I looked into the breach that happened with First American Financial Corporation in 2019. In this breach, documents containing information such as SSN numbers, bank account numbers, tax records, driver’s license information, and more were discovered to just be sitting online for anyone to access. The crazy part is it wasn’t the work of any hackers. First American did this to themselves by using a website design error that unfortunately is relatively common, that being using Insecure Direct Object Reference or IDOR. This means that specific links were created for each document and these links were only meant to be viewed by a specific party (the owner of the document). However, there is no way to verify who is actual viewing the link. So, any average Joe could discover the link and access the information. On top of that, they could do some work and change the id and parts of the URL to access other information within First American’s records. Essentially, all their documentation was just hanging out in the open online ready for someone to snatch it up. They’ve of course fixed this, but during the time it wasn’t fixed who knows how many documents were downloaded by how many people that could be used to steal peoples’ information and commit fraud. I just found it really interested that it wasn’t a hacker that did this but the company themselves. It just goes to show how careful you must be so you don’t shoot yourself in the foot when it comes to security.