Databases & Web Services Project 2023 Assignment 7

Peter Baumann, Constructor University

Submission: by team, through git repository

Deadline: 2023-nov-02 23:59

Security I

As discussed in class, email disclaimers are inappropriate for achieving the security goals of secrecy and integrity. Rather, encryption and digital signatures are the right way to do it. This is what you will establish in this task:

- Load a suitable plugin (like enigma) supporting your particular mail program
- Configure it
- Generate a key pair (cf lecture slides)
- Generate your digital signature
- Send your public key to one of the TAs, followed by an encrypted mail with signature to the same (!) TA

The task is successful if the TA can import your key, can decrypt your mail, and can see your signature.

Submission:

- Email to TA

Security II

You web service is quite susceptible to attacks. You may even try it out with your own service or that from another team, but it will not give any points, just to clarify. And you should at most leave an egg (say, an additional tuple in some table) for proving your “presence”, otherwise it won’t give you good karma either.

Now to the real task: protect your service. Basically, you have read code (search pages using SELECT) and write code (maintenance pages using INSERT, UPDATE, and DELETE). Both need to be differentiated for better security. To this end, your maintenance page(s) you should have access control via user/password:

- Create a user management table holding user name and password (don’t worry about Web access for user addition and deletion, just add an admin user through an INSERT statement).
- Extend your maintenance page(s) with two fields for user name and password input; these need to be checked in the server, rejecting any unauthorized activity. Make sure that you provide an

appropriate error message in that case. (Hint: PHP includes can make it easier to keep your set of pages in sync.)

Note that this is just one possible solution, there are several alternatives – all that works is ok.

Submission:

- Website, accessible via Web browser in the project's Web directory
- Repo code (for checking internal logic correctness)