Assignment on Preserving Privacy for CS50 Cybersecurity

1 message

Google Forms <forms-receipts-noreply@google.com> 21 August 2024 at 14:44
To: ekrishnachaitanya2004@gmail.com

Google Forms

Thanks for filling in Assignment on Preserving Privacy for CS50 Cybersecurity

Here's what was received.

Assignment on Preserving Privacy 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/cybersecurity (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/cybersecurity 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/cybersecurity 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

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.

How does the below HTML tag help to protect your privacy online?
<meta name="referrer" content="origin">

The `<meta name="referrer" content="origin">` HTML tag helps protect online privacy by controlling the information sent in the `Referer` header when a user navigates from one site to another. Typically, the `Referer` header includes the full URL of the referring page, which can expose sensitive information like query parameters or fragments. By setting the `content` attribute to "origin," this tag ensures that only the basic origin (scheme, host, and port) of the referring URL is sent, rather than the complete URL. For instance, if the original URL is `https://Krishna.in/home?query=secret`, the header would only include `https://Krishna.in/`. This reduces the risk of leaking sensitive data to third-party sites, making it harder for them to track users or gather detailed information about their browsing activities. This tag is a privacy-enhancing measure, allowing developers to limit the information shared with other websites and better protect user data.

What information is transmitted in the *User-Agent* HTTP header?

The User-Agent HTTP header transmits information about the client's software, including the browser type, version, operating system, and sometimes device details.

We discussed in lecture the concept of private browsing, also known as "incognito mode." What is an advantage of private browsing?

Private browsing, also known as incognito mode, has the benefit of not saving cookies, site data, browsing history, or form submission information. Especially on shared computers, this can improve privacy.

Why might a website use *session cookies*?

Session Cookies improves the user experience by allowing features like form data, user logins, and the ability to keep items in a shopping cart.

Tor is software that you can install on your computer that, according to its website, "prevents someone watching your connection from knowing what websites you visit." How, in no more than a paragraph, does Tor do that?

Tor protects your online privacy by routing your internet traffic through a global network of volunteer-operated servers, or "nodes," using a process called onion routing. Your data is encrypted multiple times and passed through several nodes, with each node only decrypting enough to know where to send it next. This layered encryption ensures that no single node knows both the origin and destination of your data, preventing anyone monitoring your connection from determining which websites you visit.

In what sense are domain names similar to phone numbers like 1-800-COLLECT or 1-800-FLOWERS?

Domain names are similar to phone numbers like "1-800-COLLECT" or "1-800-FLOWERS" in that both serve as memorable, human-readable addresses that direct you to specific resources. Just as these phone numbers make it easy to connect to a specific business without needing to remember a long string of digits, domain names allow users to access websites without needing to remember complex IP addresses. Both systems use a form of mapping: phone numbers are mapped to businesses or services, while domain names are mapped to IP addresses of servers hosting websites.

Browser Rankings

According to StatCounter, below are the three browsers with top market share as of September 2023.

Earlier in 2023, NordVPN, a VPN service, put out a ranking of browsers by the extent to which they take privacy-related measures seriously.

Below stats and rankings are accurate as of September 2023.

Google Chrome - User Profiles

NordVPN critiques Chrome (63% market share, ⭐⭐ privacy rating) on the basis that one of Google's primary sources of revenue is "user profiling for ad targeting".

How is Chrome able to put together a user profile for that purpose?

Google Chrome creates user profiles for ad targeting by collecting data on browsing history, search queries, website visits, and interactions with ads. As part of the Google ecosystem, Chrome integrates this information with data from other Google services like Gmail, YouTube, and Google Maps, allowing the creation of comprehensive user profiles. This aggregated data enables Google to deliver highly targeted ads, which is a significant source of its revenue.

Safari - Fingerprinting

Safari (20% market share, ⭐⭐⭐ privacy rating) receives some praise in the article for its use of "anti-fingerprinting tools".

What is fingerprinting?

Fingerprinting is a tracking method that allows websites to uniquely identify and follow users by collecting specific data about their devices, such as browser type, operating system, screen resolution, and installed fonts. This technique creates a unique "fingerprint" that can be used to track users across different websites without relying on cookies. Safari's anti-fingerprinting tools work to limit the amount of identifiable data that websites can collect, thereby enhancing user privacy and reducing the effectiveness of fingerprinting.

Edge - Sandboxes

Microsoft's Edge (5% market share, ⭐ privacy rating) comes in at the bottom of the NordVPN list, unfortunately, but receives credit for running in a "sandbox". Why is this a good thing for end-users?

Running Microsoft Edge in a "sandbox" enhances security for end-users by isolating the browser from the rest of the system. This containment prevents malicious code from affecting the operating system or other applications, reducing the risk of system-wide infections, data breaches, and unauthorized access. By keeping potentially harmful content within the browser, the sandbox provides a crucial layer of protection, ensuring safer browsing experiences.

Log Format

Captionless Image

In lecture, we discussed the above example of a standard log format that might be used by a web server to keep track of user activity, where each of the above items prefixed by a $ is effectively a "variable" that will be replaced with user data.

Without using the word "refer", what does the *$http_referer* variable represent, in layman's terms?

The address of the webpage (URL) that linked to the resource that was requested is represented by the "Shttp_referer" variable. Put differently, it displays the URL that the user used to get to the current page. In order to better understand traffic sources and user behavior, this is used to track how users find a website or specific page.

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.

200