Reiner Lueth

* Using OWASP-ZAP, I’m sure that I missed a few things, but i did notice that, after I spidered their portal, there were a couple unsecured cookies
  + I believe that they could be used to carry unencrypted information
  + I also believe that they could be used in a session cookie hijacking attack
* Able to access https://my.calstatela.edu as a guest user
  + Didn’t find much of interest here, but thought the guest user was peculiar
* The FAQ’s allow outsiders to see all of their password guidelines, as well as show that they moved from a 3-domain system (PINE, NIS, CSLA) to a single-domain system (AD)
  + Means that all users are AD/(first initial)(last name)
    - All have to be unique user ID’s now
  + https://id.calstatela.edu/idm/user/faq.jsp
* I asked Eric if he had found anything “BIG”, and he said he used Net Craft to get site information, which told us that https://cas1.calstatela.edu is using SSL version 3 protocol, which has a vulnerability (POODLE).
  + This is exploitable because it allows us to set up a man-in-the-middle attack
  + It is used to attack client-server connections
    - It doesn’t seem very easy to do because it requires the attacker to force the user to make a very large number of requests so that it can match the correct byte value.
      * Hard because there is a 1 in 256 chance of matching a single byte somewhere in the entire cipher-blocks.
  + http://toolbar.netcraft.com/site\_report?url=https%3A%2F%2Fcas1.calstatela.edu%2Fcas%2Flogin%3Fservice%3Dhttps%253A%252F%252Fmy.calstatela.edu%252Fpaf%252Fauthorize#last\_reboot
* https://id.calstatela.edu/idm/user/login.jsp could be brute forced or buffer overflowed potentially
  + Username and password fields both have a max length of 128 characters