Testing for authentication

indenty.

authentication is the process of attempting to verify the digital

vulnerabilities :

1. testing for credentials transported over an encrypted channel.
2. testing for default credentials
3. testing for weak bck out mechanism.
4. testing for bypassing authentication schema
5. test remember password functionality.
6. testing for browser cache weakness.
7. testing for weak password policy.
8. testing for weak password change or reset functionalities.
9. testing for weaker authentication in alternative channel.
10. testing for weak security question/answer.

* Test for weak or enforced username policy.

* Vulnerable remember me.

Steps: ① check any application have remember me.

② if they are storing token in plaintext or maybe weak encoding. then there is a vulnerability.

login → intercept request → see cookie (is there your user/password) if yes, it is vulnerability → copy cookie → logout → login → intercept request → change cookie → forward → if loged in it is vulnerability.

what to look in cookie?

① is password stored

② credentials are stored in clear text.

③ verifying the credentials are only sent during login, if not it is vulnerable.

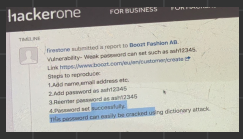
* Weak Password Policy

① What character are permitted and forbidden for use within a password

② How often can a user change their password.

③ How often user can reuse their passwords

(At least, 10 char, 1 capital, 1 small, 1 special.)



* weak password change or reset functionality.

1. Determine the resistance of the application to subversion of the account change process allowing someone to change the password of account.
2. password reset functionality against guessing or bypassing.

Steps: ① reset a password on any application
⑤ intercept request
⑬ Send to repeater.
⑭ change credentials and see results.