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

Ihackbanme
http://imthezuk.blogspot.com

zuk@zimperum.com
# whoami | presentation

Nir Goldshlager
Senior Web Applications Researcher

Twitter: @nirgoldshlager
Blog: http://nirgoldshlager.com
Reasons for bug bounty

- Money
- Credit
Reasons for bug bounty

- Money
- Credit
- Okay, mostly credit, they don’t pay much :P
Bug bounty programs

1995 – Netscape
2004 – Firefox
2005 – ZDI
2007 – Pwn2own
2010 – Google
2011 – Facebook
Know your enemy
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 Gruszczeki
- 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
Google Overview

Learn the company

• Successful acquisitions
  • 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
- 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
  - 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 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:
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

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

404. That's an error.

The requested URL
/%22%3E%3Cimg%20src=%22aaa.jpg%22onerror=javascript:alert('Hello%20Google%20Administrator')%22
was not found on this server. That's all we know.
Google Analytics

Let’s exploit this vulnerability in 2 creative ways:

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

1st 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
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
Google Analytics

- Game over. Achievement unlocked
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
Google Feedburner Stored XSS

Wait, Nothing Happened here!!!, There is “NO” XSS

My Feeds never appear in blister pack

Welcome back, goldshlager19@gmail.com.

FEED TITLE    SUBSCRIBERS
""><img src='fsd.jpg' onerror='javascript:alert(6)'>  1

ddd                0

ddd                0

-----------------------------  0
Google Feedburner Stored XSS

Lets look closer on the features of FeedBurner App
Google Feedburner Unsubscribe XSS

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

Victim: Okay

Let's be friends!!!
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:

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAA .... “><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:
Permission bypass

This document isn’t accessible via direct URL
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
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;
Google Affiliate Network

First Attack:
Manipulating Parameters on connectcommerce.com domain in order to Inject XSS Payload on google.com Domain
Google Affiliate Network

PoC: Stored XSS from Google.com Domain
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
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
Picnik Whols vpn

Site report for vpn.picnik.com

<table>
<thead>
<tr>
<th>Site</th>
<th><a href="http://vpn.picnik.com">http://vpn.picnik.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>picnik.com</td>
</tr>
<tr>
<td>IP address</td>
<td>70.32.137.5</td>
</tr>
<tr>
<td>Country</td>
<td>US</td>
</tr>
<tr>
<td>Date first seen</td>
<td>June 2011</td>
</tr>
<tr>
<td>Domain Registrar</td>
<td>unknown</td>
</tr>
<tr>
<td>Organisation</td>
<td>unknown</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Last reboot</th>
<th>unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site rank</td>
<td>unknown</td>
</tr>
<tr>
<td>Nameserver</td>
<td>ns1.google.com</td>
</tr>
<tr>
<td>DNS admin</td>
<td><a href="mailto:dns-admin@google.com">dns-admin@google.com</a></td>
</tr>
<tr>
<td>Reverse DNS</td>
<td>locke.picnik.com</td>
</tr>
<tr>
<td>Netblock owner</td>
<td>Google Inc.</td>
</tr>
</tbody>
</table>

Check another site:

Netcraft Site Report Gadget [More Netcraft Gadgets]
Google Picnik

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

- So what was the story of vpn picnik?,
- Someone installed by mistake an 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

phpList version 2.10.8 suffers from a local file inclusion vulnerability.

tag: 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
Google Picnik

Game Over

Google Security Team security@google.com
to me
Hey Nir

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

Cheers,
Adam

The Picnik is over
Summary

- Out-Of-The-Box (Hack-In-The-Box) Thinking
- Think different
- Information gathering
- Mixed services
- Permissions
Reference

- [http://www.google.com/about/company/rewardprogram.html](http://www.google.com/about/company/rewardprogram.html) - Google Reward program
- [http://www.google.com/about/company/halloffame.html](http://www.google.com/about/company/halloffame.html) - Google Hall of Fame
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
Subject: HITE Invite
Thank you!

Itzhak “Zuk” Avraham - @IHackBanMe

Nir Goldshlager - @NirGoldshlager