**Tyler Carrier**

**Information Security**

**How Hackers Combine Database Contents to Increase Harvest**

**11/5/18**

**Box #88**

Nowadays, database servers are the most useful sources for being compromised by hackers. Companies from all over are suffering data breaches. This includes even major companies like Macy’s, Sears, and Adidas. According to Business Insider, since January of 2017, at least sixteen retail companies have been hacked and had information stolen (Green). They also share another very interesting statistic, “A report from cybersecurity firm Shape Security showed that almost 90% of the login attempts made on online retailers' websites are hackers using stolen data” (Green). This is a huge number which really shows the relevance of database breachers in this day and age.

There are many methods which hackers utilize when attempting to crack into a database. One method is effectively described in an article entitled, “Extracting Data from Online Databases Using Sqlmap,” by OccupyTheWeb. Sqlmap is a great tool which can be used to hack into databases. Hackers can use a program called BackTrack to effectively utilize Sqlmap. One step that hackers can use is attempting to enumerate users of the database and therefore gain immediate access to the database (OccupyTheWeb). Another method that hackers can use to gain access to the database is by enumerating tables and columns (OccupyTheWeb). This can be effectively accomplished by using Sqlmap as well.

The main problem that lies within these database breaches is the reputation that the company has to withhold. In KPMG’s experience, they noticed 19% of their online shoppers refrain from shopping after the result of a data breach (Green). One major company which experienced a data breach was Macy’s. According to Green in BusinessInsider, “Macy's confirmed that some [customers shopping online at Macys.com and Bloomingdales.com](http://www.businessinsider.com/macys-bloomingdales-hack-disclosed-2018-7) between April 26 and June 12 could have had their personal information and credit card details exposed to a third party” (Green).

Another company which experienced a data breach was Adidas. This sporting company confirmed that “an ‘unauthorized party’ said it had gained access to customer data on Adidas' US website. Currently, the company believes only customers who shopped on and purchased items from the US version of Adidas.com may have been affected by the breach” (Green). Information that is usually taken from databases are contact information and login information. Adidas experienced the breaching of this information possibly by the millions.

According to an article by Valency Networks, there are four stages to which a hacker attempts to acquire data. These four include application (patch control and encryption), database (authentication, roles, and policies), OS (authentication control), and network (IPSec, SSL, and TLS) (Valency Networks). With databases being the second step in data breaching, it is obvious how relevant the threat of database breaches is.

One interesting method that is heavily utilized by hackers is query string manipulation. When there is a request from a browser to the web server, there is a url containing a string parameter which is used to fetch information from the database. If the web application is not secure, there can be a lot of loopholes in this method. The hacker can use search queries right from the websites in order to find information within the company’s database. Other methods that hackers can utilize are privilege elevation, vulnerability exploitation, SQL injection, packet sniffing, and database DoS (Valency Networks).

In conclusion, databases are jackpots when it comes to hackers attempting to gain information. There are many methods which can be used in order to gain access into company’s databases. Therefore, it is important that companies ensure the utmost security when considering their databases. There is no way to be fully protected from hackers, but companies can take effective steps which will make the tasks of hackers much more difficult.

**Work Cited:**

Green, Dennis. “If You Shopped at These 16 Stores in the Last Year, Your Data Might

Have Been Stolen.” Business Insider, Business Insider, 22 Aug. 2018,

[www.businessinsider.com/data-breaches-2018-4#adidas-3](http://www.businessinsider.com/data-breaches-2018-4#adidas-3).

Hunsaker, Marshall, et al. “How to Hack Databases: Hacking MySQL Online Databases

with Sqlmap.” WonderHowTo, WonderHowTo, 12 Jan. 2014,

null-byte.wonderhowto.com/how-to/hack-databases-hacking-mysql-online-datab

ases-with-sqlmap-0150368/.

Valency NetwValency Networks. “Cyber Attacks Explained: Database Hacking | Valency

Networks Blog.” Valency Networks Blog,

“Cyber Attacks Explained: Database Hacking | Valency Networks Blog.” Valency Networks Blog, [www.valencynetworks.com/blogs/cyber-attacks-explained-database-hacking/](http://www.valencynetworks.com/blogs/cyber-attacks-explained-database-hacking/).