HI THIS IS URGENT PLZ FIX ASAP: Critical Vulnerabilities and Bug Bounty Programs

black hat USA 2015

Kymberlee Price
Senior Director of Researcher Operations
Bugcrowd
@Kym_Possible

bugcrowd

UBM Tech

whoami?

- Senior Director of a Red Team
- PSIRT Case Manager
- Data Analyst
- Internet Crime Investigator
- Behavioral Psychologist

@kym_possible

Agenda

- Intro
- Red
- Blue
- tl;dr
- Questions

What this talk isn't

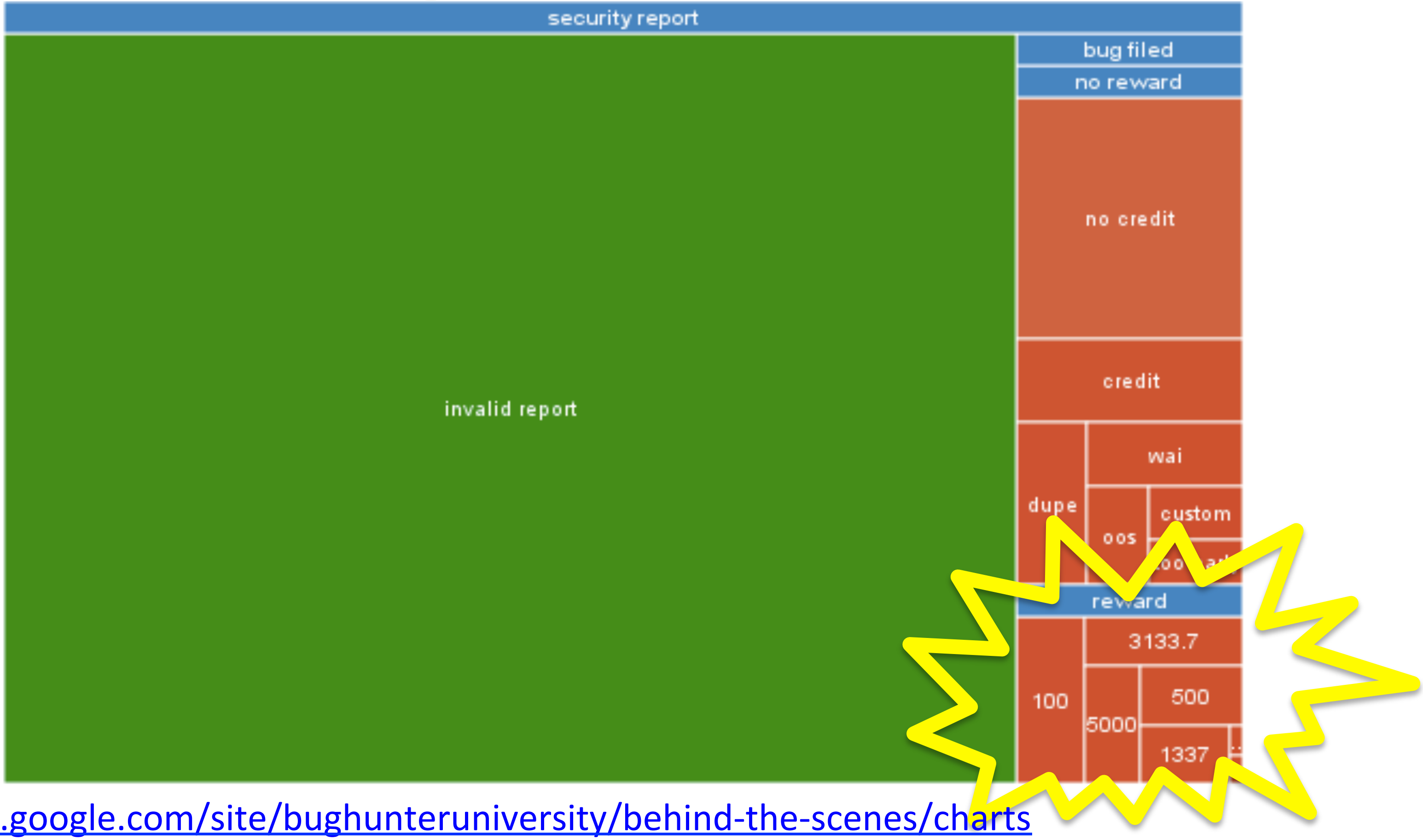
- Determining if a bug bounty program is appropriate for your company
- Selling you a bug bounty program
- Recruiting you to be a bounty hunter

black hat®
USA 2015

C:\intro

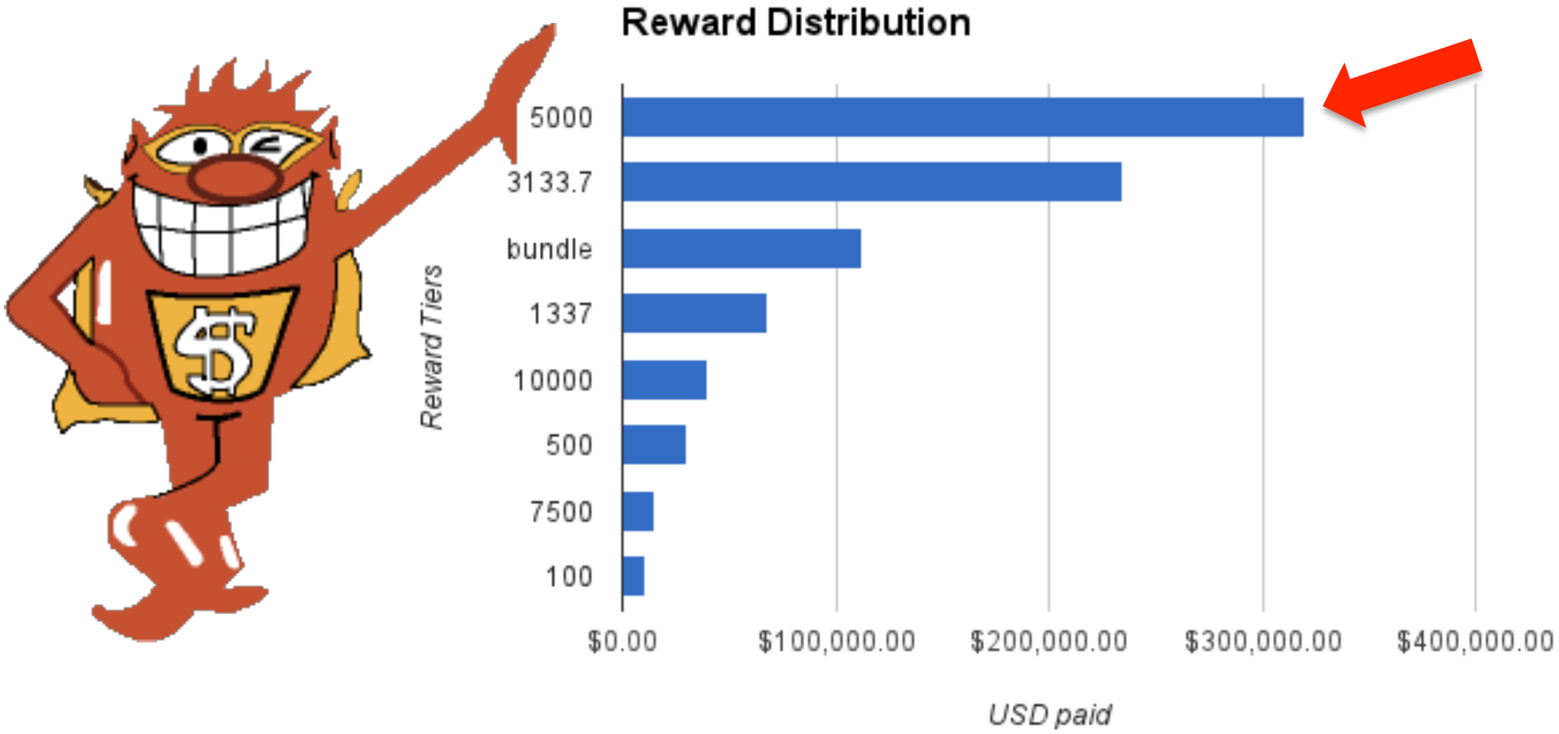
Google

Google VRP 2014



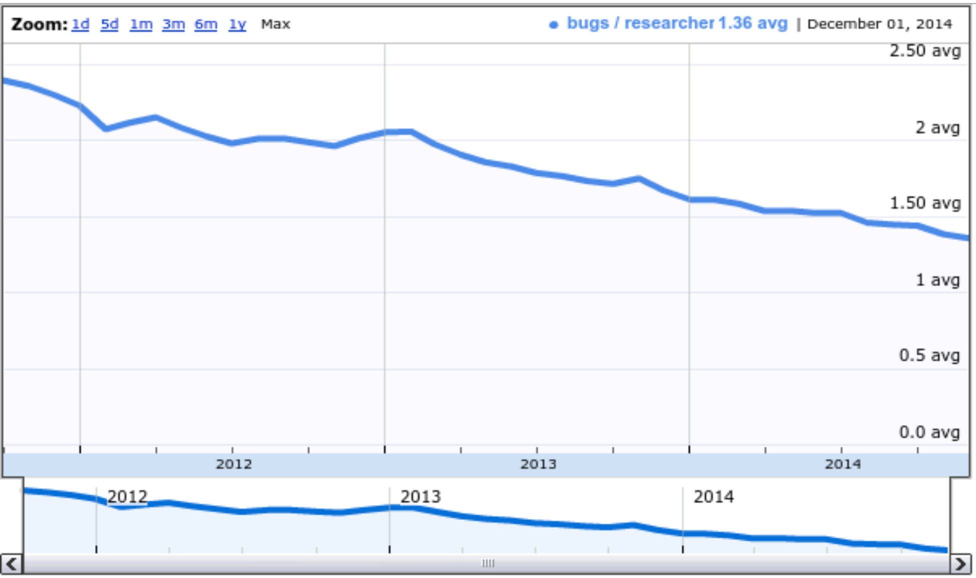
https://sites.google.com/site/bughunteruniversity/behind-the-scenes/charts

Google VRP 2014

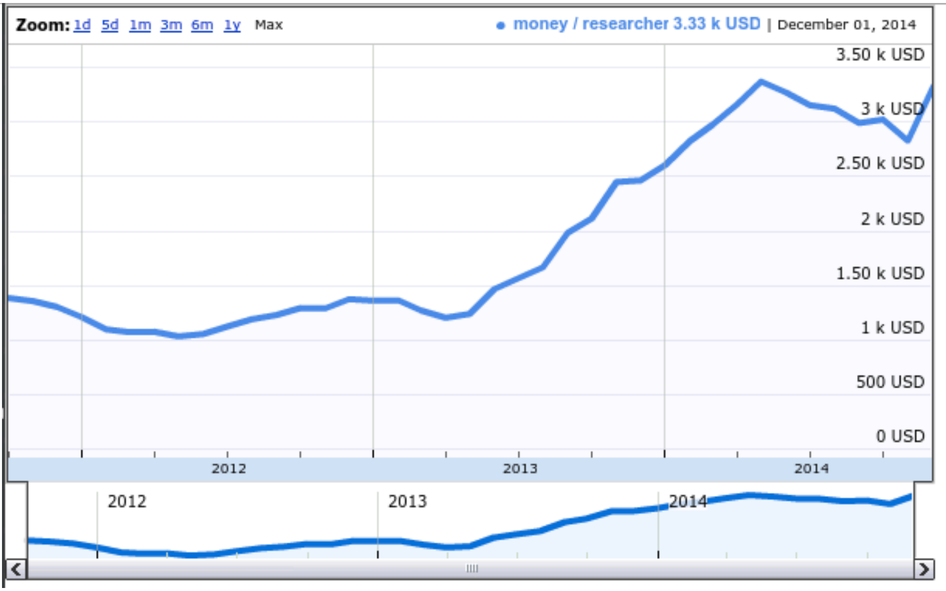


https://sites.google.com/site/bughunteruniversity/behind-the-scenes/charts

Google VRP 2014



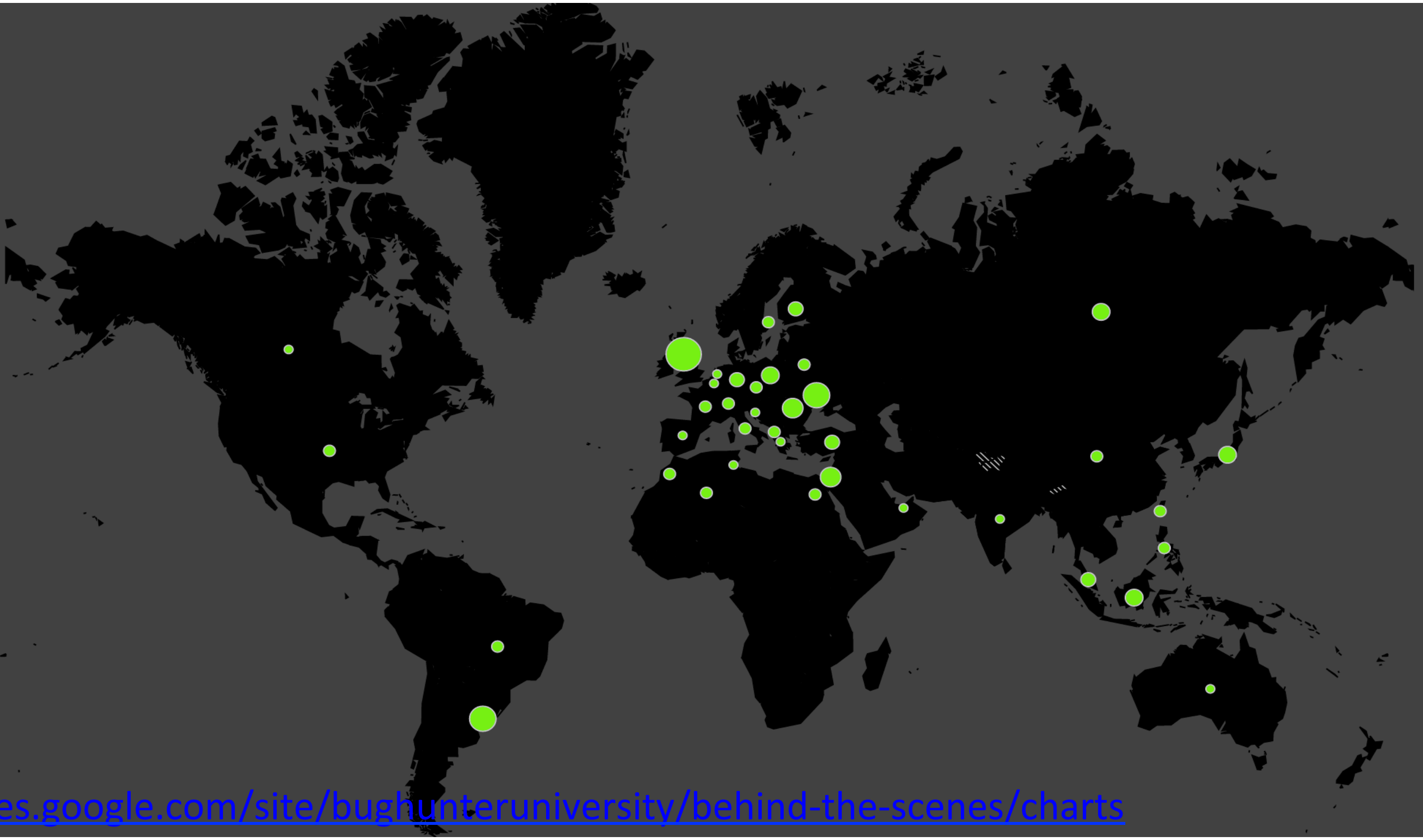
Bugs found per active researcher



Payouts

https://sites.google.com/site/bughunteruniversity/behind-the-scenes/charts

Google VRP 2014



https://sites.google.com/site/bughunteruniversity/behind-the-scenes/charts

facebook®

facebook 2014

Submissions:

- 17,011 submissions – 16% increase YoY
- 61 high severity bugs – 49% increase YoY
- Minimum reward: $500

Geography:

- 65 countries received rewards – 12% increase YoY
- 123 countries reporting bugs

https://www.facebook.com/notes/facebook-bug-bounty/2014-highlights-bounties-get-better-than-ever/1026610350686524

facebook 2014

Payouts:

- $1.3 million to 321 researchers
- Average reward: $1,788.

The top 5 researchers earned a total of

$256,750

Top 5 Countries:

• India – 196 valid bugs	$1,343	$263,228
• Egypt – 81 valid bugs	$1,220	$98,820
• USA – 61 valid bugs	$2,470	$150,670
• UK – 28 valid bugs	$2,768	$77,504
• Philippines – 27 valid bugs	$1,093	$29,511
		$619,733

bugcrowd

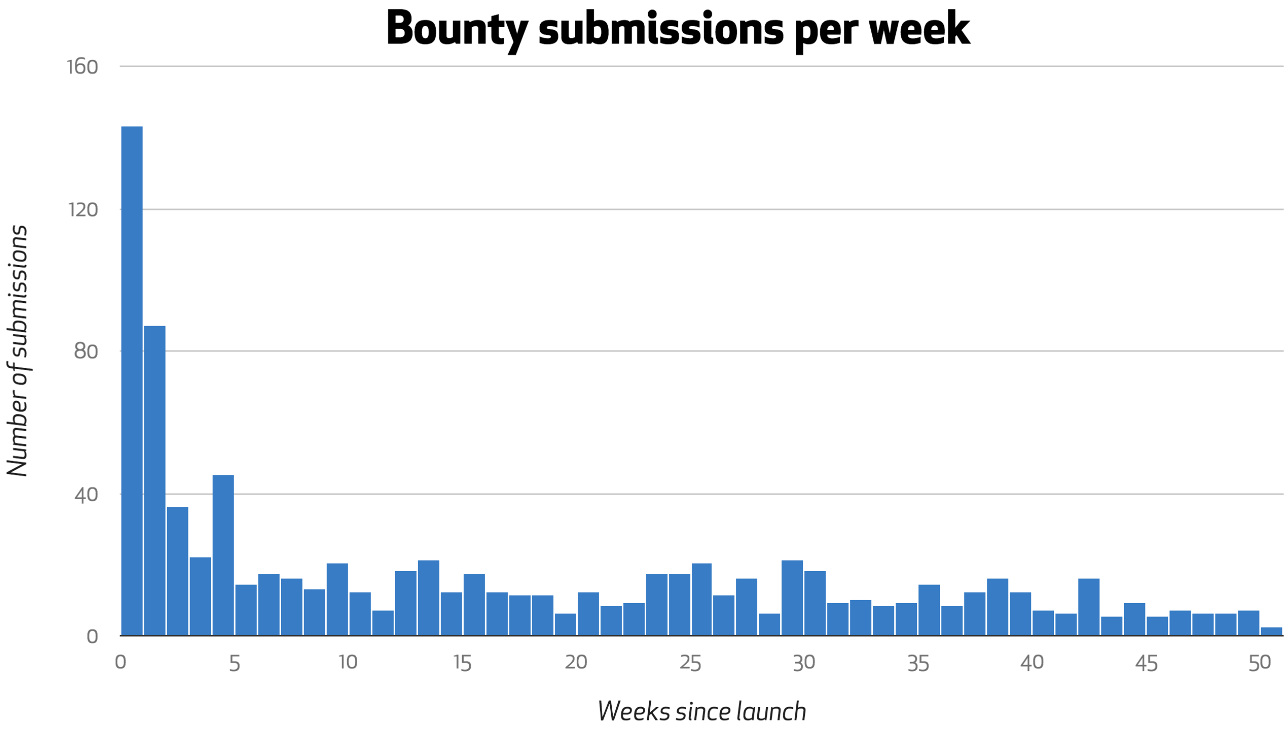
GitHub

GitHub 2014

- 73 vulnerabilities identified and fixed
- 1,920 submissions
- 33 researchers earned $50,100 for 57 bugs
- Minimum reward: $200
- Doubled maximum bounty payout to celebrate

https://github.com/blog/1951-github-security-bug-bounty-program-turns-one

GitHub 2014



https://github.com/blog/1951-github-security-bug-bounty-program-turns-one

Microsoft

Microsoft

Online Services: O365 and Azure

- 46 rewarded submissions since launch in late Sept 2014
- Reward amounts to each researcher not published
- Program offers minimum $500 up to $15,000

Mitigation Bypass

- Up to $100,000 for novel exploitation techniques against protections built into the OS

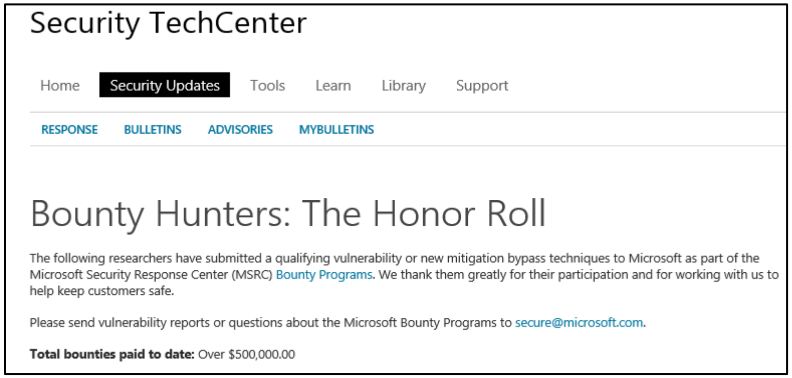
Bounty for Defense

- Up to $100,000 for defensive ideas accompanying a qualifying Mitigation Bypass submission

https://technet.microsoft.com/en-us/security/dn469163.aspx

Microsoft

Software Bounties



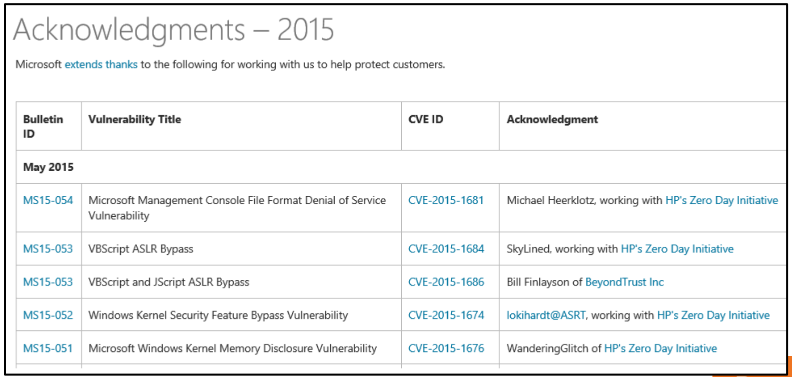
Security TechCenter

Bounty Hunters: The Honor Roll

The following researchers have submitted a qualifying vulnerability or new mitigation bypass techniques to Microsoft as part of the Microsoft Security Response Center (MSRC) Bounty Programs. We thank them greatly for their participation and for working with us to help keep customers safe.

Please send vulnerability reports or questions about the Microsoft Bounty Programs to secure@microsoft.com.

Total bounties paid to date: Over $500,000.00

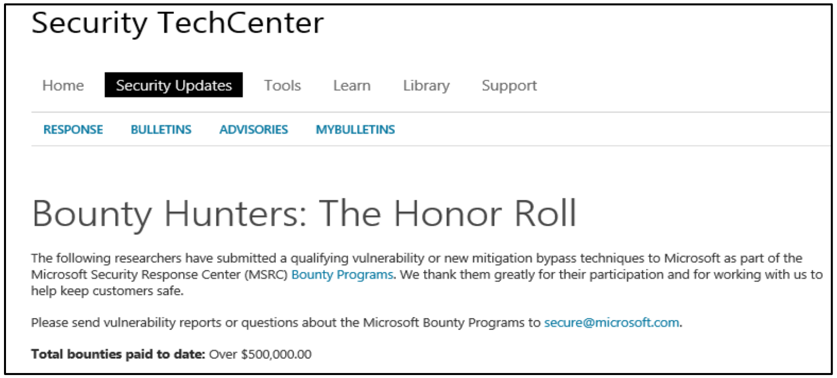


Acknowledgments – 2015

Microsoft extends thanks to the following for working with us to help protect customers.

Bulletin ID	Vulnerability Title	CVE ID	Acknowledgment
May 2015			
MS15-054	Microsoft Management Console File Format Denial of Service Vulnerability	CVE-2015-1681	Michael Heerklotz, working with HP's Zero Day Initiative
MS15-053	VBScript ASLR Bypass	CVE-2015-1684	SkyLined, working with HP's Zero Day Initiative
MS15-053	VBScript and JScript ASLR Bypass	CVE-2015-1686	Bill Finlayson of BeyondTrust Inc
MS15-052	Windows Kernel Security Feature Bypass Vulnerability	CVE-2015-1674	lokihardt@ASRT, working with HP's Zero Day Initiative
MS15-051	Microsoft Windows Kernel Memory Disclosure Vulnerability	CVE-2015-1676	WanderingGlitch of HP's Zero Day Initiative

Online Services



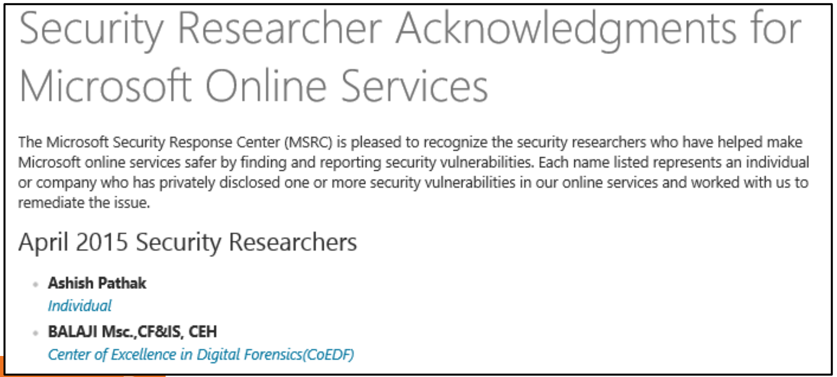
Security TechCenter

Bounty Hunters: The Honor Roll

The following researchers have submitted a qualifying vulnerability or new mitigation bypass techniques to Microsoft as part of the Microsoft Security Response Center (MSRC) Bounty Programs. We thank them greatly for their participation and for working with us to help keep customers safe.

Please send vulnerability reports or questions about the Microsoft Bounty Programs to secure@microsoft.com.

Total bounties paid to date: Over $500,000.00



Security Researcher Acknowledgments for Microsoft Online Services

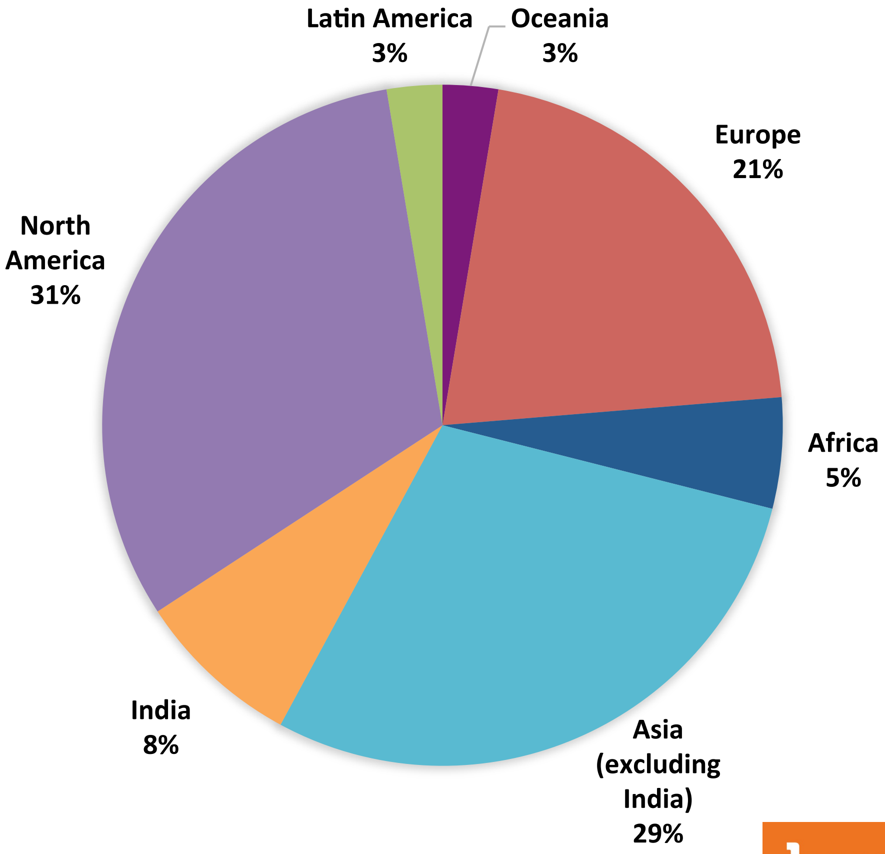
The Microsoft Security Response Center (MSRC) is pleased to recognize the security researchers who have helped make Microsoft online services safer by finding and reporting security vulnerabilities. Each name listed represents an individual or company who has privately disclosed one or more security vulnerabilities in our online services and worked with us to remediate the issue.

April 2015 Security Researchers

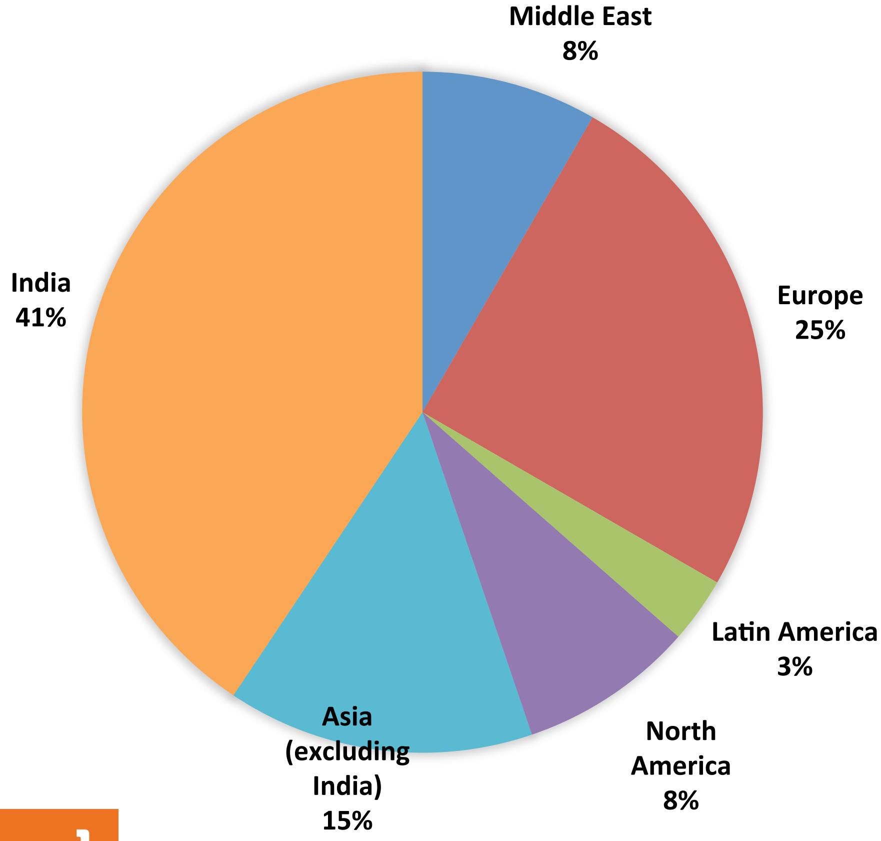
- **Ashish Pathak**
  Individual
- **BALAJI Msc.,CF&IS, CEH**
  Center of Excellence in Digital Forensics(CoEDF)

Microsoft

RESEARCHERS - SOFTWARE

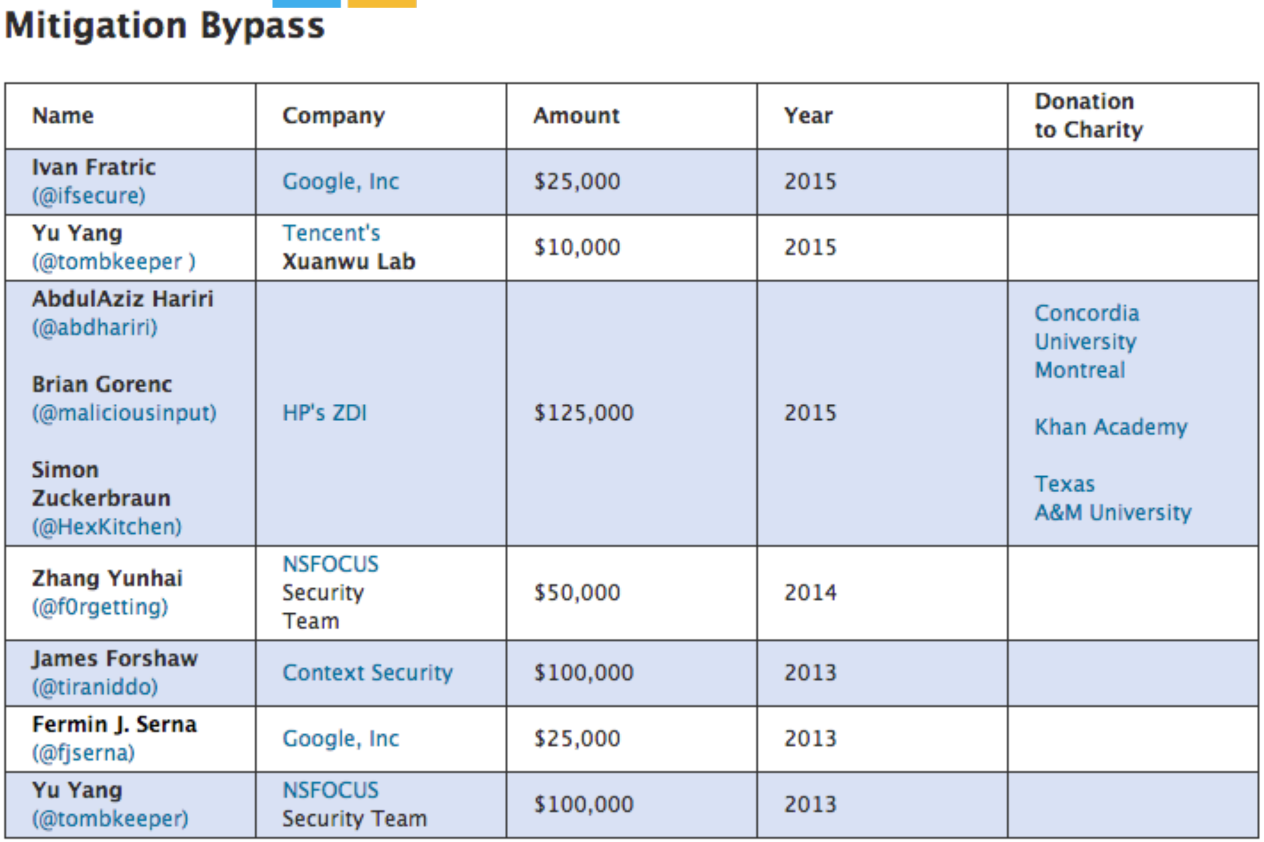


RESEARCHERS – ONLINE SERVICES



bugcrowd

Microsoft



Mitigation Bypass

Name	Company	Amount	Year	Donation to Charity
Ivan Fratric (@ifsecure)	Google, Inc	$25,000	2015	
Yu Yang (@tombkeeper)	Tencent's Xuanwu Lab	$10,000	2015	
AbdulAziz Hariri (@abdhariri) Brian Gorenc (@maliciousinput) Simon Zuckerbraun (@HexKitchen)	HP's ZDI	$125,000	2015	Concordia University Montreal Khan Academy Texas A&M University
Zhang Yunhai (@f0rgetting)	NSFOCUS Security Team	$50,000	2014	
James Forshaw (@tiraniddo)	Context Security	$100,000	2013	
Fermin J. Serna (@fjserna)	Google, Inc	$25,000	2013	
Yu Yang (@tombkeeper)	NSFOCUS Security Team	$100,000	2013	

https://technet.microsoft.com/en-us/security/dn469163.aspx

bugcrowd

bugcrowd

bugcrowd 2013-present

- 166 Customer programs
- 37,227 submissions
  - 7,958 non-duplicate, valid vulnerabilities
  - Rewarded 3,621 submissions
- $724,839 paid out
  - Average reward $200.81, top reward of $10,000

http://bgcd.co/bcsbb2015

bugcrowd 2013-present

Big Bugs:

- 4.39 high- or critical-priority vulnerabilities per program
- Total: 729 high-priority vulnerabilities
  - 175 rated “critical” by trained application security engineers

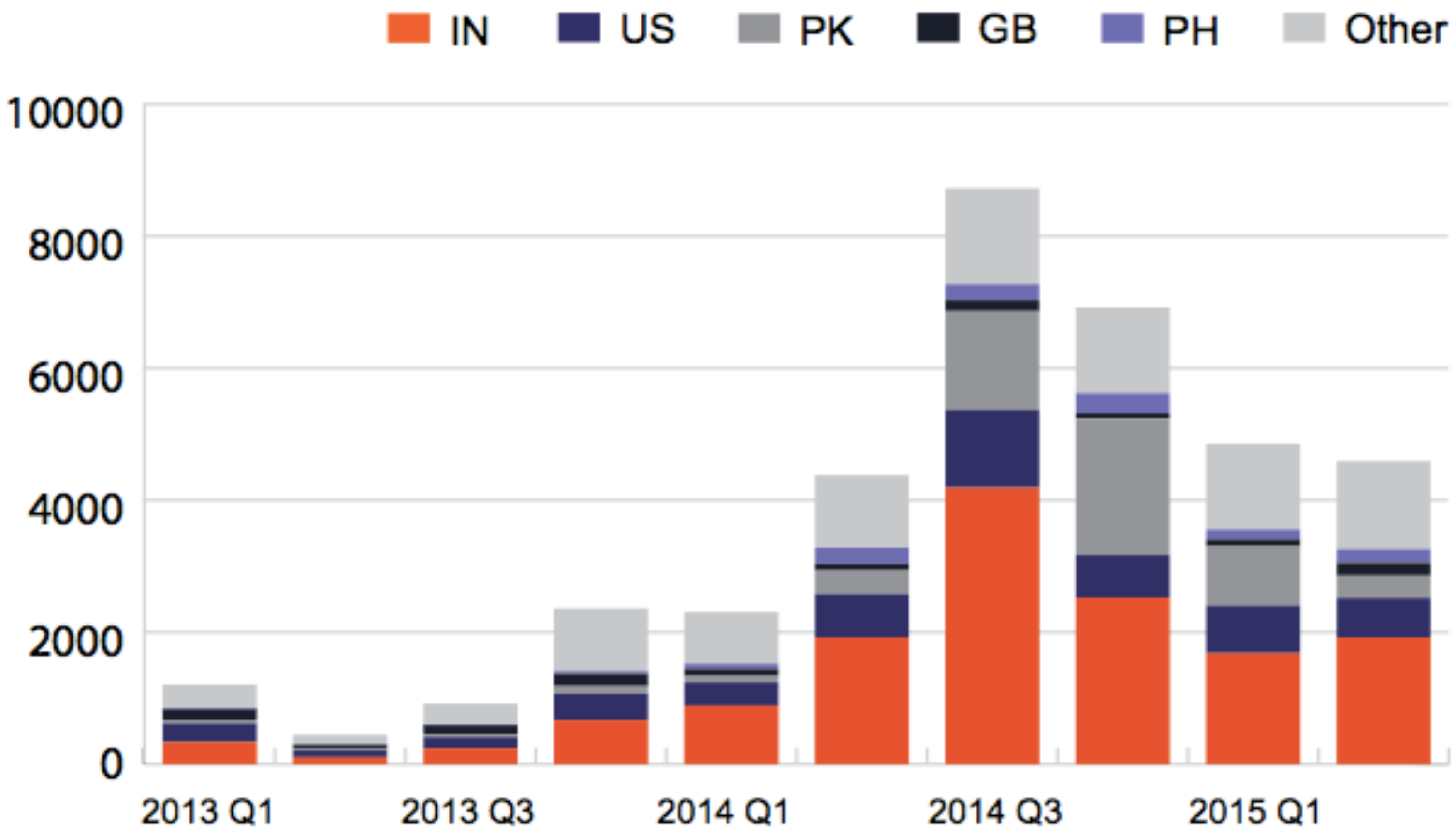
http://bgcd.co/bcsbb2015

P1 and P2 Defined

- P1 – CRITICAL
  Vulnerabilities that cause a privilege escalation on the platform from unprivileged to admin, allows remote code execution, financial theft, etc. Examples: Vertical Authentication bypass, SSRF, XXE, SQL Injection, User authentication bypass

- P2 – SEVERE
  Vulnerabilities that affect the security of the platform including the processes it supports. Examples: Lateral authentication bypass, Stored XSS, some CSRF depending on impact

Quarterly Submissions by Geography



bugcrowd

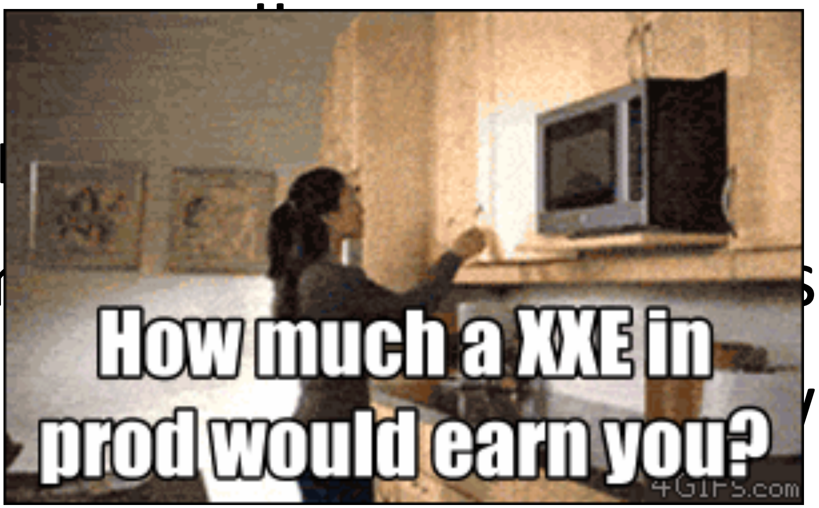
black hat USA 2015

C:\red

UBM Tech

Google

- XXE in production exploited using Google Toolbar bu
- Reported i
- Fredrik Alm sson
- Google res ithin 20 minutes



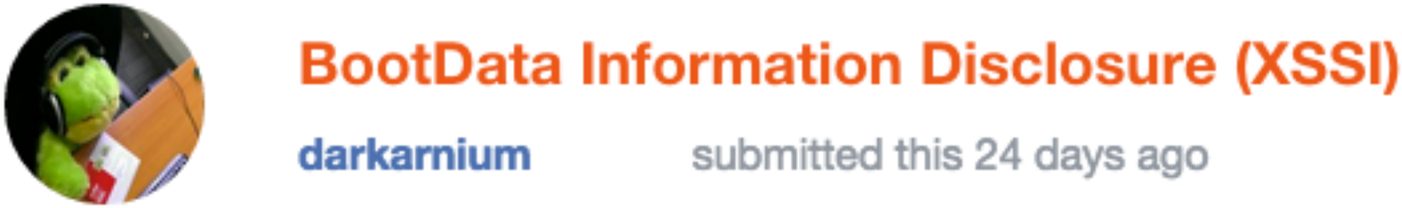
facebook

- Reginaldo Silva reported an XML external entity vulnerability within a PHP page that would have allowed a hacker to change Facebook's use of Gmail as an OpenID provider to a hacker-controlled URL, before servicing requests with malicious XML code.

facebook

- Laxman Muthiyah identified a way for a malicious user to delete any photo album owned by a user, page, or group on Facebook. He found this vulnerability when he tried to delete one of his own photo albums using the graph explorer access token.

SIMPLE



BootData Information Disclosure (XSSI)

darkarnium submitted this 24 days ago

- Cross-domain Information Disclosure

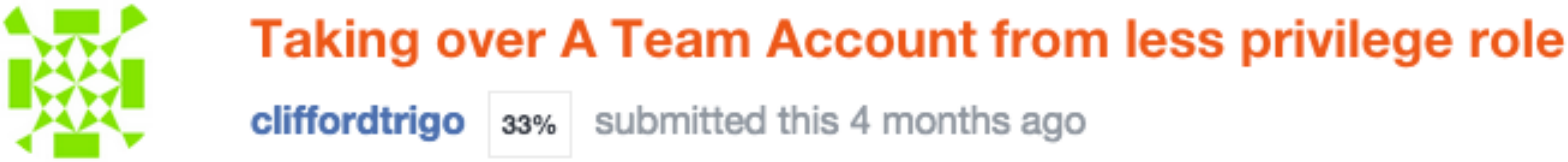
smartsheet

Taking over A Team Account from less privilege role

cliffordtrigo submitted this 4 months ago

- Clifford’s first private bounty invitation
- Launched at midnight in PH
- Found an IDOR → elevation of privilege

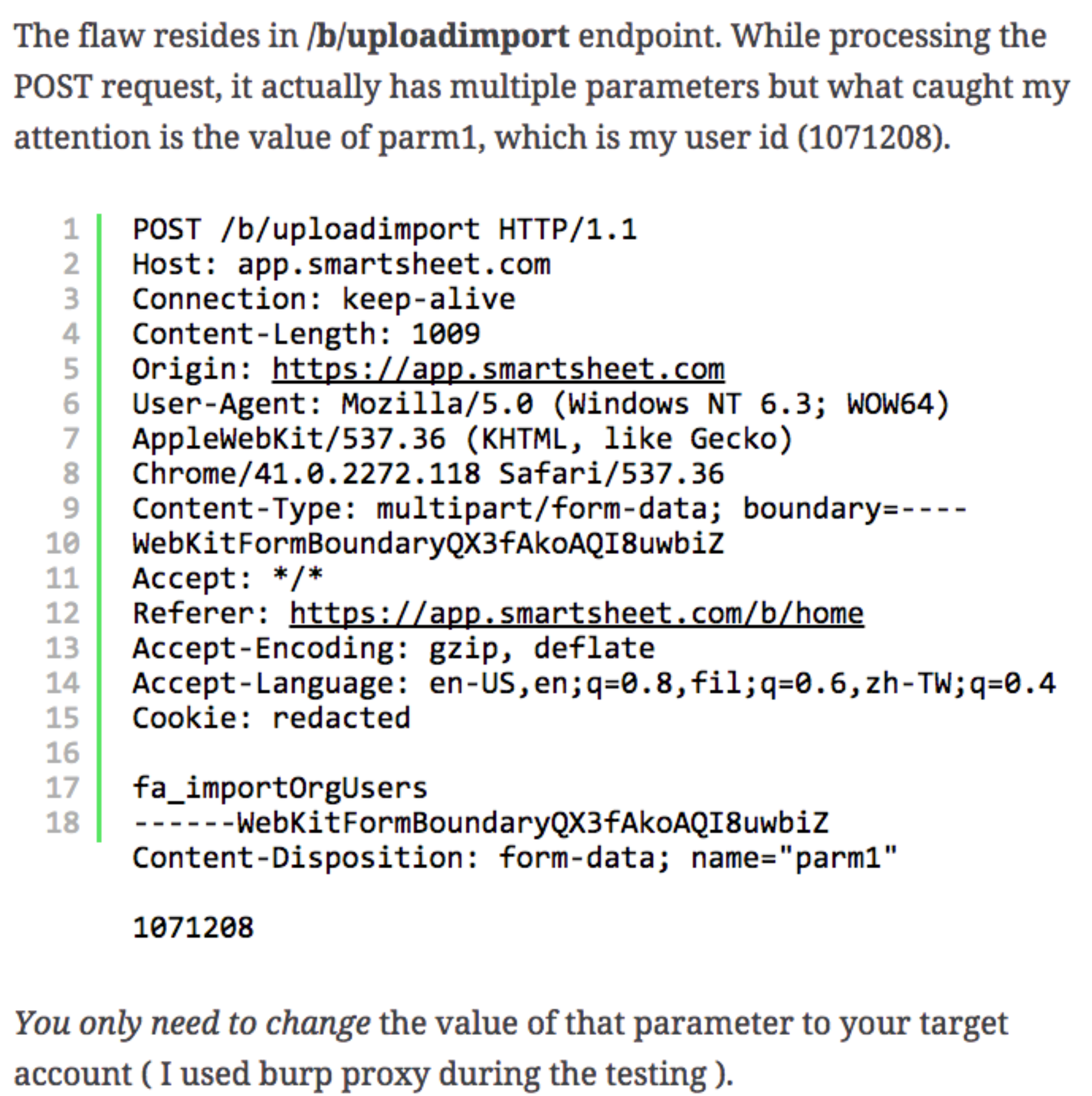
smartsheet



Taking over A Team Account from less privilege role

cliffordtrigo 33% submitted this 4 months ago

- Bug in “import user” feature
- no check whether the user who is requesting the import has the the right privilege



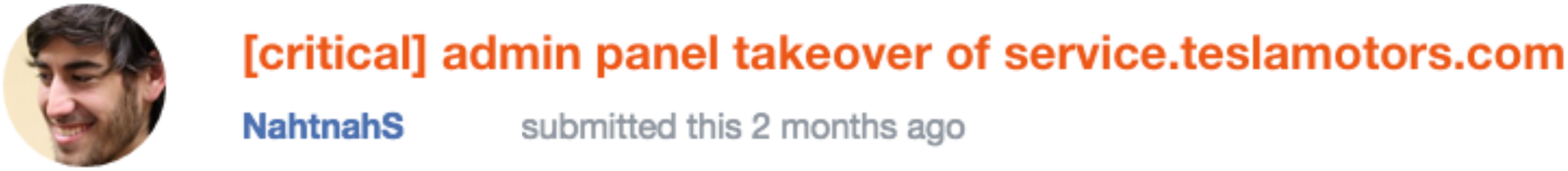
The flaw resides in **/b/uploadimport** endpoint. While processing the POST request, it actually has multiple parameters but what caught my attention is the value of parm1, which is my user id (1071208).

```
POST /b/uploadimport HTTP/1.1
Host: app.smartsheet.com
Connection: keep-alive
Content-Length: 1009
Origin: https://app.smartsheet.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/41.0.2272.118 Safari/537.36
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryQX3fAkoAQI8uwbiZ
Accept: */*
Referer: https://app.smartsheet.com/b/home
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8,fil;q=0.6,zh-TW;q=0.4
Cookie: redacted

fa_importOrgUsers
------WebKitFormBoundaryQX3fAkoAQI8uwbiZ
Content-Disposition: form-data; name="parm1"

1071208
```

You only need to change the value of that parameter to your target account (I used burp proxy during the testing).

https://www.cliffordtrigo.info/hijacking-smartsheet-accounts/

TESLA



[critical] admin panel takeover of service.teslamotors.com

NahtnahS submitted this 2 months ago

- IDOR → elevation of privilege

1) login to https://service.teslamotors.com/

2) navigate to https://service.teslamotors.com/admin/bulletins

3) now you are admin, you can delete, modify and publish documents

http://nbsriharsha.blogspot.in/2015/07/a-style-of-bypassing-authentication.html

bugcrowd

black hat®
USA 2015

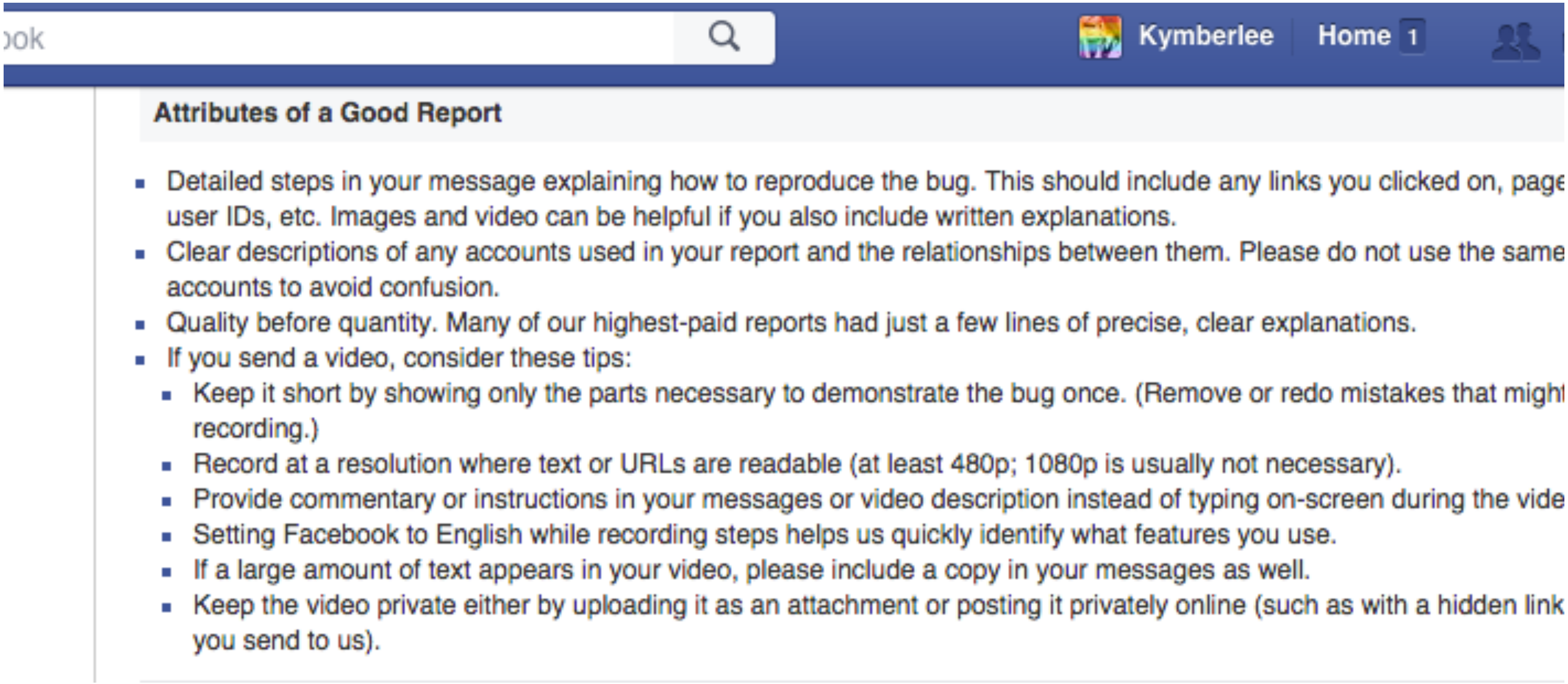
C:\blue

UBM Tech

Rapid triage & prioritization

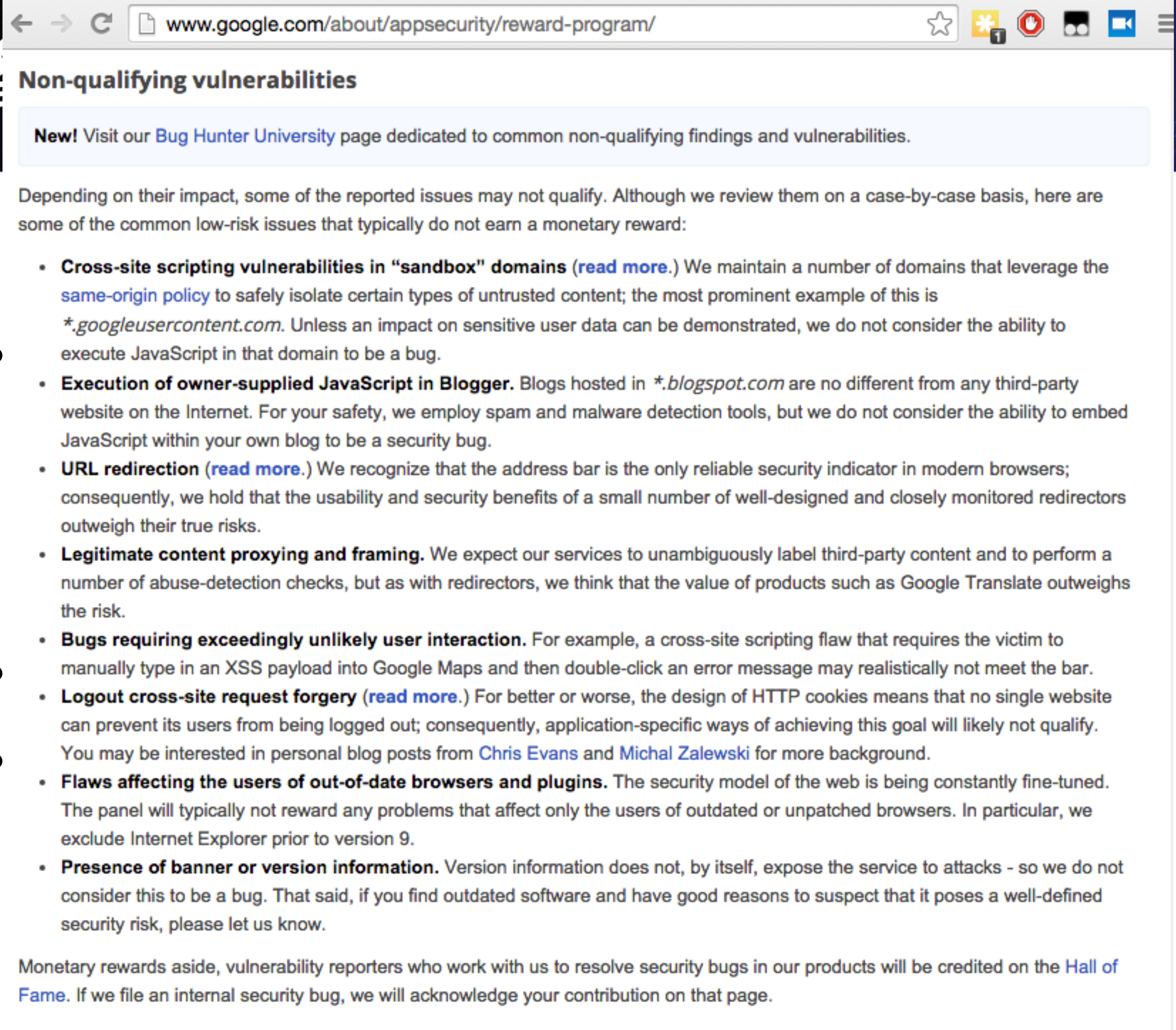
(get to the P1's faster)

- Submission framework & expectations
- ~~Eloquence of written communication~~
- Clear in and out of scope documentation



Attributes of a Good Report

- Detailed steps in your message explaining how to reproduce the bug. This should include any links you clicked on, page user IDs, etc. Images and video can be helpful if you also include written explanations.
- Clear descriptions of any accounts used in your report and the relationships between them. Please do not use the same accounts to avoid confusion.
- Quality before quantity. Many of our highest-paid reports had just a few lines of precise, clear explanations.
- If you send a video, consider these tips:
  - Keep it short by showing only the parts necessary to demonstrate the bug once. (Remove or redo mistakes that might recording.)
  - Record at a resolution where text or URLs are readable (at least 480p; 1080p is usually not necessary).
  - Provide commentary or instructions in your messages or video description instead of typing on-screen during the vide
  - Setting Facebook to English while recording steps helps us quickly identify what features you use.
  - If a large amount of text appears in your video, please include a copy in your messages as well.
  - Keep the video private either by uploading it as an attachment or posting it privately online (such as with a hidden link you send to us).



www.google.com/about/appsecurity/reward-program/

Non-qualifying vulnerabilities

New! Visit our Bug Hunter University page dedicated to common non-qualifying findings and vulnerabilities.

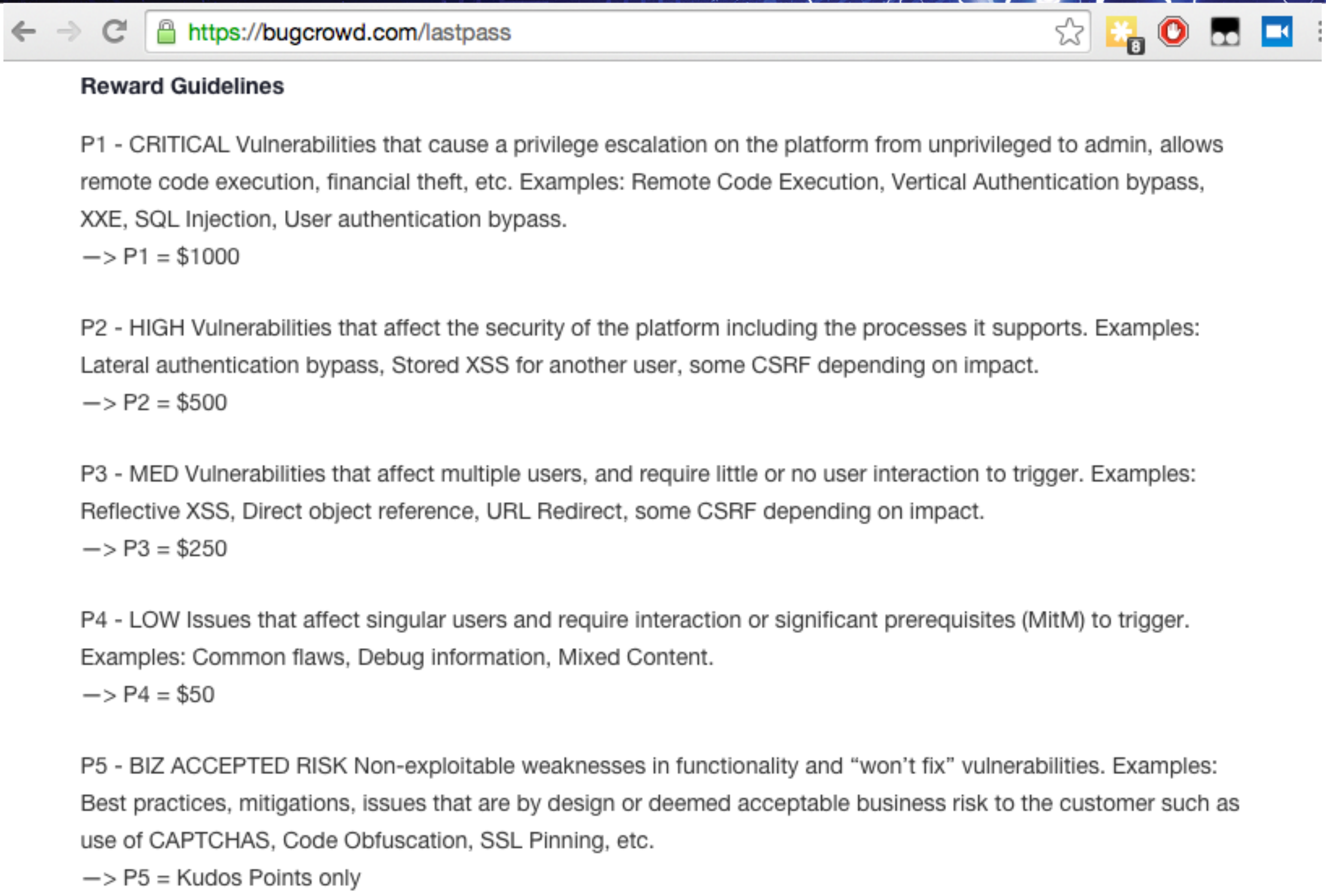
Depending on their impact, some of the reported issues may not qualify. Although we review them on a case-by-case basis, here are some of the common low-risk issues that typically do not earn a monetary reward:

- **Cross-site scripting vulnerabilities in "sandbox" domains** (read more.) We maintain a number of domains that leverage the same-origin policy to safely isolate certain types of untrusted content; the most prominent example of this is **.googleusercontent.com*. Unless an impact on sensitive user data can be demonstrated, we do not consider the ability to execute JavaScript in that domain to be a bug.
- **Execution of owner-supplied JavaScript in Blogger.** Blogs hosted in **.blogspot.com* are no different from any third-party website on the Internet. For your safety, we employ spam and malware detection tools, but we do not consider the ability to embed JavaScript within your own blog to be a security bug.
- **URL redirection** (read more.) We recognize that the address bar is the only reliable security indicator in modern browsers; consequently, we hold that the usability and security benefits of a small number of well-designed and closely monitored redirectors outweigh their true risks.
- **Legitimate content proxying and framing.** We expect our services to unambiguously label third-party content and to perform a number of abuse-detection checks, but as with redirectors, we think that the value of products such as Google Translate outweighs the risk.
- **Bugs requiring exceedingly unlikely user interaction.** For example, a cross-site scripting flaw that requires the victim to manually type in an XSS payload into Google Maps and then double-click an error message may realistically not meet the bar.
- **Logout cross-site request forgery** (read more.) For better or worse, the design of HTTP cookies means that no single website can prevent its users from being logged out; consequently, application-specific ways of achieving this goal will likely not qualify. You may be interested in personal blog posts from Chris Evans and Michal Zalewski for more background.
- **Flaws affecting the users of out-of-date browsers and plugins.** The security model of the web is being constantly fine-tuned. The panel will typically not reward any problems that affect only the users of outdated or unpatched browsers. In particular, we exclude Internet Explorer prior to version 9.
- **Presence of banner or version information.** Version information does not, by itself, expose the service to attacks - so we do not consider this to be a bug. That said, if you find outdated software and have good reasons to suspect that it poses a well-defined security risk, please let us know.

Monetary rewards aside, vulnerability reporters who work with us to resolve security bugs in our products will be credited on the Hall of Fame. If we file an internal security bug, we will acknowledge your contribution on that page.

Rapid triage & prioritization

- Clear the queue daily
- Communicate your priorities
- Dealing with Duplicates



https://bugcrowd.com/lastpass

Reward Guidelines

P1 - CRITICAL Vulnerabilities that cause a privilege escalation on the platform from unprivileged to admin, allows remote code execution, financial theft, etc. Examples: Remote Code Execution, Vertical Authentication bypass, XXE, SQL Injection, User authentication bypass.
—> P1 = $1000

P2 - HIGH Vulnerabilities that affect the security of the platform including the processes it supports. Examples: Lateral authentication bypass, Stored XSS for another user, some CSRF depending on impact.
—> P2 = $500

P3 - MED Vulnerabilities that affect multiple users, and require little or no user interaction to trigger. Examples: Reflective XSS, Direct object reference, URL Redirect, some CSRF depending on impact.
—> P3 = $250

P4 - LOW Issues that affect singular users and require interaction or significant prerequisites (MitM) to trigger. Examples: Common flaws, Debug information, Mixed Content.
—> P4 = $50

P5 - BIZ ACCEPTED RISK Non-exploitable weaknesses in functionality and “won’t fix” vulnerabilities. Examples: Best practices, mitigations, issues that are by design or deemed acceptable business risk to the customer such as use of CAPTCHAS, Code Obfuscation, SSL Pinning, etc.
—> P5 = Kudos Points only

bugcrowd

Is it worth the hassle?

"In Mortal Combat terms, it is a 'Fatality' "

"If we get nothing else from the bounty, this vuln was worth the whole program alone. Due to the critical nature of the issue, we immediately patched the Prod servers this evening to close this exploit. We are also reviewing all logs since we don't delete them yet to identify any instance where this ever happened in the past."

How to reduce noise

- Publish and stick to your program SLA
- Stop rewarding bad behavior
- Don’t create bad behavior
  - – Reward consistently
  - – Reward fairly
  - – Fix quickly
  - – Again with the documentation

black hat

USA 2015

C:\tl;dr

UBM Tech

conclusions

- Bug bounties successfully generate high severity vulnerability disclosures, delivering real value that improves application security for companies of all sizes.
- Crowdsourcing engages skilled researchers around the world that you may not have heard of.

call to action

- Write strong scope documentation
- Clear submission expectations
- Provide feedback
- Stay consistently engaged
- Reward good behavior

HI THIS IS URGENT PLZ FIX ASAP: Critical Vulnerabilities and Bug Bounty Programs

black hat
USA 2015

Kymberlee Price
Senior Director of Researcher Operations
Bugcrowd
@Kym_Possible

bugcrowd

UBM
Tech