name=exam, value=CS591F2018quiz2
name=name, value=Alta Graham
name=login, value=agraham
name=1a1, value=Integrity
name=1a2, value=md5
name=1a3, value=php interpreter takes care of the urldecode
name=1a4, value=16
name=1b1, value=Because the second step of the signing process is RSA algorithm use a private key size of 256 bytes as input.
name=1b2, value=32
name=1b3, value=RSA
name=2a, value=Because the gsc directory is owned by apache.
name=2a2, value=http://cs3110.myuccs.net/gsc/sh2b.php?cmd=ls%20-al
name=2a3, value=An python script without input validation can be easily hacked than a php script with input validation.
name=3a, value=Yes
name=3b1, value=Yes
name=3b2, value=No
name=3b3, value=No
name=3b4, value=No
name=3c1, value=Yes
name=3c2, value=No
name=3c3, value=No
name=3d1, value=No
name=3d2, value=Yes
name=3d3, value=No
name=3d4, value=Yes
name=3e1, value=Yes
name=3e3a, value=No
name=3e3b, value=Yes
name=3e3c, value=No
name=assumptions, value=In 1.b I assumed the use of RSA as in our examples and homework. In 1.b.1, because it is only talking about a single call, I was not sure what was meant by "first step," but SHA256 generates a 32 byte hash. In 3.b.3, I assumed that "ping" did NOT refer to the network scanning tool fping, and that ping as a system command was too general to considered a "tool." In 3.c.2, I assumed "system code" referred to system()? I put "No" because other general OS like exec() also potential command injection vulnerability. In 3.d.3: the 6 indicates hashing with SHA-512 - I assumed "password generation" did not mean hashing. In 3.e.1, I assumed that hidden meant less likely to be noticed (dot file name hidden folder), not completely invisible in all circumstances, and thus chose "Yes" In 3.e.2, choosing an answer wiped my answer to 3.e.1. Yes for both.
class=CS591, year=2018, semester=F term=quiz2

CS591F2018quiz2 submitted by Alta Graham

open filename=CS591F2018Grade.txt
userlogin=agraham
login correct!

Alta, Confirmed email sent to cchow@uccs.edu and agraham@uccs.edu