How not to design an online pharmacy: A case study

Sampsa Rauti
sjprau@utu.fi
University of Turku
Turku, Finland

Esko Vuorinen
etvuor@utu.fi
University of Turku
Turku, Finland

Robin Carlsson
crcarl@utu.fi
University of Turku
Turku, Finland

ABSTRACT

In today's digitized society, essential web-based healthcare services such as online pharmacies play a crucial role. This paper presents a case study on the third-party services used in an online pharmacy. We perform a network traffic analysis for the pharmacy website, revealing significant data leaks to multiple third parties. We also discuss the potential factors that have led to these privacy flaws and provide recommendations to address the found issues effectively.

CCS CONCEPTS

• **Security and privacy → Web application security**.

KEYWORDS

Online pharmacies, online privacy, data leaks, third-party services

ACM Reference Format:
Sampsa Rauti, Esko Vuorinen, and Robin Carlsson. 2023. How not to design an online pharmacy: A case study. In *2023 8th International Conference on Information Systems Engineering (ICISE 2023), December 16–18, 2023, Bangkok, Thailand*. ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3641032.3641042

1 INTRODUCTION

In today's digital age, online pharmacies have become an important component of the healthcare landscape and can be considered an essential service. One key advantage of online pharmacies is their great accessibility and convenience. Individuals living in remote geographic locations or having physical limitations can easily order medication and healthcare products with just a few clicks [5, 6]. Moreover, the COVID-19 pandemic has significantly accelerated the adoption and utilization of online pharmacies.

Privacy and confidentiality are also often touted as benefits offered by online pharmacies [4, 10]. For many customers, discussing sensitive health issues and purchasing certain medications may be more comfortable in the online environment. One would indeed expect online pharmacy websites to implement stringent privacy measures to keep patient information safe and protect confidentiality. Unfortunately, privacy in online pharmacies is not always as great as it is made out to be. A substantial privacy concern in pharmacy websites is the use of various third-party tools such as analytics services and the extent to which these third-party components may pry on the user's personal data concerning health.

ICISE 2023, December 16–18, 2023, Bangkok, Thailand

ACM ISBN 979-8-4007-0917-3/23/12
https://doi.org/10.1145/3641032.3641042

In this case study, we will take an in-depth look at a website of a Finnish online pharmacy and analyze the data leaks to third parties. Compared to earlier studies on online pharmacy privacy and third parties [2, 13], the current study provides a more detailed analysis of the pharmacy website implementation and privacy flaws from a software engineering point of view. The current study aims to highlight the reasons for poor privacy in the studied online pharmacy and gives software developers recommendations for improving the confidentiality of such pharmacy websites.

The rest of this paper is organized as follows. Section 2 describes the testing sequence we carried out and the method we used when experimenting with the online pharmacy website and recording the network traffic. Section 3 presents the results of our network traffic analysis and details the found data leaks. Section 4 describes the design flaws found in the studied online pharmacy in terms of privacy. It also offers several recommendations for improving privacy and avoiding the design flaws described related to architectural decisions and software development process. Section 5 concludes the paper.

2 STUDY SETTING AND EXPERIMENT

The chosen online pharmacy has, according to our previous findings, the largest number of third parties out of Finnish online pharmacies. This, and the fact that these parties are also present even without consent, makes it an interesting case for an in-depth case study. Although the pharmacy website is studied in detail in the current study, we believe that disclosing the name of the selected pharmacy would not provide any additional value or serve a meaningful purpose here. This is why we have decided to keep the pharmacy anonymous. The online pharmacy has been reported to Finnish data protection authorities and is being investigated.

Our experiment on the pharmacy website involved using the most critical functionalities of the pharmacy and recording the generated network traffic. The basic test sequence we followed consisted of the following steps:

- *Step 1.* Accessing the pharmacy website (front page) and denying consent to cookies and data collection.
- *Step 2.* Utilizing the search functionality on the website by searching for a specific medicine.
- *Step 3.* Accessing the product page of the medicine from the search result page.
- *Step 4.* Proceeding to order the medicine. This process consisted of undergoing strong authentication, confirming the order in the chat with a pharmacist[1] and completing the checkout.

[1] Pharmaceutical counseling, which involves providing advice and information about medications, including their appropriate use, dosage, potential side effects, and other relevant details, is legally required in Finland.

During this test sequence, all network traffic was recorded using the Google Chrome Developer Tools. The network traffic was stored in a HAR file[2] that was subsequently analyzed. From the log files, third-party requests were extracted to determine whether the online pharmacy leaked sensitive personal data to third party services. Identifying personal data items (such as IP address or person's name) as well as contextual data items (such as the URL address of the current page or the name of the medicine the user has viewed) were collected. For further validity, the test sequence was run and log files were studied by two researchers.

Lastly, the privacy policy document of the pharmacy was also analyzed to find out whether it corresponded to the actual traffic recordings. In other words, we wanted to see how transparently the user was informed about processing of personal data. More specifically, we studied whether the third parties receiving personal data were explicitly named in the privacy policy. We also wanted to see whether the contextual personal data (the current URL address, medicine details etc.) were leaked to third parties. Finally, we also studied whether the document mentioned identifying personal data items that were shared with third-party services, or the possibility that the user can be uniquely identified in general.

3 RESULTS

In total, 6 separate third parties were found on the studied pharmacy website. This included Google Analytics and Bing Ads, services provided by two technology giants – Google and Microsoft. Google Analytics is used to track website activity and pageviews of users using the site, along with many other details such as where the website users come from. Bing Ads, on the other hand, is employed to track conversions, specific actions that a website owner wants visitors to take, such as completing a purchase. Algolia, a popular third-party service used for implementing search functionality was also present. The pharmacy also used Lucky Orange, a third-party service for website optimization and customer behavior analytics. Furthermore, Omnisend, a web marketing automation platform, was likely deployed to help with marketing campaigns and other e-commerce purposes. Finally, LoyaltyLion, a service used for loyalty and reward programs, was also integrated on the pharmacy website.

Figures 1 and 2 show the pharmacy web pages corresponding to steps of the testing sequence we discussed previously: 1) the pharmacy front page, 2) the search results page, 3) the product page of a specific medicine, and 4) the medicine order page. For each of these pages, the figure shows sensitive identifying and contextual personal data that was leaked and the third parties receiving this data.

When looking at the flows of data in the alluvial diagram, we can see that several different types of personal data are being sent to third parties. Each personal data item has been color coded to make it easier to discern at each phase of our experiment. The leaked data items can be divided into two groups: identifying personal data and contextual personal data. For example, a unique ID identifying the used device and browser is one such personal data item. As we can see, this data is collected by Google, giving the technology giant an effective way to identify users. Unknown IDs, received by Bing and Omnisend, are strings that most likely identify a specific user, device or session. More traditional pieces of personal data, the user's full name and email address, are also present. It is worth noting here that the user has given the email address when registering. The user's full name, on the other hand, is acquired from strong customer authentication provided by a bank when the user proves their identity before ordering medicines. Finally, an IP address (not shown in the figures as it always leaks with web requests) is also identifying data which can usually be connected to a specific device and user.

Contextual personal data, on the other hand, often contains the previous and current URL. In the figures, we can see that the current URL is regularly leaked to 5 different third parties. The URL often reveals what the user is doing in the service, for example if they are ordering medicines. Moreover, the search term, product name as well as quantity and price may be a part of the URL, and this is exactly what happens in the case of the studied pharmacy. The fact that the user's identity can be connected to medicines they are ordering is a serious privacy violation, as delicate health data leaks to third parties. The fact that one third-party service, LoyaltyLion, directly gets the user's full name (and not just an IP address, for example) makes this violation even more severe. However, to large companies such as Google who can easily connect most IP addresses to names (e.g. if the user is logged in to their services on some other website), the IP address is as good as the name.

It seems quite clear that the developers of the online pharmacy have not understood that their pharmacy leaks this kind of information to third parties. None of the 6 third parties we found was mentioned in the privacy policy document, which means an average user has no realistic chance of finding out about their existence. The categories of sensitive data sent to the third parties were also not mentioned. Still, the user's personal data is silently leaking to these third parties in the background.

In summary, the greatest privacy flaw in the online pharmacy implementation is that the identity of the user (in the form of IP address, different identifiers and even full name in one case), along with information on the viewed and ordered medicine is sent to third parties. These personal data transfers happen without properly informing the user and without consent from the user.

4 DESIGN FLAWS AND RECOMMENDATIONS

In the studied online pharmacy, there are many design flaws and poor architectural decisions that have led to insufficient privacy and confidentiality. First one is using six different third-party services without appropriate concern for privacy. These services have quite clearly been added without understanding what kinds of personal data items end up in their servers. In the case of Google Analytics, for example, there has been a significant amount of concern regarding the transfer of users' personal data from Europe to the United States, and potentially violating European Union data protection rules [12]. Transfers of sensitive data outside the European Economic Area (EEA) gives rise to concerns regarding whether the data receives the same level of protection as mandated by the GDPR. If there's a need to use analytics, the pharmacy should retain the data locally, for instance utilizing open-source analytics tools such as

[2]A HTTP Archive file used for capturing and storing detailed information about the interactions between a web browser and a web server.

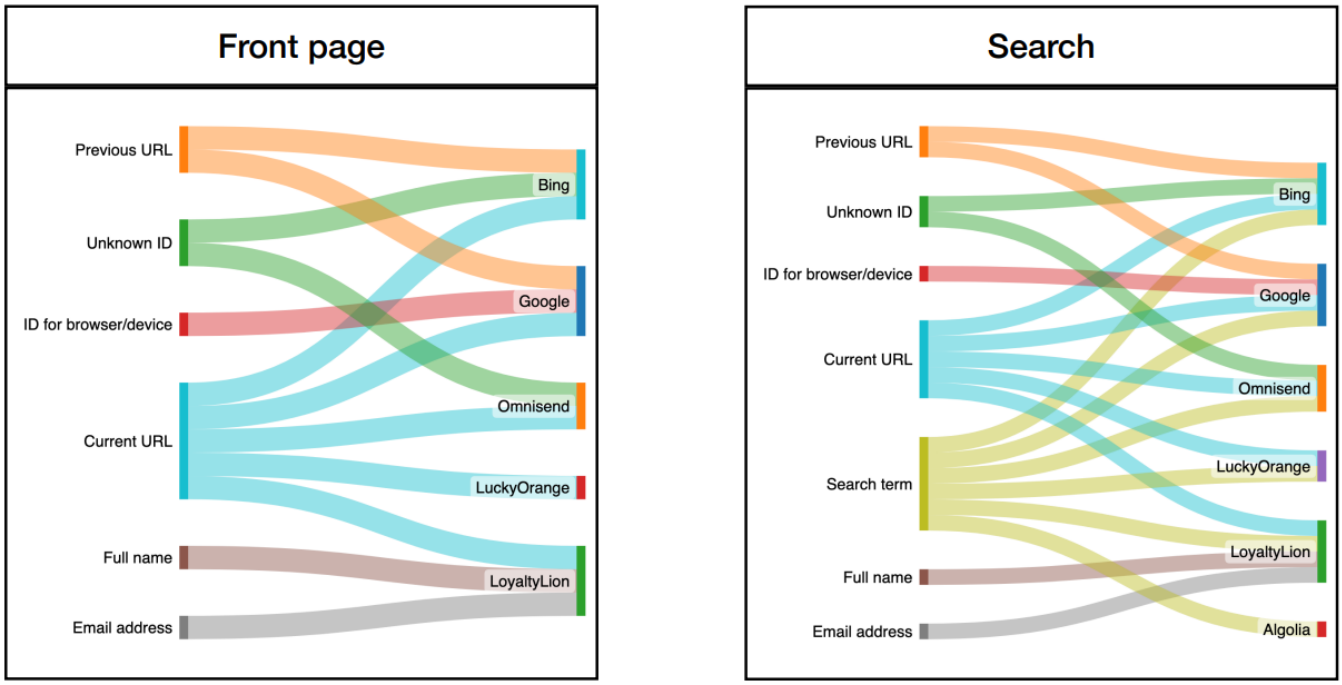

Figure 1: Data leaks on front and search result pages.

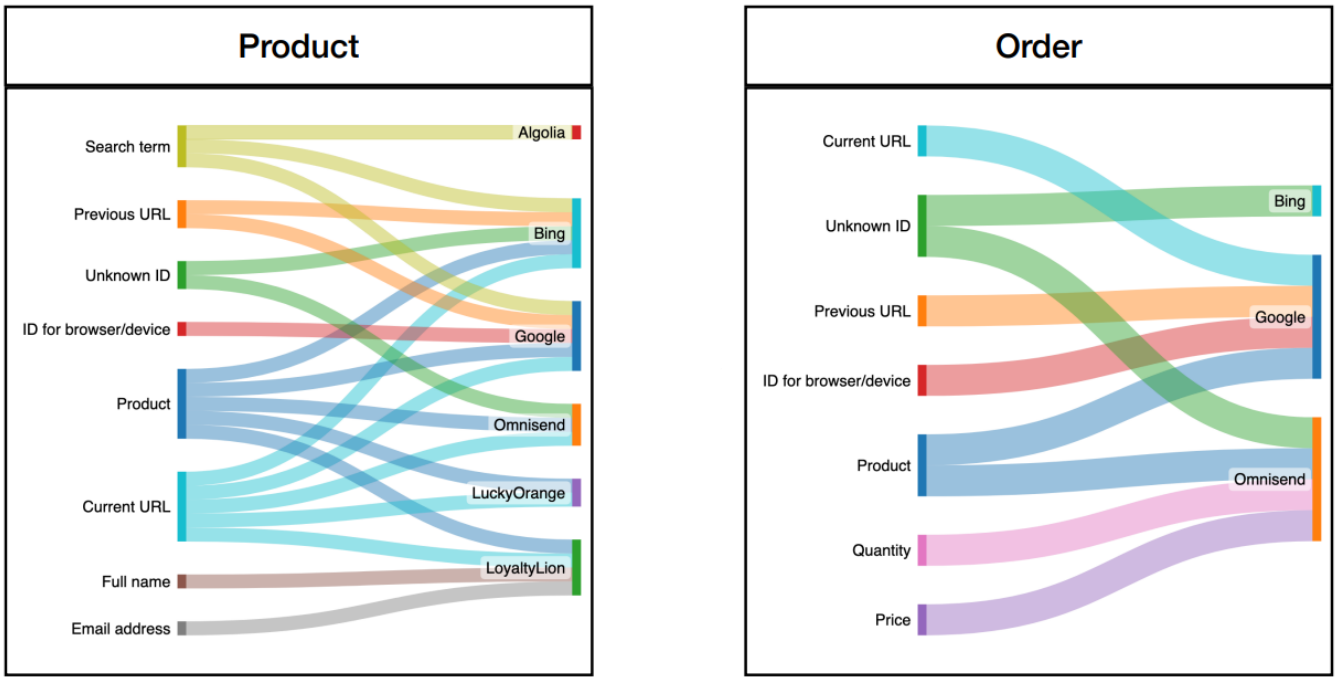

Figure 2: Data leaks on product and order pages.

Matomo [3, 11], instead of sharing users' personal data with third parties.

The platform a website is built with often influences the decisions the add third parties on the website. The studied online pharmacy

Table 1: Design flaws and possible solutions.

Design flaw	Possible solution
Using third party analytics without concern for privacy	Remove third party services or replace them with locally hosted alternatives such as Matomo
Using platforms or frameworks that easily allow adding extensions with questionable privacy	Choosing platforms and extensions carefully and reviewing their privacy
Being unaware of data flows to third parties	Network traffic analysis and external audits
Cookie management system misconfiguration	Configure cookie management correctly and perform testing
Vague privacy policies	Make sure privacy policy documents clearly and transparently discuss possible third parties and categories of personal data they process
Insufficient communication between pharmacy staff and developers	Making sure developers are aware of the privacy requirements and have sufficient understanding of the application area

uses Shopify, an e-commerce platform that allows merchants to easily add different functionalities to their online stores. This is usually done by using apps that, among other things, include numerous third-party analytics and tracking services. It is easy to plug in several apps without thinking that third parties are also being added to the website. Moreover, Shopify itself can also be considered a third party that can potentially collect sensitive information.

The worst data leak revealed in our study, the combination of a customer's real name and medicine name, takes place because of LoyaltyLion's Shopify app. While aiming to reward positive customer behavior with points and gifts, delivered through email and web notifications, the app also collects delicate personal information without consent. Developers appear to be oblivious to this, and the user is not informed adequately.

In our experiments, it did not matter whether the cookies and data collection were consented to, refused, or whether the cookie banner was not interacted with at all. Regardless of this choice, the number of third parties remained the same. It seems very likely that the consent management platform has been misconfigured and left untested. The privacy policy, which did not inform the users about the third parties or types of leaked personal data, did not make the situation any better. Unfortunately, this unclarity is not uncommon in today's web services [8, 9].

The pharmacy also lulled users into a false sense of security by emphasizing the responsible and confidential approach of the web service, as well as promising that the service maintainers "strictly adhere to the regulations set by the Finnish authorities" and operate according to ethical principles. This wrong confidence in the high privacy of the online pharmacy may be largely due to the poor communication between the pharmacy staff and the developers.

It is essential that the pharmacy and the website developers communicate effectively so that the requirement specification and risk assessment in terms of security and privacy can be successful. Developers have to understand the need for confidential data processing and ensuring that there are no flows of sensitive health data to third parties in the website. Without these rudimentary measures and privacy-by-design approach [1], an online pharmacy can hardly claim to handle personal data confidentially and adhere to regulations.

From a technical perspective, it would also be very important to perform testing to detect the data flows to third parties and examine the types of personal data they contain. Apparently, this kind of testing has not been conducted, although it would not be very time consuming and would easily reveal the leaks of sensitive personal data on most critical pages of the online pharmacy. Especially when dealing with data concerning health, such as data on medication, it would be important for developers to have a decent understanding of the application area in order to take the necessary privacy measures [7]. Critical websites of healthcare services, online pharmacies included, would also greatly benefit from external privacy auditing.

The Finnish data protection authorities have been informed about the privacy problems on the website of the studied pharmacy. We hope that our results will prompt action to address these issues and ensure the protection of users' personal information. By bringing these concerns to the attention of the relevant authorities and reporting them in the current study, we aim to contribute to the overall improvement of online privacy, not only for the studied pharmacy but also for other similar platforms and online health services. The design flaws and recommendations discussed above are summarized in Table 1.

5 CONCLUSIONS

In this case study, we examined the privacy issues encountered in an online pharmacy. Specifically, we found that sensitive user data was shared with various third parties without consent. URLs of visited pages and search terms used by users, which often include medicine names and symptoms on pharmacy websites, were transmitted to several third parties such as Google and Bing. Along with this contextual information, identifying personal data such as IP addresses and device-specific identifiers were also transmitted. Furthermore, even the user's real name and email address along with the medicine name were leaked to a third party when ordering medicines. This raises concerns about the very real possibility of linking users' real identity to ordered medicines.

Our findings emphasize the need for careful consideration of privacy requirements and implementing the privacy-by-design approach in online pharmacies. The results also highlight a strong demand for communication between the pharmacy and software developers so that the application area specific privacy concerns are adequately addressed. This way, poor design decisions such as choosing a generic web store platform with several web analytics

plugins enabled may be avoided. It is important to analyze the outgoing data flows to understand what kind of data the website sends to third parties and who receives it. The same considerations should also be transparently addressed in a privacy policy document. Hopefully, the results of this case study can serve as an educational story about the importance of safeguarding sensitive user data with robust privacy design in online healthcare services.

ACKNOWLEDGMENTS

This research has been funded by Academy of Finland project 327397, IDA – Intimacy in Data-Driven Culture.

REFERENCES

[1] Susanne Barth, Dan Ionita, and Pieter Hartel. 2022. Understanding online privacy—a systematic review of privacy visualizations and privacy by design guidelines. *ACM Computing Surveys (CSUR)* 55, 3 (2022), 1–37.

[2] Robin Carlsson, Sampsa Rauti, Sini Mickelsson, Tuomas Mäkilä, Timi Heino, Elina Pirjatanniemi, and Ville Leppänen. 2023. Several online pharmacies leak sensitive health data to third parties. In Proceedings of the 11th World Conference on Information Systems and Conference (WorldCIST). Springer. Accepted for publication..

[3] Jonas Gamalielsson, Björn Lundell, Simon Butler, Christoffer Brax, Tomas Persson, Anders Mattsson, Tomas Gustavsson, Jonas Feist, and Erik Lönroth. 2021. Towards open government through open source software for web analytics: The case of Matomo. *JeDEM-eJournal of eDemocracy and Open Government* 13, 2 (2021), 133–153.

[4] VH Jain, SA Tadv, and SP Pawar. 2017. A review on the pros and cons of online pharmacies. *Journal of Applied Pharmaceutical Research* 5, 1 (2017), 20–26.

[5] Oisín N Kavanagh, Aaron Courtenay, Fatimah Khan, and Deborah Lowry. 2022. Providing pharmaceutical care remotely through medicines delivery services in community pharmacy. *Exploratory Research in Clinical and Social Pharmacy* 8 (2022), 100187.

[6] Bill Kelly. 2015. Online pharmacies: buyer beware. *Australian Prescriber* 38, 6 (2015).

[7] Joanne Kuzma. 2011. Web vulnerability study of online pharmacy sites. *Informatics for Health and Social Care* 36, 1 (2011), 20–34.

[8] Joanne Kuzma, Kate Dobson, and Andrew Robinson. 2016. An examination of privacy policies of global On-line E-pharmacies. *European Journal of Research and Reflection in Management Sciences* 4, 6 (2016), 23–28.

[9] Trix Mulder. 2019. Health apps, their privacy policies and the GDPR. *European Journal of Law and Technology* (2019).

[10] Grazia Orizio, Anna Merla, Peter J Schulz, Umberto Gelatti, et al. 2011. Quality of online pharmacies and websites selling prescription drugs: a systematic review. *Journal of medical Internet research* 13, 3 (2011), e1795.

[11] Denise Quintel and Robert Wilson. 2020. Analytics and privacy. *Information Technology and Libraries* 39, 3 (2020).

[12] Austrian supervisory authority. 2022. Decision of 22 April 2022. Accessed 06/27/2023, https://noyb.eu/sites/default/files/2022-04/Bescheid%20geschw%C3%A4rzt%20EN.pdf.

[13] Alexander R Zheutlin, Joshua D Niforatos, and Jeremy B Sussman. 2022. Data-tracking among digital pharmacies. *Annals of Pharmacotherapy* 56, 8 (2022), 958–962.