

Forum:[Hack Forums](#)

Thread: [Curious about this attack](#)

Abathur - October 10, 2017, 11:12 am

Can anyone answer this?

Widgets.com, a company that sells widgets online, receives orders from customers through web forms. The customer completes the form in their browser window and clicks the submit button on the page. A url containing the type of widgets, the unit price and the quantity is created by javascript code in the page and sent by the user's browser to the widgets.com server. Upon receiving this request the widgets.com server extracts the values from the url and enters them into the order processing database as a new order. How might this scenario be exploited by an attacker, name the type of flaw?

Baud - October 10, 2017, 12:17 pm

The first thing that comes to mind is XSS, which basically is JavaScript code embedded in places where it shouldn't be, and which is executed whenever the page containing the injected code is loaded. It's also one of the most common vulnerabilities out there, big companies were found with XSS vulnerabilities many times before. You can learn more about it here:

[https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))

Abathur - October 10, 2017, 2:54 pm

(Oct 10, 2017 12:17 PM)Baud Wrote: [\[CITE\]](#) The first thing that comes to mind is XSS, which basically is JavaScript code embedded in places where it shouldn't be, and which is executed whenever the page containing the injected code is loaded. It's also one of the most common vulnerabilities out there, big companies were found with XSS vulnerabilities many times before. You can learn more about it here: [https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))

Great thank you!