CS458 A2
Brendan Song
b7song
20466121

Written Questions

1.

a.

i. only read
ii. neither read nor write
iii. neither read nor write
iv. both read and write
v. only write

b.

i. File A now has integrity: (TA, {assignments})
ii. Carol now has integrity: (Student, {assignments, marks})
iii. File C now has integrity: (Professor, {assignments, marks})
iv. File D now has integrity: (TA, {assignments}), Bob now has integrity: (TA, {assignments}), File E now has integrity: (TA, {assignments})
v. File F now has integrity: (Student, {marks}), Alice now has integrity: (TA, {assignments})

2.

a.

i. "kittens" is likely to be used by other users so even if the passwords are hashed, Alice can be compromised if CoolSite does not use salt and other users provide easy-to-guess hints (basically what happened with Adobe).

ii. Since the password is only 7 characters longs and a dictionary word, it can be brute-forced quite easily.

b. Assuming Eve knows that Alice is going to capitalize the first letter and the random digit is appended to the end: 10 possibilities. This is reached by simply trying all possibilities from "Kittens0" to "Kittens9"

c. "Kittens1!123"

d. Assuming Alice extends the password with symbol-digit-digit-digit ordering and Eve knows the password after ii: 6 * 10 * 10 * 10 = 6 000 possibilities. This is reached since there are 6 possible symbols, 10 possible digits, and Eve knows Alice is going to append with the symbol before the digits. Assuming Alice extends the password with symbol-digit-digit-digit ordering and Eve does not know the password after ii: 10 * 6 * 10 * 10 * 10 = 60 000 possibilities. This is reached since there is an additional unknown digit Alice used to initially extend the password.

3.

i. SHA-1 has already been broken since a collision-inducing algorithm was found in February 2017. This means there can be multiple plaintext that can be hashed to achieve the same output hash, resulting in accepted passwords that should be rejected.

ii. Since the salt is user-specific it has to be stored somewhere, meaning the attacker can probably get the file containing all user accounts and salts if they can get the file with the passwords. An alternative would be to use a global salt that is generated and stored in memory, making it less prone to being leaked.

iii. 18 bits can be easily brute forced so it serves as an inconvenience to the attacker but will not prevent accounts from being compromised. The attacker can try all possible salts until the output hashes match so they gain access to the database. An alternative is to use a longer salt that is 128 or 256 bits to make brute-forcing not viable.

Programming Questions

1.

b. To prevent SQL injection, prepared statements and parameterized queries are able to separate query data from the syntax. It forces the SQL code to be pre-defined then passes in form data that cannot be interpreted as SQL code. This separates the code from form data so users cannot inject SQL code using forms.

2.

b. No, the same-origin policy does not prevent a XSS attack since it only prevents requests across domains. XSS exploits form fields that are not sanitized and it is all contained in the same domain, meaning it is not affected by the same-origin policy.

c. To mitigate this XSS attack, escape quotes should be used and an auto-escaping template would help prevent against the injection of javascript by converting potentially harmful HTML characters to less harmful ones. Certain words could also be blacklisted like 'javascript' or '<script>'. This would make it less straight-forward to simply inject scripts into form fields.

3.

c.

i. Simply check the HTTP header and verify the source and target origins. Compare the two and ensure they match, otherwise the request is cross-origin.

ii. Issue tokens that store state and verify incoming requests, rejecting them if the tokens do not match.

d. No, HTTPS does nothing against CSRF attacks since the attack occurs through cookies and HTTPS does nothing different with them.

e. No, the server will not accept it since the source origin will be from dancingpigs.com while the target origin would likely be the server which is different.