Re: Disclosure of Security Vulnerability

From Za0gQfERuuRkbi3eX <Za0gQfERuuRkbi3eX@proton.me>

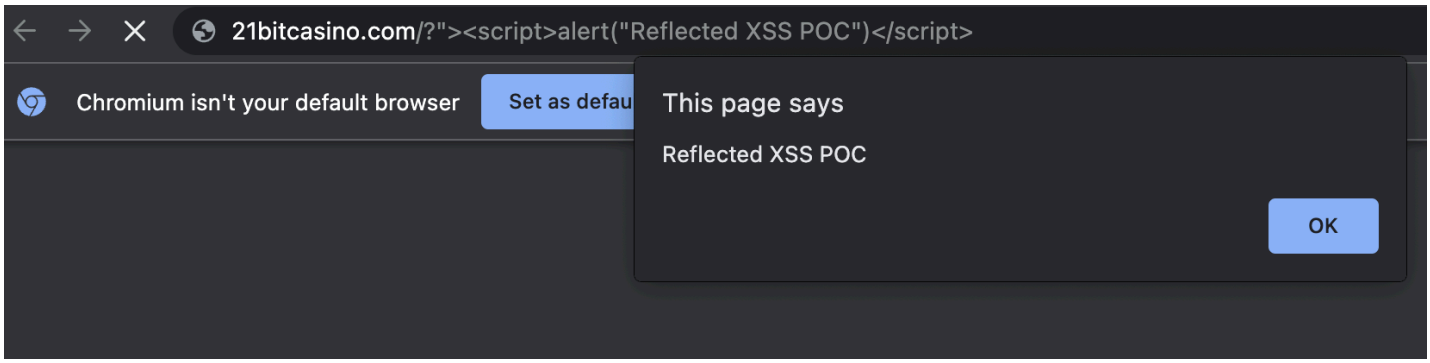
To support@21bit.com

Date Thursday, November 3rd, 2022 at 1:04 PM

This is a courtesy notification that as per responsible disclosure guidelines, I will be publicly disclosing all vulnerabilities I found on your site via social media if I do not receive a response from your security team within one week.

------- Original Message -------
On Wednesday, October 26th, 2022 at 1:42 PM, Za0gQfERuuRkbi3eX <Za0gQfERuuRkbi3eX@proton.me> wrote:

> Hi, please confirm receipt?
>
> ------- Original Message -------
> On Friday, October 21st, 2022 at 11:21 PM, Za0gQfERuuRkbi3eX <Za0gQfERuuRkbi3eX@proton.me> wrote:
>
> > Hello,
> >
> > I wish to disclose a reflected cross-site scripting vulnerability I discovered on https://21bitcasino.com. I've attached the request and response you can submit to trigger the vulnerability. Specifically, the payload used is **?"><script>alert(document.cookie)</script>** and it's reflected on the base URL In the response, look for the line: **<input type="text" name="base_cat_name" id="base_cat_name" value="?"><script>alert(document.cookie)</script>=1" hidden />**, which shows successful injection of my JavaScript payload, which displays the current user's cookie value. Another sample payload is included here.



An attacker can customize this payload slightly to point at an external malicious script, send this link+payload as a malicious link to users, collect their cookies, then take over their account via swapping the attacker's own cookies with the victim's stolen cookies. Naturally, this leads to theft of user funds if the attacker sees any in the victim's wallet

Please advise?

97.79 KB 1 embedded image

XSS POC.png 97.79 KB