What security considerations should I be aware of when using the student web environment?

By enabling your student web space or by granting the www.swe_web AFS user read or write access to files you control you are exposing these files to:

- In the case of read access, be read by others who may execute CGIs on our system. Any private information stored in those files could be disclosed.
- In the case of write access, be written to by others who may execute CGIs on our system. Files may be modified or destroyed. New files may also be created which could cause your user volume to fill up.

Neither UMBC nor DoIT will take responsibility for the security or integrity of files stored in areas where the www.swe_web AFS user has read or write access. We also ask that any user asking for "input" on web forms that store data in those areas make it clear that any information entered on such forms is stored using an insecure method.

Feedback: Correct or Suggest an Article | Request Help