

Decoding Bug Bounty Programs

Jon Rose





It's all about
YOU

What is your Role?

Builder

Breaker

Defender

Bug Bounty Programs are
Revolutionizing
the way businesses
protect themselves

ONLY?



**Traditional security
testing is**

Dead

1. Automated tools **don't** work
2. Waterfall security **isn't** Agile
3. Massive **shortage** of talent
4. **Cost** prohibitive

WANTED

Bug Bounty Program



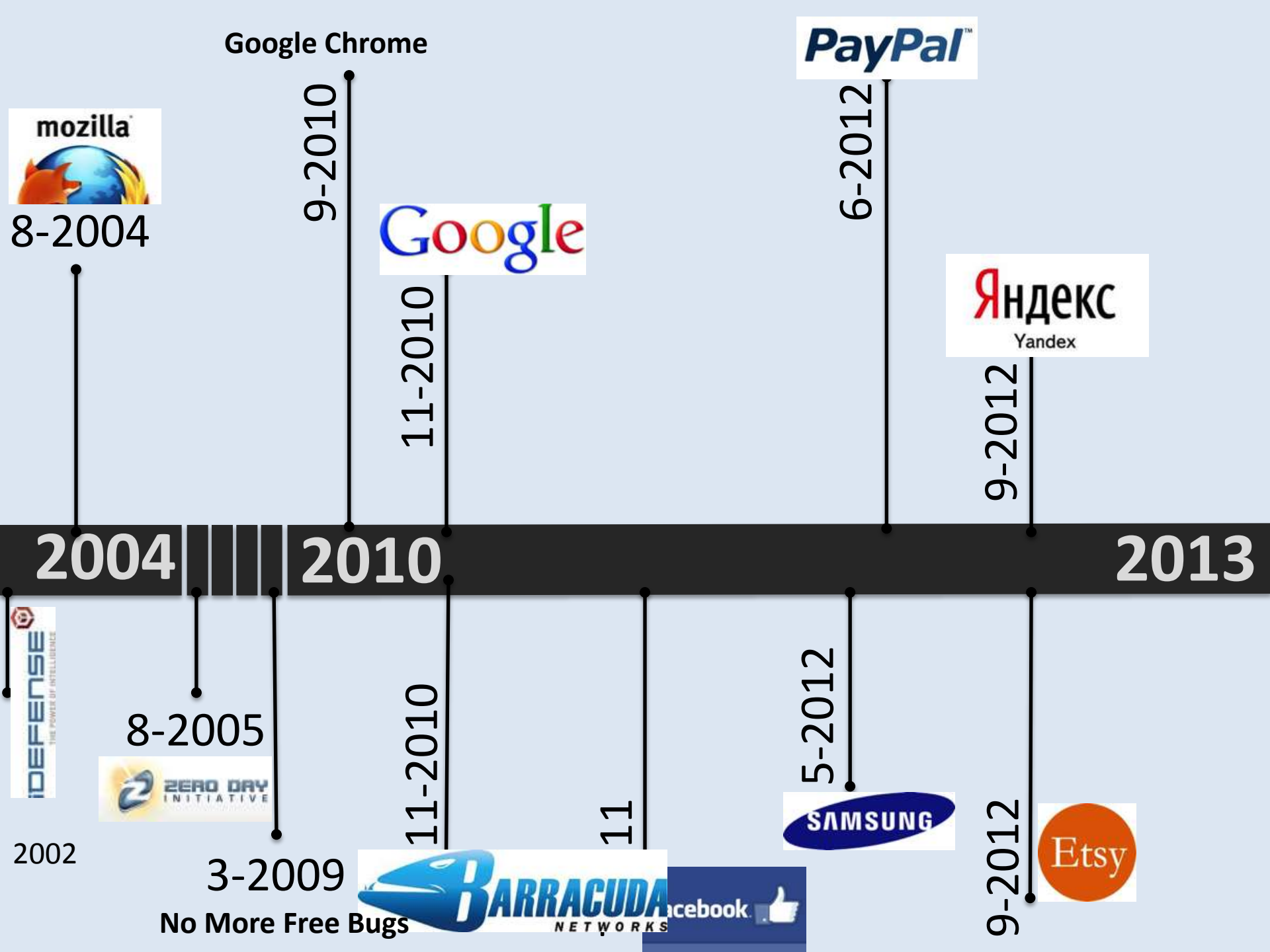
PATCHED or ALIVE

CASH REWARD

\$50 to \$500



**Responsible
Disclosure
Plus
CrowdSourcing
With
*Ca\$h***



Any Bug Reporters?



Keys to Running a Bug Bounty

5 Simple Rules

Bug Payouts



Remote
Code
Execution

Auth
Bypass

SQL
Injection

XSS

Not all bugs are
equal



Disclosure Policy

**First In,
Best
Dressed**





**Well Defined
Targets and Scope**

**Do you pay for valid
bugs that are
out of scope?**

5 Major Benefits



**Embrace
Continuous Testing**



**Market
Your Security**

**Diversity in
Tools,
Techniques,
Approach**



A large pile of various coins, including pennies, nickels, and dimes, is scattered across a white surface. In the foreground, two hands are visible, holding a small stack of coins. The left hand holds a stack of about ten coins, while the right hand holds a single coin. The background is filled with a dense collection of coins, creating a textured, metallic appearance.


**Only Pay For
Results**

**Are
companies with
bug bounties
MORE
secure?**

8 Potential Problems



International Legal Issues

A close-up photograph of several hands of different skin tones stacked together in a circle, with fingers pointing towards the center. The hands are positioned in a way that suggests a team huddle or a gesture of unity. The lighting is warm, and the background is dark and out of focus.

**Fixing bugs is hard
and requires
teamwork**



Spot the difference



Understanding Language Barriers



**FALSE
POSITIVES
ARE A
NECESSARY
EVIL**

A photograph of a beach scene. In the foreground, a sandcastle with three towers sits on a mound of sand. Behind it, the ocean waves are breaking, creating white foam. The sky is not visible, but the water is a deep blue-green color. The overall scene suggests a fragile structure in a powerful, natural environment.

Weak Security Foundation



**Unclear Policies
and Processes**

Hackers Cheat



Bounty Hunters

“

Helping *secure* popular
services, *improving* my
skills, the *credit*, and of
course the *payment* for a
job well done

”

@NightRang3r
Bug Bounty Hunter

“

...*enhances* my logical
bug finding *creativity*
and approach. It
motivates me..

”

@AjaySinghNegi
Bug Bounty Hunter

“ First of all is the
challenge, and
second, the
acknowledgement
of researcher’s hard
work and *rewarding*
them accordingly ”

@NightRang3r
Bug Bounty Hunter

“

I like the *training*
aspects of bug bounties

”

@makash
Bug Bounty Hunter

“

The new *challenges*
which I get in the bug
bounty programs and
also the *appreciation*
by the bug bounty
security team

”

@AjaySinghNegi
Bug Bounty Hunter

3

Benefits



**Prestige
and fame**

**Practice
Makes
Perfect**





Cash
Money

Pick One:

- **Money**
- **Fame**
- **Experience**

4

Problems

Ahead...



**No
Visibility**



**Terms can change at any
time**



**Inefficient
use of
testers time**

**Fixes Take
Time**



Free
Advice

“

Be *prepared* to run
such a program, have
the professional *man*
power to deal with
bug submissions and to
understand them

”

@NightRang3r
Bug Bounty Hunter

“

Proper *verification*,
timely reply to bugs
submissions with status

”

@AjaySinghNegi
Bug Bounty Hunter

Statistics
don't Lie

Almost **80%** of bug
submissions are sent in
by researchers who
submit less than 10 bugs
total

PayPal

44% percent of all bugs
are the *first and only* bug
sent by a researcher

PayPal

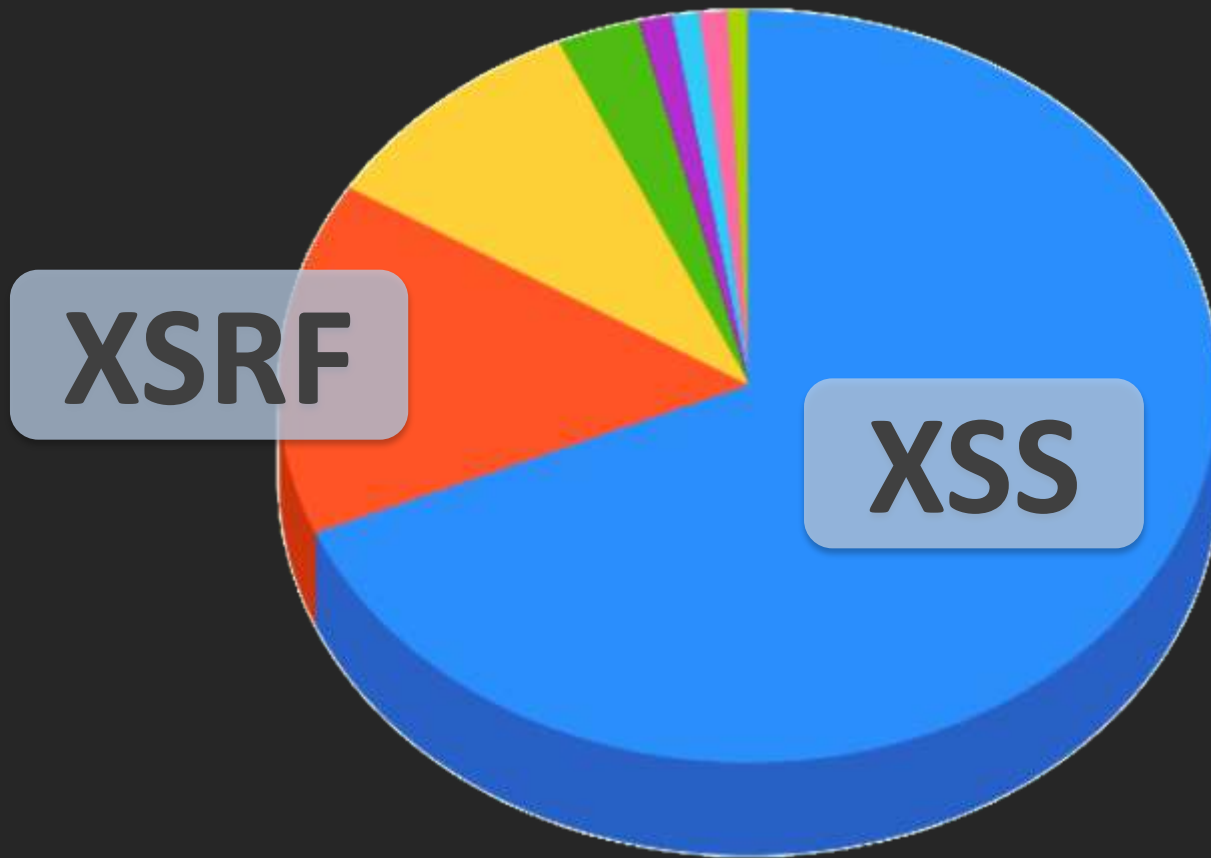
10% of the researchers
submit ***25 bugs or more***

PayPal

Google has paid out
\$806,501 as of
3/11/2013

Google

Almost **70%** of valid bugs
are **XSS**



Google

Does it
Work?

Google is reporting *fewer*
bug submissions

“Harder to find”

Google Bug Hunter

Crowd-Sourced Security
is

*changing
testing*

Outsourcing

Hack_aServer

 bugcrowd™

CrowdSecurify

Bugwolf



The Future

NEXT EXIT



Submit bugs

Accept bugs

Provide *Rewards*

Get *Secure*

Thank You!



Dark on Light

Continuous

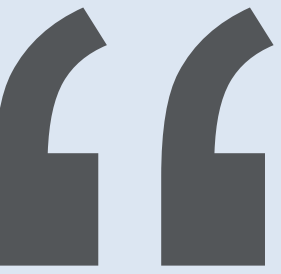
Light on Dark

“

Be *prepared* to run
such a program, have
the professional *man*
power to deal with
bug submissions and to
understand them

”

@NightRang3r
Bug Bounty Hunter



Callout for Dark

Dark Grey Text

POP

Light Grey

Callout for Light

Program Costs



Analysis



Tracking



Development



Payment

Crowd Sourcing

