Collaborative discussion 1

Choose an open-source UML tool. Select one of the coding weaknesses which have been identified by OWASP and create a flowchart of the steps which may have led to the weakness occurring. Which UML models might you use to present the design of your proposed software, and why are they the most appropriate choice(s)?

Initial Post

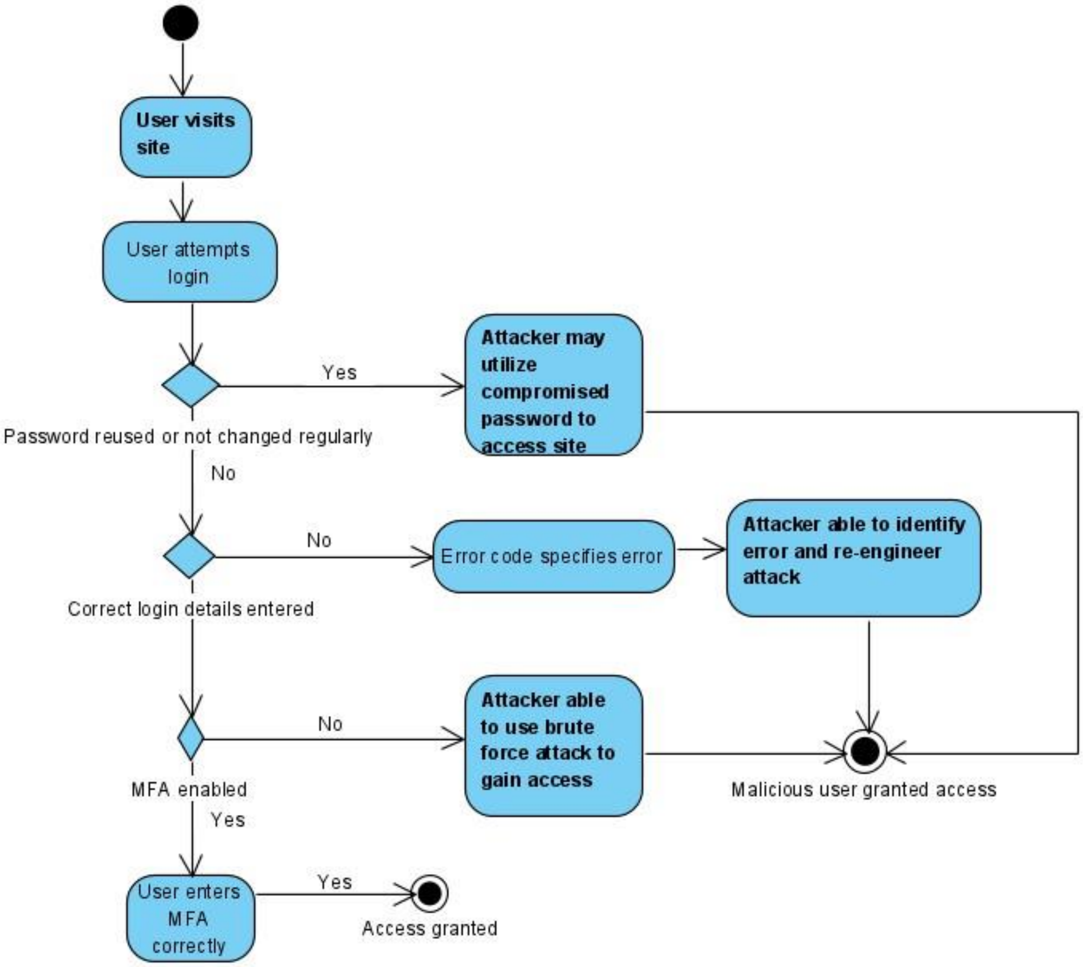
OWASP, the open web application security project is an open source nonprofit foundation to identify and help prevent the most prevalent security risks in todays ever changing information based world.

I have chosen to focus on the second most important risk- broken authentication. This method of attack includes but is not limited to compromised passwords, sessions and keys to compromise the system. Many applications use specific error messages when incorrect credentials are entered, thus providing the attacker with information as to how to access the system(“A2:2017-Broken Authentication | OWASP,” n.d.).

Another such exploit is a brute force attack, which uses computing power to try infinite combinations of username and password to gain access to the system. A useful mitigation against this type of attack is the advent of Multi factor authentication, which requires a secondary time sensitive input in order to access the system. Microsoft estimates that 99.9% of brute force attacks would be thwarted by utilization of MFA (“Microsoft: 99.9% of compromised accounts did not use multi-factor authentication | ZDNet,” n.d.). Simple measures such as regularly changing passwords, implementing MFA and returning generic error codes may prevent against most broken authentication attacks.

A2:2017-Broken Authentication | OWASP. (n.d.). Retrieved June 7, 2021, from https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication

Microsoft: 99.9% of compromised accounts did not use multi-factor authentication | ZDNet. (n.d.). Retrieved June 9, 2021, from https://www.zdnet.com/article/microsoft-99-9-of-compromised-accounts-did-not-use-multi-factor-authentication/


User visits site
User attempts login
Password reused or not changed regularly
Yes
Attacker may utilize compromised password to access site
No
Correct login details entered
No
Error code specifies error
Attacker able to identify error and re-engineer attack
MFA enabled
No
Attacker able to use brute force attack to gain access
Malicious user granted access
Yes
User enters MFA correctly
Yes
Access granted

Summary Post

Over the course of the module, I have delved into research regarding the OWASP top 10, alongside my colleagues. We all have reached similar conclusions as to the risks these vulnerabilities present, as well as ways to mitigate these risks.

With regards to Yohay's post on insufficient logging and monitoring, this is an area that has had a real world impact, such as the Ukrainian power plant intrusion in 2015 (Whitehead *et al.*, 2017). Logging of previous intrusions and subsequent analysis may have assisted engineers in providing updates to patch these vulnerabilities to prevent future breaches. Monitoring systems need to be put in place with regular analytics to detect and fix vulnerabilities.

Alexander's post on sensitive data exposure, allowed me to understand the importance of HTTPS versus standard HTTP. It is also interesting to note that the HTTPS certificate may be obtained for free, thus concluding that all websites containing sensitive data should not have a reason not to use HTTPS (Basques, 2019). It is also advisable not to use public access networks when performing sensitive data operations, as this data may be intercepted, especially when HTTPS is not used. Mitigation techniques include using a VPN and ensuring the site uses SSL encryption (Kaspersky, 2020).

David's post on broken authentication is crucial especially in todays ever changing information based online world. Generic and reused passwords should never be used, as if one site is compromised, all accounts with the same password may be vulnerable. It is also critical to use MFA, as this provides an extra layer of security against such attacks. I have found that google authenticator is very useful in this regard and have applied it to many of my personal applications. A password manager, such as last pass, enables secure storage of difficult to remember passwords. Biometric authentication such as fingerprint or retinal access is perhaps the safest method of access control today, and should be used whenever possible, and always in conjunction with other layers of security (Khan *et al.*, 2015).

IOT advancements mean that a computer chip can be placed in almost anything, and allows for network control, data analysis and overall innovation. This may come at the cost of data security as a tradeoff for expediency. Start up and legacy companies should be aware of this and provide all possible measures to ensure data security (Sohoel, Jaatun and Boyd, 2018).

In conclusion, security needs to have a dual approach from the side of the developers as well as the consumers. Developers need to ensure that their code is robust and constantly updated to prevent attacks, while consumers need to be proactive in their security approach, with regards to passwords, MFA and always employing safe browsing techniques.

Basques, K. (2019) *Why HTTPS Matters*, *Google Developers*. Available at: https://web.dev/why-https-matters/ (Accessed: 4 July 2021).

Kaspersky (2020) *Public Wi-Fi Risks and Why You Don't Have to Fear Them | Internet Safety | Kaspersky*. Available at: https://www.kaspersky.co.za/resource-center/preemptive-safety/public-wifi-risks (Accessed: 11 July 2021).

Khan, S. H. *et al.* (2015) 'Secure biometric template generation for multi-factor authentication', *Pattern Recognition*. Elsevier, 48(2), pp. 458–472. doi: 10.1016/j.patcog.2014.08.024.

Sohoel, H., Jaatun, M. G. and Boyd, C. (2018) 'OWASP Top 10 - Do Startups Care?', *2018 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2018*, (0102). doi: 10.1109/CyberSecPODS.2018.8560666.

Whitehead, D. E. *et al.* (2017) 'Ukraine cyber-induced power outage: Analysis and practical mitigation strategies', *70th Annual Conference for Protective Relay Engineers, CPRE 2017*. doi: 10.1109/CPRE.2017.8090056.