Gmail Krishna chaitanya <ekrishnachaitanya2004@gmail.com>

Assignment on Securing Accounts for CS50 Cybersecurity

1 message

Google Forms <forms-receipts-noreply@google.com> 28 May 2024 at 17:06
To: ekrishnachaitanya2004@gmail.com

Google Forms

Thanks for filling in Assignment on Securing Accounts for CS50 Cybersecurity

Here's what was received.

Assignment on Securing Accounts for CS50 Cybersecurity

All assignments in CS50 Cybersecurity are out of 10 points. A score of 7 points or better (70%) is required to be considered to have "passed" an assignment in this course. **Please do not resubmit an assignment if you have already obtained a passing score**--we consider that spam, and if detected, the submission will be deleted, meaning you will not receive the score back anyway. You don't receive a final grade at the end of the course, so it will have no bearing on your certificate, and it will only slow down our graders!

Unlike CS50x, assignments in this course are graded on a set schedule, and depending on when you submitted, it may take up to three weeks for your work to be graded. Do be patient! Project scores and assignment status on cs50.me/cs50cy (e.g. "Your submission has been received...") will likely change over time and are not final until the scores have been released.

Email *

ekrishnachaitanya2004@gmail.com

Name *

KRISHNA CHAITANYA

edX Username *

eKRISHNA2004

What is your GitHub username? *

If you do not already have a GitHub account, you can sign up for one at https://github.com/join. You can then use this account to log in to cs50.me/cs50cy to track your progress in the course (your progress will only show up after you have received at least one score release email from CS50 Bot, so do be patient!). Don't worry about seeing a 'No Submissions' message on submit.cs50.io, if you find that. The course collects submissions using Google Forms, and only the gradebook on cs50.me/cs50cy is important!

- **Be certain the username you provide is correct!** If you provide the wrong username, you will not be able to see your scores.
- **Your GitHub username should not be changed while you are taking this course.** The current gradebook system is not designed to accommodate name changes.
- **Be sure to remove extraneous characters,** such as an @ prefix. Do not input a URL or email address, just your username.

ekrishnachaitanya2004

City, State, Country *

Srikalahasthi,Andhra Pradesh,India

Acknowledgement *

Unlike our course CS50x, grading in this course is not done automatically, and there are human reviewers for each assignment. Grading may, depending on exactly when in our grading cycle you submit, take up to three weeks from the time you submit. Your grade status may change in your gradebook at cs50.me/cs50cy in the interim, but grades are never final until you receive a score release email from CS50 Bot (on this first assignment, in fact, your gradebook may not even become active until that score release email). The staff cannot entertain requests for expedited grading under any circumstance. Your patience is appreciated.

◉ I understand.

This course is graded by human graders, and has a ZERO TOLERANCE

plagiarism and collaboration policy. If *any* of your answers are copied and pasted from, or obviously based on (a) an online source, including non-course-sanctioned generative AI tools or (b) another student's work in the course, in *any* of the course's five assignments or the final project, you will be reported to edX and removed from the course immediately. There is no opportunity for appeal. There are no warnings or second chances. *

It is far better, we assure you, to leave an answer blank rather than risk it. This may be an online course, but it is offered by Harvard, and we're going to hold you to that standard. **The full essence of all work you submit to this course should be your own.**

● I understand this policy and agree to its terms; I hereby affirm that I will not plagiarize any answers in this course.

Why might being required to change our passwords regularly actually pose a threat to our security?

Frequent password changes can create problems for users, leading to forgetfulness or resorting to risky practices like writing them down, which hackers can exploit. Additionally, people often use predictable patterns when creating new passwords, making them easier for attackers to crack. To manage multiple passwords, users might choose weaker ones or reuse them across different accounts, further increasing the risk of unauthorized access. Moreover, the increased frequency of password changes can overwhelm IT support with more password reset requests, adding to their workload. Furthermore, organizations may become complacent with frequent password changes, neglecting other vital security measures like implementing multi-factor authentication or robust access controls. Therefore, while the intention behind regular password changes is security enhancement, the reality is that it can introduce various security risks and operational challenges.

If I have a six-character password consisting of uppercase (English) letters and (decimal) digits **only**, how many seconds might it take an adversary to crack, assuming they make one attempt per second?

2176782336

Humor us for a moment, and play The Password Game, trying to get through at least Rule 12.

While obviously the game itself is in many ways meant to be humorous, it also critiques the experience many of us have setting up new passwords. Explain how there's a trade-off between usability and security in the context of passwords.

In the Password Game, we learn it's tough to make a password that's both strong and easy to remember. It's like finding a key that's strong enough to keep out bad guys but simple enough for everyone to use. Balancing this is super important: if it's too hard, people get annoyed, but if it's too easy, it's a piece of cake for hackers. So, getting it right keeps accounts safe and everyone smiling.

Consider the below comic for the next two questions.

Source: xkcd.com/936/

Consider the top row of the comic above. Why are passwords like those easy (for a computer) to guess but hard (for a human) to remember?

Passwords like "Tr0ub4dor&3" are easy for computers to guess because they follow common patterns, such as using "4" for "a" and "0" for "o." These predictable patterns mean there are fewer variations for password-cracking programs to try. With only about 28 bits of entropy, these passwords can be cracked quickly, even with a moderate guessing speed.
For humans, these passwords are hard to remember because they involve confusing mixes of characters, substitutions, and punctuation. This complexity doesn't match how we naturally remember things, making it easy to forget or get wrong. So, while these passwords might look complicated, they are easy for computers to crack but hard for humans to remember.

Now consider the bottom row of the comic above. Why are passwords like those hard (for a computer) to guess but easy (for a human) to remember?

Passwords like "correct horse battery staple" are hard for computers to guess because they use random common words, increasing the number of possible combinations and boosting entropy to about 44 bits. This makes them much harder to crack.
For humans, these passwords are easy to remember because they consist of simple, familiar words in a logical sequence. Our brains find it easier to recall meaningful phrases than random characters, making these passwords both secure and memorable.

What is a "credential stuffing" attack?

Credential stuffing is a cyberattack where criminals use stolen login credentials from one system to access another. It relies on people's tendency to reuse the same username and password across multiple accounts. It's vital for individuals to use unique login information for each account to prevent such breaches.

Provide a specific example of something that would be considered ***a type of knowledge factor*** for authentication purposes.

Do NOT provide any of your own knowledge factors (or anything resembling them) themselves as an answer to this question. We are looking for you to answer the question in the general sense (a "type of").

If you provide an answer that is, or appears to be, an actual specific knowledge factor, the answer WILL be marked incorrect, without exception, and you should consider that knowledge factor to have been compromised.

Date of birth

Provide a specific example of something that would be considered ***a type of inherence factor*** for authentication purposes.

Fingerprint or Facial recognition

Why are phishing attacks so difficult to prevent?

Phishing attacks are tough to stop because they use tricks like pretending to be someone else or manipulating emotions to fool people. Also, their emails often look real, making it hard to tell them apart from genuine messages. Furthermore, phishing attacks can exploit vulnerabilities in security systems or target specific individuals with tailored tactics.

Suppose that your boss asks you whether the company should require use of password managers for all employees.

Explain in a short paragraph why you might want everyone in the company to use a password manager.

Making password managers mandatory for all employees greatly boosts company security. These tools create strong, unique passwords for every account, cutting down on the chances of reusing passwords and lessening the impact of attacks. They also offer a safe space to store credentials, guarding against breaches. By using password managers, employees can effortlessly handle their passwords for various accounts, making work smoother and lowering the risk of security problems from weak or stolen passwords.

Feedback

How did you find the difficulty of this assignment? *

	1	2	3	4	5	
Too easy	○	○	●	○	○	Too hard

About how many MINUTES would you say you spent on this assignment? *

Just to set expectations for future students.

120