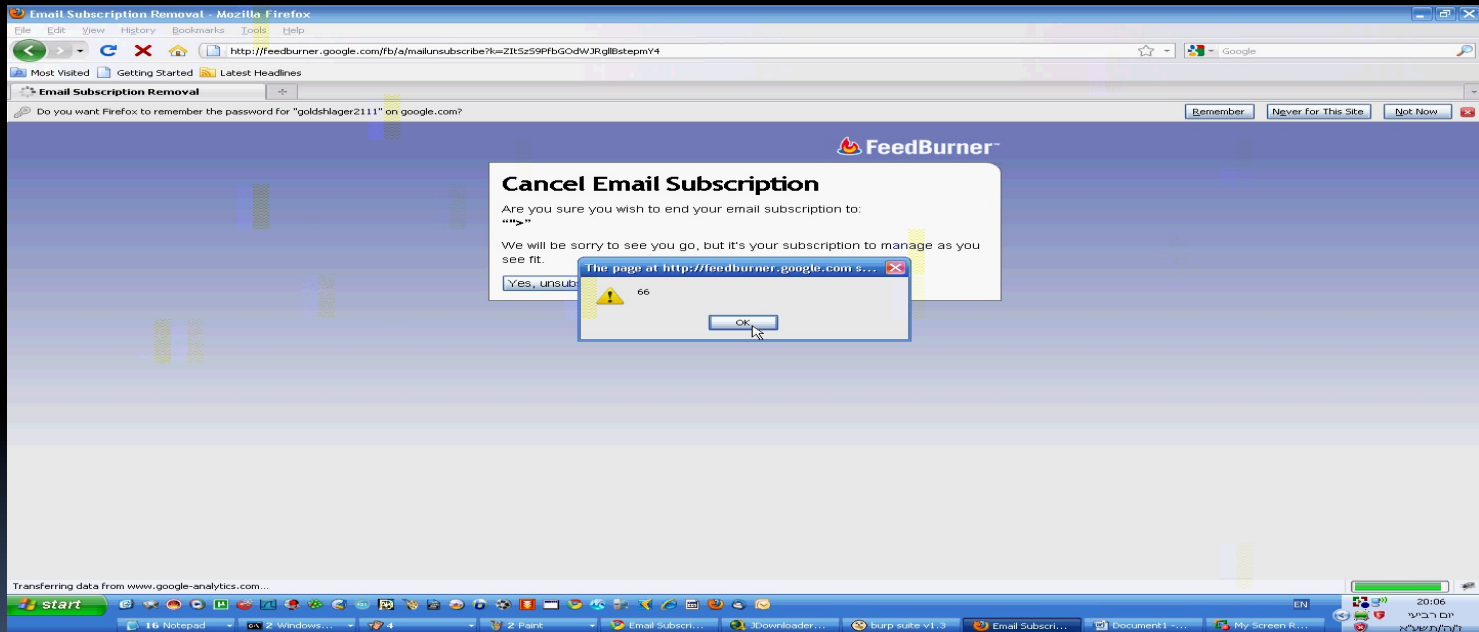
- 2 Methods to exploit this scenario:
 1. Send a malicious unsubscribe link (no permission needed)

Google Feedburner Unsubscribe XSS

- 2 Methods to exploit this scenario:
 1. Send a malicious unsubscribe link (no permission needed)
 2. Victim subscribe, unsubscribe the malicious feedburner.

Google Feedburner Unsubscribe XSS

- User unsubscribe – achievement unlocked



Google FriendConnect Error based

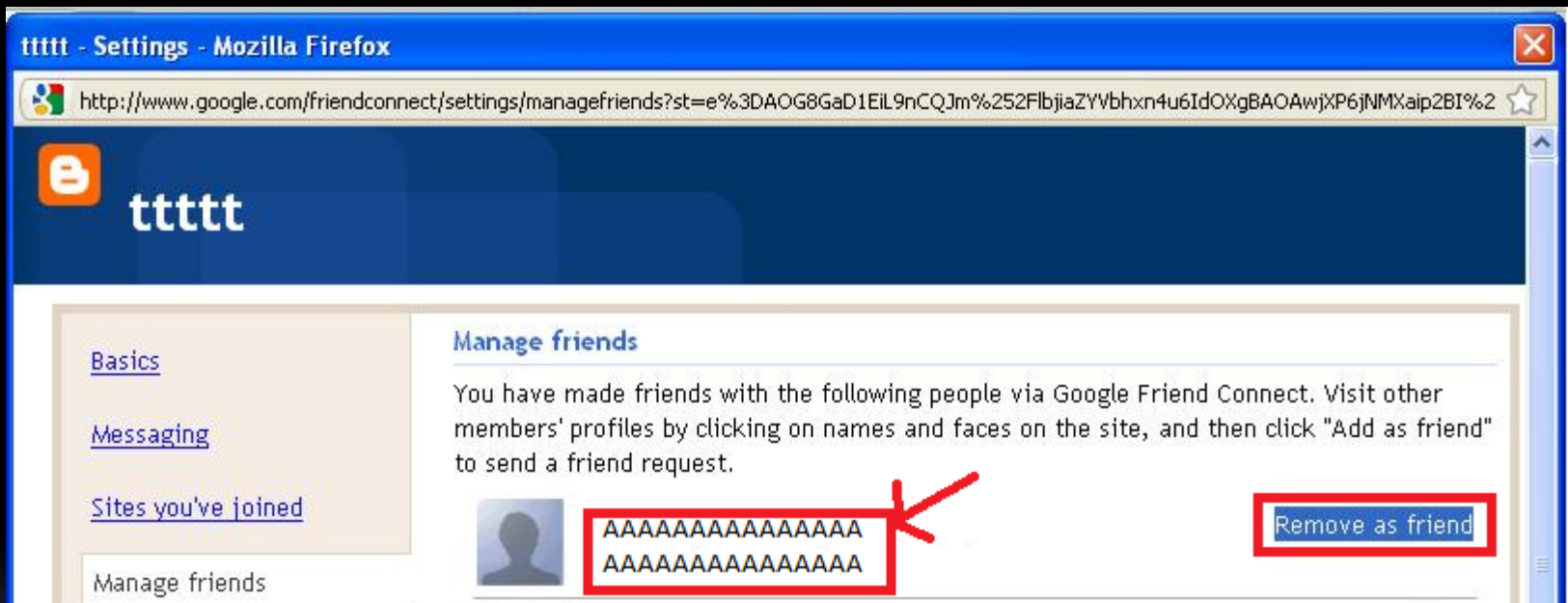
- Meet your new best friend :



Google FriendConnect Error based

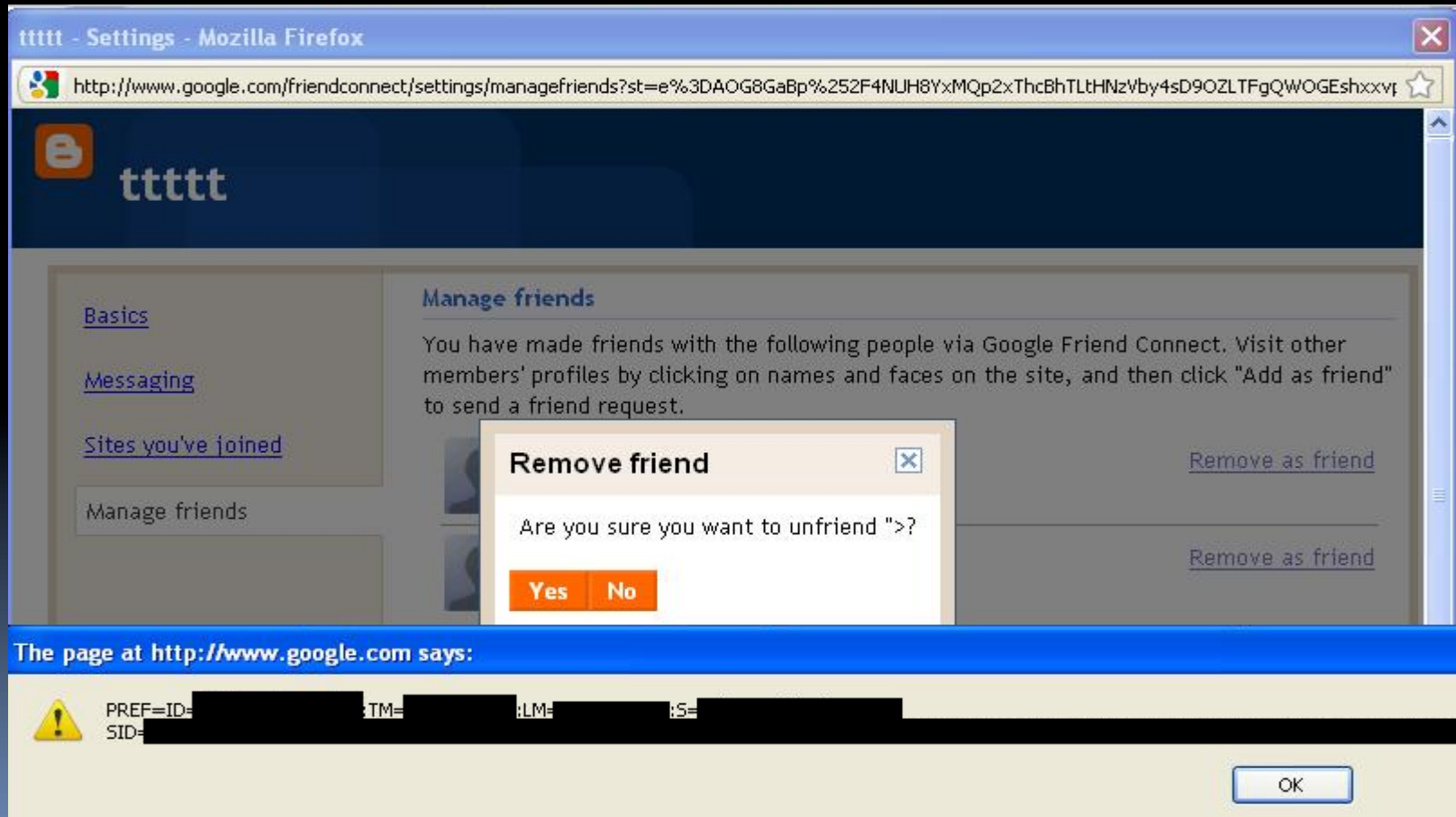
- The target approved our request.

Google FriendConnect Error based



Google FriendConnect Error based

- After User delete :
 - Achievement Unlocked.



Google Analytics – Stored XSS



Google Analytics

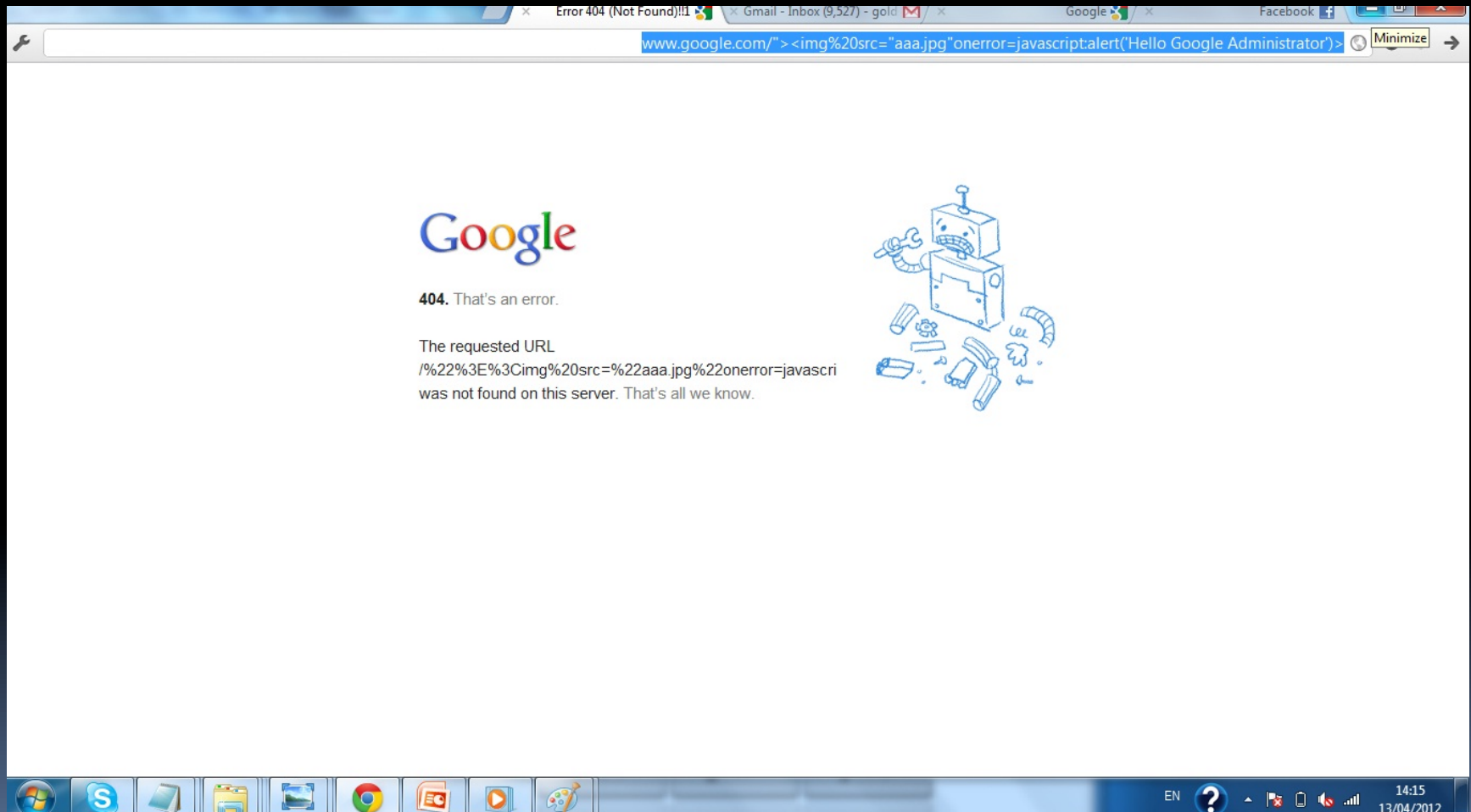
- In-page analytics doesn't escape incoming requests:
 - Meaning, an attacker can send XSS to the administrator by sending a URL

Google Analytics

- In-page analytics doesn't escape incoming requests:
 - Meaning, an attacker can send XSS to the administrator by sending a URL



Google Analytics



Google Analytics

- Let's exploit this vulnerability in 2 creative ways:
 - In-Page Analytics – When the administrator logs in boom.
 - Sharing – Infect ourselves and do share our Analytics with the victim (the link would be directly to in-page analytics)

Google Analytics

- Let's wait for our administrator to login
 - Achievement unlocked, we can run JS on any web administrator using Analytics

Google Analytics

In-Page Analytics - Google Analytics - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://www.google.com/analytics/reporting/in_page?id=40411230&pr=20101129-20101229&cmp=average

Most Visited Getting Started Latest Headlines

How To Set Up Google AdSense Video ... Google AdSense Google AdSense - AdSense for Search Google AdSense - AdSense for Domains In-Page Analytics - Google Analy...

Do you want Firefox to remember the password for "asiagechtman223" on google.com? Remember Never for This Site Not Now

Google Analytics

Analytics Settings View Reports: [redacted]blogspot.com/ My Analytics Accounts: [redacted]

Back to Content Overview

Overview >

In-Page Analytics

Content Detail

- 58 Pageviews
- 9 Unique Views
- 00:02:21 Time on Page
- 25.00% Bounce Rate
- 13.79% % Exit
- 13.79% Entrances / Pageviews
- \$0.00 \$ Index

AdSense Performance

- 29 AdSense Page Impressions
- \$0.00 AdSense Revenue
- 31 AdSense Unit Impressions

Top Demographic

Language 48 he (82.8%)

Displaying: Clicks

The page at https://www.google.com says: 6

visits with more than: 0.00% + Add Filter

Myblog

דף הבית

יום שני, 27 בדצמבר 2010

aaaa

פורסם על ידי aviadd ב- 12:05 0 תגובות

דף הבית

Done

start

10 Notepad untitled - Paint C:\WINDOWS\... burp suite v1.3 Desktop In-Page Analyti... Profile Settings ... Document1 - Mi... My Screen Rec...

EN 18:31 יום חמישי כ"ג/ד'תשע"א

Google Analytics

- Second method : Sharing with the victim our analytics
- We will add the victim with read-only permission and will submit the link for google.com/analytics account with our ID

Google Analytics

In-Page Analytics - Google Analytics - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://www.google.com/analytics/reporting/in_page?id=40411230&pdr=20101129-20101229&cmp=average

How To Set Up Google AdSense Video ... Google AdSense Google AdSense - AdSense for Search Google AdSense - AdSense for Domains In-Page Analytics - Google Analy...

Do you want Firefox to remember the password for " [redacted] on google.com? Remember Never for This Site Not Now

Google Analytics

Analytics Settings | View Reports: [redacted]blogspot.com/ My Analytics Accounts: [redacted]

Back to Content Overview Advanced Segments: All Visits

Overview >

In-Page Analytics

Content Detail

- 58 Pageviews
- 9 Unique Views
- 00:02:21 Time on Page
- 25.00% Bounce Rate
- 13.79% % Exit
- 13.79% Entrances / Pageviews
- \$0.00 \$ Index

AdSense Performance

- 29 AdSense Page Impressions
- \$0.00 AdSense Revenue
- 31 AdSense Unit Impressions

Top Demographic

Language 48 he (82.8%)

Displaying: Clicks

The page at https://www.google.com says: 6

OK

visits with more than: 0.00% + Add Filter

«הבא הבא» שחקן דוח על שימוש לרעה הבלוג הבא»

Myblog

דף הבית

יום שני, 27 בדצמבר 2010

aaaa

פורסם על ידי aviadd ב- 12:05 0 תגובות

מדוע Google

קידום אתרים עם
לחצושים

קידום אתר במחירים ללא
תחרות הצטרפו ללקוחות
שכבר נהנים מהמוצאות
www.my-pitronot.com

Google Analytics

- Achievement unlocked

The screenshot shows the Google Analytics In-Page Analytics interface within a Mozilla Firefox browser. The browser's address bar displays the URL: https://www.google.com/analytics/reporting/in_page?id=40411230&pdr=20101129-20101229&cmp=average. The Google Analytics header includes the logo, navigation links (Analytics Settings, View Reports), and account information. The main content area is titled "In-Page Analytics" and shows a "Content Detail" sidebar on the left with various metrics: 58 Pageviews, 9 Unique Views, 00:02:21 Time on Page, 25.00% Bounce Rate, 13.79% % Exit, 13.79% Entrances / Pageviews, \$0.00 \$ Index, 29 AdSense Page Impressions, \$0.00 AdSense Revenue, 31 AdSense Unit Impressions, and Top Demographic (Language 48 he (82.8%)). The main content area displays a warning message: "The page at https://www.google.com says: 6" with a yellow warning icon and an "OK" button. The background shows a "Myblog" page with Hebrew text, including a date "יום שני, 27 בדצמבר 2010" and a "aaaa" status. The browser's taskbar at the bottom shows the Windows Start button and various application icons.

Permission bypass – Google Knol



Permission bypass

Unpublished document

The screenshot shows a web browser window displaying a Knol document. The browser's address bar shows a URL ending in '@gmail.com'. The page header includes the Knol logo and navigation links. The main content area displays the text 'aaaa', 'bbbb', 'cccc', and 'ddddd'. A message states 'Comments have been disabled on this knol'. The right sidebar contains several sections: 'Edit this knol' and 'Write a knol' buttons; a language selection dropdown set to 'Hebrew - עברית'; a user profile picture and links to 'Edit My Profile' and 'Edit My Preferences'; a 'Your rating:' section; a 'Share and invite' section with a radio button selected for 'This knol is unpublished.' and a 'Publish' button; a 'Creative Commons Attribution 3.0 License' section; a 'You have permission to manage this knol' section with a 'Settings' link; and a 'Knol translations' section. A black arrow points from the 'This knol is unpublished.' radio button to the 'Publish' button, indicating a potential bypass of the unpublished state.

אפשרויות ▼

אל תתרגם לעולם אנגלית לא תרגם האם ברצונך לתרגם אותי? אנגלית ▼ ורו דף ב

@gmail.com My knols | Preferences | Home | Help | Sign out

Search Toolkit

knol
BETA A unit of knowledge.


aaaa
bbbb
cccc
ddddd

[Link](#) [Citation](#) [Email](#) [Print](#) [Favorite](#)

Comments have been disabled on this knol

Edit this knol **Write a knol**

Set display language:
[Hebrew - עברית](#)
[Arabic - العربية](#)

 [Edit My Profile](#)
[Edit My Preferences](#)

Your rating:

Share and invite

☒ This knol is unpublished. [Publish](#)

☐ [Closed collaboration](#) [Change](#)

☐ [Creative Commons Attribution 3.0 License](#) [Change](#)

☐ You have permission to manage this knol [Settings](#)

Version: 6
Last edited: 3 hours ago. [Versions](#)

Knol translations
Help [translate this knol](#) into your language.

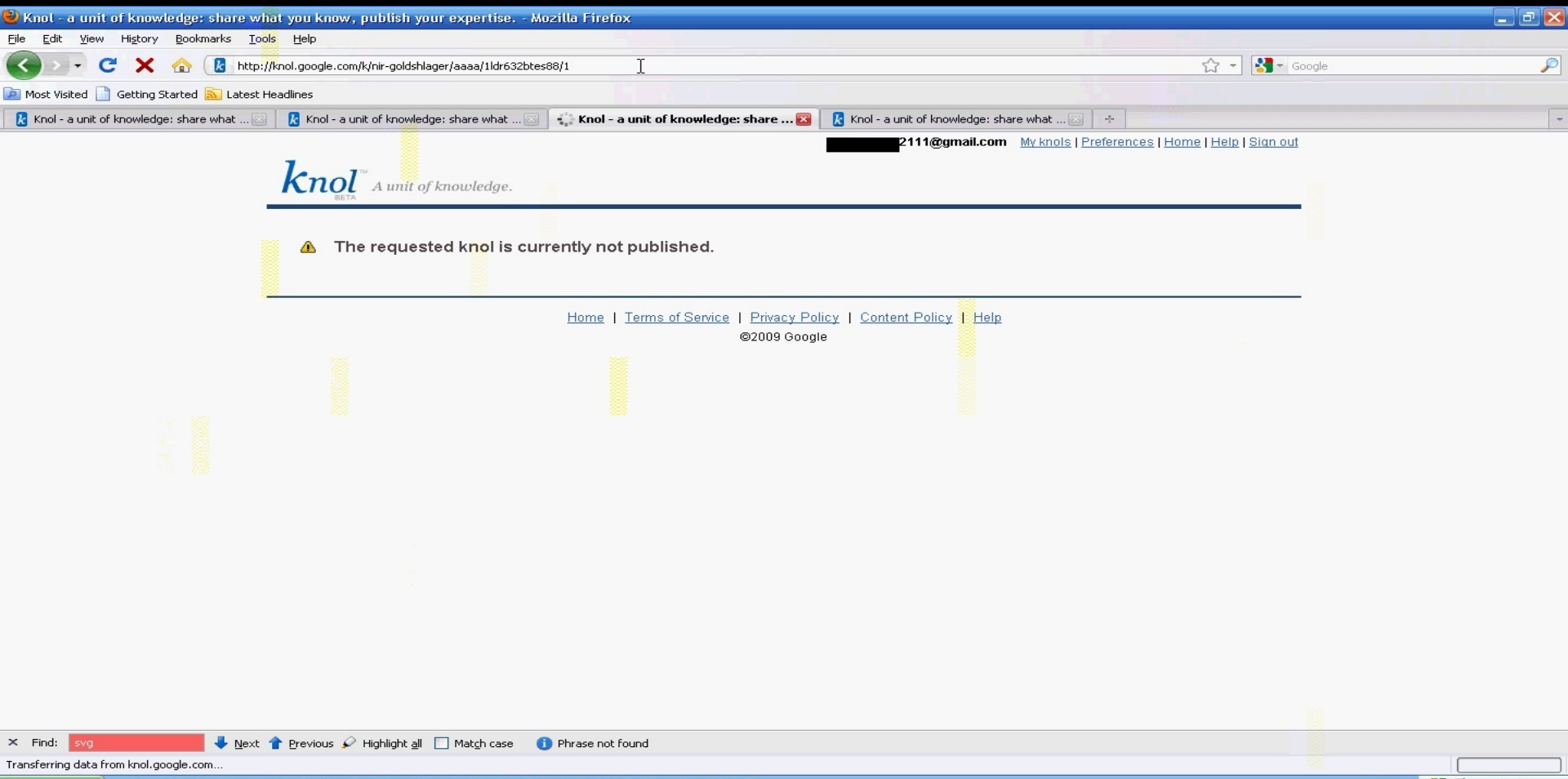
Search for uses of this page ▼

Activity for this knol

This week:
19 pageviews

Permission bypass

- This document isn't accessible via URL



Permission bypass

- We don't have permission to view the document
- KnolTranslate does, let's use the service to show us what we want and cannot access

Permission bypass

http://translate.google.com/toolkit/docupload?hl=en&kurl=http://knol.google.com/k/nir-goldshlager/aaaa/1ldr632btes88/1

Most Visited Getting Started Latest Headlines

Loading...

Uploading...

2111@gmail.com | Settings | Help | Sign out

Google translator toolkit

Upload Document for Translation

You can create a new translation by uploading a file or by specifying a URL to a web page, a Wikipedia™ article or a knol.

[Back to Google Translator Toolkit](#)

[Local file](#) [Web page](#) [Wikipedia™ article](#) **Knol**

Enter the URL of a **knol**:

What do you want to call it?

Translate from:

Translate to:

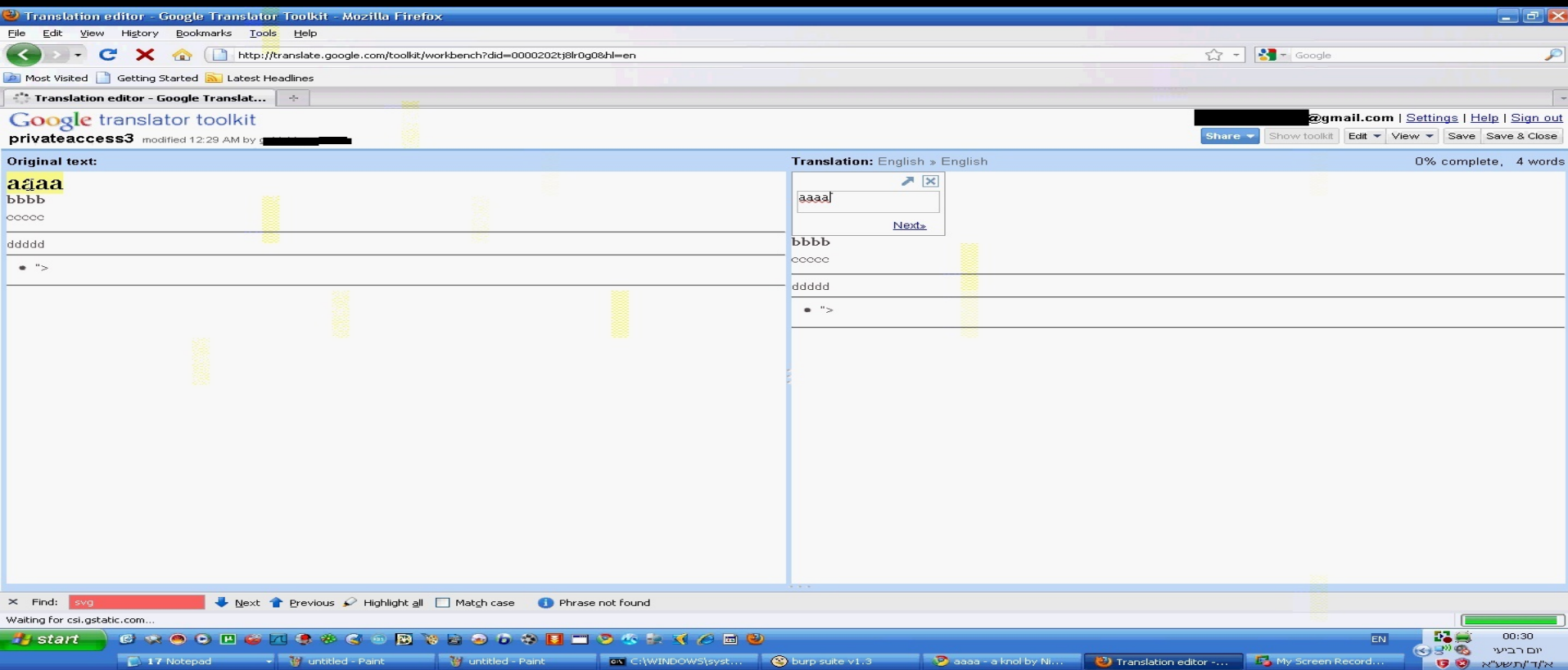
Sharing

Find: **svg** Next Previous Highlight all Match case Phrase not found

Waiting for translate.google.com...

Permission bypass

- Private document accessed using translate service.
- Achievement unlocked



Permission bypass

- Blogger

Summary

- Think different
- Information gathering
- Mixed services
- Permissions

Reference

- <http://www.nirgoldshlager.com/2011/03/blogger-get-administrator-privilege-on.html> - Blogger admin privileges bypass
- <http://www.google.com/about/company/rewardprogram.html> - Google Reward program
- <http://www.google.com/about/company/halloffame.html> - Google Hall of Fame
- http://www.slideshare.net/michael_coates/bug-bounty-programs-for-the-web - Michael Coates - Bug Bounty Program – OWASP 2011

Thank you!



Itzhak "Zuk" Avraham - @ihackbanme

Nir Goldshlager - @nirgoldshlager