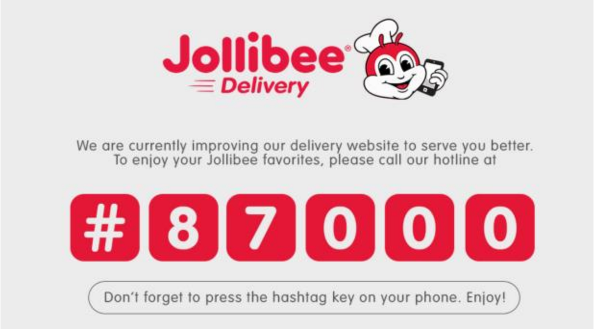
Web Application Security

Introduction

If you frequently order food through the website of 🐝, you're probably disappointed to have seen the picture below when you opened their website to order 🍔🍾🍟.



We are currently improving our delivery website to serve you better. To enjoy your Jollibee favorites, please call our hotline at

#87000

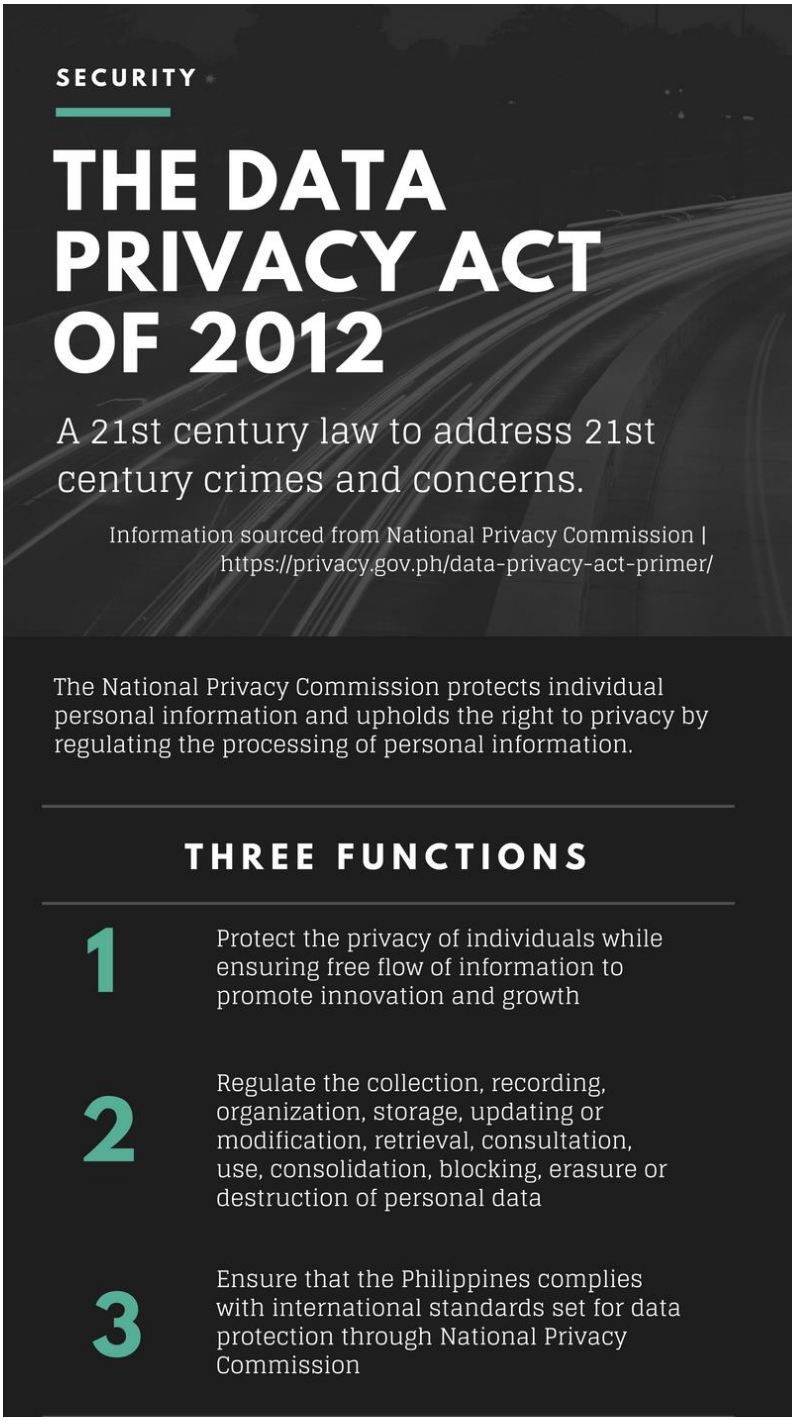
Don't forget to press the hashtag key on your phone. Enjoy!

This is due to the order of the National Privacy Commission to Jollibee to suspend its delivery website due to its vulnerabilities. The vulnerability issues were caused by not-updated database protection software, and unencrypted information, such as personal customer information (ABS-CBN News, 2018).

Since the website is vulnerable to various kinds of malicious attack, hackers may directly victimize customers of the Jollibee delivery website. They may look into their personal information and use it as means to conduct other fraudulent attacks. This vulnerability also affects the business owners, since it might leave a negative image for the business. Customers may be led not to patronize it.

Because of the risks posed by an unsecure application or website to both service providers and customers, organizations, such as the General Data Protection Regulation organization of European Union, and government agencies, such as the National Privacy Commission of the Philippines, were formed.

The National Privacy Commission is the country's privacy watchdog; an independent body mandated to administer and implement the Data Privacy Act of 2012, and to monitor and ensure compliance of the country with international standards set for data protection. (NPC)



SECURITY

THE DATA PRIVACY ACT OF 2012

A 21st century law to address 21st century crimes and concerns.

Information sourced from National Privacy Commission | https://privacy.gov.ph/data-privacy-act-primer/

The National Privacy Commission protects individual personal information and upholds the right to privacy by regulating the processing of personal information.

THREE FUNCTIONS

1 Protect the privacy of individuals while ensuring free flow of information to promote innovation and growth

2 Regulate the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of personal data

3 Ensure that the Philippines complies with international standards set for data protection through National Privacy Commission

The Data Privacy Act was enforced in order to ensure the presence of security in web applications.

Web Application Security (WAS)

WAS involves the protection of web applications on the world wide web, particularly its codes which may contain vulnerabilities or risks that can be exploited for malicious purposes. Considering how almost all online services require the use of web applications, this can greatly affect the applications' functionalities and the people using them.

In relation to web application security, the Open Web Application Security publishes their top 10 list of Application Security Risks. Their most recent list is the Application Security Risk for 2017.

Top 10

1. Injection
2. **Broken Authentication**
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. **Cross-Site Scripting**
8. Insecure Deserialization
9. **Using Components with Known Vulnerabilities**
10. **Insufficient Logging & Monitoring**

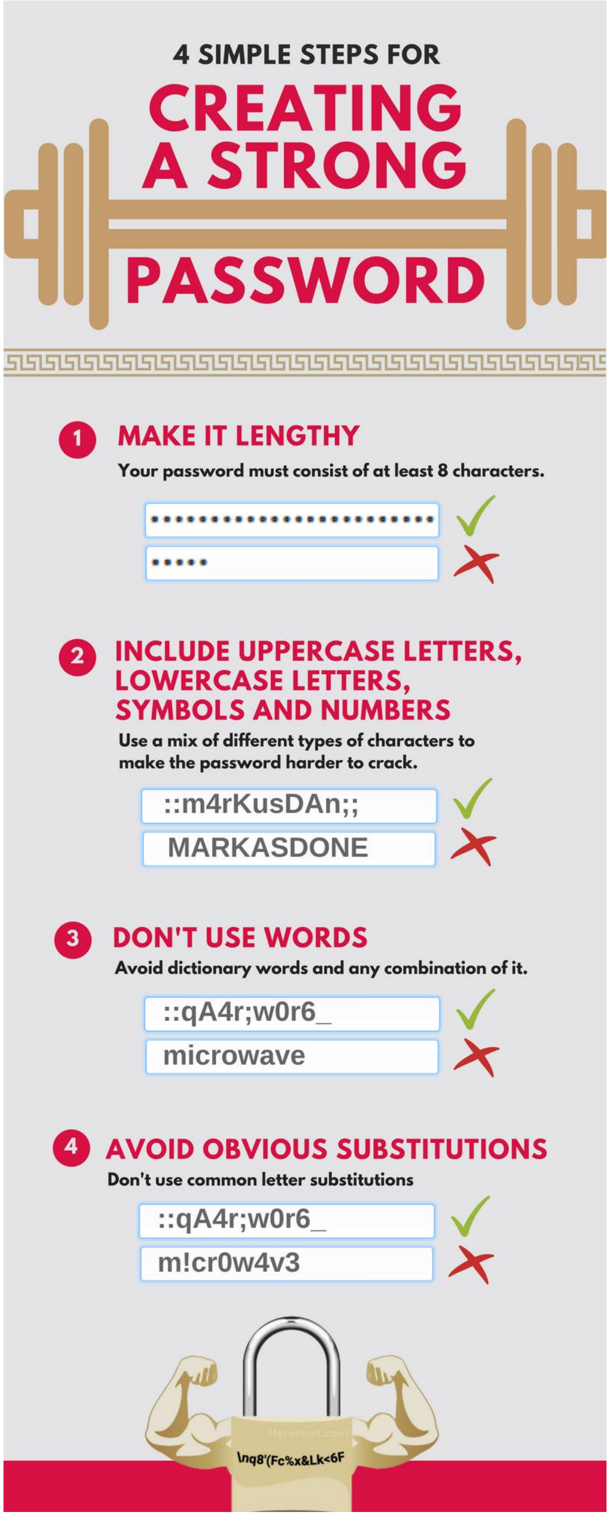
NOTE: For this lesson, we will be focusing on 4 vulnerabilities. Come back next week to learn about the remaining vulnerabilities
☺️

Broken Authentication

Broken authentication is a security risk that occurs when a hacker makes use of valid combinations of compromised account credentials, and try those combinations to enter a login page or any page that requires authentication, posing as an authentic user. Broken authentication is the result of poor authentication implementations. For example, session IDs are explicitly embedded in URLs, and unencrypted user data are transmitted to servers. Functions such as the *Reset or Forgot Password* are mostly exploited in this vulnerability, and are used by the attacker in order to retrieve the details of an account.

Mitigations

PREVENT BROKEN AUTHENTICATION
1.
\nq8'(Fc%x&Lk<6F
USE STRONG PASSWORDS
2.
DON'T REUSE YOUR PASSWORD
3.
Logout
ALWAYS LOGOUT YOUR ACCOUNT


4 SIMPLE STEPS FOR
CREATING A STRONG PASSWORD
1 MAKE IT LENGTHY
Your password must consist of at least 8 characters.
2 INCLUDE UPPERCASE LETTERS, LOWERCASE LETTERS, SYMBOLS AND NUMBERS
Use a mix of different types of characters to make the password harder to crack.
::m4rKusDAn;;
MARKASDONE
3 DON'T USE WORDS
Avoid dictionary words and any combination of it.
::qA4r;w0r6_
microwave
4 AVOID OBVIOUS SUBSTITUTIONS
Don't use common letter substitutions
::qA4r;w0r6_
m!cr0w4v3
\nq8'(Fc%x&Lk<6F

Sample Case

A case of broken authentication occurred between October and December 2015, where nearly 9,000 user accounts of an online tax preparation service company were compromised. The attack is a credential-stuffing attack where hackers obtained a multitude of username and password credentials, and used them to enter the accounts of TaxSlayer customers.

TaxSlayer LLS only noticed the attack in January 2016, when a customer of complained that hackers used their information to obtain tax refunds by filing fake tax returns with altered bank routing numbers directed to the hackers (Feigelson, J., & Bucher, W.).

In order to end the attack, the TaxSlayer imposed multi-factor authentication requirements. The Federal Trade Commission, who is working on this issue, filed their final approval of settlement with TaxSlayer LLC on November 8, 2017, containing the rules TaxSlayer must follow to continue its services (FTC, 2018).

Using Components with Known Vulnerabilities

Codes nowadays tend to link to open-source external components such as modules, libraries, and frameworks. Most of the time, no standards or requisites are given which means that anyone can create, use, or edit the components as they wish. This poses a security risk, especially for companies or developers that use these components.

Not every component can affect different applications in the same way. This solely depends on how deeply embedded these components are inside the software and programs that use them. As these components run on the same access level as the application that uses them, attackers can exploit vulnerable components to access sensitive information and perform tasks that can compromise the companies that use these components.

Mitigations

1. Proper management of all dependencies and libraries are required
2. Components should be analyzed for insecure codes (such as codes unintentionally allowing users to access private files or even sensitive computer processes)
3. Remove or update old library components that may potentially be vulnerable
4. All components and/or sources should be checked for approved licenses (that indicate that they have already been reviewed for security)
5. Unapproved libraries should be removed; otherwise, if the companies will decide to take the risk of using them, then there should be restricted use.

Sample Case

One particular case involving this security risk involves a hacking incident that happened on a blogging website used by Thomson Reuters. Damages to the blog site includes false posts, which includes a false interview with a Syrian rebel army leader. Following the attack was a security breach on his twitter account, which the hackers have taken control of. The website was taken back after some time.

According to the security team of WordPress, the hacking happened because Reuters was using an outdated version of Wordpress, which is publicly known for having a lot of security issues. The reason why websites, like the blogging website being used by Reuters, are prone to attacks could be because customers assume that vendors have already taken care of the security issues, and they find no need for updates.

Insufficient Logging & Monitoring

Insufficient logging and monitoring is a situation where some user activities within the website are not recorded. It is also the case when all user activities are logged but important details such as activity, time in, time out, or even frequency of visits are not recorded.

Not being able to track any suspicious activities or sensitive actions happening within an application or a system, such as change of passwords, financial transactions, or not being able to store logs, properly give way for attackers to prevent or damage security controls.

The lack of logs causes security breaches to remain undetected, which allows attackers to have more time to escalate further into the application or the system, and to further exploit stolen data. The said attacks will, in turn, result in a more difficult and longer process of repairing any damage done and/or recovering any data loss.

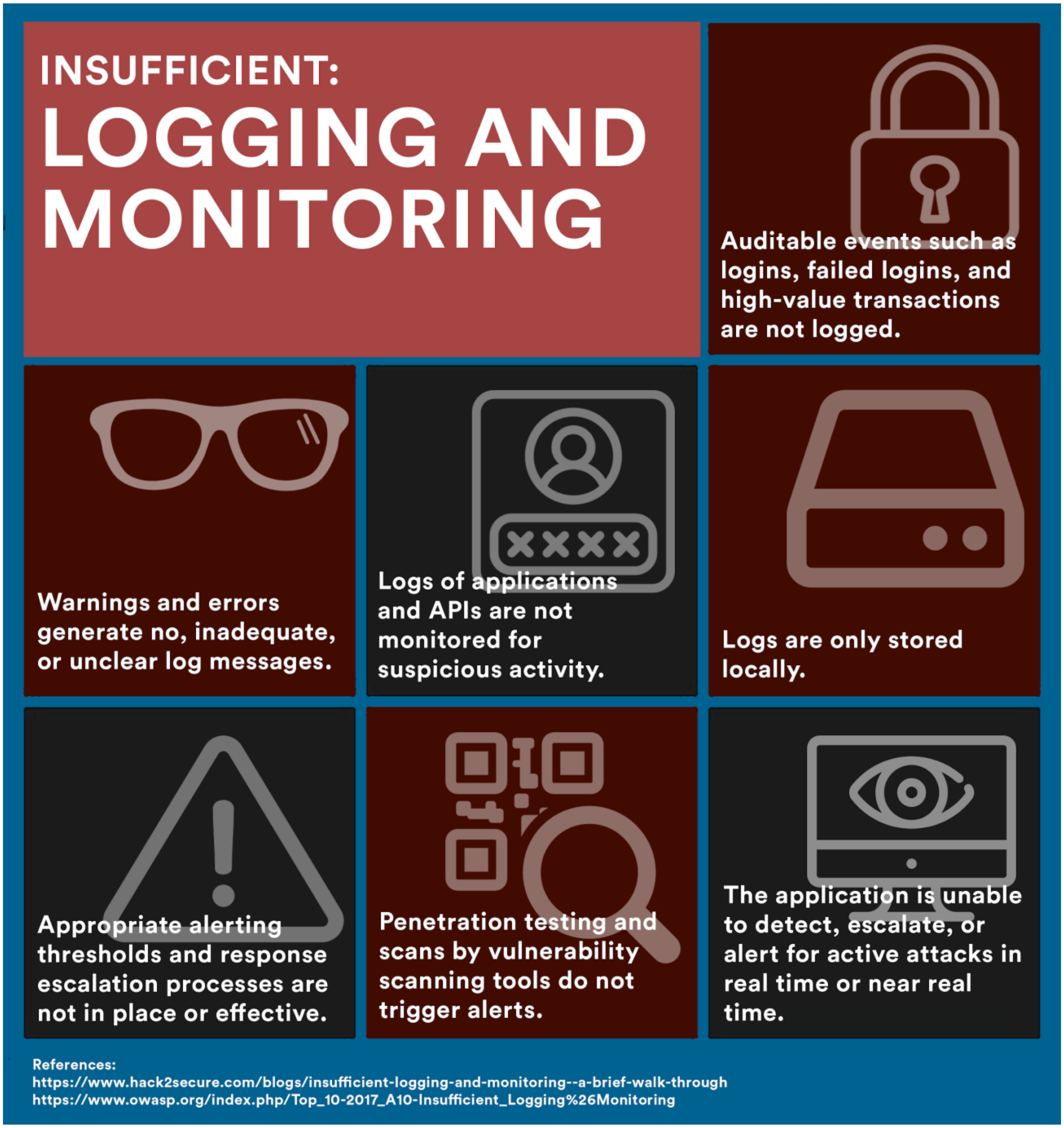
Mitigations

1. A proper logging and monitoring system must be planned and developed to track all activity within the application, suspicious or not.
2. Generated logs should be easily understood and provide sufficient information about any activity within the application.
3. Alerts concerning suspicious activities must be ensured that they are effective enough and that an incident response and recovery plan is well established
4. A penetration test must also be conducted wherein the system will be tested if it successfully logs and monitors any activity within the application properly, including any suspicious activities. This is to test the sufficiency of the logs being generated by the logging and monitoring system (Hack2Secure, 2018).

Sample Case

An example case where the vulnerability of insufficient logging and monitoring was exploited, happened in 2013 where the German branch of Vodafone was hacked. A third-party subcontractor was reported to steal the names, addresses, bank account numbers, birthdates, and possibly phone credit card details and passwords of over 2 million customers.

Though unclear of when the breach took place, it appeared that the hackers were able so successfully compromise an internal server on their network. A software which could have alerted the company of the attack as soon as the breach happened and in turn would have mitigated the breach was believed to be absent.



INSUFFICIENT: LOGGING AND MONITORING

Auditable events such as logins, failed logins, and high-value transactions are not logged.

Warnings and errors generate no, inadequate, or unclear log messages.

Logs of applications and APIs are not monitored for suspicious activity.

Logs are only stored locally.

Appropriate alerting thresholds and response escalation processes are not in place or effective.

Penetration testing and scans by vulnerability scanning tools do not trigger alerts.

The application is unable to detect, escalate, or alert for active attacks in real time or near real time.

References:
https://www.hack2secure.com/blogs/insufficient-logging-and-monitoring--a-brief-walk-through
https://www.owasp.org/index.php/Top_10-2017_A10-Insufficient_Logging%26Monitoring

Cross-Site Scripting (XSS)

It is a kind of vulnerability in websites or web applications wherein a hacker does an injection attack that exploits the vulnerability of the site to attack any visitors of the site. This happens when the attacker injects malicious scripts into a website without the awareness of the user. These scripts can alter the website in such a way that it changes the links within it to lead to a separate page that installs malware into the user's device, or copies a user's session to steal any information they can from that user.

Mitigations

1. Escaping data is a means of preventing vulnerabilities by which data received by an application is taken to ensure its security before sending it to an end user. This will prevent any interruption in sending payloads to end users.
2. Validation is the process ensuring the correctness of data within the application, thus preventing any malicious data from harming the site, its database, and its users by giving restrictions to user inputs.
3. Sanitization is the process by which user input is modified to ensure its validation. This is normally used in conjunction with validation as a form of double checking the data received such that they would not harm users and the database.

Sample Case

One of the most famous cases of XSS is the Samy Worm created by Samy Kamkar for MySpace. Samy created a script that would force users who visited his profile to add him as a friend, and add "*but most of all, Samy is my hero*" under the "*my heroes"* category. He programmed the script such that it would copy itself to the visitors' profile as well.

References

Hack2Secure. (2018, January 27). Insufficient Logging And Monitoring A Brief Walk Through. Retrieved May 10, 2018, from https://www.hack2secure.com/blogs/insufficient-logging-and-monitoring--a-brief-walk-through

ABS-CBN News. (2018, May 8). Jollibee delivery website suspended due to 'vulnerabilities'. Retrieved May 10, 2018, from http://news.abs-cbn.com/business/05/08/18/jollibee-delivery-website-suspended-due-to-vulnerabilities

NPC. About Us. Retrieved May 10, 2018, from https://privacy.gov.ph/about-us/#visionmission

Dabirsiaghi, A. & Williams, J. (n.d.). The Unfortunate Reality of Insecure Libraries. Retrieved from
Contrast Security: https://cdn2.hubspot.net/hub/203759/file-1100864196-pdf/docs/Contrast_-_Insecure_Libraries_2014.pdf?t=1501279222788

Feigelson, J., & Bucher, W. (n.d.). Cybersecurity Enforcers Wake Up to Unauthorized Computer Access Via Credential Stuffing. Retrieved from https://biglawbusiness.com/cybersecurity-enforcers-wake-up-to-unauthorized-computer-access-via-credential-stuffing/

FTC Gives Final Approval to Settlement with Online Tax Preparation Service. (2017, November 08). Retrieved from https://www.ftc.gov/news-events/press-releases/2017/11/ftc-gives-final-approval-settlement-online-tax-preparation

Hack2Secure. (2018, January 27). Insufficient Logging And Monitoring A Brief Walk Through. Retrieved May 10, 2018, from https://www.hack2secure.com/blogs/insufficient-logging-and-monitoring--a-brief-walk-through

Infosec Institute. (2018, April 10). 2017 OWASP A10 Update: Insufficient Logging & Monitoring. Retrieved May 10, 2018, from http://resources.infosecinstitute.com/2017-owasp-a10-update-insufficient-logging-monitoring/#gref

Labs,F. (2017). New and Old Techniques in the Fight Against Credential Stuffing. [online] https://forkbomb.us/assets/posts/fighting-credential-stuffing/document/New%20and%20Old%20Techniques%20in%20the%20Fight%20Against%20Credential%20Stuffing.pdf

Lamb, C., Piepgrass, S. C., & Butler, T. (2018, January 09). Tax Preparation Firm Settles FTC Claims
Flowing from Data Breach. Retrieved from https://www.consumerfinancialserviceslawmonitor.com/2017/11/tax-preparation-firm-settles-ftc-claims-flowing-from-data-breach/

Leyden, J. (2013, September 12). Hacker cracks Vodafone Germany, steals data of 2 million customers. Retrieved May 10, 2018, from https://www.theregister.co.uk/2013/09/12/vodafone_germany_breach/

Protalinski, E. (2018). *Reuters was using old WordPress version when it was hacked | ZDNet*. [online] ZDNet. Available at: https://www.zdnet.com/article/reuters-was-using-old-wordpress-version-when-it-was-hacked/ [Accessed 11 May 2018].