Hi Team
I am a freelance web security auditor and bug bounty hunter. I identity security loop holes and flaws that can lead to the website secruity compromise or website users security
compromise. I have discovered a bug in your website that can allow for attackers to frame your website. Please find the details about the reported issue below.
I am hoping to receive a bug bounty reward for reporting this.

Bug type : UI Redressing
Impact : Phishing (account compromise)

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 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. Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

POC:

```
 <html>
<body>
<h1> Website is vulnerable to click jacking<h1>
<iframe width =100% height=80% src =" https://platform.cmcmarkets.com/#/login?b=CMC-CFD&r=UK&l=en"></iframe>
</body>
</html>
```

Impact:
The site can also be opened in an iframe after the user has logged it making it hard for the user to avoid phishing.A user can be tricked into entering his credentials in what he may are the placehoder for the original website details. And thus his credentials would be sent to the attacker. Further More the Payment page is also vulnerable to UI redressing Allowing for an attacker to gain access to the users payment credentials.
Remediation :
Add an iframe destroyer in the header of the page . Also if you would like for your website to open is specified Iframe origin headers then you can define the Origin headers for those website or origins.
Note :
I am also attaching a screen shot as proof of concept. Further more its not just the login page that is affected by this vulnerability.
waiting for your response
Regards

lookout.net/test/clickjack.html

Apps | Forgotten Password... | Synacor, Inc. - Care... | Response List 2 - G... | Untitled spreadshe... | Google Sheets

Test a page for clickjacking/framing vulnerability

Enter the URL to frame:

https://platform.cmcmarkets. Test it!