Learn About Application Security Fundamentals and Put it to Use on Your Own Website

Gain awareness of what needs to be secured

Q 1/11: A curious user, with username `curious`, notices that the URL of the profile page is `https://www.website.com/profile/curious`. She changes its URL to `https://www.website.com/profile/admin` and is able to see the admin's information. Which category does this best fall into?

This is an example of broken access control as User A is able to gain access to User B's information without having User B’s identity. Reference: https://owasp.org/Top10/A01_2021-Broken_Access_Control/#example-attack-scenarios

Q 2/11: Given the context of the previous question, which of the following options is a valid way to remediate the vulnerability?

Session based authentication is the right way to approach this. User A cannot access User B’s information. Reference: https://owasp.org/Top10/A01_2021-Broken_Access_Control/#how-to-prevent

Q 3/11: Your company recently experienced a data breach. As part of the breach, user credentials were stolen due to an insecure database design. You are now responsible for evaluating third party vendors that offer a user authentication service. Which of the following would you expect the vendor to do?

This elevates the difficulty on a per users basis and is how modern systems deal with credentials. Using a unique salt per user prevents the classic rainbow table attack. Reference: https://owasp.org/Top10/A02_2021-Cryptographic_Failures/#example-attack-scenarios

Q 4/11: You have a large text file that you need to store safely. Which of the following are valid if you _only_ are concerned with the security of said file?

Encrypt, then compress | Compress, then encrypt

Both A and B are secure. B is preferred because compression saves more space on unencrypted text. Reference https://owasp.org/Top10/A02_2021-Cryptographic_Failures/#how-to-prevent

Q 5/11: You are working on an assignment at a coffee/boba/bubble tea shop, connected to their free wifi, and visit your favorite lifestyle blog `http://www.cool-blog.com` on your phone. Who could see what you are reading?

ISP, Wifi Users

Q 6/11: You notice "weird" things happening with your work computer. It has automatically restarted. Your CPU is consistently at 100% and applications are running slowly. You are not able to login to your work account. Which of the following should you do?

There is a non-zero likelihood that your machine has been compromised. To be on the safe side, you should report it to a security professional. Reference: n/a

Q 7/11: Which of the following is not something that is commonly done to prevent injection attacks?

Preventing users from submitting data would make most applications unusable. Reference: https://owasp.org/Top10/A03_2021-Injection/#description

Q 8/11: You are building a web application and find a library on Github that has the exact feature that you are looking for. The last commit was from 2011. Which of the following should you do?

Scan the Issues for newer forks of the project or alternative libraries that are currently maintained.

An existing, well-maintained solution is the most productive way to move forward. Reference: https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/#description

Q 9/11: Why does Django require that you set `ALLOWED_HOSTS` in `settings.py`?

Web Servers do not reliably validate the Host header.

Web Servers like Apache are notoriously hard to configure the right way so relying on it for Host header validation is not a good idea. Reference: https://docs.djangoproject.com/en/3.2/topics/security/#host-header-validation

Q 10/11: You are responsible for designing the password policy for your employer. Common passwords are disallowed by default. Which policy do you prefer?

Longer passwords are harder to crack than shorter ones, even if there are less restrictions. Furthermore, since they are easier to remember (where did I place the exclamation mark?!), people tend to not change them to common ones. Reference: https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/

Q 11/11: If you have time remaining, you can work on improving the security of the provided Django web application. The instructions are in Task2_handson.md and the starter files are in mysite.zip. What did the QR Code URL in the Django Admin start with?

otpauth://