Timothy De Block
Address 1
Address 2

(803) 477-2629
timothy.deblock@gmail.com

January 13, 2016

Company
Address line 1
Address line 2

Dear Hiring Authority,

I would like to express my interest in the security engineer position at <COMPANY>. I like GIFs and memes. Here's one of <SITE> doing the Harlem Shake: <GIF>. And here's a YouTube video with sound: <LINK>. This is an example of cross site scripting (XSS) and <COMPANY> isn't the only one that I can perform this demo on. The details on how to perform this little demonstration are on Troy Hunt's site: http://www.troyhunt.com/2015/09/introducing-you-to-browser-security.html. The short version is that I ran this bit of code (in the article) in Chrome's developer tools. The code attempts to load a .css and .mp3 file that causes the action and sound on the site. The issue is in the Content Security Policy (CSP). If you try the same code on Twitter you get the following error message.

Refused to load the stylesheet** 'https://s3.amazonaws.com/moovweb-marketing/playground/harlem-shake-style.css' **because it violates the following Content Security Policy directive: "style-src** https://fonts.googleapis.com https://twitter.com https://*.twimg.com https://translate.googleapis.com https://ton.twitter.com 'unsafe-inline' https://platform.twitter.com https://maxcdn.bootstrapcdn.com https://netdna.bootstrapcdn.com **'self'".

Refused to load media from** 'https://s3.amazonaws.com/moovweb-marketing/playground/harlem-shake.mp3' **because it violates the following Content Security Policy directive: "media-src** https://twitter.com https://*.twimg.com https://ton.twitter.com **blob: 'self'".

I am currently a Security Analyst III for the state of South Carolina. I don't have a lot of development experience, but I have a desire to learn. I have a broad background in IT and a strong interest in application security. Previously, I worked for <COMPANY> in a volunteer capacity. I would love to have an opportunity to work there full-time and make a positive impact on the security of those sites.

Sincerely,

Timothy De Block