Project 1 Questions

CSEC 380 Team 4

11/24/19

Activity 3-7 Questions

CSEC 380 Team 4: Jacob Ruud, Jack McKenna, Daniel Monteagudo, Dylan Rabasca

# Activity 3: Authentication Questions

1. Provide a link to the test cases you generated for this activity.
2. How do you ensure that users that navigate to the protected pages cannot bypass authentication requirements?
3. How do you protect against session fixation?
4. How do you ensure that if your database gets stolen passwords aren’t exposed?
5. How do you prevent password brute force?
6. How do you prevent username enumeration?
7. What happens if your sessionID is predictable, how do you prevent that?

# Activity 4: The Content Questions

1. How do you prevent XSS is this step when displaying the username of the user who uploaded the video?
2. How do you ensure that users can’t delete videos that aren’t their own?

# Activity 5: SQL Injection (Classic/Blind) Questions

1. How would you fix your code so that these issues were no longer present?
2. What are the limitations, if any that, of the SQL Injection issues you’ve included?

# Activity 6: SSRF Questions

1. How would you fix your code so that this issue is no longer present?
2. How does your test demonstrate SSRF as opposed to just accessing any old endpoint?

# Activity 7: Command Injection Questions

1. How would you fix your code so that this issue is no longer present?
   1. To fix command injection, all we would have to do is specify the file type that can be uploaded to the server, then users would be unable to upload shell scripts instead of videos on the upload page