jscrambler

Web banking security threats

A data sheet by Jscrambler

Web banking platforms need client-side security

Banks use JavaScript to develop **highly advanced web and mobile banking platforms in record time.** However, JavaScript is exposed and opens the door to client-side attacks.protect your client-side against web supply chain attacks.

97%
Modern web apps using JavaScript.

100%
Fortune 500 banks using JavaScript.

$2.5M
Annual cost of web-based attacks per company.

Attacks to web banking platforms are growing

The client-side of web banking platforms has **too many security gaps.** Attackers are taking advantage of this and the cost of attacks is growing.

$500M
Losses from the biggest banking trojan attack to date (Citadel).

On average
Big banks spend over $20 million per year on fraud prevention.

Average loss
Of roughly $3.7 million per year because of fraudulent online transactions.

The threats to web banking platforms

Key business threats

Loss of customer data including financial details, user credentials, or personally identifiable information (PII).

Heavy GDPR/CCPA fines following data breaches, which can amount to several hundred million dollars.

Lack of PSD2 compliance, namely in transaction monitoring, which can lead to significant penalties.

Loss of customer trust, with clients terminating accounts following a data breach or fraudulent transactions.

Client-side attacks to web banking

Magecart-like data breaches

The JavaScript code that handles the logic of web banking platforms is exposed and can be modified to steal data. These platforms also rely on third-party code that may be breached and start injecting malicious code directly on the web banking latform, silently exfiltrating user data.

Transaction fraud

Attackers can use webinjects to tamper with banking transactions. This enables them to change every detail of the transaction without the end-user being able to detect it.

Adware and malicious interface changes

By injecting malicious code into the website's front-end, attackers can display fake banners, leading end-users to malware, competitor websites, or fake mobile apps.

Intellectual property theft

Digital banking evolves with continuous innovation. Because client-side JavaScript is exposed by default, competitors can freely retrieve proprietary logic, putting competitive advantages at stake.

Organizations have zero client-side visibility and are still underprepared

15%
Increase over 3 years. The global average cost of a data breach in 2023 was USD 4.45 million.

48%
Of financial attacks start with malicious actors.

March 2023
A data breach occurred at Latitude Financial, with more than 14 million records compromised.

Web banking meets client-side security

Key business benefits

Minimize exposure to data breaches, by protecting JavaScript code and gaining real-time visibility of client-side attacks like data leakage.

Minimize exposure to losses from transaction fraud, by preventing banking trojan webinjects and other client-side exploits.

Code Integrity protects the source code of your web banking platform

Enterprise-grade application shielding

With Jscrambler's resilient obfuscation, environment checks and defenses against malicious modification/ injection of code, attackers won't be able to reverse engineer, debug or tamper with your app's JavaScript and native code.

Best-in-class runtime protection

Give self-defending capabilities to your web banking platform, which will detect debugging/tampering attempts and trigger countermeasures like breaking the application.

Increase compliance with regulations such as PSD2 by increasing client-side security and monitoring web pages in real-time.

Easily integrate with your SIEM to maximize your organization's ability to respond to threats in real-time.

Webpage Integrity secures your platform against malicious code

Full client-side visibility

Monitor the behavior of each of your website's scripts in real-time, see the full details of each detection and receive warnings for critical security threats.

Webpage threat mitigation

Mitigate client-side attacks to your website in real-time regardless of the attack vector and keep your users safe at all times. Prevent web supply chain attacks, data leakage, banking trojan webinjects, adware and customer hijacking.

References

SEON, “Global Banking Fraud Index 2023”, https://seon.io/resources/global-banking-fraud-index/

npm Blog, “Managing JavaScript in the Enterprise”, February 21st, 2019, https://blog.npmjs.org/post/182958759735/managing-javascript-in-the-enterprise

Accenture, “The Cost of Cybercrime”, March 2019, https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

IBM, “Cost of a Data Breach Report 2023”, https://www.ibm.com/reports/data-breach

G. Cluley, “Author of Citadel malware, used to steal $500 million from bank accounts, pleads guilty”, March 2017, https://www.tripwire.com/state-of-security/featured/author-of-citadel-malware-used-to-steal-500-million-from-bank-accounts-pleads-guilty/

R. Anderson et al., “Measuring the Changing Cost of Cybercrime”, May 2019, https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_25.pdf

Kroll, “2021 Data Breach Outlook”, June 2021, https://www.kroll.com/en/insights/publications/cyber/data-breach-outlook-2021

Verizon, “2021 Data Breach Investigations Report”, May 2021, https://enterprise.verizon.com/resources/reports/dbir/

ICO, “ICO fines British Airways £20m for data breach affecting more than 400,000 customers”, June 2021, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/

If you want to know more about how Jscrambler can help you prevent client-side attacks, don’t hesitate to contact us.

hello@jscrambler.com | +1 650 999 0010