Ritesh Gohil Follow
Jul 18 · 2 min read · Listen

Softr Version 2.0 is vulnerable to HTML injection via the first name field on the creation of the Victim Account.

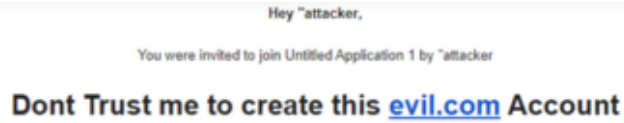
We can inject malicious payload in the first name field and whenever we will do create a New Victim account then the payload will reflect in the email.

There's an HTML injection vulnerability present inside emails sent from slack when the FIRST name on the account contains HTML. The HTML is stored in the backend database and when emails are sent (promotional, etc), the HTML is sent along with the rest of the email.

> ***An example payload may be:***
> *Attacke Says "<h1>Dont Trust me to create this evil.com Account</h1>*
> *<h2>Anything long string, message,paragraph</h2>*

Steps-To-Reproduce:
1) Use Demo Product of https://www.softr.io/
2) Put Payload in First Name parameter: Attacke Says "<h1>Dont Trust me to create this evil.com Account</h1>
3) Create an account. You will get it Long string HTML payload reflected with a hyperlink to the victim's email.

POC:



Impact:
This vulnerability can lead to the reformatting/editing of emails from an official email address, which can be used in targeted phishing attacks. This could lead to users being tricked into giving logins away to malicious attackers.

😎🎯 I got my 7th **CVE-2022–32407** 🎯 😎

Tip: if the product owner tells you that this is a known bug to them and refuses to pay Go ahead and apply for CVE ✌️ 👉 Refused To Pay it's Okay! I will go for CVE 😇

Cheers! Happy Hunting Guys :)
Linkedin: https://ie.linkedin.com/in/riteshgohil25
Twitter: https://twitter.com/RiteshG37659480