Collaborative Discussion 1

Initial Post

A system with a logical gap or a business flaw without disciplining could introduce security flaws that damage the whole software. These flaws usually could not be fixed by good coding, using a more restricted encrypting method, or applying good practices on authentication and authorization. You can imagine when constructors follow a lower-quality blueprint to build a house, it doesn't matter how good the material is, and people still can't make a solid and high-quality building.

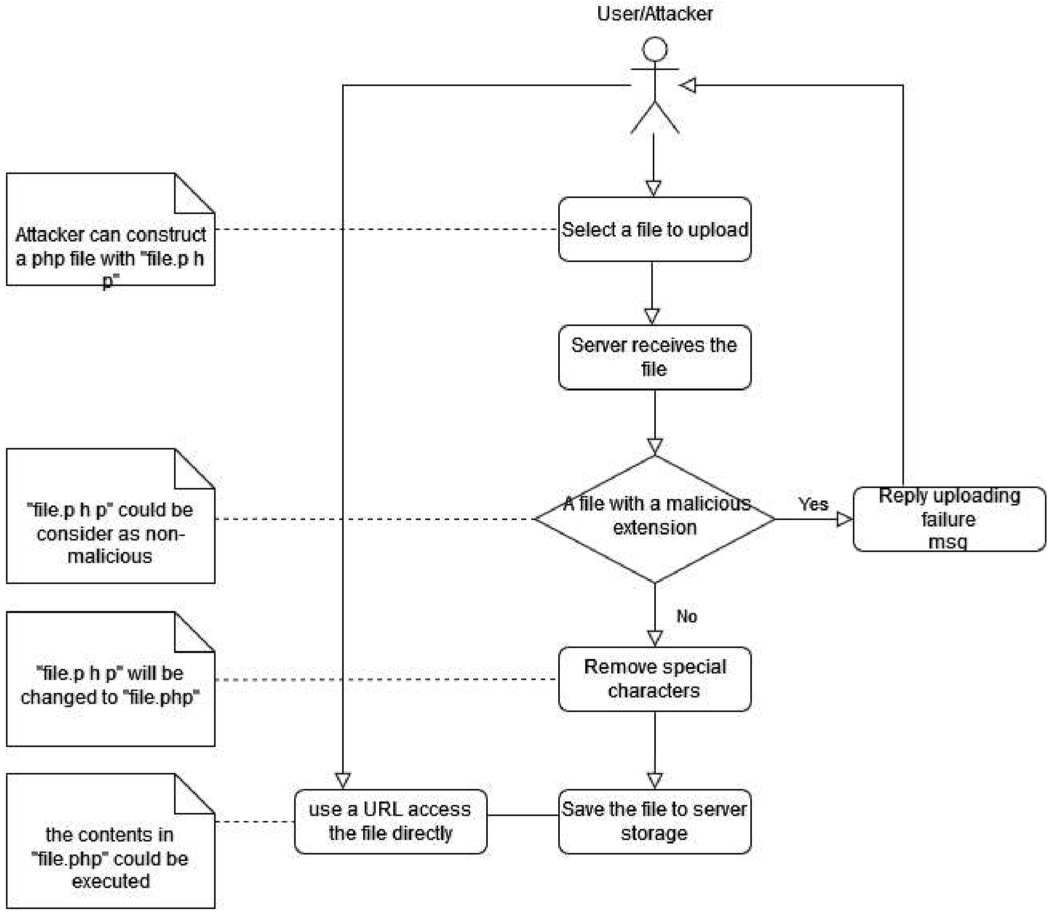
The OWASP 2021 TOP 10 introuduces a new category - insecure design, described as the security reason caused by "missing or ineffective control design." (OWASP, 2021).

CVE-2021-24370 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24370) is a typical security issue that can fall into an insecure design one (). The WordPress plugin code can let users upload an attribute file to the remote server, and later people can access it with a URL. The software author had applied one step to check whether the file is malicious or not based on the file extension name. In the happy flow, if people upload an image or PDF, a user can access the file with "https://..../.../file.png". However, you can look at the flowchart below to find out that it had a flaw with workflow.

To mitigate security issues caused by insecure design, OWASP 2021 TOP Ten offers many good suggestions (OWASP, 2021). This specific issue could tell us that people should put security principles across the whole system, not just a few places.

Reference:
owasp.org. (2021). A04 Insecure Design - OWASP Top 10:2021. [online] Available at: https://owasp.org/Top10/A04_2021-Insecure_Design/.

cve.mitre.org. (n.d.). CVE - CVE-2021-24370. [online] Available at: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24370 [Accessed 25 Jun. 2022].


User/Attacker
Attacker can construct a php file with "file.p h p"
Select a file to upload
Server receives the file
"file.p h p" could be consider as non-malicious
A file with a malicious extension
Yes
Reply uploading failure msg
No
"file.p h p" will be changed to "file.php"
Remove special characters
the contents in "file.php" could be executed
use a URL access the file directly
Save the file to server storage

Peer Review to Richard Allen

Hi Richard, thanks for your excellent presentation to show the JSON injection attack case.

Because of the importance of data for an enterprise, we could consider the database aspect as the most critical role in a modern system. Recently, more and more information systems have applied NoSQL databases as big data is popular, and NoSQL injection has become a spotlight in IT security.

Ron, Shulman-Peleg and Bronshtein offered some suggestions to mitigate NoSQL injection risk, like monitoring and analysing JSON string, more restricted REST API defined, and control access (Ron, A., Shulman-Peleg, A. and Bronshtein, E., 2015). Among these strategies, I feel that the most essential and effective point is data access with the least privilege principle against the rejection attack. The principle has been around a long time, but it is still working no matter the technology used.

Reference:

Ron, A., Shulman-Peleg, A. and Bronshtein, E., 2015. No sql, no injection? examining nosql security. arXiv preprint arXiv:1506.04082.

Peer Review to Maja Tagt

Hi Maja, thanks for sharing an excellent example of access control.

In my view, I think access control is the most vital element of a system's security. From Linux to database, from banking to git, they all need good access control practices themself to support daily activity.

One of the best practices is that access control with at least privilege can gain a system's high security. For example, a file/folder should just be accessed by the owner if there is no explicit requirement to share with other groups or users. In addition, if the file was designed by reading from a specific user/role, then people should remove the write and execute permission of the file to the user/role they will not use.

A root/administrator account opened to access from outside could be considered very dangerous and should be limited access from an unsafety environment (e.g. remote login via the internet).

Also, as Roberto mentioned in his post, checking permission before performing any action is an excellent way to resolve these problems.

Summary Post

Secure Design

OWASP 2021 TOP Ten gets insecure design as a new category and takes it as the primary root cause of security flaws.
If we want to mitigate the security impact caused by insecure design, the best practice is to apply the secure method initially. So what is the secure design？
"...focused on discovering real cybersecurity problems related to insecure use of modern products"(Sharevski, F., Trowbridge, A. and Westbrook, J., 2018). It requires software designers to intend to mitigate security by design and have a clear and specific security goal. Many software developers could agree the design is the most critical factor in the quality of a final product. In addition, a secure design can significantly reduce system maintenance costs (Dougherty, C., Sayre, K., Seacord, R.C., Svoboda, D. and Togashi, K., 2009.).

Rushby suggested that to assure system security, components of a system should be isolated, and each part could have its own security policy/strategy (Rushby, J.M., 1981). Change to other words, a system can have multiple independent levels of security (MILS) property. The classical computer science theory of breaking a big/complex problem into small ones is a good style, and MILS also uses a similar way to handle security challenges (Greve, D., Wilding, M. and Vanfleet, W.M., 2003).

Review the case in my initial post again with the MILS concept. I could say the big problem was that the author had not considered the specific attacking way but blind trust data/info passed by other internal modules. A good design would get multiple dedication components/classes to provide necessary services. For example, there are various classes, one for uploading a file, one for saving, and one for loading. Imagine if the author applied some security flaw in the saving user's file functionality, it could miss determining whether the file was malicious or not. Even if the malicious file bypasses the last part, it could still be detected by the loading module with some security checking; assigning restricted permission could avoid executing the attribute code case in the final stage. When attackers want to break the whole system, they will face many different defending mechanisms, and the system will be more solid because one weakness will not lead to the entire system breaking.

reference

Sharevski, F., Trowbridge, A. and Westbrook, J., 2018, March. Novel approach for cybersecurity workforce development: A course in secure design. In 2018 IEEE integrated STEM education conference (ISEC) (pp. 175-180). IEEE.

Dougherty, C., Sayre, K., Seacord, R.C., Svoboda, D. and Togashi, K., 2009. Secure design patterns. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Rushby, J.M., 1981. Design and verification of secure systems. ACM SIGOPS Operating Systems Review, 15(5), pp.12-21.

Greve, D., Wilding, M. and Vanfleet, W.M., 2003, July. A separation kernel formal security policy. In Proc. Fourth International Workshop on the ACL2 Theorem Prover and Its Applications.