because some only fix issues you've reported and they aren't pro-active and don't utilise the hackers knowledge to uncover more. This is where browsing disclosed reports can help because it may be fixed in **one area**, but is it fixed **throughout**?

- **Site-wide CSRF issue**

Relatively simple, the company in question had CSRF tokens on each request but if the value was blank then it would **display an error asking you to re-submit the form**, with the changes you intended to make reflected on the page. So imagine you have tried to update your email but you sent a blank token. **It would reflect your NEW email address but require you to submit the form again**. This was a site-wide issue as every feature produced the same results. The website had no X-FRAME-OPTIONS so I could simply send the request and display the results in an iframe, and then force the user to re-submit the form without them realising. You can actually find this as a challenge on bugbountyhunter.com , can you figure it out?

- **Bypassing identification process via poor blacklisting**

The site in question required you to verify your identity via a PHONE CALL in order to claim a page, except a **new feature introduced for upgrading your page allowed me to bypass this process** and I only had to provide payment details. The only problem was they didn't blacklist sandbox credit card details so armed with that I was able to claim any page I wanted without verifying my identity at all. How? Because sandbox credit card details will always return "true", that's their purpose. They tried to fix this by blacklisting certain CC numbers but I was able to bypass it by using numerous different details.

This was a fun bug as the company argued there was no problem, but being able to bypass their default verification purposes in my opinion is a very valid issue. Companies will often have "protection" in place on some features but they introduce new features (to generate income usually) overtime. New developers building on old code.