

Hi Team

I am a freelance web security auditor and bug bounty hunter. I identify security loop holes and flaws that can lead to the website security 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 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://www.bullhorn.com/client-login/"></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 see as the placeholder for the original website details. And thus his credentials would be sent to the attacker. Furthermore, the Payment page is also vulnerable to UI redressing, allowing for an attacker to gain access to the user's payment credentials.

**Remediation :**

Add an iframe destroyer in the header of the page. Also, if you would like for your website to open in a specified Iframe origin headers, then you can define the Origin headers for those website or origins.

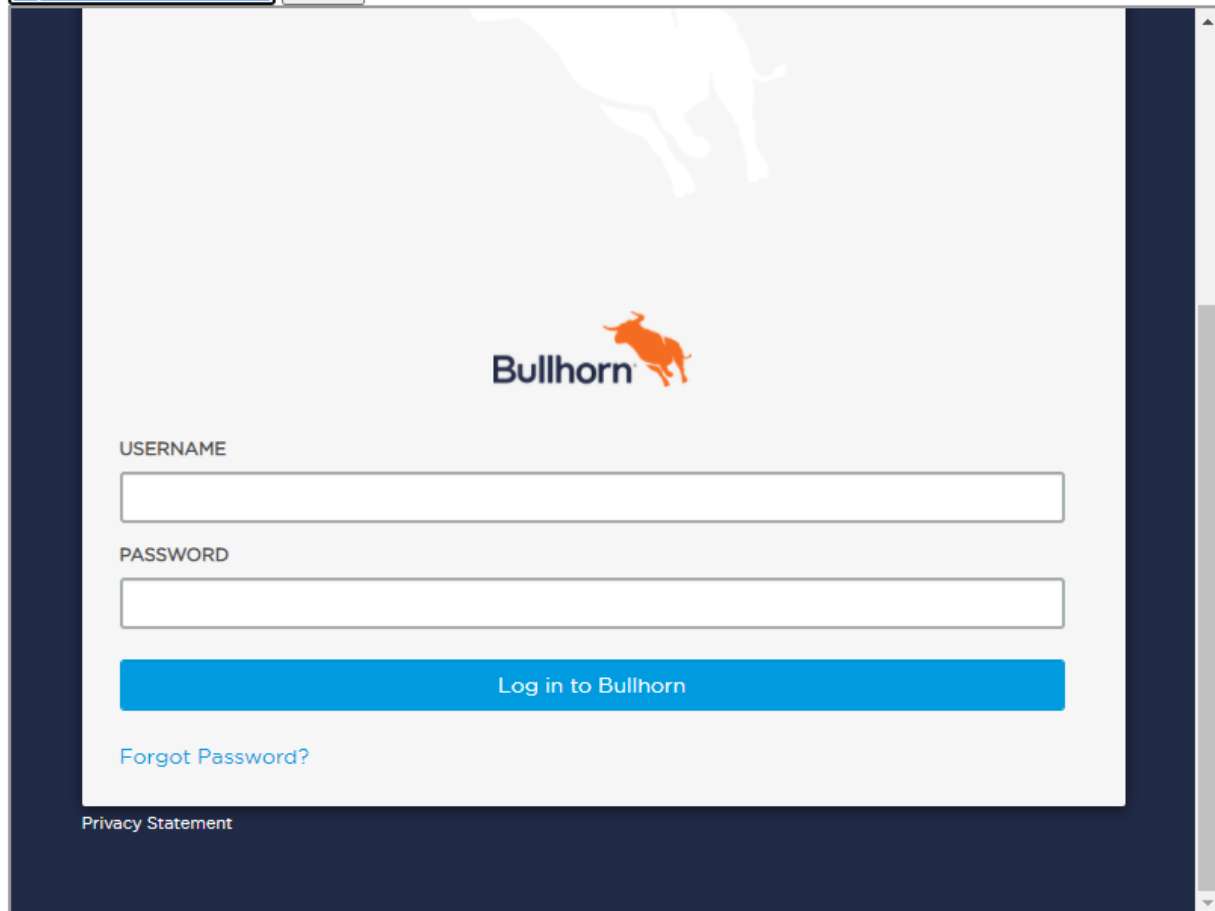
**Note :**

I am also attaching a screen shot as proof of concept. Furthermore, it's not just the login page that is affected by this vulnerability. Waiting for your response. Regards

## Test a page for clickjacking/framing vulnerability

Enter the URL to frame:

<https://www.bullhorn.com/cliq> Test it!



The screenshot shows a web browser window displaying a login page for Bullhorn. The page is framed within a browser window with a dark blue header and footer. The main content area is light gray and contains the Bullhorn logo (an orange bull head) and the text "Bullhorn". Below the logo are two input fields labeled "USERNAME" and "PASSWORD". A blue button labeled "Log in to Bullhorn" is positioned below the password field. A link labeled "Forgot Password?" is located below the button. At the bottom of the page, there is a link labeled "Privacy Statement".