Aaron Shipley

CS 405: Case Study – Security Breaches

Southern New Hampshire University

Wasim Alim

09/30/2022

The First American Financial data breach of 2019 was one of the largest data breaches documented. This data breach happened in May 2019 to First American Financial, a major company in the insurance business sector. The reason for this data breach making the news was due to 885 million sensitive documents being leaked. The documents contained sensitive data such as bank account numbers, mortgage documents, social security numbers, and photos of government-issued identification cards. Some of the 885 million documents dated back to 2003. Unlike some attacks and data breaches, there was no clear path left by the attacker(s) showing a breach of the network or unauthorized access gained to user information. This attack, according to 2019 article in Forbes (Dellinger, 2019), was an IDOR, or Insecure Direct Object Reference, was targeted by the attacker(s) to gain access to a link to a webpage containing sensitive data.

Being a large insurance corporation, First American Financial is an obvious target for attack due to their large database of sensitive information provided by its customers. This sensitive data, as mentioned previously, is the lifeline of customers to make any large-scale purchases, pay bills, protect their family from accidents, or to just drive to work each day. This data is essential to one’s ability to function in everyday life. A vulnerability, such as an IDOR can be exploited freely and in terms of the data breach, the sensitive data was freely available to access and was not stolen. This type of exploitation, according to Dave Farrow (Dellinger, 2019) is exposed and the attacker simply walks through the front door, instead of sneaking in.

In terms of policies or procedures that could be used to help prevent this attack, many warnings and documentation of the vulnerability were made in 2018 regarding this attack. The procedure used to identify the issue was the process of fuzz testing to verify input data was in its distinct format, which was not the case for First American Financial. This disregard to the flags raised ahead of time, resulted in the 2019 data leak. According to Avatao (2022) there are multiple methods and procedures that may be used in terms of preventing IDOR attacks. The first method involves the first A of AAA, authentication. The use of syntactical and logical validation should be used in terms of sensitive information. Setting up markers to verify minimum and maximum lengths for characters, and bounds for numeric values is a must. Creating parameters for acceptable characters should be used as well. Pattern verification for data like phone numbers, SSN, or id numbers must also be used.

The next method involves the second A in AAA, authorization. Access control checks should be used to help prevent IDOR attacks. An example of this is the method of doing database checks to ensure the data or information is authentic. The practice of the principle of least privilege should be instilled into the development as well. This principle implements e method to give access to the least amount of information necessary while still being functional to the user. This method can cover the third A of AAA, accounting as well. Accounting involves creating logs of access by the user to particular data in order to create a path to follow in the event of a potential attack. The use of access control checks in this way would be have resource values in session and on submit are checked at a timed interval with stored values on the server.

These methods described to help prevent IDOR attacks, like the one on First American Financial, should be implemented into multiple layers of the Defense in Depth in order to create a security net over the website and its sensitive data. The use of syntactical and logical validation would utilize the perimeter layer of DoD. This initial layer provides a foundation of security for the website. The network layer of DoD would implement access control checks and the principle of least privilege in order to safeguard the sensitive data in the network. Having proper encryption put in place on sensitive information within the endpoint layer of DoD is vital. With the use of proper syntactical and logical validation, the information entered by the user, once accepted, should have a layer of encryption used upon it to safeguard the information in yet another layer to ensure its safety.

References

Avatao. (2022, July 20). *Best practices to prevent IDOR vulnerabilities*. Avatao. Retrieved October 1, 2022, from https://avatao.com/blog-best-practices-to-prevent-idor-vulnerabilities/

Dellinger, A. J. (2019, May 26). *Understanding the first American financial data leak: How did it happen and what does it mean?* Forbes. Retrieved October 1, 2022, from https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/?sh=2dd60a04567f

Symanovich , S. (2019, September 5). *What is a security breach?* Norton. Retrieved October 1, 2022, from https://us.norton.com/blog/privacy/security-breach#

Team Password. (2021, September 7). *The first American Corporation Data Leak what happened?* TeamPassword. Retrieved October 1, 2022, from https://teampassword.com/blog/the-first-american-corporation-data-leak-what-happened

Tungal, A. (2022, September 22). *The 67 biggest data breaches (updated September 2022): Upguard*. RSS. Retrieved October 1, 2022, from https://www.upguard.com/blog/biggest-data-breaches