mozilla

Lessons Learned from a Bug Bounty Operator

$ whoami

Jonathan Claudius

- Joined Mozilla in 2015
- IT/Security for 15 years
- Product Owner for Security Assessments
- Web Bug Bounty Program

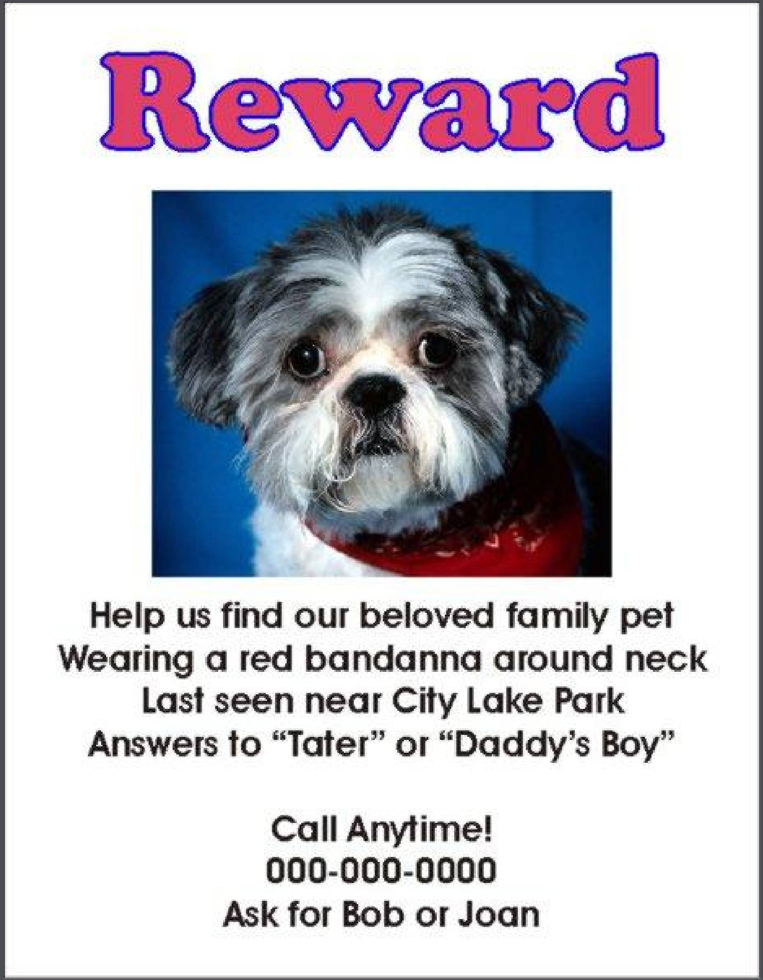
What is this talk about?

- What is a bug bounty?
- Why run a bug bounty?
- Why participate in a bug bounty?
- How to run a good bounty?
- How to be a good bounty hunter?

“What is a bug bounty?”

What is a bounty?

Money or reward offered for the capture of a **person** or **thing**



Reward

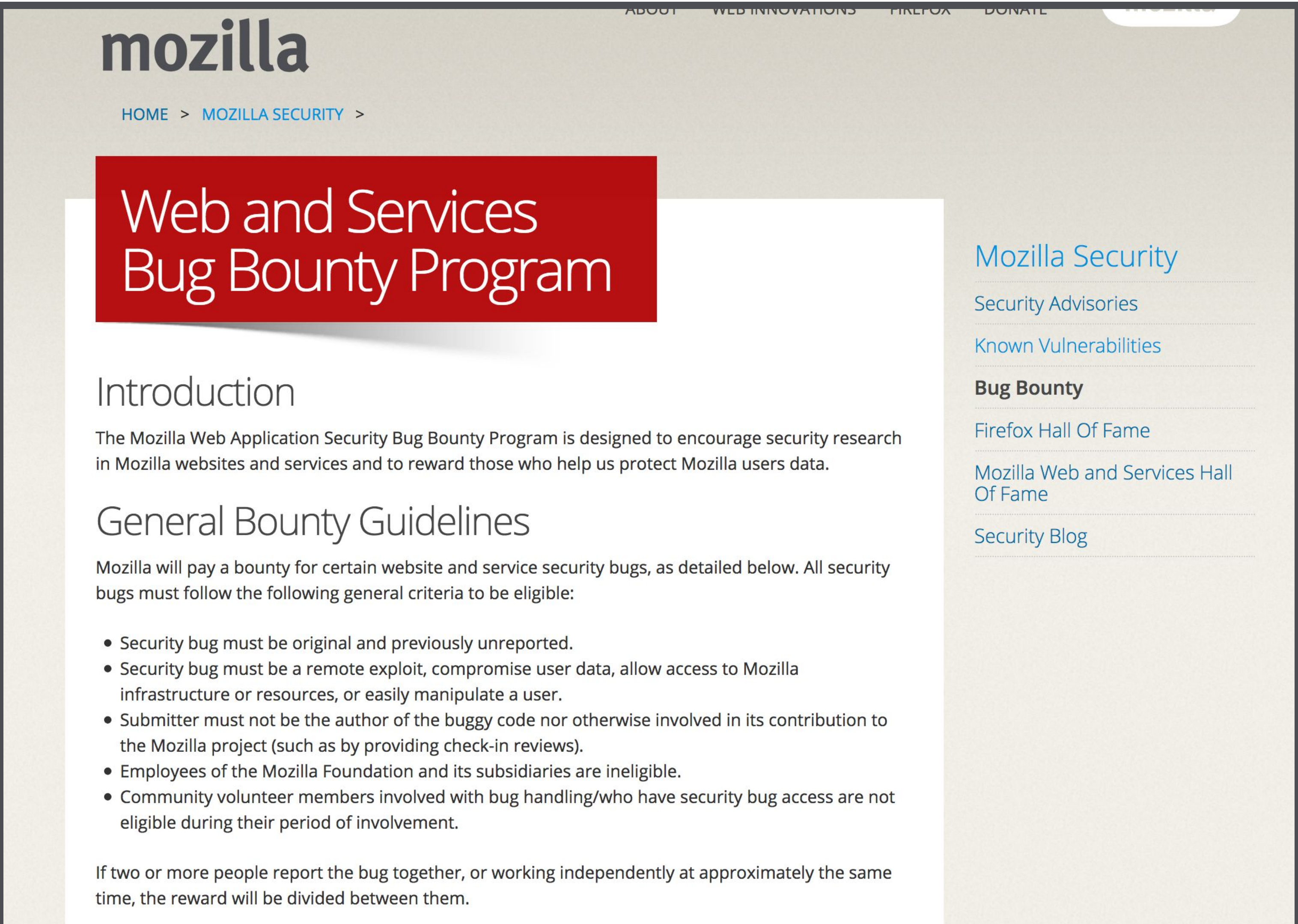
Help us find our beloved family pet
Wearing a red bandanna around neck
Last seen near City Lake Park
Answers to “Tater” or “Daddy’s Boy”

Call Anytime!
000-000-0000
Ask for Bob or Joan

What is a bug bounty?

Puppy == Bug (aka: security vulnerability)

Organizations announce intent to pay for the discovery of security bugs in their products/services.



Web and Services Bug Bounty Program

Introduction

The Mozilla Web Application Security Bug Bounty Program is designed to encourage security research in Mozilla websites and services and to reward those who help us protect Mozilla users data.

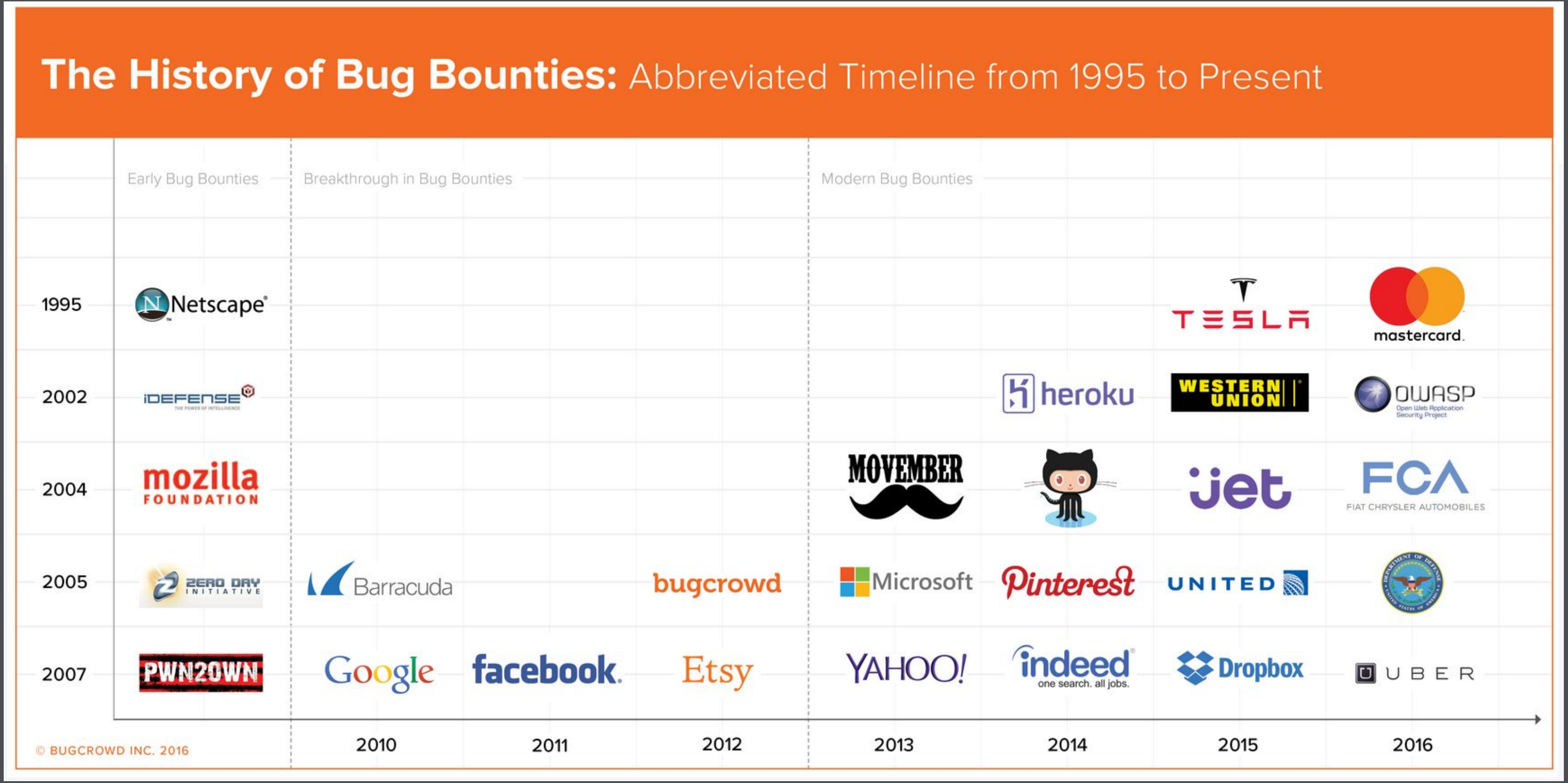
General Bounty Guidelines

Mozilla will pay a bounty for certain website and service security bugs, as detailed below. All security bugs must follow the following general criteria to be eligible:

- Security bug must be original and previously unreported.
- Security bug must be a remote exploit, compromise user data, allow access to Mozilla infrastructure or resources, or easily manipulate a user.
- Submitter must not be the author of the buggy code nor otherwise involved in its contribution to the Mozilla project (such as by providing check-in reviews).
- Employees of the Mozilla Foundation and its subsidiaries are ineligible.
- Community volunteer members involved with bug handling/who have security bug access are not eligible during their period of involvement.

If two or more people report the bug together, or working independently at approximately the same time, the reward will be divided between them.

Bounty Ubiquity



Source: https://bugcrowd.com/resources/history-of-bug-bounties

“Why run a bug bounty?”

PROTECT USERS

COMMUNITY

CONFIDENCE

“Why participate in a bug bounty?”

Curiosity

Money & Fame

CareeR Development

#dadjokes

“How to run a good bounty?”

Have a Bounty Committee

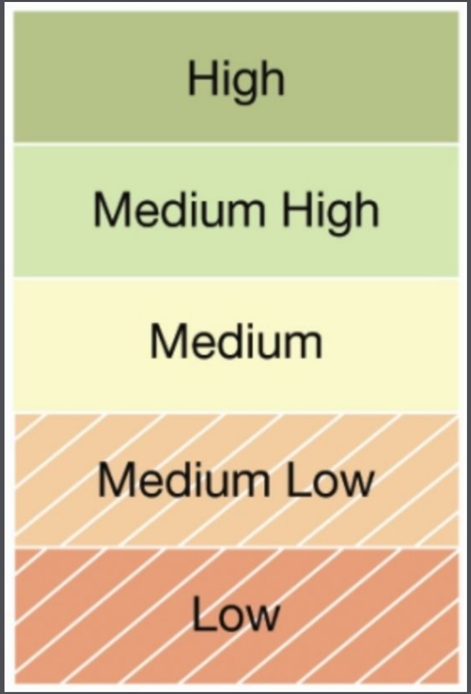
- A group of trusted individuals to govern the program
- Membership consists of representatives of affected products
- Meet regularly to discuss bugs that have been nominated for payment (all bugs submit via bounty program are nominated)

Do Bounty Triage

- Make it clear who’s responsible for triaging a bug
- Need to be very technical
- Have an SLA (< 1 business day)
- Ensure that you understand impact as soon as possible
- Consider a triage rotation

Example: https://wiki.mozilla.org/Security/Web_Bug_Rotation

Severity Levels



High

Medium High

Medium

Medium Low

Low

- Establish a ranking scale for evaluating the impact of security bugs.
- Easier to set expectations with stakeholders.

Example: https://wiki.mozilla.org/WebAppSec/Web_App_Severity_Ratings#Severity_Ratings

Acknowledgement

- Must quickly acknowledge and thank every person who submits a bounty
- Demonstrates that you value their contribution

- In cases where a bounty is awarded, make sure to expedite payment
  - positive re-enforcement
  - increases chances to future participation

Patience

- You will get “bad” submissions
    - offensive language
    - misunderstandings
    - ~30 min ransom videos
    - demands for payment
    - disrespect

- Keep your cool and keep it professional
- Be willing to adapt the program or guidance as needed

Transparency/Openness

- Involving bounty hunters in the solution (part of the workflow)
- They participate in communications with developers, service owners, etc.
- Rarely have to wonder about lack of status

- We make bounty bugs public after they are fixed!

Example: https://bugzilla.mozilla.org/show_bug.cgi?id=1293111

Feedback to Security Program

- Looking at trends in the bounty program
- Figuring out ways to squash entire classes of bugs
  - Examples
    - https://wiki.mozilla.org/Security/Server_Side_TLS
    - https://wiki.mozilla.org/Security/Guidelines/Web_Security
    - https://wiki.mozilla.org/Security/Guidelines/OpenSSH
    - https://observatory.mozilla.org/

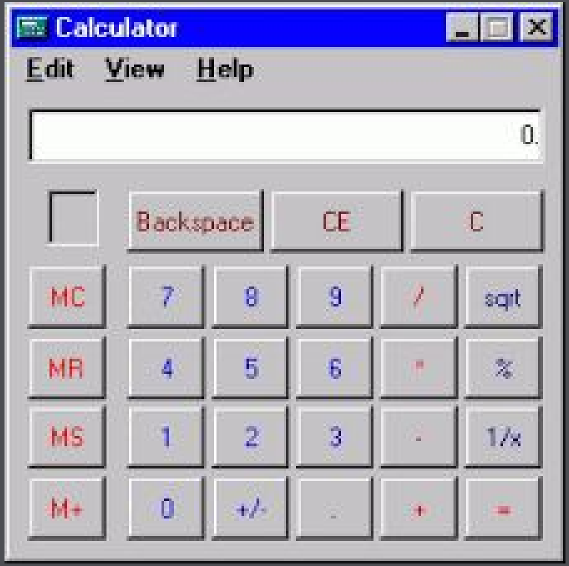
- If you aren’t using bounty results to shape your security program, you’re leaving value on the table

“How to be a good bounty hunter?”

Proof of Concept

- Providing a clear proof of concept
- This should include...
  - a clear description of the problem
  - steps for safe reproduction
  - why it’s an issue

- Try to describe threat scenarios to help impact assessment.



Follow Instructions

- Every bounty program is a little bit different
- If you’re going to work with a new program, read their instructions
- Our most successful bounty hunters read our guidelines carefully to ensure successful results
  - Examples
    - Eligible sites
    - Vulnerability Classes

Example:

https://www.mozilla.org/en-US/security/bug-bounty/faq-webapp/

Ask Questions

- Our most successful bounty hunters ask a lot of questions

- Why?
  - Context is important
  - Better understand impact drivers
  - Helps to continually refine your focus (different orgs have different weaknesses)
  - Understand why the issue happens and you might find other bug classes

Obscure Bug Classes

- Work on bug classes that are less common
  - You have less competition with other bounty hunters
  - Better chance it was missed
  - It’s fun to work on something different

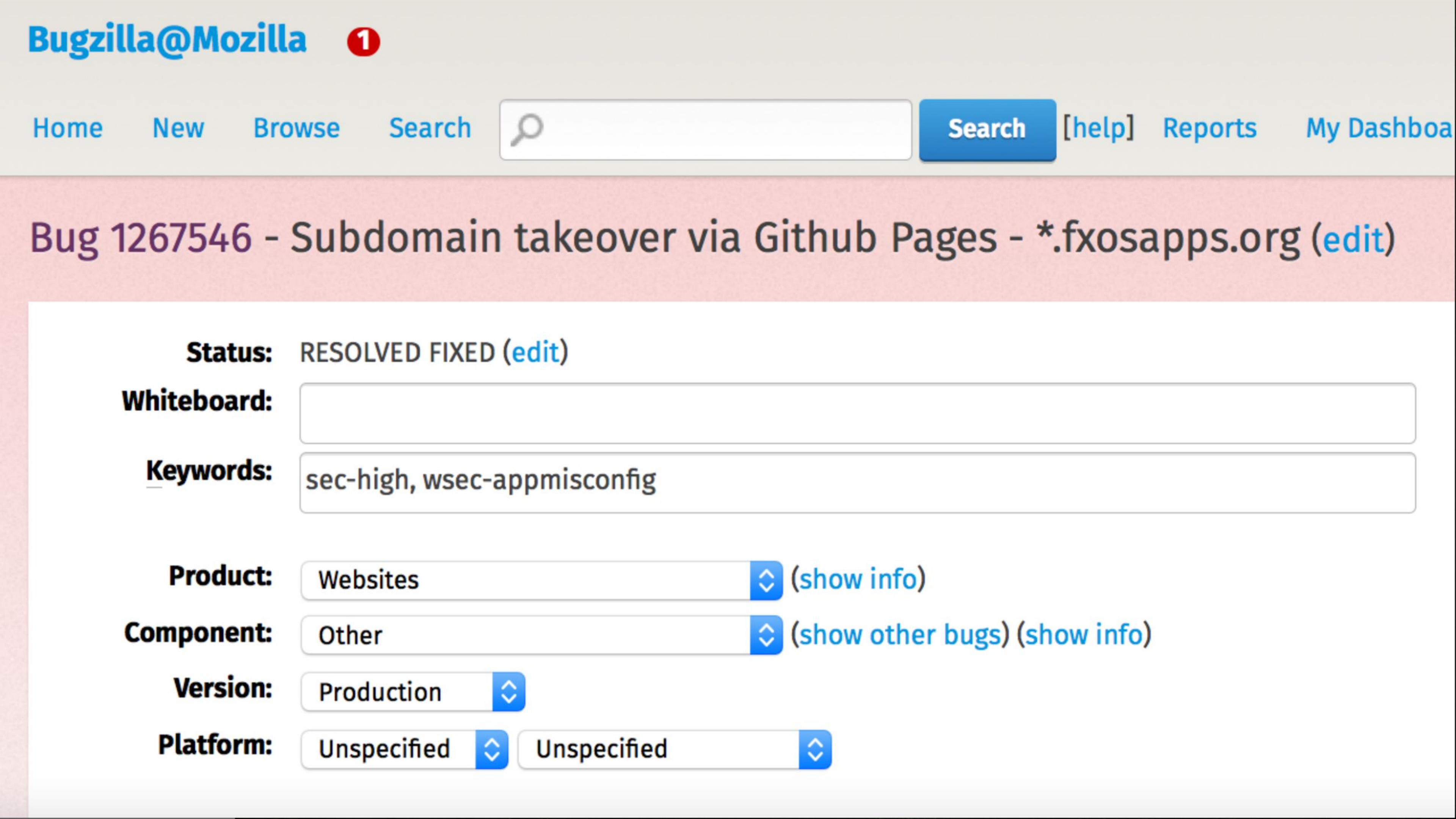
- Example
  - Hostile Subdomain Takeover Vulnerabilities

Be Nice, Or Leave

- Remember that you are criticising someone else’s hard work
- Try to remain professional
- If you build a strong reputation with the bounty team, you increases chances of…
    - Public acknowledgement
    - Fix/Bounty payout
    - Job offers
    - Shape the program

Success Story

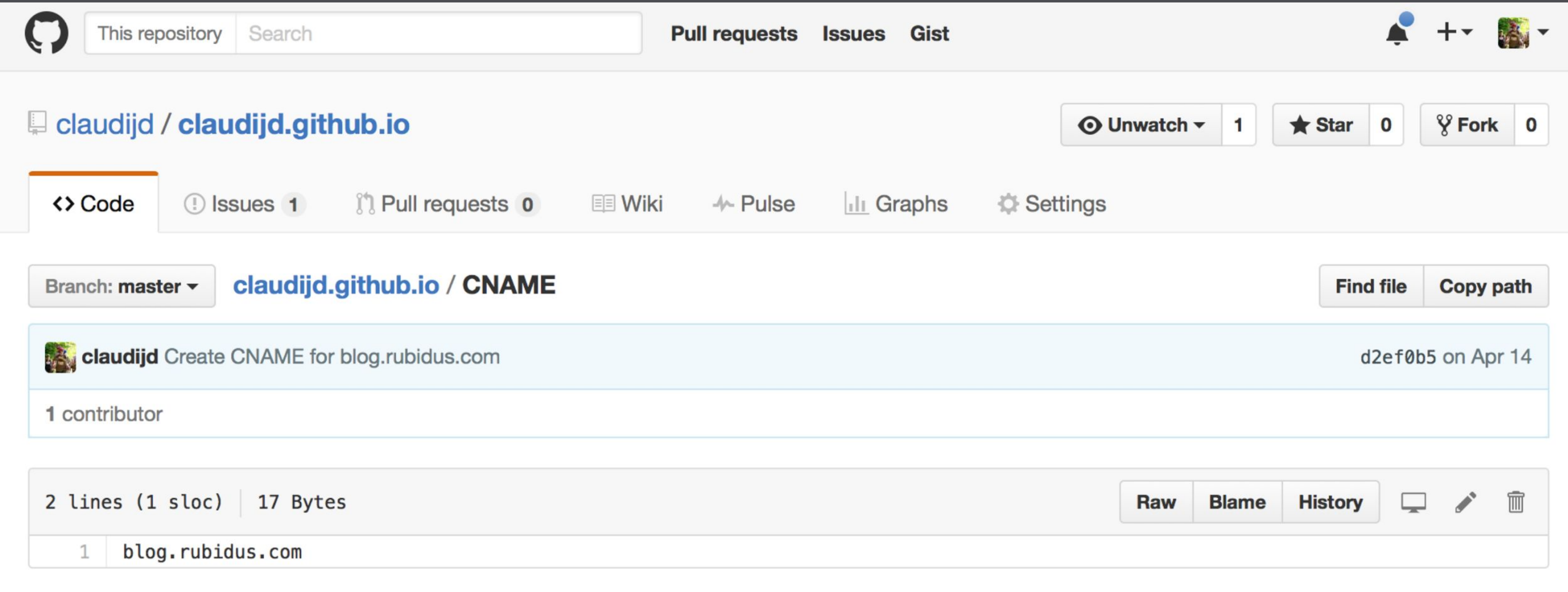
Affected 50+ domains…



Bug 1267546 - Subdomain takeover via Github Pages - *.fxosapps.org (edit)

Status:	RESOLVED FIXED (edit)
Whiteboard:	
Keywords:	sec-high, wsec-appmisconfig
Product:	Websites (show info)
Component:	Other (show other bugs) (show info)
Version:	Production
Platform:	Unspecified Unspecified

We Missed this...



claudijd / claudijd.github.io

claudijd.github.io / CNAME

claudijd Create CNAME for blog.rubidus.com d2ef0b5 on Apr 14

1 contributor

2 lines (1 sloc) | 17 Bytes

```
blog.rubidus.com
```

mozilla