Explain how a cross site script (XSS) is able to attack the users of a website rather than the website administrator/owner.

Cross-site scripting (XSS) attacks are a type of injection attack where malicious scripts are injected into trusted websites. These attacks target the users of a website rather than the website administrator/owner.

An attacker exploits a vulnerability in a website's code to inject malicious scripts, typically in the form of JavaScript, into the web pages. This can be done through input fields, comments, or other user-generated content. When a user visits the compromised web page, the injected malicious scripts are executed by their web browser. Since the scripts are embedded within the trusted website, the browser considers them as legitimate code and executes them. The executed malicious scripts have access to the user's browser and can manipulate the web page content, steal sensitive information, or perform unauthorized actions on behalf of the user. This can include stealing login credentials, session cookies, or personal information entered on the website. Once a user's browser is compromised, the attacker can use the compromised user session to launch further attacks. This can involve spreading the malicious scripts to other users by injecting them into web pages or sending them as part of malicious links or emails.

The consequences of an XSS attack on users can vary depending on the attacker's intentions. It can range from stealing sensitive information, such as credit card details or personal data, to performing unauthorized actions on the user's behalf, such as making unauthorized transactions or modifying account settings.

References:

PortSwigger. (2023). What is cross-site scripting (XSS) and how to prevent it? Portswigger.net. https://portswigger.net/web-security/cross-site-scripting

S, K. (2020). Cross Site Scripting (XSS) | OWASP. Owasp.org; OWASP. https://owasp.org/www-community/attacks/xss/

What Is Cross Site Scripting (XSS) and How Does It Work? | Synopsys. (n.d.). Www.synopsys.com. https://www.synopsys.com/glossary/what-is-cross-site-scripting.html#:~:text=Definition