Killing a bounty program
By: Itzhak (Zuk) Avraham; Nir Goldshlager;
# whoami | presentation

Itzhak Avraham (Zuk)
Founder & CEO

Twitter: @ihackbanme
Blog: http://imthezuk.blogspot.com

zuk@zimperium.com
# whoami | presentation

Nir Goldshlager
Senior Web Applications Researcher

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

- Money
- Fame
Reasons for bug bounty

- Money
- Fame
- Okay, mostly fame, 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 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
    • New services – Knol(???)
    • 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 Calender Stored XSS
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
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
Google Calendar Error based

- And again
Google Calendar Error based

- And again ...
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
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

- 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

• The target approved our request.
• Now, let’s force him to delete us, not before we’re going to change our name to:
• AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAA .... "><XSS Payload>
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

404. That's an error.

The requested URL
/%%23E%3Cimg%20src=%%22aaa.jpg%%22onerror=javascript:alert('Hello Google Administrator')>
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 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
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

- Achievement unlocked
Permission bypass – Google Knol
Permission bypass

Unpublished document
Permission bypass

- This document isn’t accessible via URL
Permission bypass

- We don’t have permission to view the document
- Knol Translate does, let’s use the service to show us what we want and cannot access
Permission bypass
Permission bypass

- Private document accessed using translate service.
- Achievement unlocked
Permission bypass

- Blogger
Summary

- 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
Thank you!

Itzhak “Zuk” Avraham - @ihackbanme
Nir Goldshlager - @nirgoldshlager