

# Hack In The Box 2012

Killing a bounty program, Twice.

By : Itzhak ([Zuk](#)) Avraham; Nir [Goldshlager](#);

05/2012

# # whoami | presentation

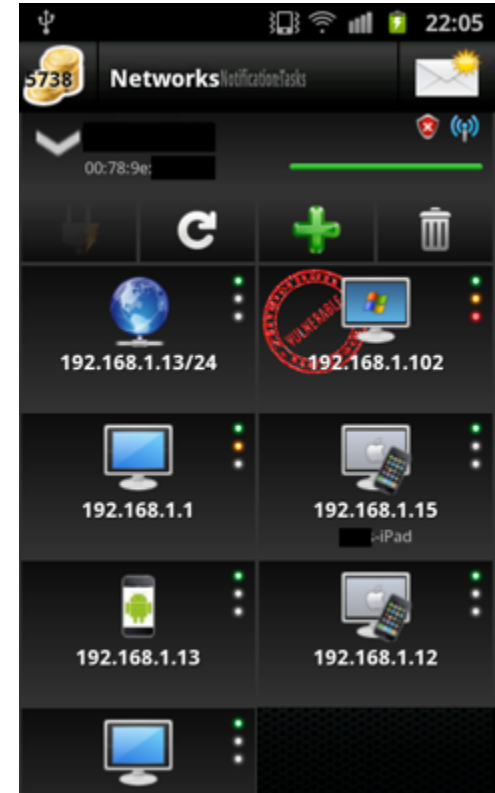
**Itzhak Avraham (Zuk)**

Founder & CEO

[lhackbanme](#)

<http://imthezuk.blogspot.com>

zuk@zimperum.com



# # whoami | presentation

**Nir Goldshlager**

Senior Web Applications Researcher



Twitter: @nirgoldshlager

Blog : <http://nirgoldshlager.com>

**Overview**

**Know  
your  
enemy**

**Agenda**

**Weak spots**

**Demos**

# Reasons for bug bounty

- ✓ Money
- ✓ Credit



facebook.

Google™

# Reasons for bug bounty

- ✓ Money
- ✓ Credit
- ✓ Okay, mostly credit, they don't pay much :P



facebook.

Google™

# Bug bounty programs

1995 – Netscape

2004 – Firefox

2005 – ZDI

2007 – Pwn2own

2010 – Google

2011 – Facebook



facebook.

Google™

Know your enemy

Google™



# 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



# 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](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](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/**calender**
- 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](http://Google.com/knol)
  - No
- Friends Connect  
[Support.google.com/friendconnect](http://Support.google.com/friendconnect)
- Calendar  
[Support.google.com/calendar](http://Support.google.com/calendar)
- Analytics  
[Support.google.com/analytics](http://Support.google.com/analytics)
- Blogger  
[Support.google.com/blogger](http://Support.google.com/blogger)
- Admob  
[Support.google.com/admob](http://Support.google.com/admob)



# Google Calendar Stored XSS



Google™  
Calendar

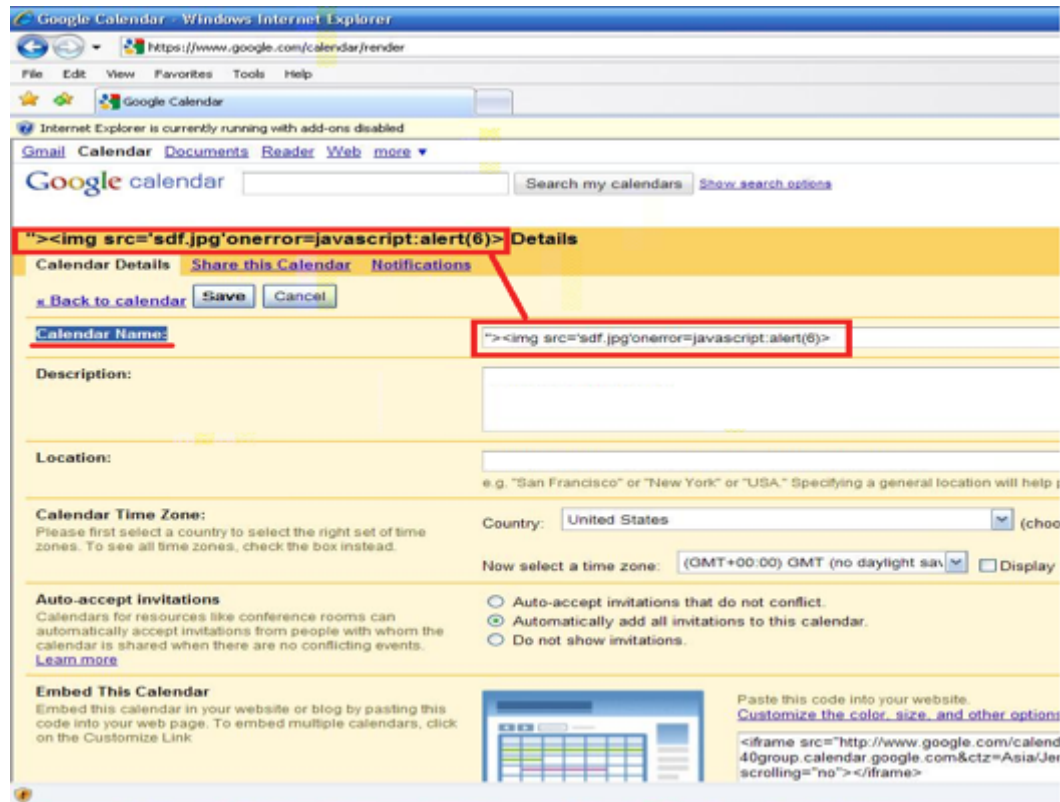
# Google Calendar Error based

- General Attacks against Google Calendar.
- Going Deep Into the Application.
- What we found.
- We need to find a way to trigger it for REMOTE users.



# Stored XSS (Error based)

“Self” Xss Payload



# Google Calendar Error based

- Changing the attack vector
- Resolving the Self XSS Issue By using the Sharing Option

# Google Calendar Error based

The Sharing process:

**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 | <a href="#">Add Person</a> |

# Google Calendar Error based

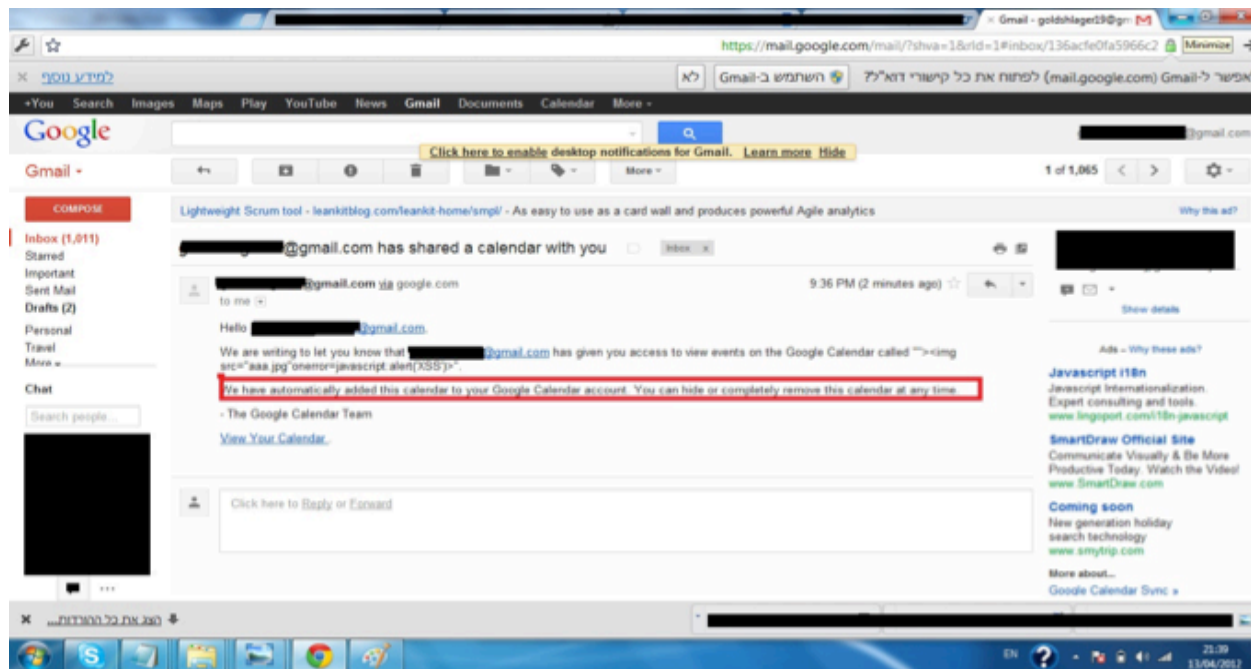
Wait,  
HOUSTON WE HAVE A  
PROBLEM!!!  
user must delete his calendar  
1-5 times.

How can we force our  
Target to delete our  
malicious calendars?



# Google Calendar Error based

- Resolving the problem: **No sharing limit.**
- Users gets email for each share & our Calendar Is added Automatically to the victim account.





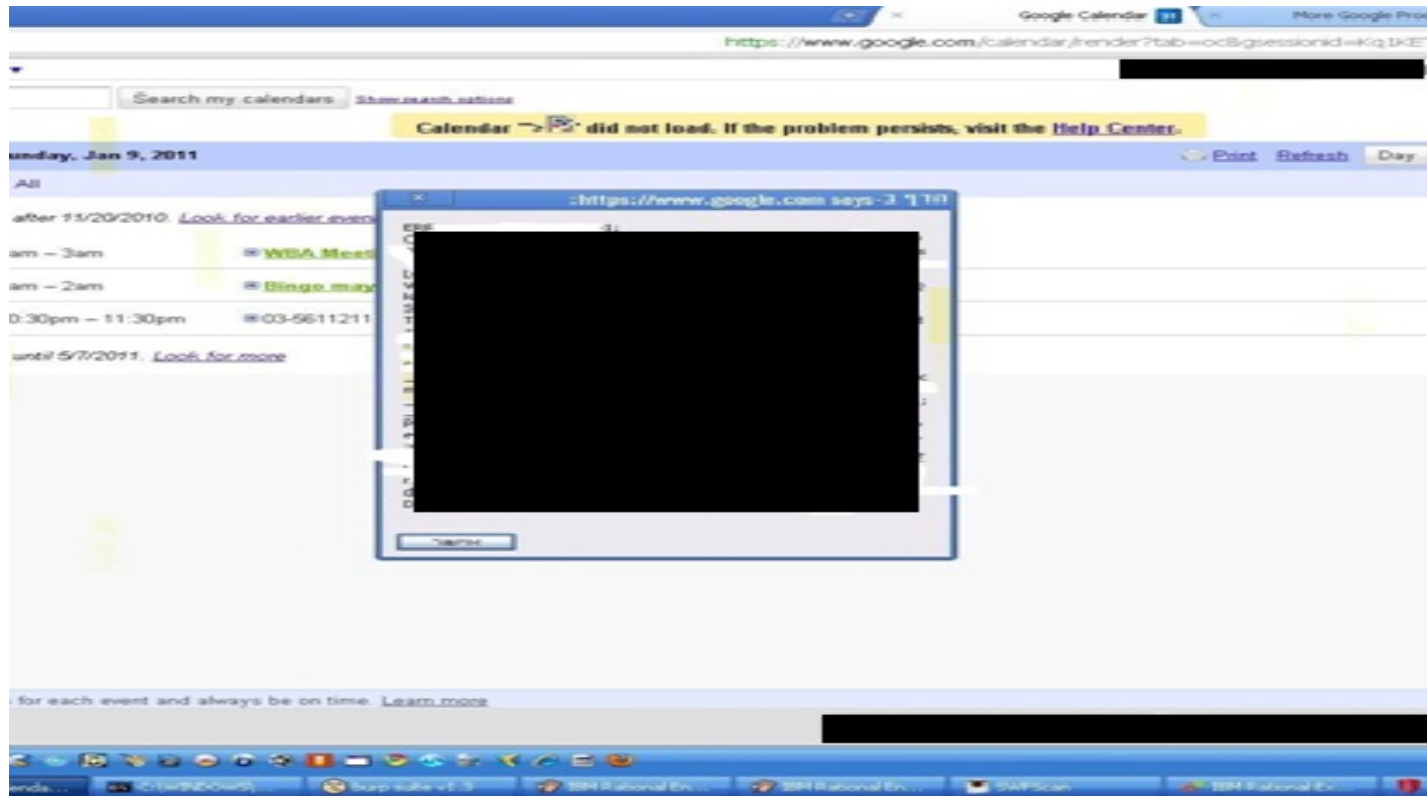
# Google Calendar Error based

- Calendar SPAM !!!
- After the user deletes 1-5 , Error occurred
- Error Message Details:
- Calendar (calendar name) not load, After that a Stored XSS will be trigger 😊



# Google Calendar Error based

Game over! Achievement unlocked.



# Google Analytics – Stored XSS



Google Analytics

# Google Analytics

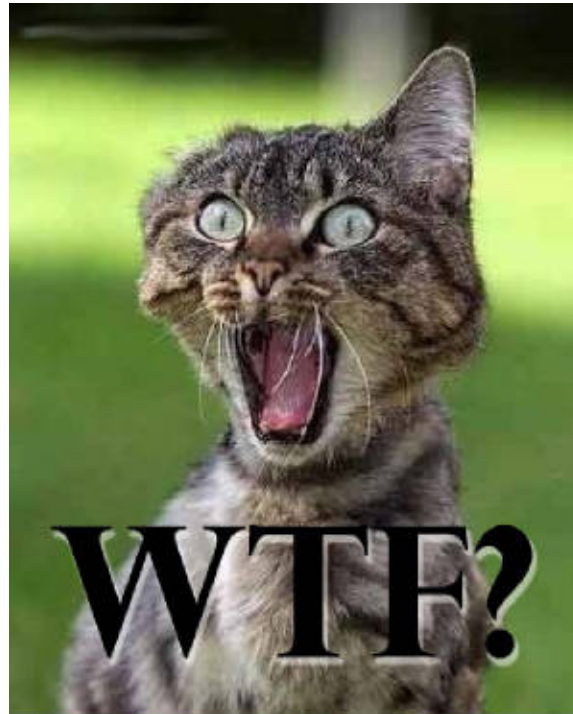
In-page analytics doesn't escape incoming requests:

- Meaning, an attacker can send XSS to the administrator by sending a URL

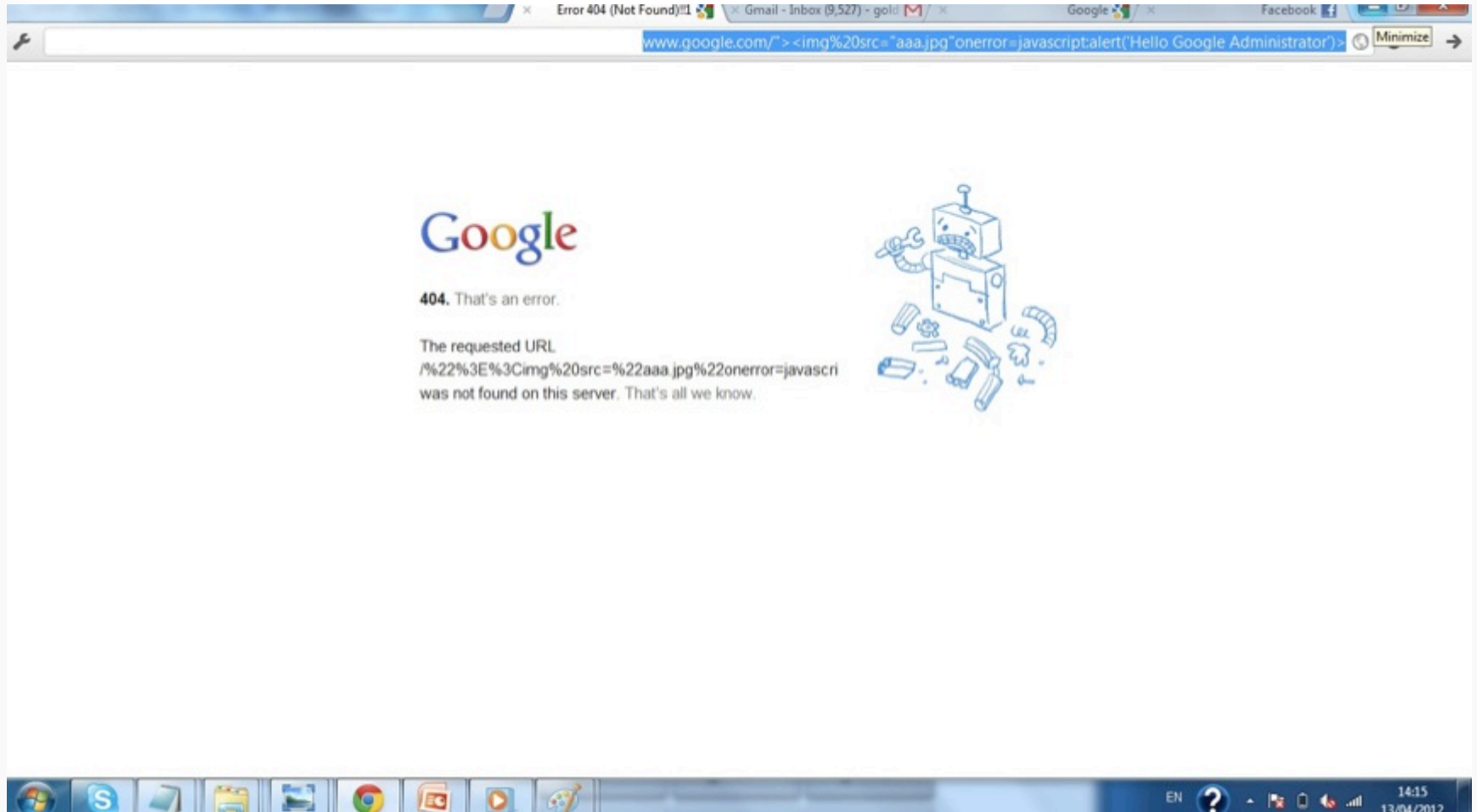
# Google Analytics

In-page analytics doesn't escape incoming requests:

- Meaning, an attacker can send XSS to the administrator by sending a URL



# Google Analytics



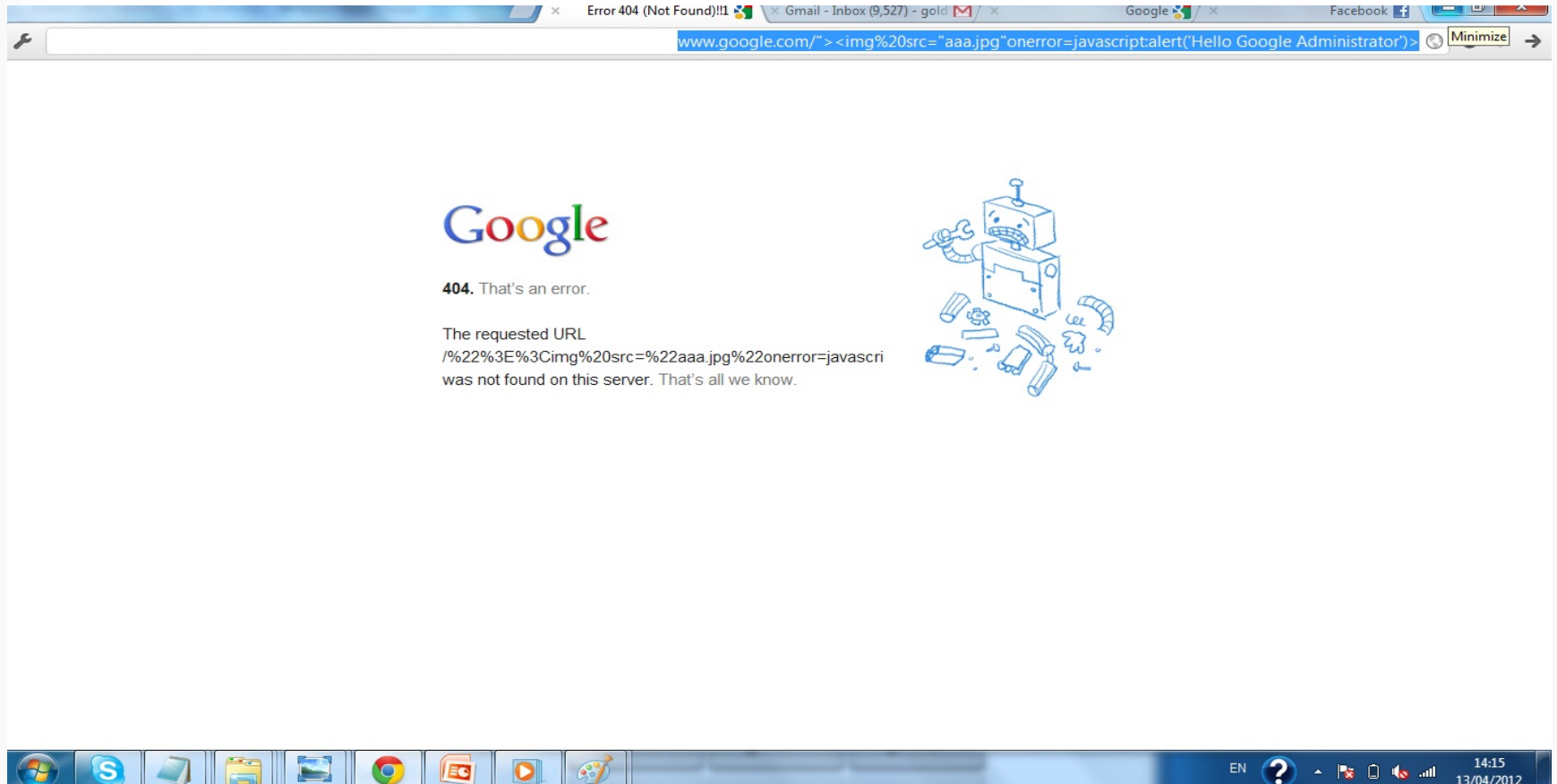
# Google Analytics

Let's exploit this vulnerability in 2 creative ways:

- In-Page Analytics – When the administrator logs in. Ouch.
- Sharing – Infect ourselves and share our Analytics with the victim (direct link to in-page analytics)

# Google Analytics

1<sup>st</sup> method:





# Google Analytics

Let's wait for our administrator to login

# Google Analytics

Let's wait for our administrator to login

- Achievement unlocked, we can run JS on any web administrator using Analytics

# Google Analytics

The screenshot displays the Google Analytics In-Page Analytics interface within a Mozilla Firefox browser window. The browser's address bar shows the URL: [https://www.google.com/analytics/reporting/in\\_page?id=40411230&pd=20101129-20101229&crp=average](https://www.google.com/analytics/reporting/in_page?id=40411230&pd=20101129-20101229&crp=average). The page title is "In-Page Analytics - Google Analytics".

The main content area shows the "In-Page Analytics" report for the "blogspot.com" account. The "Content Detail" section is expanded, displaying the following 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

The "AdSense Performance" section shows:

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

The "Top Demographic" section shows:

- Language 48 he (82.6%)

A warning dialog box is overlaid on the report, stating: "The page at <https://www.google.com> says: 6 visits with more than: 0.00%". The dialog box includes a yellow warning icon and an "OK" button.

The background of the report shows a preview of the "Myblog" page, which includes the text "aaaa" and "2010 ב'שנ"א, 27 בדצמבר".

The Windows taskbar at the bottom shows the Start button, several application icons, and the system tray with the date and time (10:31).

# 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](https://google.com/analytics) account with our ID

# Google Analytics

The screenshot displays the Google Analytics In-Page Analytics interface within a Mozilla Firefox browser. The browser's address bar shows the URL: `https://www.google.com/analytics/reporting/in_page?id=40411230&pd=20101129-20101229&crp=average`. The page title is "In-Page Analytics - Google Analytics - Mozilla Firefox".

The Google Analytics interface includes the following elements:

- Navigation:** "Back to Content Overview" link and "Advanced Segments: All Visits" dropdown.
- Overview:** "Overview" link and "In-Page Analytics" title.
- Content Detail:** A sidebar on the left with the following 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
- AdSense Performance:**
  - 29 AdSense Page Impressions
  - \$0.00 AdSense Revenue
  - 31 AdSense Unit Impressions
- Top Demographic:** Language 48 he (82.8%)

The main content area shows a warning message: "The page at https://www.google.com says: 6". The message box includes a yellow warning icon and an "OK" button. The background content is a page titled "Myblog" with a search bar and a footer containing the text: "2010 שנה, 27 בדצמבר", "aaaa", "פורסם על ידי", "מחברת Google", "קידום אתרים עם למקצוענים", "קידום אתר במחירים ללא תחרות הצטרפו ללקוחות שכבר נהנים מהמומחיות", and "www.mypittonet.com".

# Google Analytics

- Game over. Achievement unlocked

The screenshot shows the Google Analytics In-Page Analytics interface for a website named "Myblog". The browser window title is "In-Page Analytics - Google Analytics - Mozilla Firefox". The address bar shows the URL: [https://www.google.com/analytics/reporting/in\\_page?id=404112306pd=20101129-20101229&cmp=average](https://www.google.com/analytics/reporting/in_page?id=404112306pd=20101129-20101229&cmp=average). The page title is "Myblog".

The main content area displays a report for "Clicks" with a filter of "with more than: 0.00%". A dialog box is overlaid on the report, displaying a warning icon and the text: "The page at https://www.google.com says: 6". The dialog box has an "OK" button.

The left sidebar shows the following 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

The AdSense Performance section shows:

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

The Top Demographic section shows:

- Language 48 he (82.8%)

The bottom of the page shows the date "יום שני, 27 בדצמבר 2010" and the text "aaaa". The footer includes social media icons and the text "פורסם על ידי addvd - 12.05.10 תגובות 0".

# Google FeedBurner Stored XSS



FeedBurner provides custom RSS feeds and management tools to bloggers, podcasters and other web-based content publishers

# Google Feedburner Stored XSS

Feed title is “vulnerable” to an XSS

`><img src='fsd.jpg' onerror=javascript:alert(6)>` 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](#) [Troubleshootize](#) [My Feeds](#)

**VIEW**

**Feed Stats**

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

**SERVICES**

- Configure Stats

### Feed Stats Dashboard

Show stats for

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) [f](#)
- **0** reach (on average) [f](#)





# Google Feedburner Stored XSS

Lets look closer on the features of FeedBurner App

The screenshot displays the Google Feedburner dashboard. At the top, a red banner contains a stored XSS payload: `"><img src='fsd.jpg' onerror=javascript:alert(6)>`. Below the banner are navigation tabs: Analyze, Optimize, Publicize, Monetize, and Troubleshootize. A sidebar on the left lists various services, with 'Email Subscriptions' and 'Subscription Management' highlighted. The main content area is titled 'Email Subscriptions' and includes a 'Subscription Management' section. This section provides instructions on how to use a 'Subscription Form Code' and includes a language selection dropdown set to 'English'. Below the instructions is a code editor containing the following HTML code:

```
<form style="border:1px solid #ccc;padding:3px;text-align:center;" action="http://feedburner.google.com/fb/a/mailverify" method="post" target="popupwindow" onsubmit="window.open('http://feedburner.google.com/fb/a/mailverify?uri=blogspot/gJOas', 'popupwindow', 'scrollbars=yes,width=550,height=520');return true"><p>Enter
```

# Google Feedburner Unsubscribe XSS

- We already know that there is a Subscription feature in Feed burner, Right???
- What about Unsubscribe option, Maybe this can help us?


---

You are subscribed to email updates from [Nir Goldshlager Web Security Blog](#)

Email delivery powered by Google

To stop receiving these emails, you may [unsubscribe now](#).

Google Inc., 20 West Kinzie, Chicago IL USA 60610

 YouTube - Videos from this email



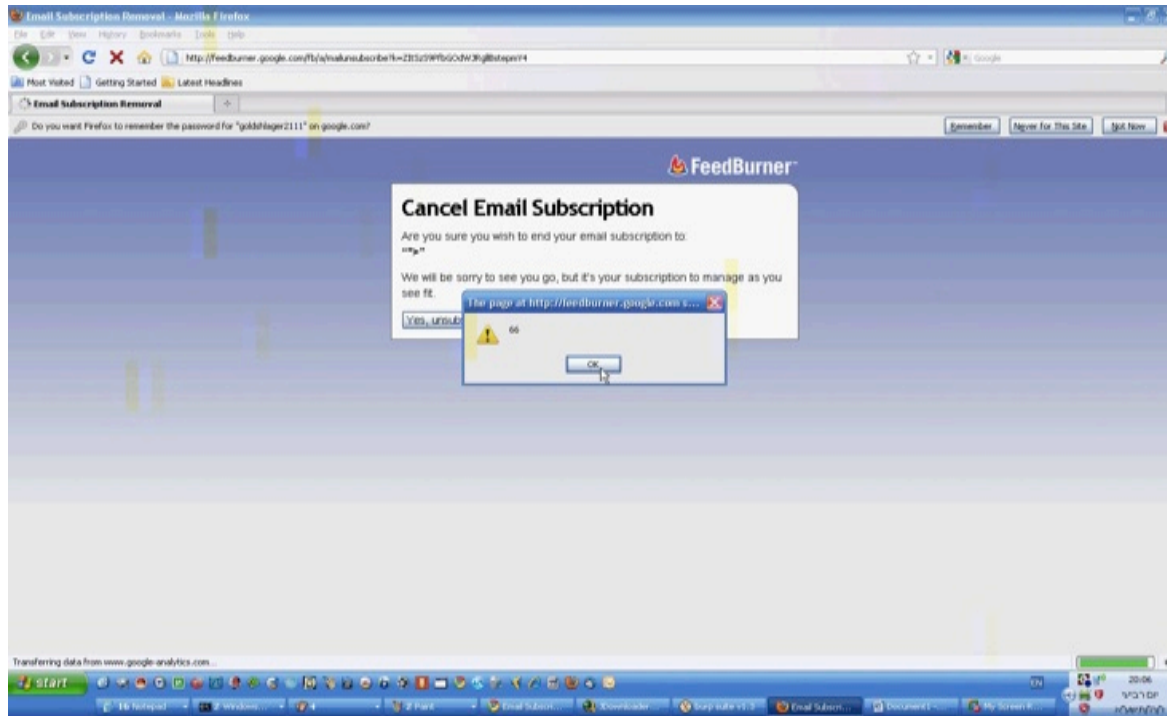
---

Click here to [Reply](#) or [Forward](#)

---

# Google Feedburner Unsubscribe XSS

When the victim will decide to unsubscribe from the malicious feed burner a stored xss will be run on his client.



# Google Feedburner Unsubscribe XSS

Lets Exploit it with two methods:

1. Victim subscribe to the service & Later unsubscribe from the malicious FeedBurner.
2. Attacker Send a malicious unsubscribe link to the victim (Victim dont need to be subscribe to the malicious feed).



# Google FriendConnect Error based

Meet your new best friend :



# Google FriendConnect Error based

The target approved our request.

# Google FriendConnect Error based

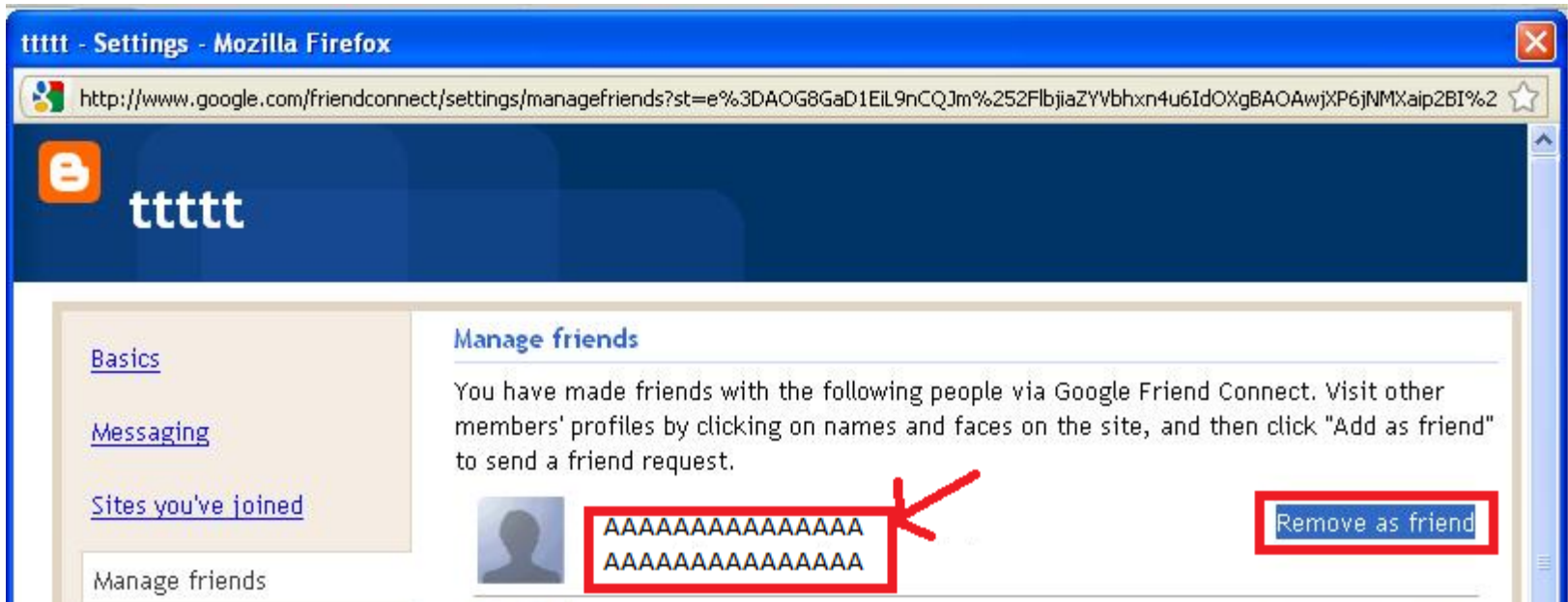
The target approved our request.

Now, let's force him to delete us, not before we're going to change our name to :

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAA ..... "><XSS Payload>
```



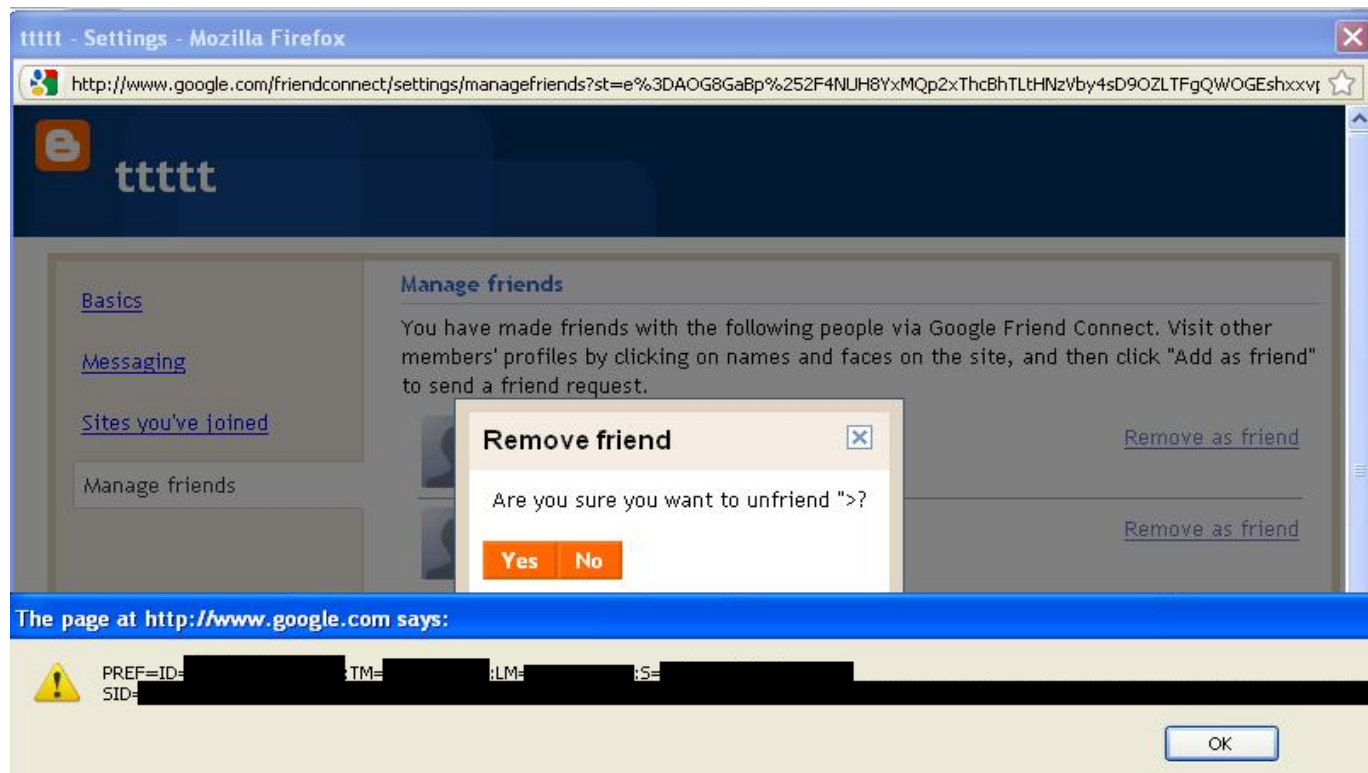
# Google FriendConnect Error based



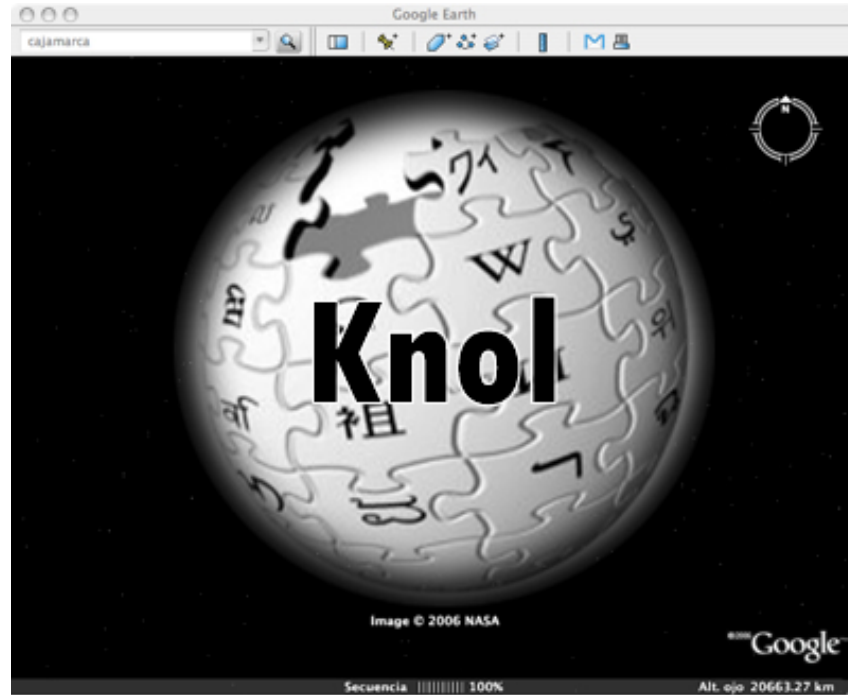
# Google FriendConnect Error based

After User delete :

- Achievement Unlocked.



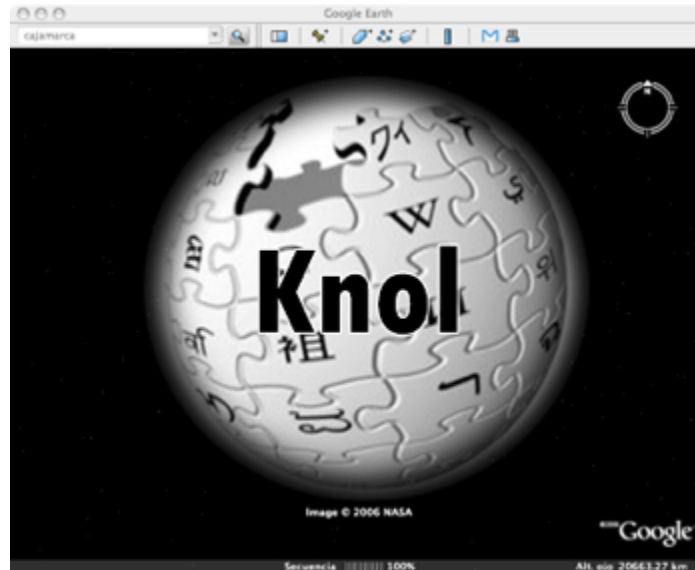
# Permission bypass – Google Knol



Knol is an online knowledge Portal

# Permission bypass

- Privacy in Google Knol
- Function :Publish, Unpublished Docs



# Permission bypass

Example of 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 Knol logo and tagline 'A unit of knowledge.' are visible at the top left. The document content consists of several lines of text: 'aaaa', 'bbbb', 'oooo', and 'dddd'. Below the text are links for 'Link', 'Citation', 'Email', 'Print', and 'Favorite'. A message states 'Comments have been disabled on this knol'. On the right side, there is a sidebar with various controls. At the top of the sidebar are buttons for 'Edit this knol' and 'Write a knol'. Below these are language selection options for Hebrew and Arabic. A user profile picture is shown with links to 'Edit My Profile' and 'Edit My Preferences'. The 'Your rating:' section is empty. The 'Share and invite' section includes a 'Publish' button and options for 'Closed collaboration' and 'Creative Commons Attribution 3.0 License'. Below this, it states 'You have permission to manage this knol' and shows 'Version: 6' and 'Last edited: 3 hours ago'. The 'Knol translations' section offers to translate the knol. The 'Activity for this knol' section shows 'This week: 19 pageviews'.

# Permission bypass

This document isn't accessible via direct URL



The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.

# Permission bypass

Google Validate Permission,  
Block us from viewing the  
unpublished  
Document

What can we do ????



# Permission bypass

Lets meet our new friend 😊

Google Knol Translator Toolkit

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?

- bypassprivateaccess
- bypassprivateaccess2

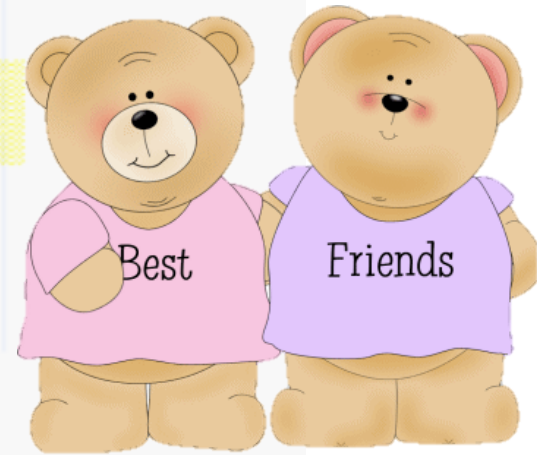
English

Translate to:

Hebrew

Sharing

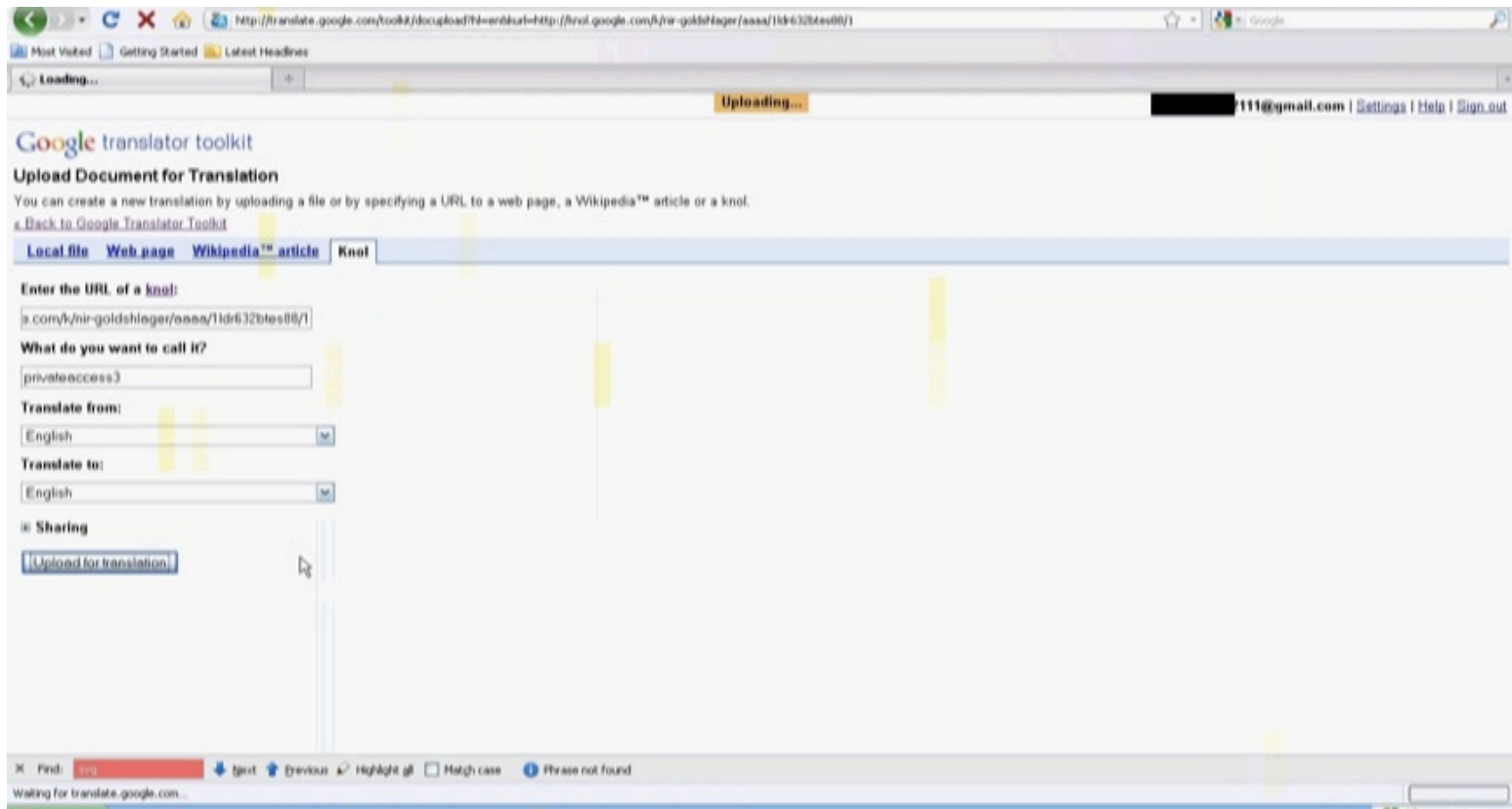
Upload for translation





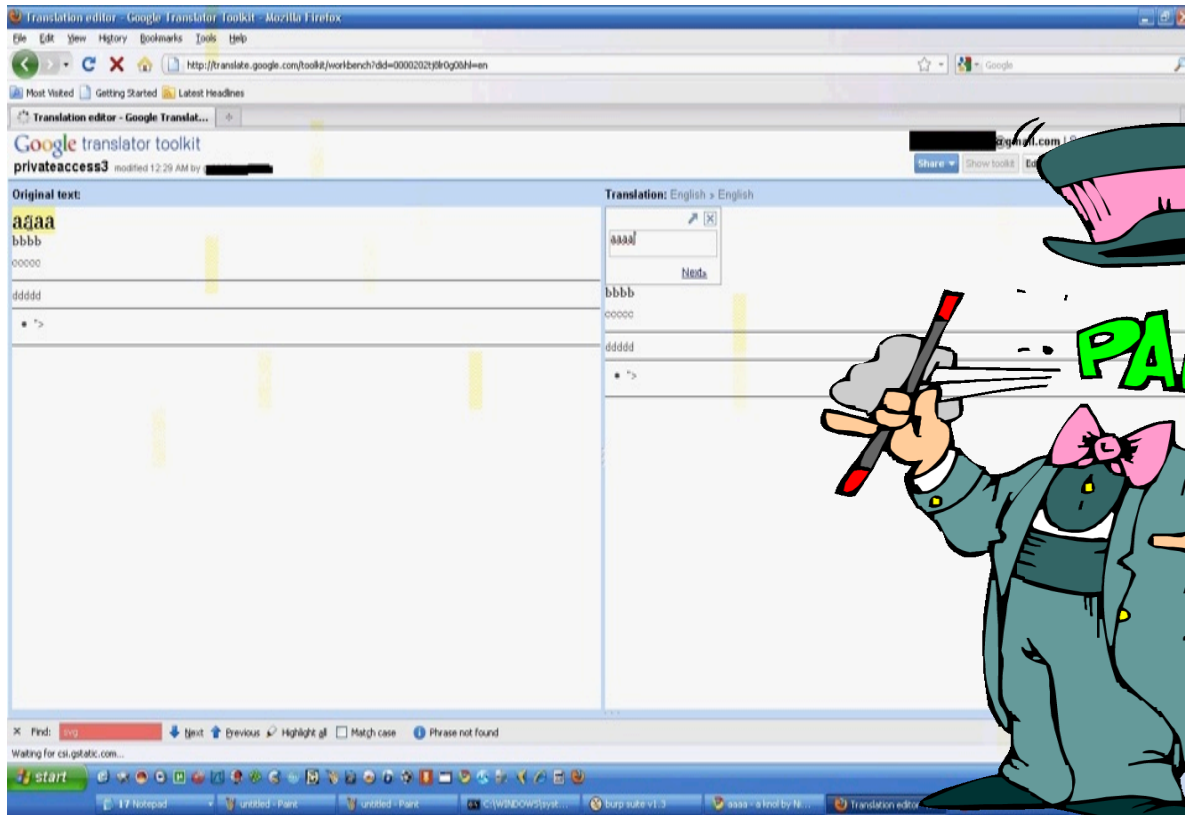
# Permission bypass

Attacker Provide the url of the Unpublished Doc



# Permission bypass

And magic happens



# Google Affiliate Network – Stored XSS + Administrator Priv!



# Google Affiliate Network

What Is Google Affiliate Network??

# Google Affiliate Network

Google Affiliate Network is a free program that makes it easy for website publishers to connect with quality advertisers and get rewarded for driving conversions.

- Discover high-performing advertisers
- Save time with a speedy and intuitive interface
- Track conversions and access real-time reporting
- Enjoy local payments via your AdSense account
- VIP and Rising Star status for top publishers

# Google Affiliate Network

## The goals:

1. XSS an account.
2. Gaining Administrator Privilege



# Google Affiliate Network

## First Attack:

ConnectCommerce->Performics->DoubleClick->Google;

The screenshot shows the 'Edit Link' interface in the Google Affiliate Network. The URL in the browser is `www.connectcommerce.com/links/edit.html?action=partner_edit_byo&LinkID=41000000035197710&partnerid=210000000003414358.c`. The user is logged in as `benzenberg7@gmail.com`. A warning message at the top right states: **Attacker Manipulate LinkID, Partnerid Fields,**. The page has a navigation bar with 'Links' selected. On the left, there are filters for 'By advertiser' (New, Approved advertisers, All advertisers, Links BETA). The main content area is titled 'Edit Link' and shows details for 'Barnes & Noble.com'. The 'Required Link Information' section includes fields for Link Name (aaa), Link Type (Build-Your-Own), Last Updated (2011-03-17 03:51:22), Commission (0 days), and Click-Thru URL. The Click-Thru URL field contains the malicious script: `*=<script>alert(111)</script>`. The 'Recommended Link Information' section has a 'Creative' field with options to 'Add from a URL', 'Upload from my computer', or 'Choose from existing'. The 'Merchandising Text' field contains the script: `*=<script>alert(111)</script>`. An 'Optional Link Information' section is partially visible at the bottom.

# Google Affiliate Network

## First Attack:

Manipulating Parameters on connectcommerce.com domain in order to Inject XSS Payload on google.com Domain

The screenshot displays the 'Edit Link' interface of the Google Affiliate Network. The browser's address bar shows the URL: `www.connectcommerce.com/links/edit.html?action=partner_edit_byo&LinkID=41000000035197710&partnerid=210000000003414358.c`. The page title is 'Attacker Manipulate LinkID, Partnerid Fields,'. The 'Required Link Information' section shows the 'Link Name' field containing 'aaa'. The 'Recommended Link Information' section shows the 'Merchandising Text' field containing the XSS payload: `<script>alert(111)</script>`. The 'Optional Link Information' section also shows the same XSS payload. Three black arrows point to the manipulated parameters in the URL, the 'Attacker Manipulate LinkID, Partnerid Fields,' message, and the injected XSS payload in the 'Merchandising Text' field.



# Google Affiliate Network

PoC : Stored XSS from Google.com Domain

The screenshot shows a browser window with the URL `http://www.google.com/affiliatenetwork/c.html?repType=links#p341506:ads`. The page is the Google Affiliate Network interface. A modal dialog box is open, displaying the message "The page at http://www.google.com says: 111" with a warning icon and an "OK" button. The background page shows the "Links" section with a search bar and filters. The list of links includes:

| Tracking URL  | Creative URL  | Duration          | Category              | Type   | Advertiser earnings per 100 clicks |
|---|---|-------------------|-----------------------|--------|------------------------------------|
| <code>http://gan.doubleclick.net/gan_click?lid=410000000351977</code> | <code>http://gan.doubleclick.net/gan_impression?lid=4100000003</code> | 2011-03-17 to n/a | Apparel & Accessories | Banner | \$39.88 3 month \$44.21 7 day      |
| <code>http://gan.doubleclick.net/gan_click?lid=410000000350235</code> |   |                   | Road Runner Sports    |        | \$39.88 3 month \$44.21 7 day      |

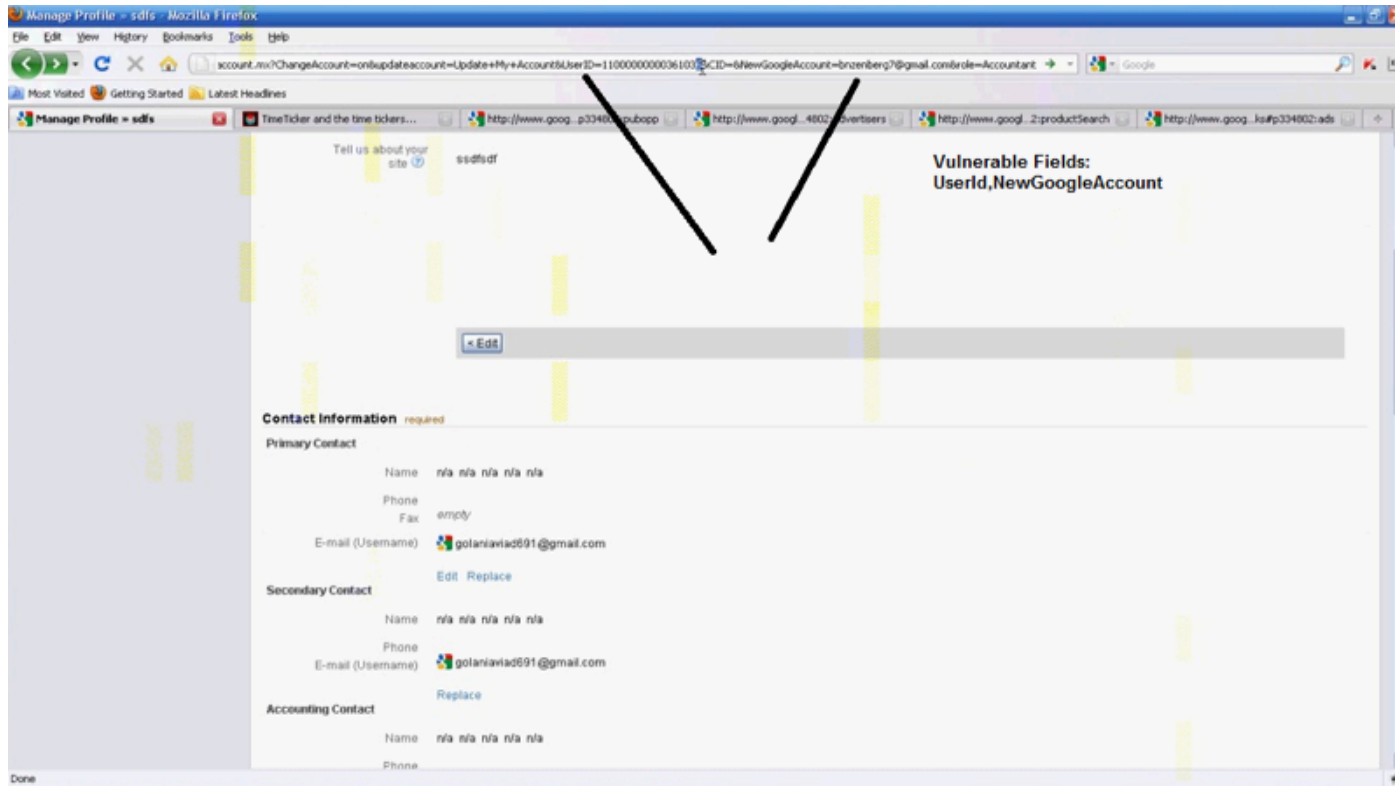
# Google Affiliate Network

## Second attack??

Manipulate, Gaining administrator privilege on any Google Affiliate account.

# Google Affiliate Network

Manipulate UserID, Email fields



**Game Over 3133.7\$!!!!!!**



# Google Picnik – Local File Inclusion

The word "picnik" is written in a lowercase, rounded, green font with a slight 3D effect. The letters are thick and have a soft shadow, giving them a bubbly appearance. The 'i' and 'k' have distinct dots and a tail respectively, maintaining the rounded aesthetic.

# Google Picnik

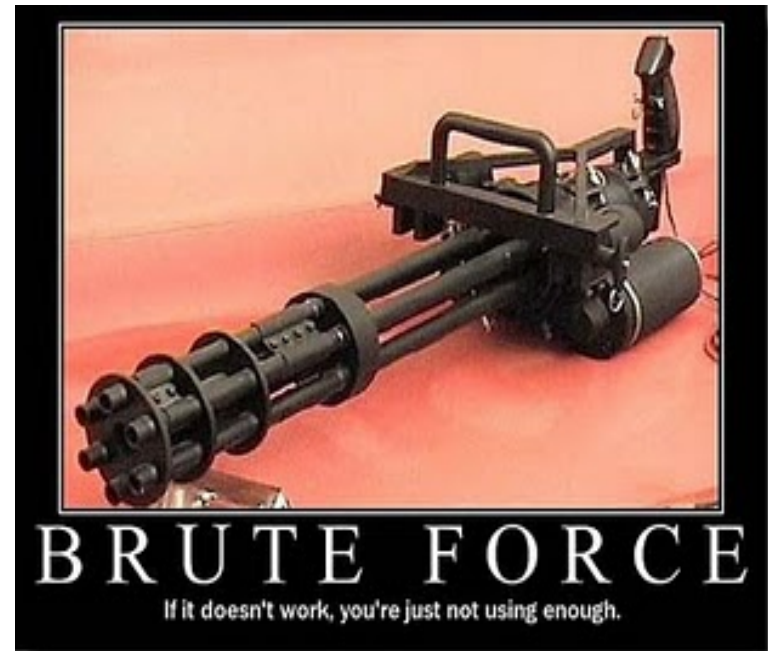
Picnik.com seems to be Secure

So what is the way to crack the lock?



# Google Picnik

1. Execute a BruteForce to Files, Dir Attack
2. Execute a Sub domain Brute Force Attack
3. Port Scanning

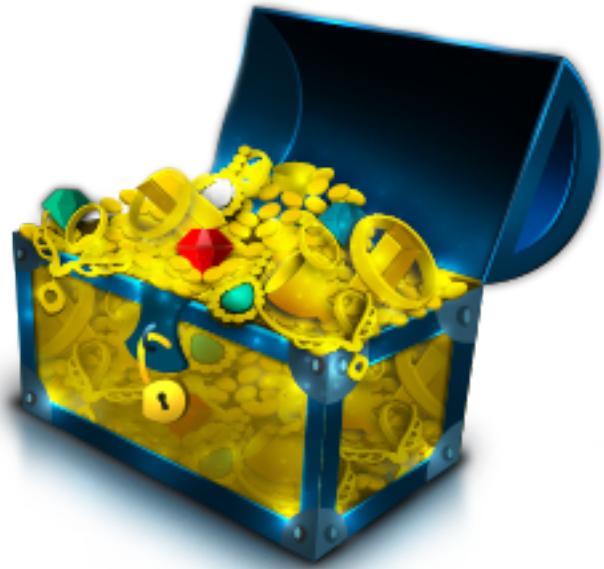


# Google Picnik

Treasure Found!!!!!!

Result:

Sub domain: [vpn.picnik.com](http://vpn.picnik.com)





# Picnik Whols vpn



INTRODUCING THE SINGLEHOP  
**BILL OF RIGHTS**

THE HOSTING INDUSTRY'S FIRST CUSTOMER BILL OF RIGHTS

SEE WHY IT'S BETTER

## Site report for vpn.picnik.com

### Netcraft Toolbar

- [Home](#)
- [Download Now!](#)
- [Report a Phish](#)
- [Top Reporters](#)
- [Phishiest Countries](#)
- [Phishiest Hosters](#)
- [Most Popular Websites](#)
- [Branded Toolbars](#)

Search...

|                            |   |                                    |   |
|----------------------------|---|------------------------------------|---|
| <b>Site</b>                | <a href="http://vpn.picnik.com">http://vpn.picnik.com</a> | <b>Last reboot</b>                 | unknown <a href="#">Uptime graph</a>  |
| <b>Domain</b>              | <a href="http://picnik.com">picnik.com</a>                | <b>Netblock owner</b>              | <a href="#">Google Inc.</a>   |
| <b>IP address</b>          | 70.32.137.5   | <b>Site rank</b>                   | unknown   |
| <b>Country</b>             | <a href="#">US</a>  | <b>Nameserver</b>                  | <a href="#">ns1.google.com</a>  |
| <b>Date first seen</b>     | June 2011   | <b>DNS admin</b>                   | <a href="mailto:dns-admin@google.com">dns-admin@google.com</a>  |
| <b>Domain Registrar</b>    | unknown   | <b>Reverse DNS</b>                 | <a href="#">locke.picnik.com</a>  |
| <b>Organisation</b>        | unknown   | <b>Nameserver Organisation</b>     | Google Inc., Please contact <a href="mailto:contact-admin@google.com">contact-admin@google.com</a> 1600 Amphitheatre Parkway, United States |
| <b>Check another site:</b> | <input type="text"/>                                      | <b>Netcraft Site Report Gadget</b> | <a href="#">[More Netcraft Gadgets]</a>   |

# Google Picnik

- So what was the story of vpn picnik?,
- Someone installed by mistake a older version of phpList in Picnik vpn sub domain



# Google Picnik

- So what was the story of vpn picnic?,
- Someone installed by mistake a older version of phpList in Picnik vpn sub domain
- No way!!! With **Default Password** 😊 ?



# What Is phpList???



phplist is open source email application & suffers from well known Vulnerabilities



## phpList 2.10.8 Local File Inclusion

Authored by [AmnPardaz Security Research Team](#) | Site [bugreport.ir](#)

Posted Jan 15, 2009

phpList version 2.10.8 suffers from a local file inclusion vulnerability.

tags | [exploit](#), [local](#), [file inclusion](#)

MD5 | [59485f67bcd2e29afa9a1d268c69cc7a](#)

[Download](#) | [Favorite](#) | [Comments \(0\)](#)

# Google Picnik

File Inclusion vulnerability that allow me to get a Shell with a leet bounty \$3133,7



```
Warning: require_once(/var/www/localhost/htdocs/lists/admin/) [function.require-once]: failed to open stream: Success in /var/www/localhost/htdocs/lists/admin/index.php on line 83
Fatal error: require_once() [function.require]: Failed opening required '/var/www/localhost/htdocs/lists/admin/' (include_path= './usr/share/php5/usr/share/php') in /var/www/localhost/htdocs/lists/admin/index.php on line 83
```

# Google Picnik

## Game Over



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

to me ▾

Hey Nir

Congratulations! We determined this was was exploitable and could have led to full server compromise -- \$3133.70

Cheers,  
Adam



# Summary

- Out-Of-The-Box (Hack-In-The-Box) Thinking
- 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](http://www.slideshare.net/michael_coates/bug-bounty-programs-for-the-web) - Michael Coates - Bug Bounty Program – OWASP 2011

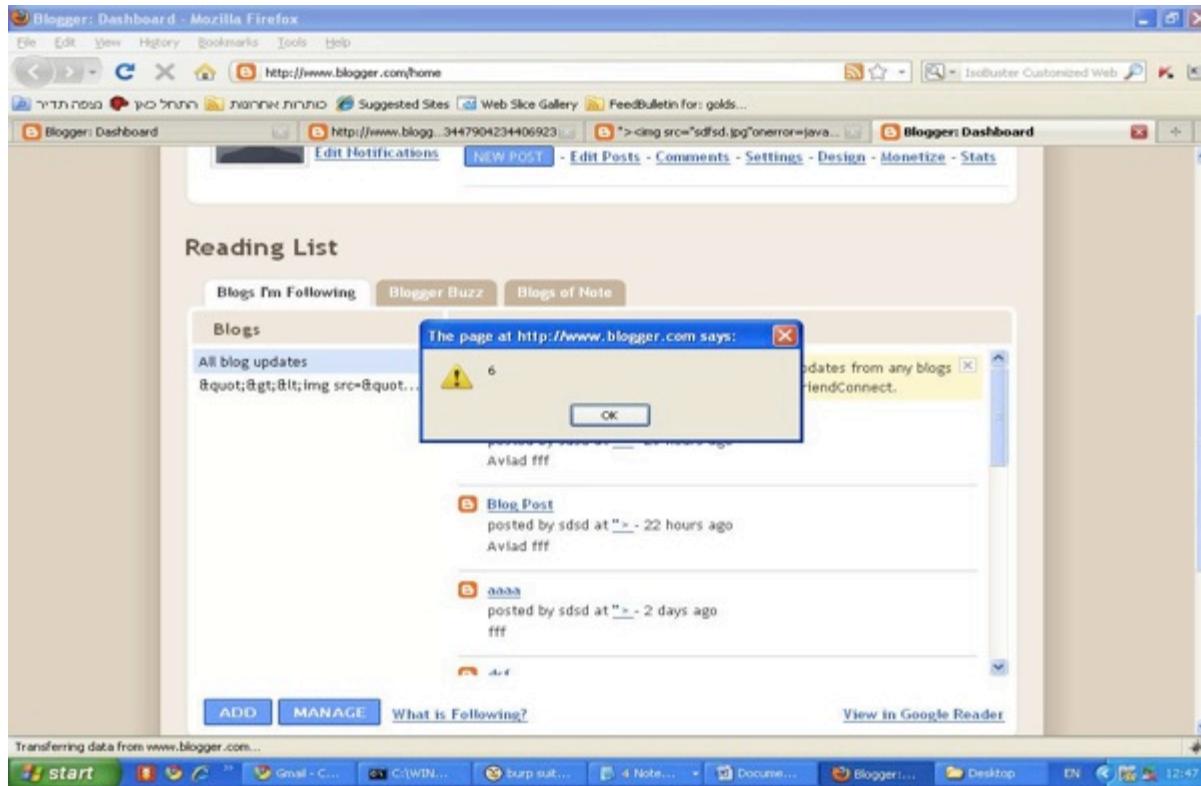


# One more

Maybe it's not a good idea to follow our blogs

# One more

Maybe it's not a good idea to follow our blogs



# Okay okay, one more

Blogger video...

HPP Attack

**Join us tonight at  
Hack-In-The-Empire event  
For invites : [RSVP@zimperium.com](mailto:RSVP@zimperium.com)  
Subject : HITE Invite**



# Thank you!

Itzhak “Zuk” Avraham - [@IHackBanMe](#)

Nir Goldshlager - [@NirGoldshlager](#)

