USAA Web Auditing

By; Shangmin Chen, Michael Mei, Isaac Chan, Dylan Ramdhan

BOSTON UNIVERSITY

Technical Analysis

Cookies: a lot of tracking cookies

HSTS: [104.104.110.147] (chrome tools)

LiveRamp (3rd Party): data connectivity

Maxymiser (3rd Party): cloud-based marketing service

Utag Tealium: Event tracking

No CSRF defense found

Fully uses https! ... Overall decently secure

Privacy Policy

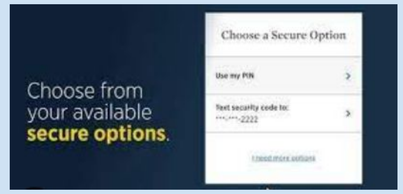
According to USAA's "USAA Private Policy', many of its usage is used for being shared with the company and its affiliated companies (i.e. Garrison Property and Casualty Insurance Company).

Utilizes data for running daily business performances, as well as regular interaction with USAA performances, such as opening an account, deposition money, paying bills, using credit/debit cards from bank account.

Potential Exploits

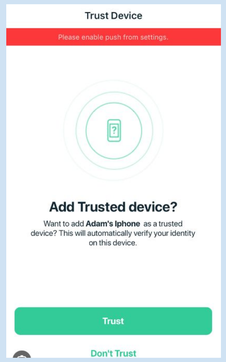
<u>Multifactor-Authentication</u>

Quick Log on: one-time secure code



Biometrics: Face ID or Fingerprint

Browser Recognition: Trusted devices bypass MFA



CyberCode Text or Token: replace PIN with one-time 6-digit code

GDPR

- Two linked documents: European Privacy Statement and California Consumer Privacy Act (CCPA) Privacy Notice
  - Complies with 7 GDPR Principles
- Cookies and tracking
  - Session and persistent cookies
  - Purposes
    - Marketing and UX
    - Business operations and legal compliance

Login and Password Reset Flow

- Register for Access
  - Answer a series of questions to check for eligibility
  - If eligible → input personal information
- Log in
  - Input USAA ID
- Alternatives
  - Recover ID: USAA #, SSN, or Tax ID and phone #, email, or government ID
  - Reset Password: Same as above