Auth Misbinding Vulnerability in GeoGuessr's Google Sign-In Flow

Discovered: June 2025

Disclosure status: Unacknowledged as of July 3, 2025

This disclosure was made by a data security professional with experience in PCI-regulated and critical infrastructure environments.

TL;DR

GeoGuessr's Google OAuth login implementation can route users into other people's accounts, resulting in persistent, unauthorized access. This occurred on multiple devices and browsers, even after clearing all site data and re-authenticating via Google.

Attempts to contact GeoGuessr support went unanswered. A direct escalation to company leadership also received no acknowledgment after a full business day in their time zone.

This outlines the timeline, reproduction steps, security implications, and potential legal exposure.

Timeline of Events

April 28, 2025 – The account the reporter was misrouted into was created, based on visible metadata.

Early June 2025 – The reporter's first visit to GeoGuessr.com. The reporter signed up using Google OAuth. The reporter had never used or visited the site prior to this date.

June 28, 2025 – The reporter received a GeoGuessr email encouraging them to "come back and play." Clicking the included login button routed them into an account that:

- Was not theirs
- Had a different username and avatar
- Had a creation date ~45 days prior to their first visit

The reporter immediately:

- Cleared all cache, cookies, and site data
- Closed and reopened the browser – also tried another browser
- Navigated manually to GeoGuessr.com
- Signed in again using Google OAuth (prompted for full MFA re-verification)
- Was once again logged into the same incorrect account

The reporter emailed GeoGuessr support, clearly outlining what occurred. The reporter received only an automated vacation autoreply stating they may be slow to respond.

July 2, 2025 – After more than 2 days of silence, the reporter sent a formal escalation email directly to the CEO (Daniel Antell) and CTO (Erland Ranvinge) using verified contact addresses. The reporter received no bounce-back from either address.

July 3, 2025 – After a full business day had passed in their time zone (Sweden), the reporter had received no reply or acknowledgment of any kind.

Reproducible Issue Summary

- OAuth misbinding may cause Google-authenticated users to be mapped to the wrong internal account
- Behavior is persistent across sessions, browsers, and devices

- Reauthentication with Google (even after clearing all stored data) still routes user to the same incorrect account

This is not a mistaken or forgotten registration. This is a session binding flaw at the application level. The account where the reporter is being directed was created more than a month prior to their first visit and registration at GeoGuessr.com.

Why This Is a Serious Security Issue

This isn't just a weird glitch or customer service annoyance – it's a fundamental security failure:

- The reporter gained full access to someone else's account through legitimate OAuth login
- The reporter could view or modify profile settings and access any stored data associated with that account
- The reporter was unable to access their own account – the reporter was always routed to someone else's

If misbound accounts have:

- A paid subscription: the incorrect user could see billing status or possibly payment info
- A minor's profile: This could result in unauthorized adult access to a child's data or activity history – a serious concern in jurisdictions with child data protections

GeoGuessr may not appear to host sensitive data, but:

- It does process credit card payments
- It supports Google federated login
- It can retain identifiable user activity history
- It presents itself as a global multiplayer platform, where identity matters

Legal and Regulatory Implications

Depending on the user affected, this flaw may violate:

- GDPR (EU)
    - Article 5 (data accuracy & integrity)
    - Article 6 (lawful basis for data processing)
    - Article 32 (security of processing, access controls)
- CCPA (California)
    - User data (including behavioral or usage history) is protected from unauthorized access, even if not strictly PII
- COPPA (U.S. Child Online Privacy Protection Act)
    - If a child's account can be accessed by another authenticated user, this constitutes a serious compliance failure
- PCI DSS
    - GeoGuessr accepts payment cards and must comply with relevant portions of PCI DSS 4.0, including:
    - Requirement 7/8: Restrict access to cardholder data by business need to know
    - Requirement 8.3.1: Strong authentication for all non-console access
    - Requirement 10.2.5: Ensure access to payment systems is tied to individual users – not ambiguous sessions

    - While GeoGuessr may use third-party payment processors, they still bear responsibility under PCI DSS 4.0 for protecting access to user accounts that control or display billing status.

Even absent PII, unauthorized behavioral tracking or billing information visibility is unacceptable under modern privacy standards. Also, the potential for adult-minor interaction, where the minor may have no reason to believe they are communicating with an adult who has been granted access to their friend's account, is blatantly irresponsible.

This flaw undermines those requirements if account access is misrouted or if login is not reliably tied to the actual user.

Reporter's Background

The reporter has worked for organizations handling:

- Software development for:
    - Municipal water infrastructure operators with full GIS mapping
    - DoD
    - Military biolabs
- PCI-compliant data

In addition to managing enterprise-scale data, the reporter:

- Developed credential encryption design
- Implemented secure transfer protocols for sensitive data

This isn't a kneejerk complaint. It's a misbinding flaw – the kind we would immediately lock systems down for in critical environments.

Responsible Disclosure Attempted by Reporter

- Emailed GeoGuessr support on June 28 – no reply after auto-response
- Emailed CEO and CTO on July 2 – no acknowledgment as of July 3 (close of business, Sweden)
- Reached out to Google OAuth security team – not applicable, as the issue lies with GeoGuessr's account binding, not Google's token handling

What Needs to Happen

- Suspend OAuth login – some users will be upset they temporarily can't play, but it is necessary
- Fix session binding code for OAuth login – the account returned must reliably belong to the authenticating Google user
- Audit for other potentially misbound users and accounts
- Publish a postmortem or security advisory for public trust

The reporter is making this disclosure publicly now only after multiple failed attempts to report the issue responsibly and privately.

The reporter urges GeoGuessr to take immediate action to safeguard its users and restore trust in its authentication flow – particularly for those relying on federated login systems to keep them safe.