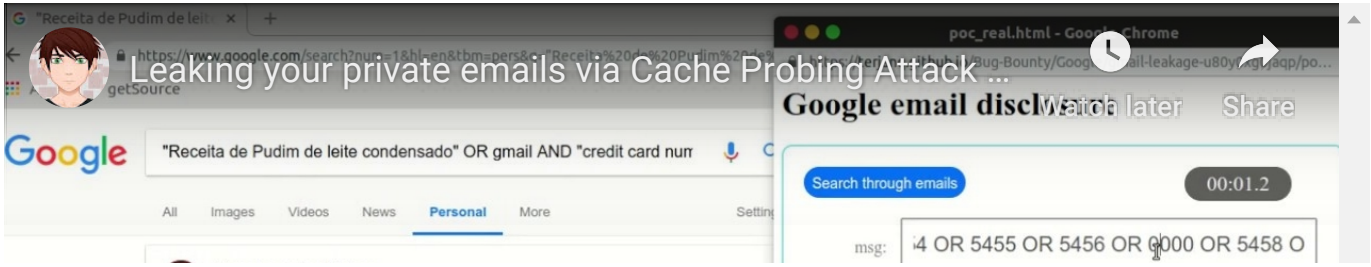
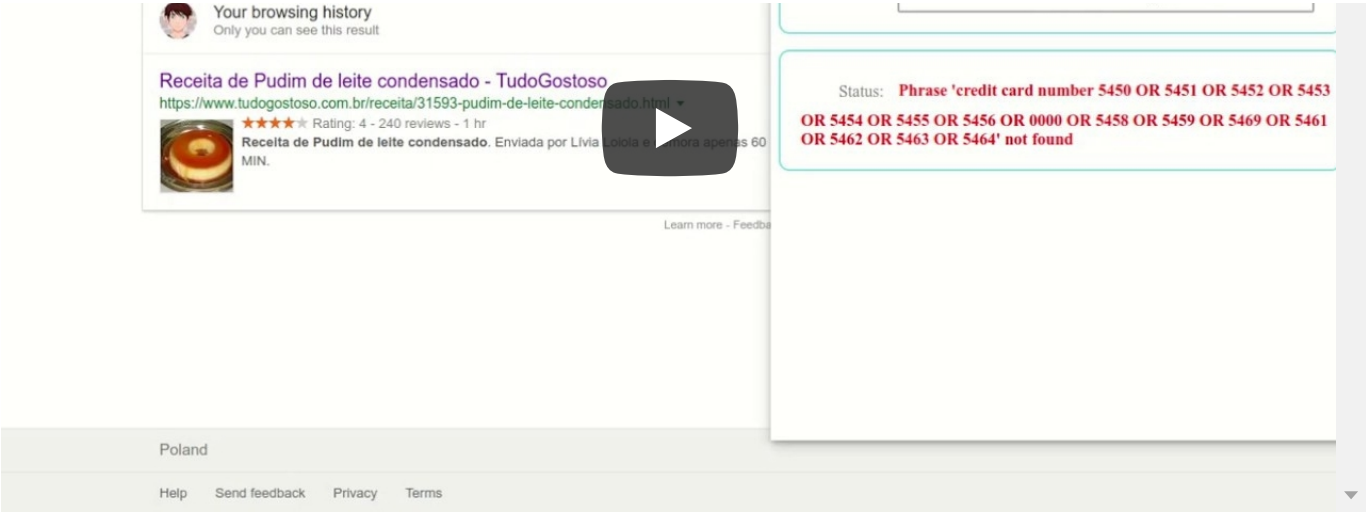
Massive XS-Search over multiple Google products

terjanq Follow
Nov 12 · 2 min read

A couple of months back, I took a part in researching dangers that come from Cache Probing Attack and new ways to exploit the vulnerability across multiple platforms. I was able to prove that it was possible to leak significant information about the user on several Google products such as their **private emails**, **tokens**, **credit card numbers**, **phone numbers**, **bookmarks, private notes** and much more.





Leaking user's emails — Proof of Concept

A brief summary of the attack

1. The attacker controls a malicious website, let's call it **evilwebsite.com**
2. On the malicious **evilwebsite.com**, the attacker **removes a specific resource from the browser cache**, e.g. "not found" image
3. The **malicious website forces the user to search** in the background for a controlled by the attacker phrases, which for example can be done by using manipulation of window.opener

4. The **evilwebsite.com** checks if the resource has been loaded by probing if the resource was loaded from the browser cache.

Protections

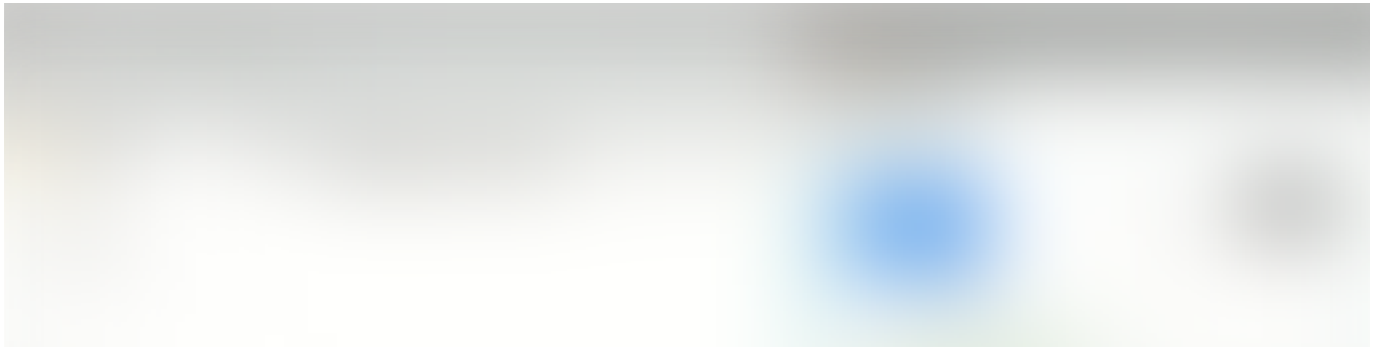
Google and the browsers took the vulnerability very seriously. They invented and implemented several protections that are intended to protect against this specific attack but also that will mitigate much more XS-Leaks. Some of these protections are:

- Fetch Metadata Request Headers
- Cross-Origin-Opener-Policy (COOP)
- Partition the HTTP Cache
- Limit `Referer` header's length to 4k
- Chrome XSS Auditor removal

The report

I reported my findings in detail to Google on *Feb 14, 2019* in the markdowned report where you can find more details about what information I was able to leak. As a result of this and other xs-leaks reports, Google realized they need serious protection against cross-site leaks in general and suspended these leaks in their VRP program until further notice. But before that decision, they treated researchers with full respect (in contrast to some other companies that started following the trend) paying them full bounties just before the announcement. Kudos to them for that! It was a pleasure working with the Google team on putting all the effort together to kill the issue :)

In the original report, I included a proof of concept that worked at the time and probably is not working anymore, but given the issue was not yet fully fixed over other platforms and browsers, I decided to keep it private yet.



PoC in action

Cybersecurity Bug Bounty Browsers

66 claps

WRITTEN BY

terjanq

Follow

Security enthusiast that loves playing CTFs and hunting for bugs in the wild. Also likes to do some chess once in a while.
twitter.com/terjanq

Write the first response

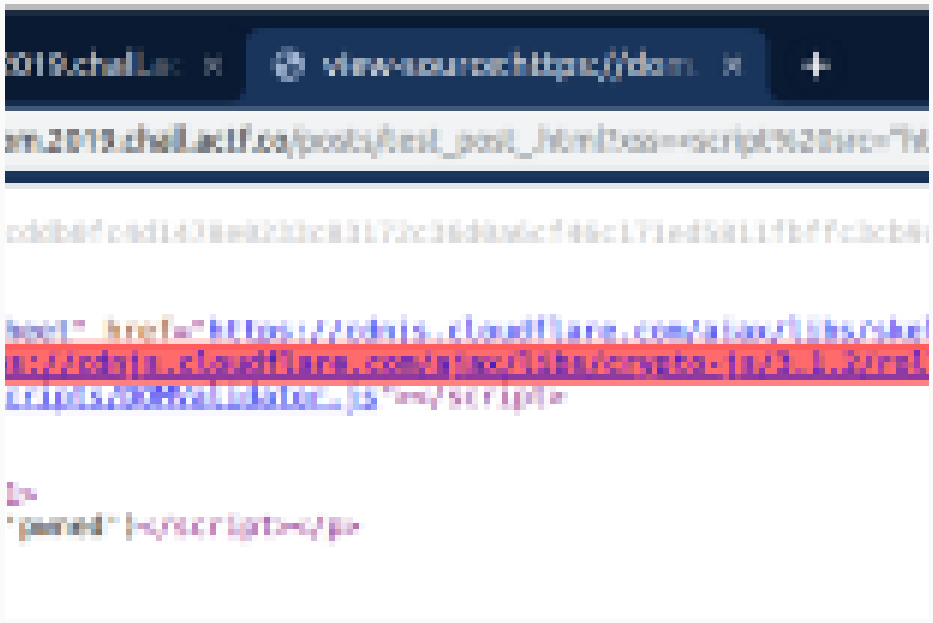
More From Medium

More from terjanq

XSS-Auditor — the protector of unprotected

terjanq in InfoSec Write-ups
Apr 25 · 4 min read ★

448

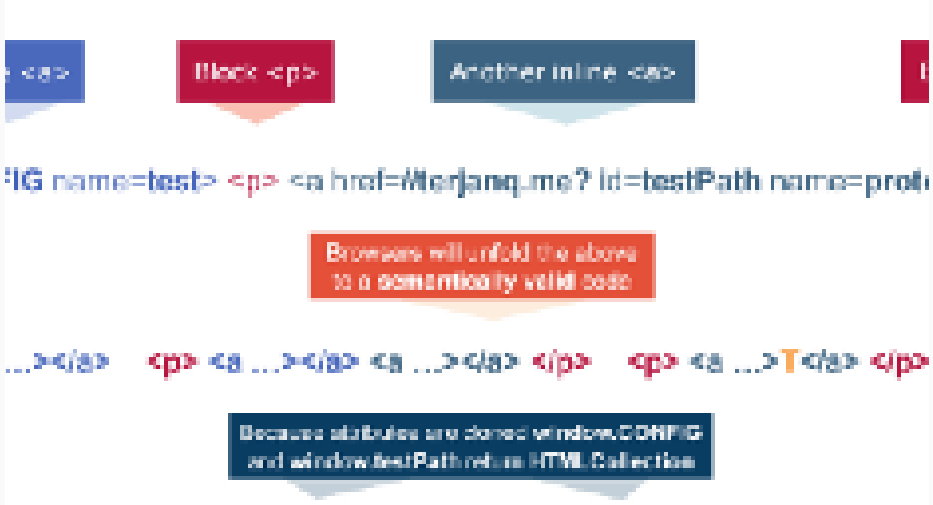


Related reads

Clobbering the clobbered — Advanced DOM Clobbering

terjanq
Sep 26 · 9 min read ★

68



Related reads

The Bugs Are Out There, Hiding in Plain Sight

A Bug'z Life in A Bug'z Life
Jul 15 · 6 min read ★

775

Discover Medium

Welcome to a place where words matter. On Medium, smart voices and original ideas take center stage - with no ads in sight. Watch

Make Medium yours

Follow all the topics you care about, and we'll deliver the best stories for you to your homepage and inbox. Explore

Become a member

Get unlimited access to the best stories on Medium — and support writers while you're at it. Just $5/month. Upgrade