The Economics of Security Research, Bug Bounties, and Firefox 4

Something for Everyone

chofmann@mozilla.org

- About:me
- About:you?

People Who build things

People Who break things

People Who manage people and projects

People that like to tinker with technology

lets have a discussion

- The economics of security bug finding and fixing are broken

- Chasm between awareness and strategies for dealing with the problems - Dr. Anton Chuvakin

- bridging the gap

Charlie Miller Claims "No More free bugs"

...But someone is paying

There are ALot of External costs

- **The “blackmarket” pays... Why aren’t there other markets?**

- **users pay** when their systems are hit by exploits

- **software vendors pay** when 0-days are released

- For good researchers **there are paths to Contracts, Jobs, and compensation,** but the road is Frustrating and complicated.

- This is all **WAY TO HARD**
- Need a faster, more streamlined way to make the web more secure.
- Resolve the imbalances

- **Maybe Widespread Use of Security Bug Bounties could help**

- get software companies to embrace the idea that **Creative research is a good thing**?

- **create a marketplace** for researchers to work in that is not a "blackmarket", and gets security research into the right hand?

- advance from the "wild west age" around research, disclosure, and bug fixing?

Looking at Mozilla's Motivations

- At Mozilla our Mission and Motivation is to Provide Choice and Innovation... Make the web better and more useful

- build a better browser Not for profit -- Public Benefit -- Keep Users First!

- Security Plays a big roll in the Mission

  6 things- Security, Stability, Compatibility, Memory use, Speed, Features

- What we are we working on?
- Fuzzers, Security Reviews, Improving the Development Process
- Staying on Top of Security Problems with Fixes and Releases, Updating Users quickly.
- Being Transparent -- Sharing Information
- Stay "Highly Leveraged" - Combine Volunteers with Paid staff

Alot of Room for Improvement

- Software is a Human Endeavor
- Dealing with all the Complexity of Internet and the Web and 5 Million Lines of Code
- Browser as a Platform with 100's of APIs
- Reducing Complexity
- Encourage More People to Participate

Bounties are a Natural Fit

- We Encouraged Research from the Beginning of Mozilla.org Six Years Ago
- In the last few months we started re-examiine our security bug bounty program and ways we could improve it
- Keep all the good things, and expand the program to make it better.

A New Bounty Program

- Encourage Research and Participation
- Find Problems Early and respond Quickly
- Open And Transparent -- "Design-IN" Security from the start
- Protect Users

- Build on Bug Bounty program Successes
- In the last 6 years 80 Researchers have worked on Over 110 Bugs that have qualified for bounties
- How can we increase Participation even more and expand the partipants?

Some Participants

- Billy Rios
- Nate Macfetters
- Dan Kamisky
- Chris Evans
- Michal Zalewski
- Petko Petkov
- Moxie Marlinspike
- Nils
- Collin Jackson and Adam Barth
- and many more

What Do you Know about Mozilla's BuG Bounty Program

- How Much Does it Pay?
- What Kinds of Bugs?
- Where does it Apply?

Current Bounty Program

- We have been paying $500
- What Kinds of Bugs? Remote Exploits
- Where does it Apply? Latest Firefox, Thunderbird

New Changes

- Increasing from $500 to $3000
- why $3000 when some offer 5k, 10k, 100k
- Streamlined Process
- Don't have to "weaponize", Don't have to prove "without a Doubt Exploitability"

None of the Classic Vendor problems

- denial of the problem
- Slow Acknowledgement of the problem
- Discourage Participation er, Cease and Desist
- Communication Gaps

- Mozilla Ties to Avoid All these problems
- Easy and Low Friction interaction
- No Dealing with “The Vendor”

Also Expand the Eligible Systems

- must be a remote exploit
  allow execution of arbitrary code
  allow access to users' Critical confidential information (e.g., passwords, credit card numbers.

- Is present in the most recent supported version of Firefox, and/or Thunderbird, as released by the Mozilla Corporation **+ our expanding set of Web services. Downloads, Updates, addon site, Plugin Checks, Firefox Sync...**

The Process is the same

- File A bug http://bugzilla.mozilla.org
- Attach PoC
- contact security@mozilla.org
- Participate in the Solution

- Updates To the Program were pushed out last night. Check Them out. google for “mozilla bug bounty”
- http://www.mozilla.org/security/
- http://www.mozilla.org/security/bug-bounty.html
- http://www.mozilla.org/projects/security/security-bugs-policy.html

Where to Focus

- Follow the Herd http://www.mozilla.org/security/announce/
- v. Breaking New Ground
- We benefit from both
- How about You?

Moving on Beyond Mozilla

- What if Other Organizations Started Offering Bounties?

- Seems like others interested in Finding problems and Funding security Research should be interested in bounty programs
- am I crazy? Mark Curphey's 8th Idea
- Is it really Possible?
- What Would be the Challenges?
- How Many Have Worked inside Med/Large Companies?

Ideas on Steps to Success

- Framing the Problem & Convincing People
- Budget
- Spending the Money
- Measuring Results

Tapping in to common Understandings

- Expect to Be Hacked?
- Yes, Most Companies do -- 94% [1]...
- Survey Differences -- some say 50/50 chance
- Who are You Polling? - Which Companies? Which People?.. How The Question is Framed

http://darkreading.com/security/intrusion-prevention/showArticle.jhtml?articleID=217300227

Reducing Cost of Security

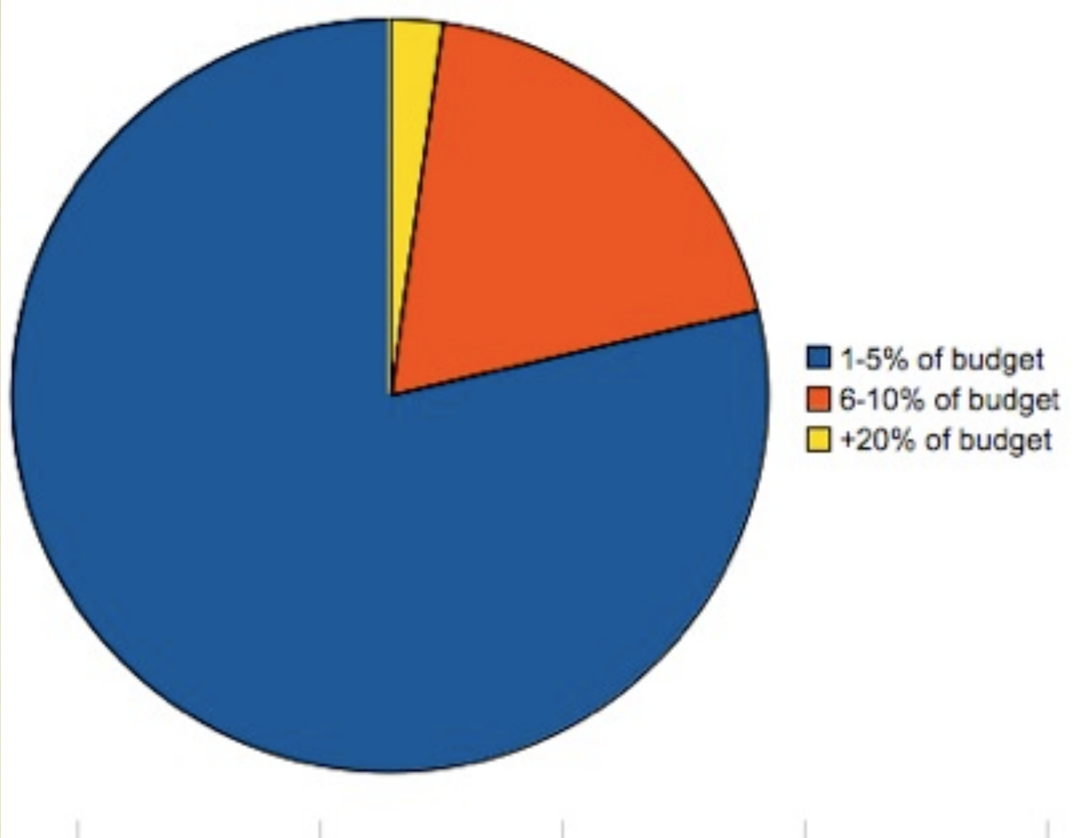
- Cost of Breaches?
- $100k - $6Million
- Lack of Transparency Makes Good Numbers Are Hard to Get At both Inside organizations and outside..

Funds Might already Exist

- Could existing budgets be redirected?
- 60% Budget for Pen Testing
- 38% Don’t Pen Test... lack of manpower or money and skills to fix vulnerabilities that are discovered (70 percent), 5 percent said they worry that the results of the pen test "could be embarrassing,"

Where does the money go?

- 70% Spend 1-5%
- 17% spend 6-10%
- 2% spend +20%



- Spending for Compliance == NO Go
- Spending to Get Bugs Found and Fixed. ROI?

Spending the Money is Hard

- “In-House” Research No one has the time/ staff/Expertise...
- Contractors/Domain Specialists... Administration Cost Eat Up Research Funds
- Try A Bounty Program As and Experiment

- Maybe Somewhere, Somehow with the right combination of forward thinking Security and Management Team there is a chance...

Enough About Bounties and Other Orgs

- Lets Get Busy With Making Firefox 4 A Great Release

- Where you can find out what is going on...
- https://developer.mozilla.org/devnews
- Beta Release Notes, Links to Feature/Planning Info

What is Already There?

- HTML5 Parser
- Web Sockets
- Retain layers and layer contents
- CSS transitions, CSS :Visted
- WebM, 64-bit Builds, and More Stuff Coming

- Lots of stuff for Security Researchers
- Lots of stuff for web Developers

Content Security Policy

- CSP one of the interesting features in Firefox 4 that tries to help web developers
- The Web Wasn't Designed for User Generated Content... Remember the old Days Before User Content Generations and Webmasters Ruled the Web?

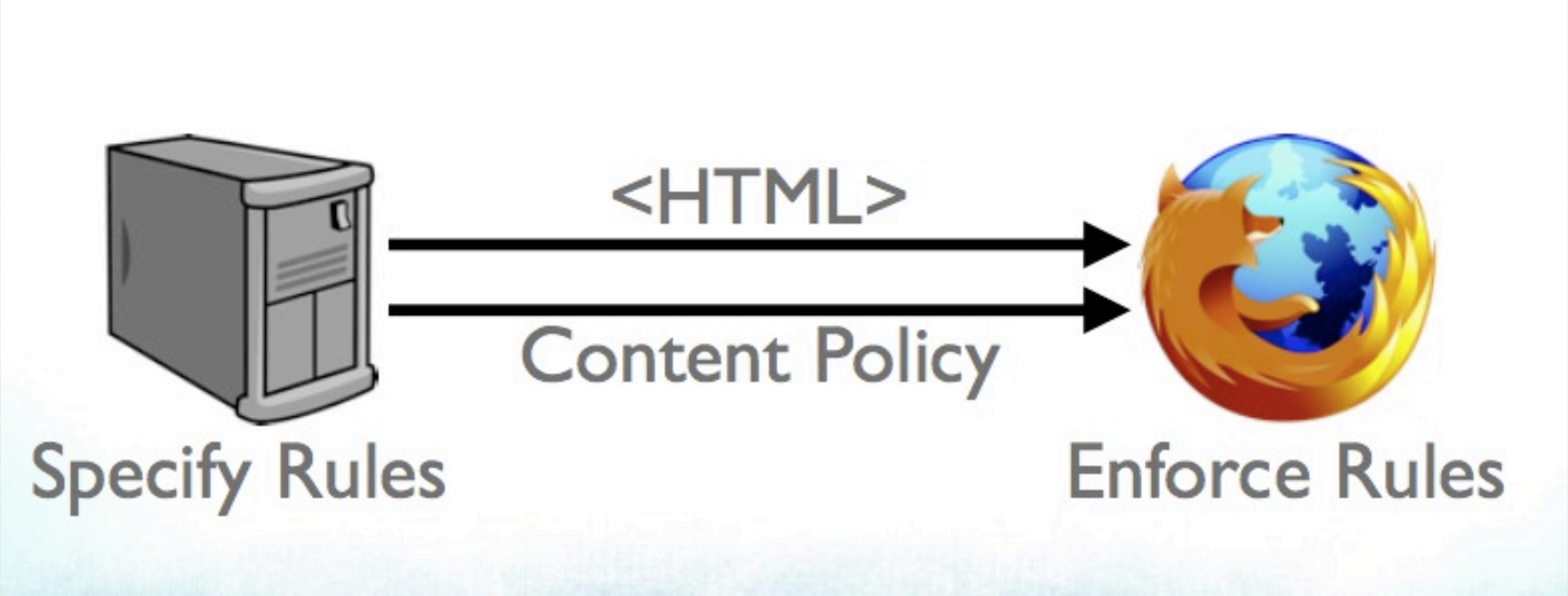
- XSS continues to plague Web security
  http://news.google.com/news?q=xss

- #2 on the OWASP Top 10
  www.owasp.org/index.php/Top_10_2010-Main

- Browser treats all content in server response with equal privilege. No way to differentiate legitimate & injected content

- CSP is about using Browser as a Protector

- Stop recreating the Content Sanitization wheel for every web application.. Send the Browser Instructions on how to handle the Content and Let it Do the enforsement



- CSP has Lots of Controls, an Flexibility
- Docs At https://developer.mozilla.org/en/Introducing_Content_Security_Policy

Strategies for Using CSP

- Identify what "Normal Behavior" is for your site. What kind of content is allowed and Where should content come from

- Specify in a policy file that Enforces the Rules

- Block Violations or Just Catch and Report

Some Policy File Examples

Allow 'Self'

- Site wants all content to Only come from the same source (scheme, host, port)

```
allow ‘self’; frame-src ads.net
```

- Site wants all content to come from the same source (scheme, host, port), except content in iframes may be served by a third-party advertising network.

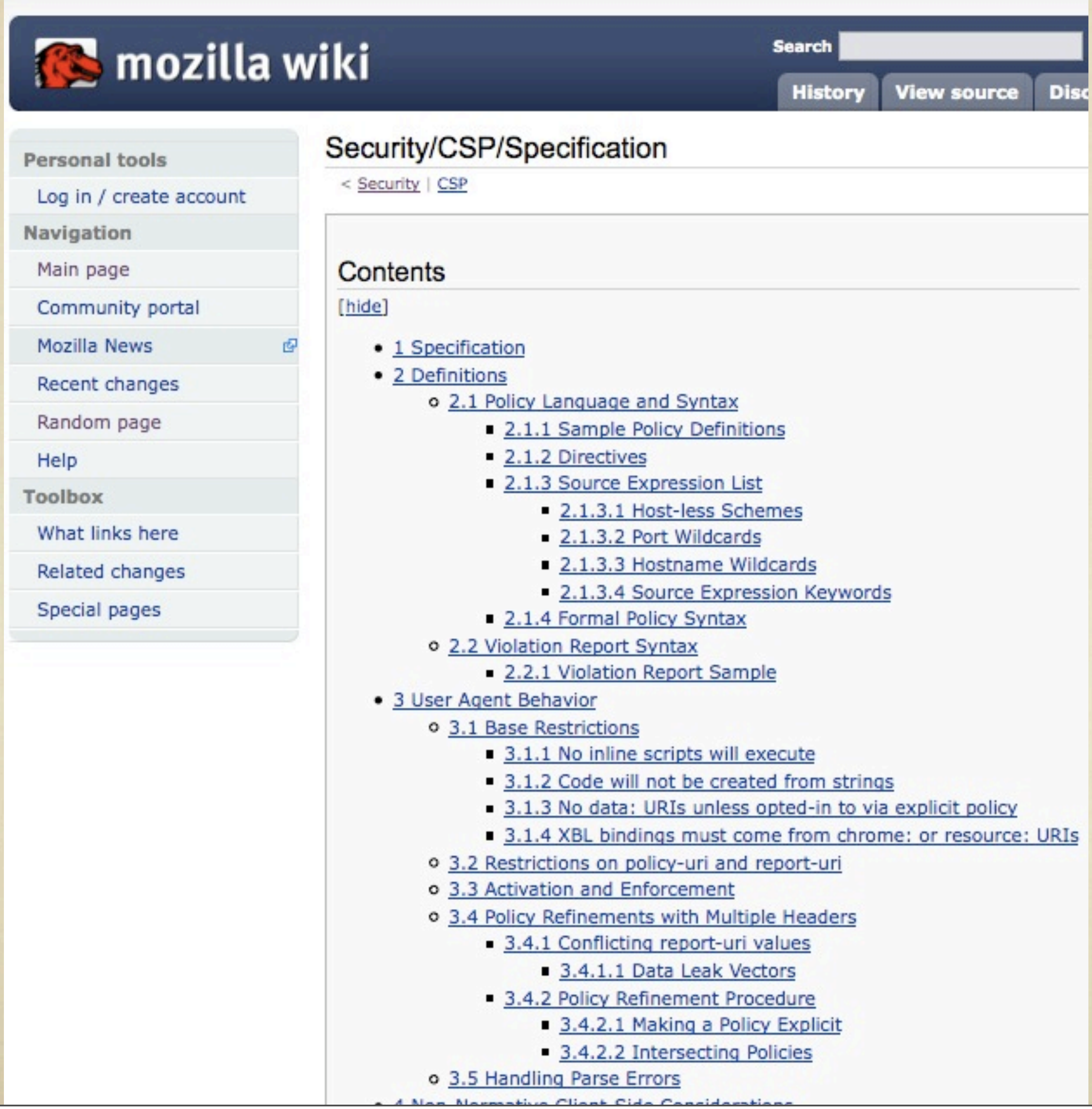
```
allow ‘self’; img-src *;
object-src *.teevee.com;

script-src myscripts.com
```

- Auction site wants to allow images from anywhere,
- plugin content from a trusted media provider
- network, and scripts only from its server hosting sanitized JavaScript

- Wait! This is Firefox only! How is it Useful?
- W3C Web App Working Group Discussions Started. standard is planned
- Interest in CSP From Chrome, Webkit, Microsoft

Draft Spec Posted on wiki.mozilla.org



Security/CSP/Specification

< Security | CSP

Contents

[hide]

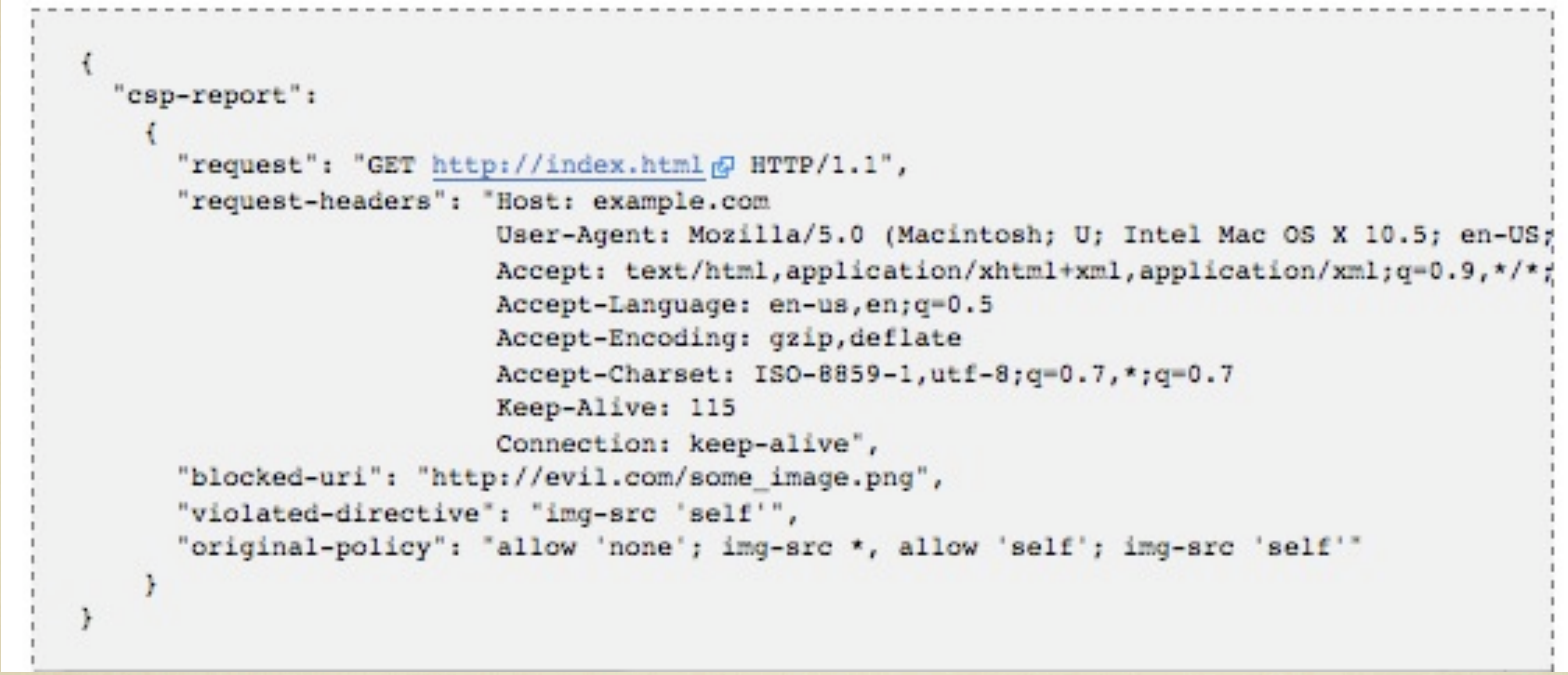
- 1 Specification
- 2 Definitions
    - 2.1 Policy Language and Syntax
        - 2.1.1 Sample Policy Definitions
        - 2.1.2 Directives
        - 2.1.3 Source Expression List
            - 2.1.3.1 Host-less Schemes
            - 2.1.3.2 Port Wildcards
            - 2.1.3.3 Hostname Wildcards
            - 2.1.3.4 Source Expression Keywords
        - 2.1.4 Formal Policy Syntax
    - 2.2 Violation Report Syntax
        - 2.2.1 Violation Report Sample
- 3 User Agent Behavior
    - 3.1 Base Restrictions
        - 3.1.1 No inline scripts will execute
        - 3.1.2 Code will not be created from strings
        - 3.1.3 No data: URIs unless opted-in to via explicit policy
        - 3.1.4 XBL bindings must come from chrome: or resource: URIs
    - 3.2 Restrictions on policy-uri and report-uri
    - 3.3 Activation and Enforcement
    - 3.4 Policy Refinements with Multiple Headers
        - 3.4.1 Conflicting report-uri values
            - 3.4.1.1 Data Leak Vectors
        - 3.4.2 Policy Refinement Procedure
            - 3.4.2.1 Making a Policy Explicit
            - 3.4.2.2 Intersecting Policies
    - 3.5 Handling Parse Errors
- 4 Non-Normative Client-Side Considerations

Other Benefits

- Why wait for the other browsers?
- Understand Your Site better Using CSP in report only mode
- when ever a violation is encountered The Browser Uploads a json object to your site
- Imagine All the Firefox users visiting your site Helping to Test and Find Problems.

CSP Violation Logging

- Try A Partial/limited roll-out



```
{
  "csp-report":
    {
      "request": "GET http://index.html HTTP/1.1",
      "request-headers": "Host: example.com
                          User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US;
                          Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;
                          Accept-Language: en-us,en;q=0.5
                          Accept-Encoding: gzip,deflate
                          Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
                          Keep-Alive: 115
                          Connection: keep-alive",
      "blocked-uri": "http://evil.com/some_image.png",
      "violated-directive": "img-src 'self'",
      "original-policy": "allow 'none'; img-src *, allow 'self'; img-src 'self'"
    }
}
```

- http://people.mozilla.org/~bsterne/content-security-policy/demo.cgi

- Questions? Want help implementing CSP?

- We're willing to help!
  Brandon Sterne bsterne@mozilla.com
  Sid Stamm sid@mozilla.com
  dev-security@lists.mozilla.org

- So Thats it...
- Hope this had something for everyone
- Thanks for Listening and Sharing Your Ideas
- Hope you get Invoved!
- chofmann@mozilla.org