```
import java.util.Base64;
import java.util.concurrent.ConcurrentHashMap;
import java.util.regex.Matcher;

import burp.api.montoya.BurpExtension;
import burp.api.montoya.http.message.HttpRequestResponse;
import burp.api.montoya.ui.UserInterface;

public class ZeroXGUIDScanner implements BurpExtension, ScanCheck
{
```

Hacker vs. Triage

Inside the bug bounty battleground

Richard Hyunho Im & Denis Smajlović





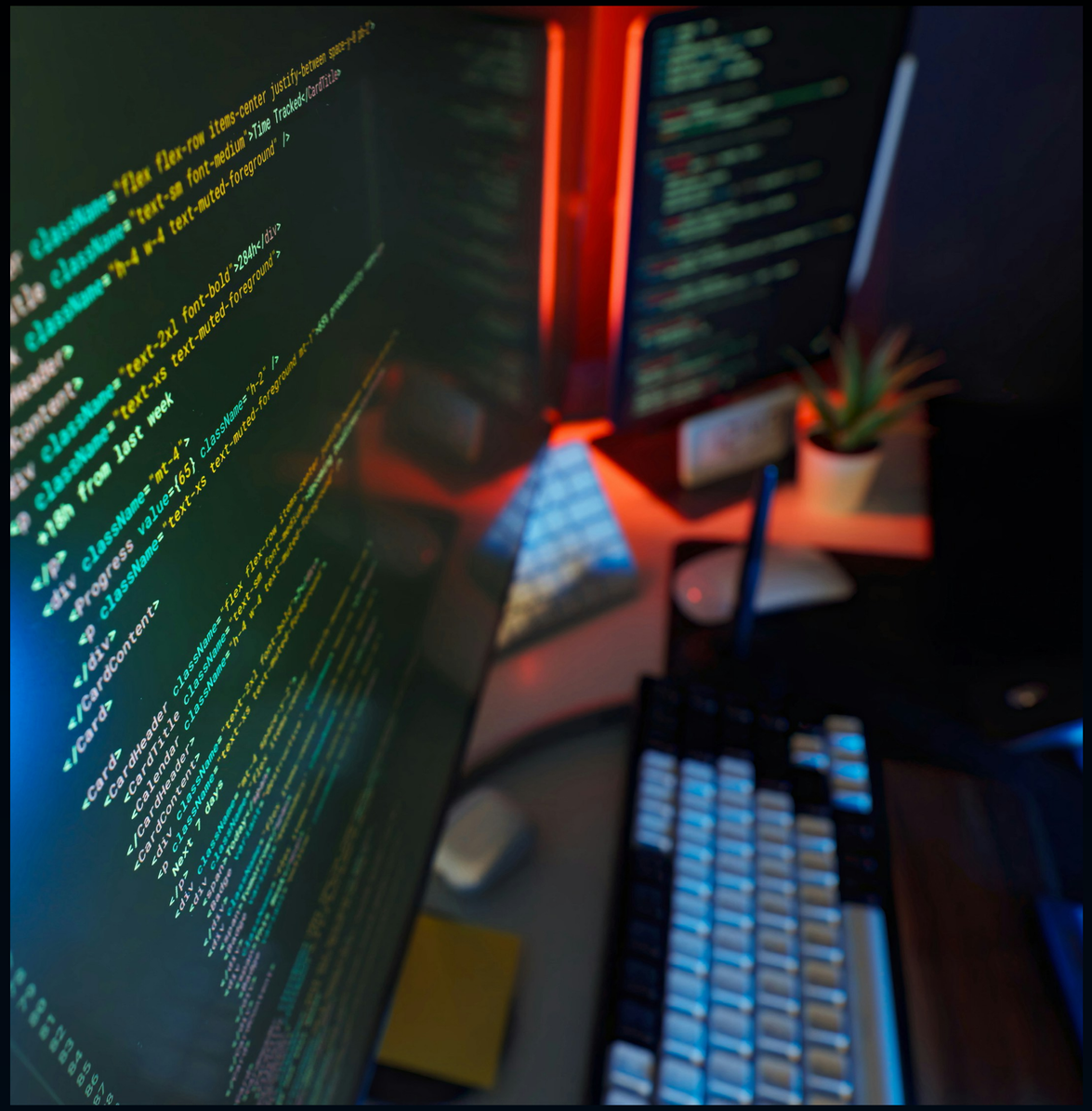
Richard Hyunho Im
@richeeta
Security researcher



Denis Smajlović
@deni
Principal at Nova Information Security

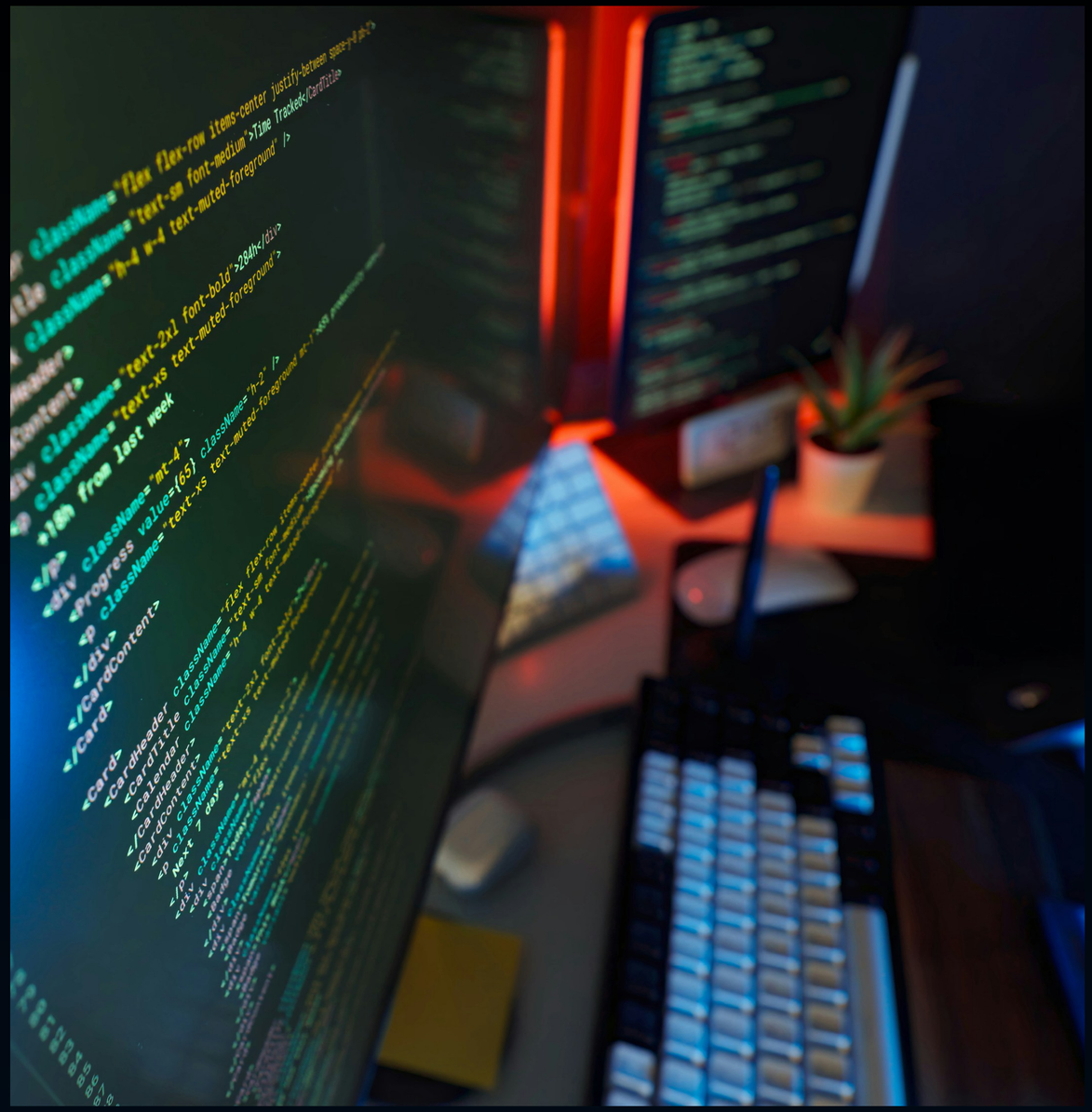
How to bug bounty

1. Do research, find issues
2. Write and submit report
3. Company validates issue
4. Payout $$
5. Company fixes issue



How to bug bounty

1. Do research, find issues ✅
2. Write and submit report ✅
3. Company send generic response
4. Company replies after 3 months
5. You never hear from them again



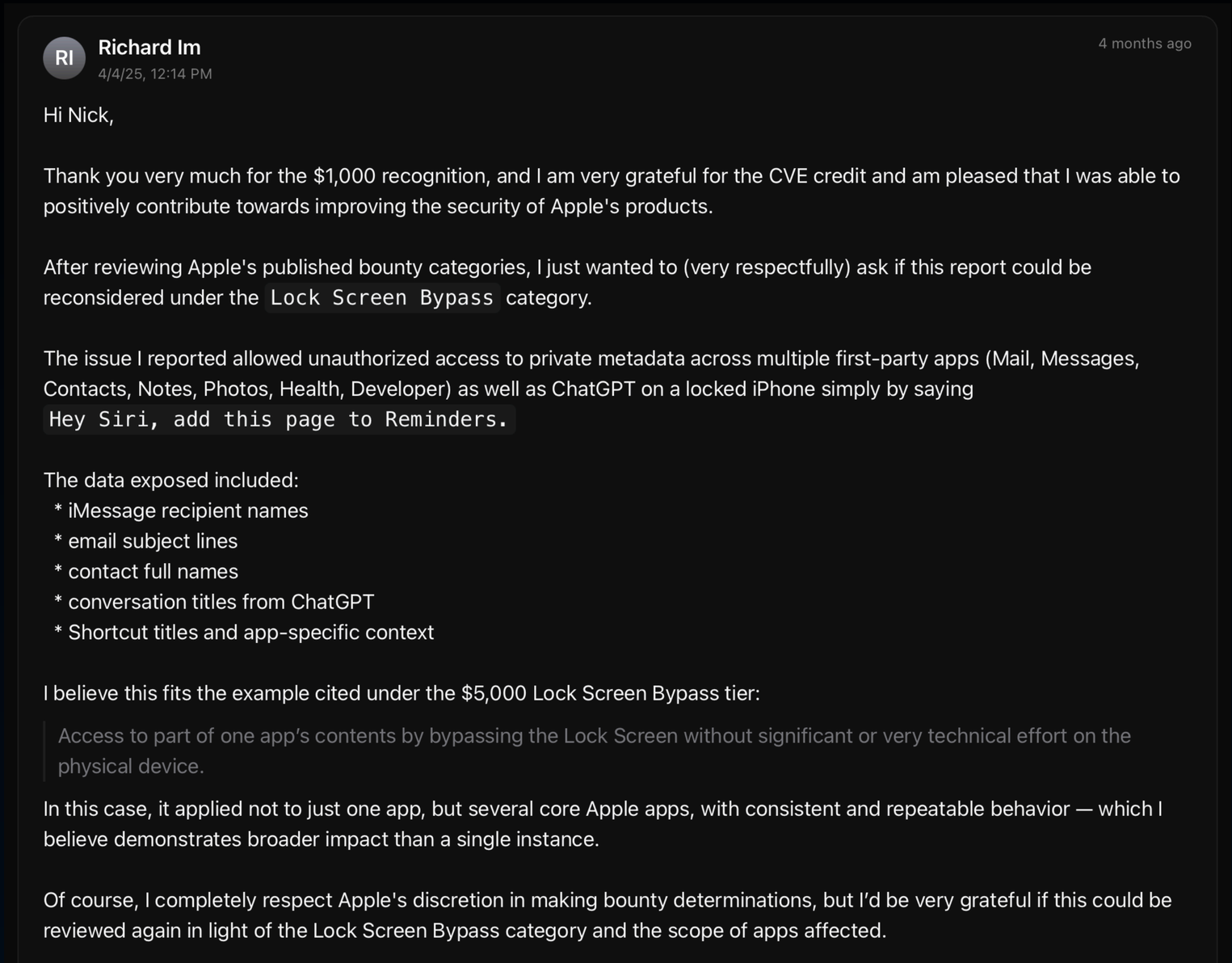
- Slow (or no) responses
- Severity being downplayed
- Valid issues getting rejected (and you can’t talk about it)
- Offensively low payouts

- Lack of knowledge/experience
- Wrong prioritization within program team(s)
- Processes not being established

Anecdotes

Challenging Decisions Without Conflict

- Real-world case: Successful Apple bounty appeal for CVE-2025-24198 (bounty increased **5x**)
- When and how to push back respectfully
- The right way to escalate a dispute without burning bridges



RI **Richard Im** 4 months ago
4/4/25, 12:14 PM

Hi Nick,

Thank you very much for the $1,000 recognition, and I am very grateful for the CVE credit and am pleased that I was able to positively contribute towards improving the security of Apple's products.

After reviewing Apple's published bounty categories, I just wanted to (very respectfully) ask if this report could be reconsidered under the `Lock Screen Bypass` category.

The issue I reported allowed unauthorized access to private metadata across multiple first-party apps (Mail, Messages, Contacts, Notes, Photos, Health, Developer) as well as ChatGPT on a locked iPhone simply by saying `Hey Siri, add this page to Reminders.`

The data exposed included:
* iMessage recipient names
* email subject lines
* contact full names
* conversation titles from ChatGPT
* Shortcut titles and app-specific context

I believe this fits the example cited under the $5,000 Lock Screen Bypass tier:

> Access to part of one app's contents by bypassing the Lock Screen without significant or very technical effort on the physical device.

In this case, it applied not to just one app, but several core Apple apps, with consistent and repeatable behavior — which I believe demonstrates broader impact than a single instance.

Of course, I completely respect Apple's discretion in making bounty determinations, but I'd be very grateful if this could be reviewed again in light of the Lock Screen Bypass category and the scope of apps affected.

Improving your program

Scaling programs

Conclusion

- Short, to-the-point reports are easier to write and more likely to be actioned
- Programs are far from perfect; good bugs/reports can still be neglected
- Challenging programs in a polite way is a healthy way to share feedback
- Your program probably has space to improve; be involved
- Bad experiences for researchers are often trivial to turn around
- It’s not too late to get into bug bounty; the community is just getting started

Thank you.



Questions

