PENTEST REPORT

BITGO

https://www.bitgo.com/

Tester – Krishanu Chakraborty
Phone Number – +91-9547915974
Email – shanu.16k@gmail.com

Document Control

Owner & Role	**Status & comments**
Krishanu Chakraborty – Penetration Tester	Prepared for technical assessment

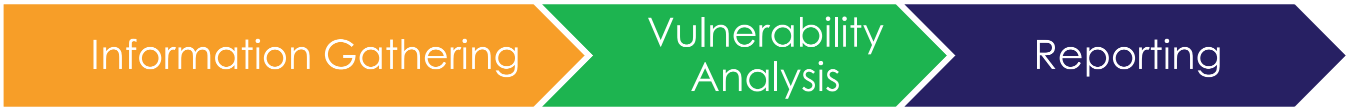
Security Posture

The scope was to exploit vulnerabilities on Example Organization servers and apps that may be exploited by malicious attackers. The aim of the tests was to go as far as possible.

NOTE: - Dots Color Signify ⋗ Red - High Risk Orange - Mid Risk Green - Low Risk Grey - Safe

Methodology

I utilized a widely adopted approach to performing penetration testing during the tests to test how well the target environment is secured. Below, a breakdown of the applied methodology is provided.



- Information Gathering – Reconnaissance [Footprinting, Scanning and Enumeration]
- Vulnerability Analysis – Researching Potential Vulnerabilities and Analyzing them
- Reporting – Reporting the findings in a proper Proof of concept (POC) report.

Detailed Findings

1. Vulnerable for clickjacking attack – Medium (6.5)

- URL – https://www.bitgo.com/
- Vulnerability – Vulnerable for clickjacking attack
- Severity Rating – Medium

Description

Clickjacking, also known as a "UI redress attack", is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top-level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both.

Impact

The hacker has several ways they can use the redirected clicks for their own gain. A common form of clickjacking involves mirroring a login and password form on a website. The user assumes that they're entering their information into a usual form but they're actually entering it in fields the hacker has overlaid on the UI. Hackers will target passwords, credit card numbers and any other valuable data they can exploit.

An attacker may also choose to redirect the clicks to download malware or gain access to vital systems as a starting point for an advanced persistent threat (APT). This spells trouble for any organizations that rely on protecting sensitive data and intellectual property.

Clickjacking attacks trick web users into performing an action they did not intend, typically by rendering an invisible page element on top of the action the user thinks they are performing. Clickjacking won't affect your site directly, but it could potentially affect your users.

Clickjacking Examples for references

Links can be hidden under media and trigger a particular action, such as liking a Facebook page or ordering a product on Amazon. The user may need to meet certain conditions for the attack to actually be successful, such as staying logged into social media accounts.

If the user gets tricked into downloading something on their computer, then they have to deal with a compromised computer. In the best-case scenario, they can get rid of the malware through an anti-virus scan. In the worst case, they would need to reformat their computer and reinstall the operating system.

Clickjacking can turn system features on and off, such as enabling your microphone and camera when a JavaScript prompt asks for permission to access this information. It could also pull location data from your computer or other details that could facilitate future crimes.

Remediation

- Sending the proper Content Security Policy (CSP) frame-ancestors directive response headers that instruct the browser to not allow framing from other domains.
- The older X-Frame-Options HTTP headers is used for graceful degradation and older browser compatibility
- Properly setting authentication cookies with SameSite=Strict, unless they explicitly need None.
- Prevent framing from other domains: Stop a hacker from putting an invisible overlay on your popular content. The only way that your page can get served in a frame with this configuration is if it's the same domain as the website.
- Moving the current frame to the top: This type of code ensures that the currently active frame is the one on the top, which makes it difficult to overlay the UI with hidden elements
- Client-side anti-clickjacking add-ons: Some web browsers, such as Firefox, have add-ons that stop scripts from running on a webpage. This approach prevents the hacker from being able to execute the script.
- Add a framekiller to the website: Javascript has a framekiller function that stops pages from being pulled into an iFrame
- Use a robust cybersecurity solution: A comprehensive cybersecurity solution, such as Forcepoint, considers multiple attack vectors when securing your website and systems from hackers.

Steps to Reproduce

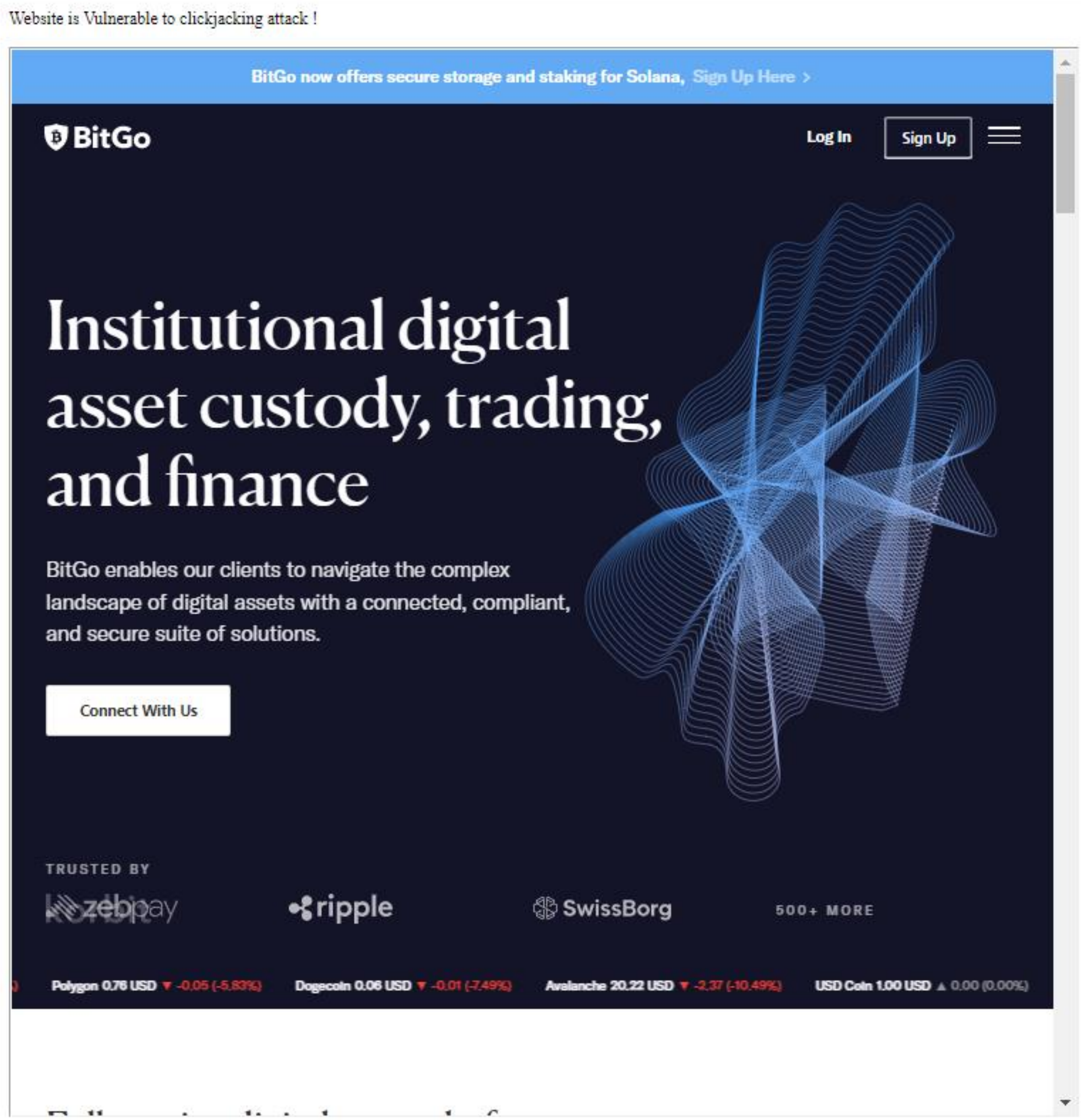
1. Copy the URL - https://www.bitgo.com/
2. Put the URL in the below code of the iframe and save the file with a extension .html and open that file

Code :

```
<html>
        <head>
                <title> ClickJacking Test Page .. </title>
        </head>
        <body>
                <p> Website is Vulnerable to clickjacking attack ! </p>
                <iframe src="https://www.bitgo.com/" width="1000" height="1000"></iframe>
        </body>
</html>
```

3. Observe that site is getting displayed in Iframe

P.S – Screenshot is attached on the PDF below.



Website is Vulnerable to clickjacking attack !

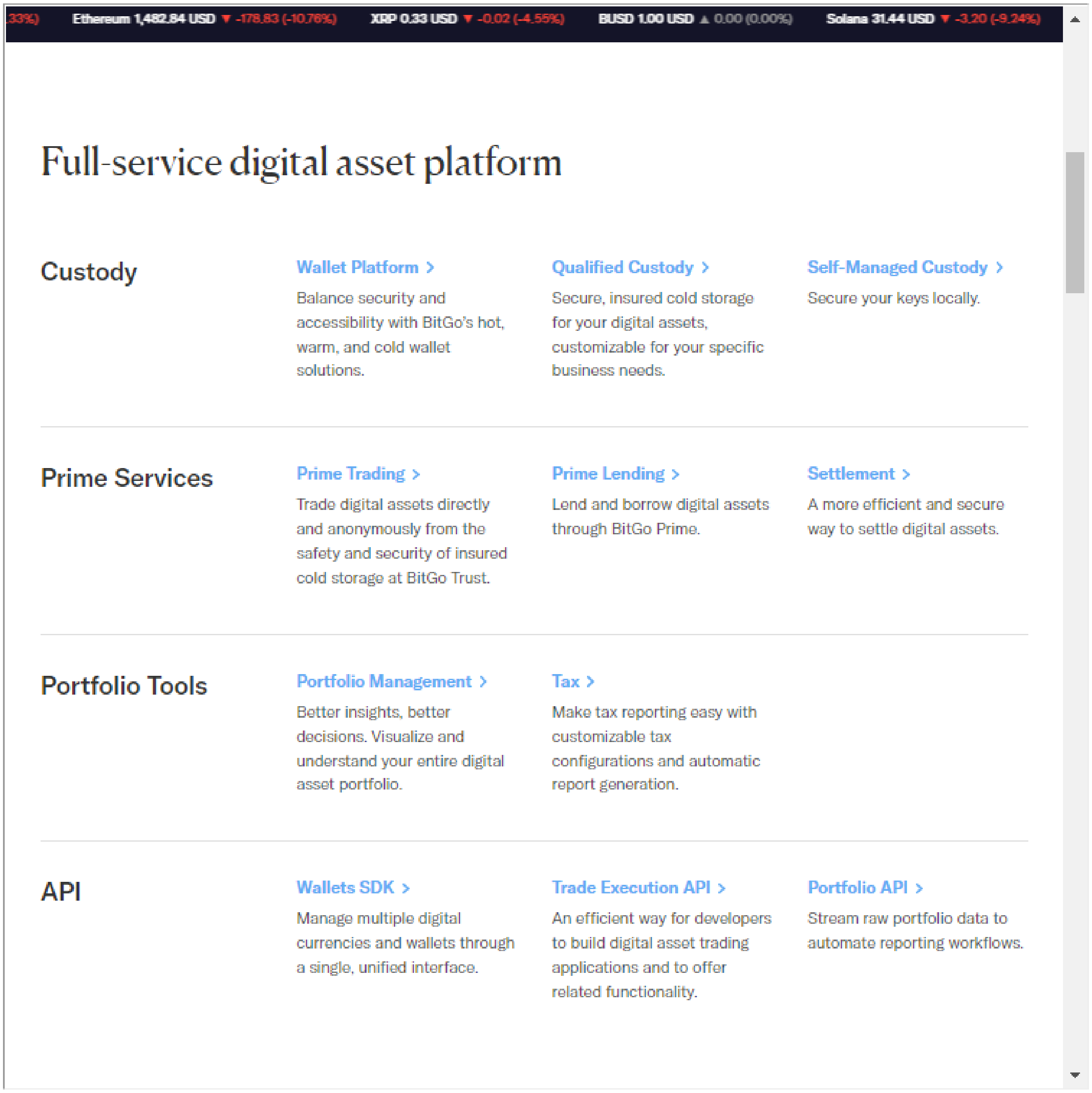
BitGo now offers secure storage and staking for Solana, Sign Up Here >

Institutional digital asset custody, trading, and finance

BitGo enables our clients to navigate the complex landscape of digital assets with a connected, compliant, and secure suite of solutions.

Polygon 0.76 USD ▼ -0.05 (-5.83%) Dogecoin 0.06 USD ▼ -0.01 (-7.49%) Avalanche 20.22 USD ▼ -2.37 (-10.49%) USD Coin 1.00 USD ▲ 0.00 (0.00%)

Website is Vulnerable to clickjacking attack !



.33%) Ethereum 1,482.84 USD ▼ -178.83 (-10.76%) XRP 0.33 USD ▼ -0.02 (-4.55%) BUSD 1.00 USD ▲ 0.00 (0.00%) Solana 31.44 USD ▼ -3.20 (-9.24%)

Full-service digital asset platform

Custody

Wallet Platform >
Balance security and accessibility with BitGo's hot, warm, and cold wallet solutions.

Qualified Custody >
Secure, insured cold storage for your digital assets, customizable for your specific business needs.

Self-Managed Custody >
Secure your keys locally.

Prime Services

Prime Trading >
Trade digital assets directly and anonymously from the safety and security of insured cold storage at BitGo Trust.

Prime Lending >
Lend and borrow digital assets through BitGo Prime.

Settlement >
A more efficient and secure way to settle digital assets.

Portfolio Tools

Portfolio Management >
Better insights, better decisions. Visualize and understand your entire digital asset portfolio.

Tax >
Make tax reporting easy with customizable tax configurations and automatic report generation.

API

Wallets SDK >
Manage multiple digital currencies and wallets through a single, unified interface.

Trade Execution API >
An efficient way for developers to build digital asset trading applications and to offer related functionality.

Portfolio API >
Stream raw portfolio data to automate reporting workflows.