Initial Post

J Irvine

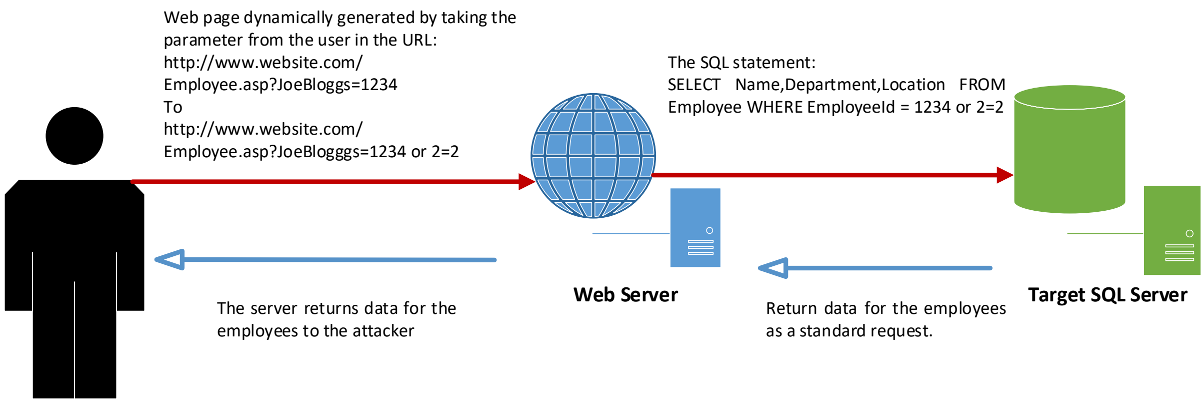
A06:2021-Vulnerable and Outdated Components

Vulnerable and Outdated Components has moved up from ninth to sixth in the OWASP Top 10 Web Application Security Risks. Having worked for many years in education and now in a Government Department I have witnessed these organisations sweating out the use of hardware and software in order to keep costs down. This can lead to components becoming vulnerable to attacks or being out of date.

Java-script libraries are used by web developers in order to make sites more functional, however this can be open to attacks if not kept up-to-date and result in the site being potentially exposed **(**Lauinger et al, 2018). According to Tang et al (2015), you are able to predict these vulnerabilities through text mining or software metrics, with software metrics seen as the most cost-effective.

Another area where this is an issues is through SQL injection attacks, this can allow sensitive data to be updated or read as well as running commands and accessing files from the servers (Guimarães, 2009). An example of this can be seen in Figure 1.

Figure 1
SQL Injection Attack



Web page dynamically generated by taking the parameter from the user in the URL:
http://www.website.com/Employee.asp?JoeBloggs=1234
To
http://www.website.com/Employee.asp?JoeBlogggs=1234 or 2=2

The SQL statement:
SELECT Name,Department,Location FROM Employee WHERE EmployeeId = 1234 or 2=2

The server returns data for the employees to the attacker

Return data for the employees as a standard request.

The Internet of Things (IoT) is seen as a revolution, however this can be susceptible to attacks due to insecure software configuration (Jiang, Lora, and Chattopadhyay, 2020). Old/unpatched dependencies in the dependency chain of the components being used. There is also an issue with IOT that older dependencies or those that are unpatched can be exploited by cybercriminals. This is particularly an issue when industries use this technology to gain efficiencies, for instance the Amazon Ring was subject to an attack, whereby the hackers could get live streams from the systems through weak, recycled and default identifications (Smith, 2020).

B. D. A. Guimarães, Advanced SQL injection to operating system full control, Black Hat Europe, white paper, 2009.

Initial Post

Jiang, X., Lora, M. and Chattopadhyay, S., 2020. An experimental analysis of security vulnerabilities in industrial IoT devices. ACM Transactions on Internet Technology (TOIT), 20(2), pp.1-24.

Lauinger, T., Chaabane, A., Arshad, S., Robertson, W., Wilson, C. and Kirda, E., 2018. Thou shalt not depend on me: Analysing the use of outdated javascript libraries on the web. arXiv preprint arXiv:1811.00918.

Omolara, A.E., Alabdulatif, A., Abiodun, O.I., Alawida, M., Alabdulatif, A. and Arshad, H., 2022. The internet of things security: A survey encompassing unexplored areas and new insights. Computers & Security, 112, p.102494.

Sengupta, J., Ruj, S. and Bit, S.D., 2020. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. Journal of Network and Computer Applications, 149, p.102481.

Smith, S.W., 2020. Securing the Internet of Things: An Ongoing Challenge. Computer, 53(6), pp.62-66.

Tang, Y., Zhao, F., Yang, Y., Lu, H., Zhou, Y. and Xu, B., 2015, August. Predicting vulnerable components via text mining or software metrics? An effort-aware perspective. In 2015 IEEE International Conference on Software Quality, Reliability and Security (pp. 27-36). IEEE.

https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/