Topics for today

- How to make use of bug repositories
- Find out about latest crashes by using Mozilla crash reports
- How to browse source code using DXR and use search tools
Where to find bugs?

- Mozilla uses Bugzilla, a popular online bug-tracking tool
- Bugzilla Page for Mozilla
- Security disclosures: Sample disclosure
- Search for Buffer Overrun
How to find bugs?

- Use **simple search**, limit scope
- Example: status: All, Product: Firefox, Words: buffer overrun
- Or, use **advanced search**
- Sample **Bug report**
- Weekly **update** from Mozilla team
Q: Why do we care about fixed bugs?

- Might expose other similar bugs
- Might be a sign that the “area” of code is poorly written or tested or just buggy in general
Interesting cases to look for

There are a lot of asserts in firefox, what happens when they are broken?

- **JS_STATIC_ASSERT**
- **MOZ_ASSERT**
Crash reports

- Another way to find interesting bugs
- Mozilla crash reports
- More specific, Firefox 36.0a1
I found an interesting bug, now what?

- Go to the source!
- DXR: code browser and search engine
- DXR for Mozilla [here](#)
- Annotated view of source [here](#)
Try out a few bugs yourself

- Old firefox versions [download]
- Firefox bug POC, [here]
- Heap Spray Bug [Report]
Q: What happens when there is a bug in your bug tracker?

A: It could reveal sensitive information about as-yet unfixed security holes.
References used

- Bugzilla Zero-Day Exposes Zero-Day Bugs
- Bugzilla Search Tips
- Bugzilla Quick Search Guide
- Bugzilla Firefox Add-on