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

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

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

Mozilla Raises Bug Bounty To $3000 For Security Bugs

Yahoo Japan says 22 million user IDs may have been stolen

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

Microsoft: Hackers obtained high-profile Xbox Live accounts

Nir Goldshlager Founds XSS Vulnerability in Google And Twitter

AMol NAik earned $5000 after finding CSRF vulnerability in Facebook

Google ups bug bounty to $20,000 per flaw
Crowdsourcing security
Responsible Disclosure
REWARD PER BUG, $$$, SWAGS AND T SHIRTS
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, Adobe, Nokia, Avast, Barracuda Networks, MediaFire.
Instant recognition
BENEFITS TO ORGANIZATIONS
Easy to manage
Diversity in Tools, Techniques and Approach
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)

- 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
- Mozila - http://www.mozilla.org/ssl
- Piwik - http://piwik.org/security/
- Barracuda - http://www.barracuda
- Yandex - http://company.yandex.com
- Gallery - http://codex.gallery2.org
- Qmail - http://crypto.to/djb/asn/guant
- AT&T - http://developer.att.com/d/ZipDetailPage.jsp?passedTrmId need to sign up to the Developer
- Tarsnap - https://www.tarsnap.com
- Samsa - https://samsungtvbox.com
- Access - https://www.acessnow.com
- Hex-Rays - http://www.hex-rays.com
- Kaneva - http://docs.kaneva.com
- Cryptocat - https://crypto.cat/bu

PRODUCTS AND SERVICES (HALL OF FAME ONLY)

- HP Zero-Day Initiative (ZDI) - http://www.zerodayinitiative.com/about/benefits/
- Packet Storm - http://packetstormsecurity.com/bounty
- Exodus Intelligence - https://www.exodusintel.com/eip/
- ExploitHub - https://www.exploithub.com/request/index/developmentrequests/
- Insight Partners - https://gvp.isightpartners.com/program_details.gvp?page=3&title=1&section=0
- Netraged - http://pentest.snosoft.com/netrags-eap

PRODUCTS AND SERVICES (HALL OF FAME + SWAG)

- Dropbox - https://www.dropbox.com/special_thanks (Reward: T-shirt)
- Amazon - aws.amazon.com/security/vulnerability-reporting (Reward: T-shirt)
- T1318
- om/us/security/cc308589
- knowledge/articles/66234
- n/dev/hall-of-fame
- security/disclosure
- security/whitehats
- ex.php/Contributors#Security_Researchers
- w/report-security-issue
- port_security.php
- t/security/hall-of-fame
- w.nokiasiemensnetworks.com/about
- m/security/
- security/acknowledgements/
- tycenter/ResearchersAAcknowledgement.html
- m/devblog.asp?a=blog&nbid=2384
- i.com/legal/responsible-disclosure-policy
- node/6857#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
IRISH FORTUNETELLERS
KAY & MARIE SEEN ON TV
HANDS CARTS
CRYSTAL BALL & TEACUP READINGS
NO APP NEEDED
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
Google: Default (Cont’d)

WHAT A CATCH!
REWARD!!

Google Security Team <security@google.com>  
to me  

Hello,

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

<table>
<thead>
<tr>
<th>Quarter</th>
<th>Name</th>
<th>Email or Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q4 2012</td>
<td>Eric &quot;Cosmo&quot; Taylor</td>
<td>@CosmoTheGod</td>
</tr>
<tr>
<td>Q4 2012</td>
<td>Mohamed Ramadan</td>
<td>Attack-Secure</td>
</tr>
<tr>
<td>Q4 2012</td>
<td>Kamal Sevi</td>
<td>@kamalsevi</td>
</tr>
<tr>
<td>Q4 2012</td>
<td>Bharadraj Machiraju - HACK UR LIFE</td>
<td><a href="http://www.tunnelshade.in">www.tunnelshade.in</a></td>
</tr>
<tr>
<td>Q4 2012</td>
<td>Martin Obols</td>
<td><a href="http://makensi.es">http://makensi.es</a></td>
</tr>
<tr>
<td>Q3 2012</td>
<td>Daniel Cocking &amp; Glenn Mangham</td>
<td><a href="http://gmangham.blogspot.co.uk/">http://gmangham.blogspot.co.uk/</a></td>
</tr>
<tr>
<td>Q3 2012</td>
<td>Jason Calvert</td>
<td><a href="http://appset.ws/">http://appset.ws/</a></td>
</tr>
<tr>
<td>Q3 2012</td>
<td>Devesh Bhatt</td>
<td></td>
</tr>
<tr>
<td>Q3 2012</td>
<td>Michele Spagnuolo</td>
<td><a href="http://michele.spagnuolo.me">http://michele.spagnuolo.me</a></td>
</tr>
<tr>
<td>Q3 2012</td>
<td>Amir Etemadine</td>
<td>@Zenofex</td>
</tr>
<tr>
<td>Q3 2012</td>
<td>Shai Rod</td>
<td>@NightRang3r</td>
</tr>
<tr>
<td>Q3 2012</td>
<td>Sam &quot; trueui &quot; Jay</td>
<td><a href="http://trueui.blogspot.com">http://trueui.blogspot.com</a></td>
</tr>
<tr>
<td>Q3 2012</td>
<td>Andrs Atteka</td>
<td>Blue Coat Systems</td>
</tr>
<tr>
<td>Q3 2012</td>
<td>Saket Jayodia</td>
<td>Dzire 2 Dzine (D2D): Logo Designing</td>
</tr>
<tr>
<td>Q3 2012</td>
<td>Takeishi Terada</td>
<td>Mitsui Bussan Secure Directions, Inc.</td>
</tr>
<tr>
<td>Q3 2012</td>
<td>Riyaz Walkkar</td>
<td><a href="http://www.riyazwalkkar.com">http://www.riyazwalkkar.com</a></td>
</tr>
<tr>
<td>Q3 2012</td>
<td>Eywind Niklassson</td>
<td><a href="http://eywinderiklassen.se/">http://eywinderiklassen.se/</a></td>
</tr>
<tr>
<td>Q3 2012</td>
<td>Dmitry Shcherbatov</td>
<td><a href="http://vk.com/id133353396">http://vk.com/id133353396</a></td>
</tr>
<tr>
<td>Q3 2012</td>
<td>João Lucas Melo Braso</td>
<td>White Hat Hackers Consultoria de Segurança da Informação LTDA (Brazil)</td>
</tr>
<tr>
<td>Q3 2012</td>
<td>Masato Kinugawa</td>
<td></td>
</tr>
<tr>
<td>Q3 2012</td>
<td>Nils Juenemann</td>
<td><a href="http://www.nilsjuenemann.de/">http://www.nilsjuenemann.de/</a></td>
</tr>
<tr>
<td>Q3 2012</td>
<td>Sergey Markov</td>
<td></td>
</tr>
</tbody>
</table>
Obvious Vulnerabilities

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

Site:secure.paypal.com inurl:.com

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/affiliates/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/affiliates/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/affiliates/paypal@bmezine.com
  A description for this result is not available because of this site's robots.txt – learn more.

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

- https://secure.paypal.com/affiliates-thomash@throne...
  A description for this result is not available because of this site's robots.txt – learn more.
Information Disclosure Channel Intelligence
Obvious Vulnerabilities

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

Site: apple.com inurl: admin


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
Freebase: XSS

Obvious Vulnerabilities
Zong.com: XSS
Obvious Vulnerabilities

Zagat.com: XSS
cards.io:Ififrame Injection
Obvious Vulnerabilities

- Default usernames/password
- Sensitive information disclosure
- Admin interfaces
- XSS

- Account enumeration

- Clickjacking
Account Enumeration

Error message for correct username

We've noticed you've had some difficulties signing in. We'd like to help.

Error message for non-existing username

Please enter a valid username and password. Check to see if you have activated your Caps Lock key.
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
Soundcloud: enumeration via a "/?author=x" redirection

```plaintext
D:\Research\PythonScripts>wp_userenum.py
Starting enumeration on https://blog.soundcloud.com
Enumerating the first 60 users
```
Sorry, deveshbhatt11@gmail.com is not recognized as a user name or an e-mail address.
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.
Obvious Vulnerabilities

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

- Clickjacking
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
Fixing is important
False positives
Responsible Disclosure is hard to comply with
WAY FORWARD
Best model for security testing
WIN – WIN
SITUATION
Increase in security awareness
References

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


http://www.riyazwalikar.com/

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

http://ravivaldiyaphotography.com/
QUESTIONS?
THANK YOU!!