



IT-Gefahren, die Sie kennen sollten

Cross-Site Scripting (XSS)

Cross-Site Scripting ist eine Art von Angriff, bei dem schädlicher Code in eine vertrauenswürdige Website eingebettet wird. Wenn die manipulierte Seite von einem Nutzer aufgerufen wird, wird der schädliche Code ausgeführt.

ZIEL / SCHADEN

Diese Angriffe können genutzt werden, um persönliche Daten zu stehlen, die Sitzungen der Nutzer zu kapern und Malware zu verbreiten.

INFEKTIONSWEG

Durch das Besuchen einer mit XSS infizierten Website, bei der schädlicher Code in den Webbrowser des Benutzers geladen wird.

ABWEHR

Aktualisieren Sie Ihren Browser und Ihre Sicherheitssoftware regelmässig. Seien Sie vorsichtig beim Klicken auf Links, insbesondere in E-Mails oder Nachrichten von unbekanntem Absendern.

BEFREIUNG MÖGLICH?

Ja, durch Aktualisierung des Browsers, Löschen von Cookies und Änderung von Passwörtern.

ANGRIFF - WAS NUN?

Wenn Sie glauben, dass Sie Opfer eines XSS-Angriffs geworden sind, löschen Sie Ihre Browser-Cookies, ändern Sie Ihre Passwörter und führen Sie einen Antiviren-Scan durch.