To: William H. Flathead III

From: Matteo Franzil

Subject: Security issues pt. 2: Pathname attacks

Date: October 2, 2021

Note for the instructor: this memo is written so that this breach happened chronologically after the SQLi one, as stated by the exercise page.

At the light of more security issues in our company, I have decided to write this additional memo.

This time, the offending component was found in our memo dissemination system. In the `http://localhost/cgi-bin/memo.cgi` page, attackers are able to basically visit any file present in our system by exploiting a vulnerability known as "path traversal". The problem lies in the fact that the webpage, although providing an apparently innocent dropdown menu, can be hijacked in order to input any path the user desires. This corresponds to visiting the corresponding file on the server. Using Unix pathname shorthands such as "`..`", one could write `/home/megaboz/memo/../../../etc/shadow` and get access to the `/etc/shadow` file.

I managed to promptly fix this by adding input validation and removing SUID-root permissions by avoiding the use of the `memo.cgi` wrapper and calling the Perl script directly. Indeed, all the memos in the root folder are already readable by the world, so there's zero need about giving permissions to scripts that do not need them. In order to be truly sure for the future, we can just make all memo folders readable from the world (and not executable or writable!) and we should be set.

Regarding the input validation, I made sure that the whole path is first resolved and then checked for validity, so that incidents like the aforementioned ones can no longer happen. In short, attackers that try to jump directories will see their requests condensed to the actual, compact pathname, and then rejected because they are not inside the correct memo folders.

I think that this breach was far, far worse than the SQLi one. Attackers have been able to visit basically *any* file in our server, including highly sensitive ones containing credentials! While now illegal accesses has been shut down, we cannot be sure of how much data was filtered out and how it was used. A serious contingency plan is needed, tracking down misuses of credentials and completely changing any sensitive data found in our server.