

**Team** : System Admin

**Members : Student Number**

Nikolay Nichev : 18039464

Sam Hogan : 18044522

Ajay Davies : 17045592

Levi Goldsworthy : 18035868

Employability

Vulnerability Document

**Introduction**

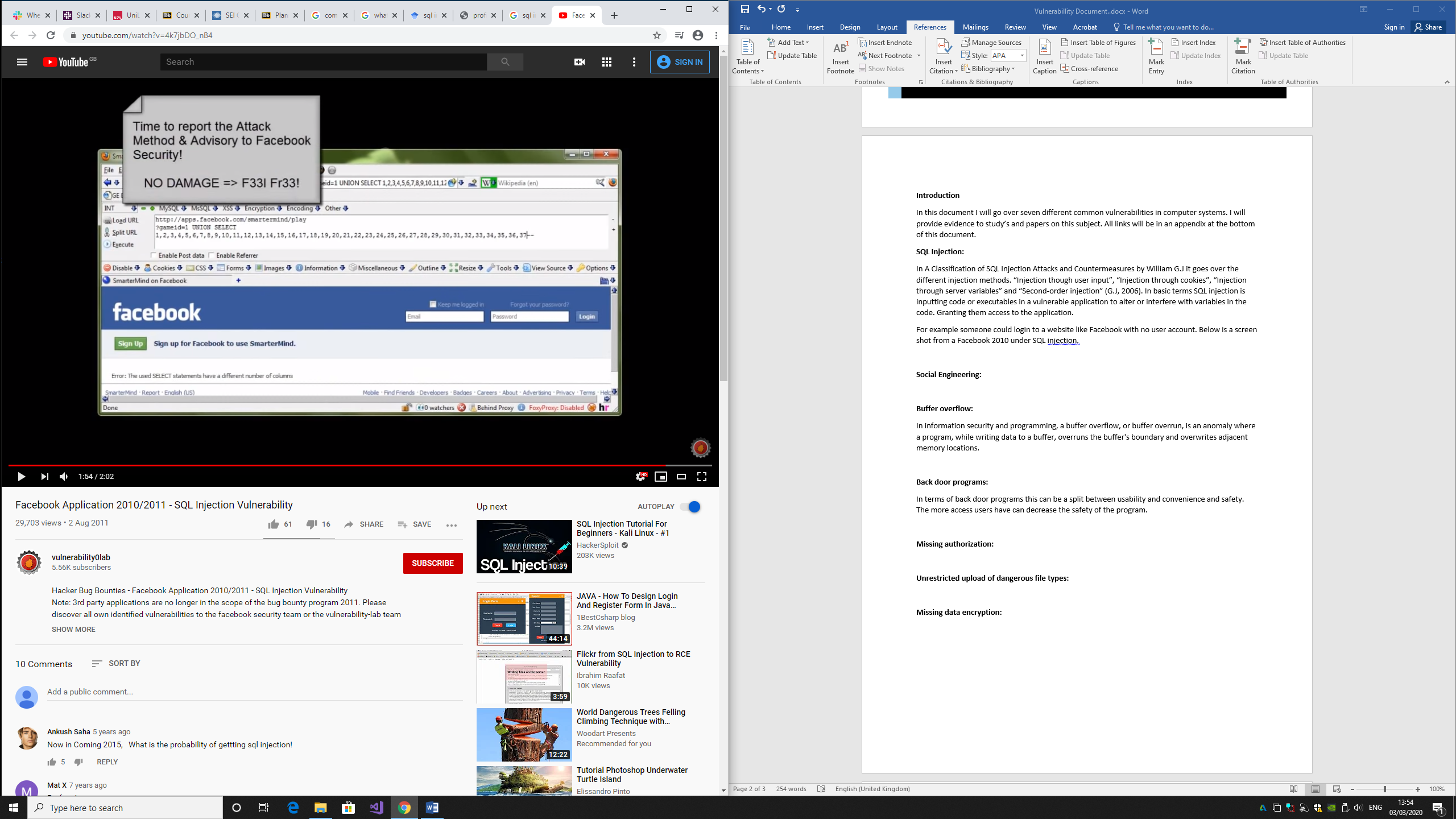
In this document I will go over seven different common vulnerabilities in computer systems. I will provide evidence to study’s and papers on this subject. All links will be in an appendix at the bottom of this document.

**SQL Injection:**

<https://www.cc.gatech.edu/fac/Alex.Orso/papers/halfond.viegas.orso.ISSSE06.pdf>

In A Classification of SQL Injection Attacks and Countermeasures by William G.J it goes over the different injection methods. “Injection though user input”, “Injection through cookies”, “Injection through server variables” and “Second-order injection” (G.J, 2006). In basic terms SQL injection is inputting code or executables in a vulnerable application to alter or interfere with variables in the code. Granting them access to the application.

For example, someone could login to a website like Facebook with no user account. Below is a screen shot from a Facebook 2010 under an SQL injection attack. This shows using SQL code thought user input. Showing that’s this is possible. This could possibly cause good deal of damages to a website if attacker were to use this with malicious intent.



There are more methods to achieve injection however there is no need to go over this. Now I will go over the counter measures.

Some ways to prevent it is by not allowing SQL code inside of the textboxes, which can be done using SQL functions, which will help read over inserted characters and preventing any SQL from being injected. Another could be to use non-dynamic SQL, meaning that prepared statements and parametrized queries. One final way to help protect against SQL injections is to use web application firewall.

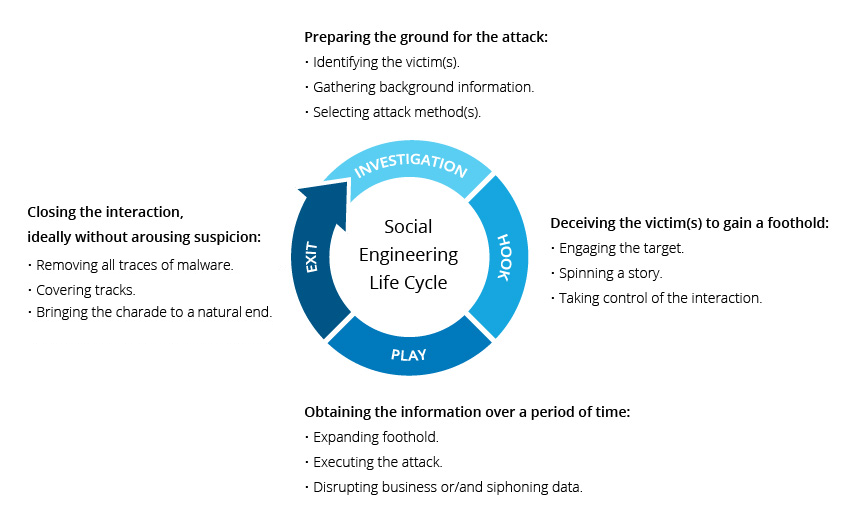
**Social Engineering:**

Social engineering is a unique type of vulnerability in that the “typical” form of hacking that everyone knows is not used. Instead of using software or files that can get into another machine, they simply manipulate others into giving away vital information that the hackers can use. The only software the hackers may use is something like TeamViewer, which allows a user to remotely control a machine, or a key logger which will track passwords and usernames.

*“Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software.”* (What is Social engineering?, n.d.)

Therefore, it’s so dangerous as a vulnerability, because no matter how much technology is implemented into your company, it won’t stop user error from being exploited. This is why staff members will need to be trained about simple principles like do not give your password to anyone, do not click suspicious links, etc.

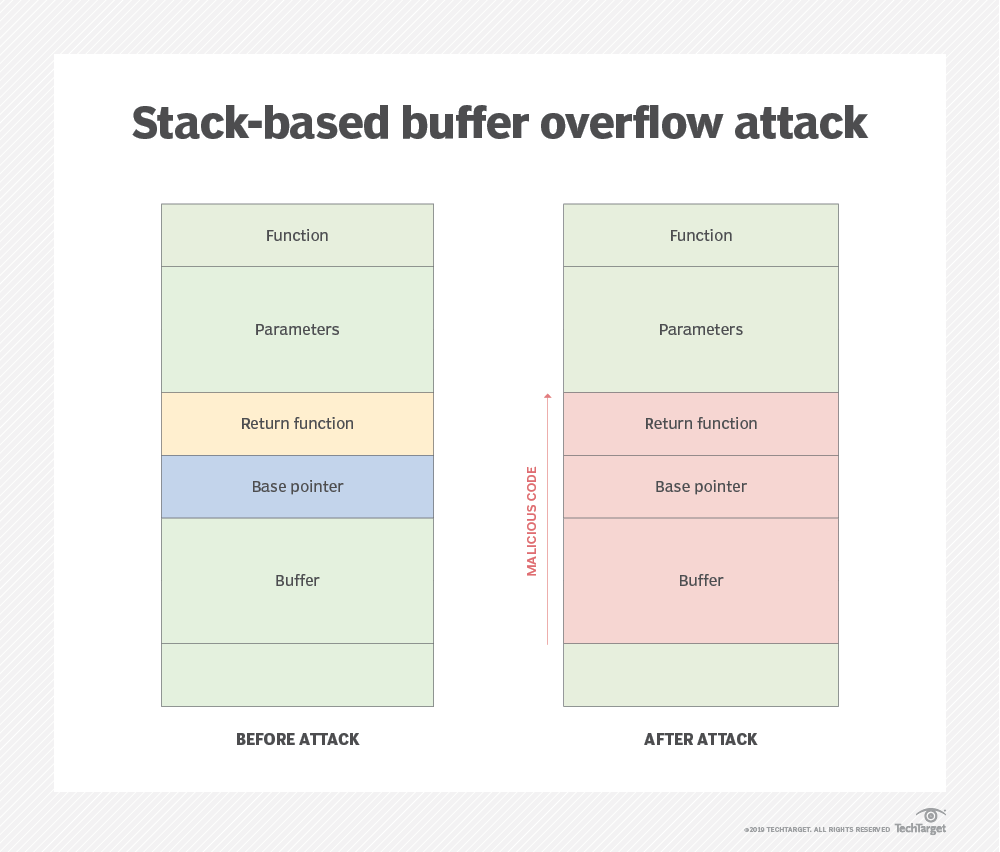
As much as staff is trained however, users of the company’s software can still fall victim to social engineering. Although the company won’t be at a loss, the user will and may result in them using a different company.



**Buffer overflow:**

In information security and programming, a buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations. What is a buffer? It’s a section of memory that contains practically anything like strings or integers. So, if you had a buffer that can hold 80 integers and you input 81 integers, you’d have a buffer overflow. Overflows can lead to corruption or a crash of the program. Hackers can take advantage of this vulnerability. They could overflow a vital program or server, crashing entire websites or programs, or in very dire situations they can cause an overflow and enter a server or program, letting them modify or take information to their benefit. *“Exploiting a buffer overflow allows an attacker to control or crash the process or to modify its internal variables.”* (Rouse, 2016)

To avoid running into buffer overflows you should hire professional and well-trained programmers, since they will be well versed in buffer overflows, and their code wouldn’t allow for that to happen. By hiring a cheaper programmer, or perhaps doing it yourself, you could potentially run into that error and leave your program or website vulnerable.



**Backdoor attacks:**

Even if your website or program has incredibly good security measures when looking at it, there may always be a way for hackers to skirt around those issues and find another way inside, this is why it’s known as a backdoor attack, since they are avoiding the obviously well defended front door and sneaking in through the other side.

Backdoor attacks are often done with what many people refer to as a trojan, a very typical computer attack. A trojan is a malicious file that is often disguised as something else, like an email attachment or a program. Backdoors can also be built in. Built-in are often done by the creator of the program so they can quickly test their program during the development phase, sometimes however they ship with the final program which could lead to hackers taking advantage of them, luckily however this is quite rare.

With a backdoor being exploited, hackers can do a lot with your system, some of which are very well known like spyware or ransomware as an example. Spyware is malware that will spy on the user’s passwords, usernames, emails, credit card information, files, etc, which the hacker can take advantage of as much as they want. Ransom ware is also a type of malware that will lock the user’s PC off from them unless they pay a specified amount of money, which then they may unlock the user’s PC.

*“Kaspersky recently reported that in the second half of 2018, 3.1 percent of all attacks blocked by its distributed antivirus network were backdoor attacks”* (Flores, 2019)

**Missing authorization/Wrong authorization:**

Missing authorization is a very simple yet devastating vulnerability. When you enter a page, you have to enter your username and password, or sometimes be sent a text message with a code. However, due to an issue with the authorization of the program or website, it may lead to the authorization being broken and letting any user inside it. This user could be logged in with an admin account, which they could take advantage of to steal or modify information.

Wrong authorization has a similar issue to missing and can lead to the same faults. Wrong authorization is when users are given admin access by mistake, or the manager of the network gives every person admin access to avoid simple problems. However, if everyone has top level access and if just one of them is hacked, the hacker could do serious damage with admin privileges.

The damage that could be done is stealing vital information to do with the company or user, lock users out of their machine, install malware or trojans, etc.

*“Even more interesting is that the Avecto 2016 report highlights that if sysadmins had forced users to utilize a low-privileged account instead of an admin-level profile, they would have mitigated 100% of all critical Internet Explorer and Microsoft Edge browser vulnerabilities patched during the past year.”* (Cimpanu, 2017)

**Unrestricted upload/download of dangerous file types:**

Most companies with many employee’s should have restricted uploading and downloading of suspicious files or file types.

What is considered a suspicious file or file type? Well, a suspicious file may have a dangerous name, or may be downloaded from a not-trusted website. Suspicious file types are the more dangerous, however, since some files can make critical changes to a computer. The most well known is .exe, this file type is just a runnable program, however any program can be very dangerous, or used maliciously. With .exe it is always safe to check the file size and see if it corresponds with what it should be doing, or making sure it isn’t used as a wrong file extension, as many hackers may use .exe on files that shouldn’t be using executables, like an image or a music file. *“Server-side attacks: The web server can be compromised by uploading and executing a web-shell which can run commands, browse system files, browse local resources, attack other servers, or exploit the local vulnerabilities, and so forth.”* (Soroush Dalili, n.d.)

Here is a known list of file types that aren’t necessarily bad, but if are received in untrusted source or in unexpected circumstances, would be recommended to not download/upload them.

ADE, ADP, APP, ASA, ASP, BAS, BAT, CER, CHM, CMD, COM, CPL, CRT, CSH, DLL, EXE, FXP, HLP, HTA, HTM, HTML, HTR, INF, INS, ISP, ITS, JS, JSE, KSH, LNK, MAD, MAF, MAG, MAM, MAQ, MAR, MAS, MAT, MAU, MAV, MAW, MDA, MDB, MDE, MDT, MDW, MDZ, MHT, MHTM, MHTML, MSC, MSI, MSP, MST, OCX, OPS, PCD, PIF, PRF, PRG, REG, SCF, SCR, SCT, SHB, SHS, TMP, URL, VB, VBE, VBS, VBX, VSMACROS, VSS, VST, VSW, WS, WSC, WSF, WSH, XSL

Uploading should also be restricted because any user within the company could upload a virus or malware onto a company machine, which can lead to infecting the entire network. This could be malicious by a disgruntled worker or could be done accidently with an infected USB. Either way both downloading and uploading should be restricted to avoid any issues.

**Missing data encryption:**

Encryption is the jumbling of data being sent across networks to help hide them from those who would want to steal it or take advantage of it, and it is unjumbled once it reaches its destination. Encryption is used in almost every type of information sending, whether it be from putting in a password and username or sending a file across to a friend. Almost every company uses encryption now, since it is a sure-fire way to keep information safe.

Although some information being sent may be trivial, a lot of it may be crucial information to some companies or users. If a hacker managed to get unencrypted information, they could gain a username and password to someone’s amazon account, or could find out important company secrets, and they could do many things with the information they gain.

Some hackers may a job out of selling the information they gain. *“the hacker will package up personal information like names, addresses, phone numbers, and email addresses and sell them, typically in bulk. These are more valuable the more recent they are.”* (Editor, 2017) Which can earn them a lot of money, depending on the information they gained.

If they found information that would gain them access into a network or user’s account, they could buy items in their name, edit information, blackmail, modify the network, which could be devastating.

Therefore, every company encrypts their data, and almost all ways of sending information will come prebuilt with encryption, since it is that important, and you may be hard pressed to find any type of information being sent across the internet without encryption.

# References

Cimpanu, C. (2017, Febuary 24th). *Removing User Admin Rights Mitigates 94% of All Critical Microsoft Vulnerabilities*. Retrieved from BleepingComputer: https://www.bleepingcomputer.com/news/microsoft/removing-user-admin-rights-mitigates-94-percent-of-all-critical-microsoft-vulnerabilities/

Editor, T. (2017, May 18th). *Once Stolen, What Do Hackers Do With Your Data?* Retrieved from Secplicity: https://www.secplicity.org/2017/05/18/stolen-hackers-data/

Flores, B. (2019, May 7). *The Dangers of Backdoor Software Vulnerabilities and How to Mitigate Them*. Retrieved from Cyber Defense Magazine: https://www.cyberdefensemagazine.com/the-dangers-of-backdoor-software-vulnerabilities-and-how-to-mitigate-them/

G.J, W. (2006). A Classification of SQL Injection Attacks. *A Classification of SQL Injection Attacks*, 11.

Rouse, M. (2016, September 21st). *What is Buffer Overflow?* Retrieved from TechTarget: https://searchsecurity.techtarget.com/definition/buffer-overflow

Soroush Dalili, D. W. (n.d.). *Unrestricted File Upload*. Retrieved from OWASP.

*What is Social engineering?* (n.d.). Retrieved from Webroot: https://www.webroot.com/au/en/resources/tips-articles/what-is-social-engineering