Underestimated Risk: XSS via Cookie

Dawid Czagan
SECURITY INSTRUCTOR

@dawidczagan

Overview

XSS via cookie

Cross-origin exploitation

Demo

Fixing the problem

XSS via Cookie

XSS via cookie ≠ local exploitation

a.example.com (XSS via cookie)

Cross-origin exploitation

b.example.com (XSS)

↓

a.example.com (XSS via cookie)

Cross-origin Exploitation

b.example.com (XSS)

↓

set cookie with domain=.example.com

↓

cookie sent to a.example.com

↓

a.example.com (XSS via cookie)

Demo

Cross-origin exploitation

1. `<p> <script> alert("XSS") </script> </p>`

↓ sanitize special characters

2. `<p> &lt;script&gt; alert("XSS") &lt;/script&gt; </p>`

Fixing the Problem

1. <script> alert("XSS") </script> EXECUTED
2. <script> alert("XSS") </script> DISPLAYED

Summary

XSS via cookie ≠ local exploitation

Cross-origin exploitation

Sanitize special characters