everywhere possible. It's mentioned a few times, but sometimes things can be overlooked. **Leave no stone unturned**.

- **If I can input my own URL on my profile**, what filtering is in place to prevent something such as javascript:alert(0)? This is a *key* area I look for when setting up my profile.

- **Is updating my account information different on the mobile app?** Most mobile apps will use an API to update information so maybe it's vulnerable to IDOR. As well as this, different filtering may apply. I've had lots of cases where XSS was filtered on the desktop site but it wasn't on the mobile application. Perhaps the mobile team is not as educated on security as the desktop team? Maybe it was rushed.

- **How do they handle photo/video uploads (if available)**? What sort of filtering is in place? Can I upload .txt even though it says only .jpg .png is allowed? Do they store these files on the root domain or is it hosted elsewhere? Even if it's stored elsewhere (example-cdn.com) check if this domain is included in the CSP as it may still be useful.

- **What information is actually available on my public profile that I can control**? The key is what you can control and how and where it's reflected. What's in place to prevent me from entering malicious HTML in my bio for example? Perhaps they've used htmlentities so < > " is filtered, and it's reflected as:

```
<div id="example" onclick="runjs('userinput&lt;&amp;quot;');">
```

But you could use **');alert('example');** which results in:

```
<div id="example" onclick="runjs('userinput');alert('example');">
```