inject basic HTML such as “><script>alert(0)</script> - and upon visiting, my XSS would execute. A lot of researchers skip through a website and the requests quickly and can miss interesting functionality that only happens once. The very first time you open a mobile application sometimes requests are made only once (registering your device). Don’t miss it!

This is why it’s also key to go through the web application you’re testing more than once. You can never see everything on your first look. I have been through some bug bounty program assets over 50 times. If you aren’t prepared to put in the work, don’t expect results.

- **IDOR which enabled me to enumerate any users’ personal data, patch gave me insight as to how the developers think when developing**

This bug was relatively simple but it’s the patch that was interesting. The first bug enabled me to just simply query api.example.com/api/user/1 and view their details. After reporting it and the company patched it they introduced a unique “hash” value which was needed to query the users details. The only problem was, **changing the request from GET to POST caused an error which leaked that users’ unique hash value**. A lot of developers only create code around the intended functionality, for example in this case they were expecting a GET request but when presented with a POST request, the code essentially had “no idea” what to do and it ended up causing an error. This is a clear example of how to use my methodology because from that knowledge I knew that the same problem would probably exist elsewhere throughout the web application as I know a developer will typically make the same mistake more than once. From them patching my vulnerability I got an insight as to how the developers are thinking when coding. Use patch information to your advantage!

I have also had this happen when developers **will only fix the endpoints that you report**, however this type of bug (IDOR) may affect their entire web application. This can actually give you an insight into how companies handle vulnerability reports