# Your website has been hijacked: Raising awareness for an invisible problem

Anne Hennig[1]

**Abstract:** Running a business without having a website is nearly impossible nowadays. Content management systems (CMS) provide features which make it easy for laypersons to create sophisticated websites. But those can pose security risks and provide vulnerabilities for manipulations. With vulnerability notifications, website owners are notified about security risks. The work of this doctoral thesis is divided into two main parts: At first it is necessary to identify common themes with respect to vulnerability notifications and provide more information on how to improve future vulnerability notifications. The second main part is to develop and evaluate suitable awareness materials.

**Keywords:** web security; vulnerabilities; security notification; security awareness

## 1 Introduction

Information about services are mainly retrieved from online resources nowadays [Eu21]. Therefore, running a business without having a website is nearly impossible. Especially for small businesses, individuals or non-profit associations, content management systems (CMS) provide features to create and maintain sophisticated websites. But CMS's frameworks, plugins, and templates also provide vulnerabilities for manipulations. Conţu et al. [Co16] describe four main threats for open-source content management systems, from which different kinds of attacks can result.

Some attacks aim at the search results of the original website. In case of search engine Spam (SEO Spam) or Pharma Hacks, an attacker deploys code on a website to redirect to fake web shops [Ma20; Ma21b]. In the search engine results, these sites appear as shops selling illegal or banned drugs and medicines, or luxurious brand-name clothing for cheap. But the manipulation is not visible on the genuine website and the malicious code is often hidden in the CSS files of a website where it cannot be easily found [Ma21b]. Website owners, therefore, have to rely on vulnerability notifications to be informed about the problem.

The work of this doctoral thesis is divided into two main parts: At first, a suitable way to contact the affected website owners will be established. The second main part is to develop and evaluate suitable awareness materials for website owners. A description of the different parts and the current status of each part is described in the following sections.

[1] Karlsruhe Insitute of Technology, Institute of Applied Informatics and Formal Description Methods, Kaiserstraße 89, 76133 Karlsruhe, Germany anne.hennig@kit.edu

ⒸⓘⓈ

## 2 Related Work

Since the problem is not easy to detect, most website owners have to rely on vulnerability notifications by the security community to be informed about the manipulation. Within the project as well as in the literature it could be shown, that there is no easy way to notify affected website owners in case of a vulnerability. The basic finding is that notifying a website owner about the problem increases remediation rates (i.a. [Çe16; Çe17; Du14; St18; VM12]). Many of these studies, however, report low remediation rates and problems to reach out to the recipients of their vulnerability notifications.

### 2.1 Raising awareness by providing sufficient information and establishing trust

According to Stock et al. [St18], three key factors that lead to a successful notification campaign are the e-mail reading rate, awareness rising factors and the aware-to-fix rate. So far, different aspects of these factors have been researched.

Experimental studies with modifications of **sender, message framing, subject, and language** showed that although some senders or message types work better than others, there was no statistically significant difference in the remediation rate between the treatment groups. This indicates that factors like sender reputation or framing alone do not drive remediation rates [Çe16; Ma21a; St18; Ze19].

Aspects that establish **trust** in vulnerability notifications have been identified with a quantitative survey: **formal aspects** (e.g. sender or correct spelling), **content-related aspects** (e.g. description of the problem and a motivation that is not attached to financial demands), and **verifiability aspects** (providing verification possibilities, like contact information) [Ma21a]. Furthermore, previous research has shown that providing **detailed information** were more effective with respect to remediation rates [Çe16; Li16; VM12].

Nevertheless, even if a vulnerability notification is deemed trustworthy, remediation rates are still low. Therefore, further factors need to be included for notifications to be successful.

### 2.2 Increasing remediation beyond establishing trust

**Diligence** of website operators, **popularity** of a website, as well as the **severity** of an issue, and the **media attention** the issue gets, seem to influence remediation rates as well [VM12; Ze19]. But besides intense media coverage, a significant amount of vulnerable websites was left unfixed in one study [Du14].

It has been proposed that **external incentives** also increase remediation rates [Ze19]. Recent studies showed that legal consequences and fines [Ma21a], as well as technical consequences imposed by the hosting provider [Çe19] increase remediation rates. Other authors proposed that loss of reputation can serve as an external incentive, too [VM12].

# 3 Identifying a suitable communication channel and message content

## 3.1 Interviews with affected website owners

As stated above, website owners' reactions to vulnerability notifications are mainly retrieved from experimental studies or quantitative surveys. Only a few studies have used qualitative approaches so far, but all of them were dedicated to a different target group or to answer different questions (e.g. [Di18; Je20; Li19]). But because qualitative approaches are more applicable for *understanding* opinions, we directly talked to affected website owners to assess their opinions and to identify common themes about vulnerability notification. An interview guideline was developed that covered three main topics: notification of a previous incident, possible notifications in case of future incidents, and channels, which the persons use to actively inform themselves about security incidents. Socio-demographic data that were found to have an impact on the remediation rate were also collected [Çe16; St18].

With this we would like to answer the following research questions: (1) How did website owners receive previous web vulnerability notifications? (2) What are suitable senders and communication channels that the website owners deem trustworthy? (3) What aspects should we consider in future notifications to be deemed trustworthy? (4) What – if any – channels do website owners use to actively inform themselves about security incidents?

Between November 2020 and March 2021, our project partner compiled a list of domains that were affected by a Pharma Hack or a related SEO spam infection. In April 2021, the complete list was sent to associated project partners or the State Offices of Criminal Investigations, which were supposed to inform the website owners about the vulnerability.

Between July and September 2021, we contacted 65 website owners from this list via e-mail, and asked, if we could call them for an interview. We used the contact information given on their websites. In total, we conducted 25 qualitative interviews with website owners (response rate: 39 %) and could confirm that distrust in unexpected notifications is high. We further found that verifiability is the most important factor to establish trust in notifications. We also endorse the findings that raising awareness for the severity and the complexity of the problems is crucial to increase remediation rates.

## 3.2 Evaluating the effectiveness of a vulnerability notification

As described above, designing a message content that is not only trustworthy, but also provides *convincing* incentives, like legal [Ma21a], reputational [VM12], or technical [Çe19] sanctions, is currently an open area of research. It has also not been investigated whether incentives that are tied to a sender that has the executive power to enforce the proposed consequences can increase the aware-to-fix rate even more. Since this is up to this point an open area of research, we expect these findings to be a major contribution.

We plan an experimental study to answer the following research questions: (1) Which sender has which impact on the remediation rate? (2) Which framing of the message has which impact on the remediation rate? (3) Do sender and framing of a message correlate with respect to the remediation rate?

We used the results of our interview study to design a vulnerability notification that includes the major trust-promoting factors like verification possibilities, a clear description of the problem and a plausible motivation. These basic information are either combined with a framing that contains technical, one that contains reputational, or one that contains no incentives. We also identified senders which were deemed plausible by our interviewees and which match one of the three framings with respect to the consequences they can impose.

## 4 Awareness as prevention

As the results of our interview study and the current research show, raising awareness for vulnerability notifications in general and especially for the severity of this vulnerability is still an open area of research. The development of effective awareness materials that are tailored to certain target groups is therefore deemed crucial to increase the aware-to-fix rate. It is planned to include the website owners, hosting provider, industry branches, and other intermediaries like internal (web) administrators or CISOs, into this process. Figure 1 gives an overview of the timeline of this doctoral thesis until the end of the research project. It is possible to further evaluate and improve materials, as well as to extent the reach of the project (for example by contacting website owners in non-German speaking countries) beyond the duration of the project, if funding is provided.

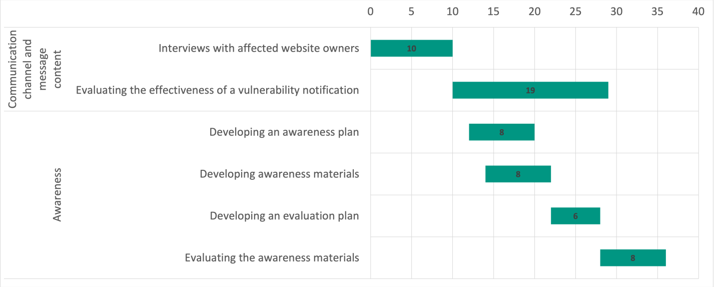

Fig. 1: Timeline for the doctoral thesis in month until the end of the research project

## Acknowledgements

This research is supported by the Federal Ministry of Education and Research, Germany, as part of the BMBF „INSPECTION“ project (Zuwendungsnummer 16KIS1113).

## References

[Çe16] Çetin, O.; Jhaveri, M. H.; Gañán, C.; Eeten, M. v.; Moore, T.: Understanding the role of sender reputation in abuse reporting and cleanup. Journal of Cybersecurity 2/1, pp. 83–98, 2016, ISSN: 2057-2085, URL: https://academic.oup.com/cybersecurity/article/2/1/83/2629556.

[Çe17] Çetin, F. O.; Ganan, C. H.; Korczynski, M. T.; Eeten, M. J. G. v.: Make notifications great again: learning how to notify in the age of large-scale vulnerability scanning. In. 16th Workshop on the Economics of Information Security (WEIS 2017), San Diego, pp. 1–23, 2017, URL: http://resolver.tudelft.nl/uuid:621f4a4f-e5d9-4f04-abc4-46252f9db3db.

[Çe19] Çetin, O.; Gañán, C.; Altena, L.; Tajalizadehkhoob, S.; Eeten, M. v.: Tell Me You Fixed It: Evaluating Vulnerability Notifications via Quarantine Network. 2019 IEEE European Symposium on Security and Privacy (EuroS&P) 00/, pp. 326–339, 2019, URL: https://www.readcube.com/library/42cf3704-a798-4336-b319-363ceea244b9:55032f97-a10f-4272-baa8-31cb68b24da4.

[Co16] Conţu, C. A.; Popovici, E. C.; Fratu, O.; Berceanu, M. G.: Security issues in most popular content management systems. In: 2016 International Conference on Communications (COMM). Pp. 277–280, 2016, URL: https://ieeexplore.ieee.org/document/7528327.

[Di18] Dietrich, C.; Krombholz, K.; Borgolte, K.; Fiebig, T.: Investigating System Operators' Perspective on Security Misconfigurations. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security/, pp. 1272–1289, 2018, URL: https://www.researchgate.net/publication/328329898%5C_Investigating%5C_System%5C_Operators%5C%27%5C_Perspective%5C_on%5C_Security%5C_Misconfigurations.

[Du14] Durumeric, Z.; Li, F.; Kasten, J.; Amann, J.; Beekman, J.; Payer, M.; Weaver, N.; Adrian, D.; Paxson, V.; Bailey, M.; Halderman, J. A.: The Matter of Heartbleed. In: Proceedings of the 2014 Conference on Internet Measurement Conference, IMC '14. IMC '14, Association for Computing Machinery, Vancouver, BC, Canada, pp. 475–488, 2014, ISBN: 9781450332132, URL: https://doi.org/10.1145/2663716.2663755.

[Eu21] Eurostat: Anteil der Personen, die das Internet zur Suche nach Informationen über Waren und Dienstleistungen genutzt haben, in den Ländern der Europäischen Union (EU-28) im Jahr 2020, Mar. 2021, URL: https://de.statista.com/statistik/daten/studie/806662/umfrage/internetsuche-nach-informationen-ueber-waren-und-dienstleistungen-in-der-eu/, visited on: 10/28/2021.

[Je20] Jenkins, A.; Kalligeros, P.; Vaniea, K.; Wolters, M. K.: “Anyone Else Seeing this Error?”: Community, System Administrators, and Patch Information. 2020 IEEE European Symposium on Security and Privacy (EuroS&P) 00/, pp. 105–119, 2020, URL: https://www.readcube.com/library/42cf3704-a798-4336-b319-363ceea244b9:a0e7c73b-8876-4cd4-81a7-f25b6b36240e.

[Li16] Li, F.; Durumeric, Z.; Czyz, J.; Karami, M.; Bailey, M.; McCoy, D.; Savage, S.; Paxson, V.: You’ve Got Vulnerability: Exploring Effective Vulnerability Notifications. In: 25th USENIX Security Symposium (USENIX Security 16). Pp. 1033–1050, 2016, ISBN: 978-1-931971-32-4, URL: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/li.

[Li19] Li, F.; Rogers, L.; Mathur, A.; Malkin, N.; Chetty, M.: Keepers of the Machines: Examining How System Administrators Manage Software Updates. In: Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019). USENIX Association, Santa Clara, CA, pp. 273–288, 2019, ISBN: 978-1-939133-05-2, URL: https://www.usenix.org/conference/soups2019/presentation/li.

[Ma20] Martori, A.: Spamdexing: What is SEO Spam and How to Remove It, Feb. 2020, URL: https://blog.sucuri.net/2020/02/spamdexing-seo-spam.html, visited on: 10/28/2021.

[Ma21a] Maass, M.; Stöver, A.; Pridöhl, H.; Bretthauer, S.; Herrmann, D.; Hollick, M.; Spiecker, I.: Effective notification campaigns on the web: A matter of Trust, Framing, and Support. In: 30th USENIX Security Symposium (USENIX Security 21). USENIX Association, pp. 2489–2506, 2021, ISBN: 978-1-939133-24-3, URL: https://www.usenix.org/conference/usenixsecurity21/presentation/maass.

[Ma21b] Malcare: What is WordPress Pharma Hack & How to clean it?, Jan. 2021, URL: https://www.malcare.com/blog/what-is-pharma-hack-how-to-clean-it/.

[St18] Stock, B.; Pellegrino, G.; Li, F.; Backes, M.; Rossow, C.: Didn’t You Hear Me? - Towards More Successful Web Vulnerability Notifications. Proceedings 2018 Network and Distributed System Security Symposium/, pp. 1–15, 2018, URL: https://swag.cispa.saarland/papers/stock2018notification.pdf.

[VM12] Vasek, M.; Moore, T.: Do Malware Reports Expedite Cleanup? An Experimental Study. In: 5th Workshop on Cyber Security Experimentation and Test, CSET ’12, Bellevue, WA, USA, August 6, 2012. USENIX Association, pp. 1–8, 2012, URL: https://www.usenix.org/conference/cset12/workshop-program/presentation/vasek.

[Ze19] Zeng, E.; Li, F.; Stark, E.; Felt, A. P.; Tabriz, P.: Fixing HTTPS Misconfigurations at Scale: An Experiment with Security Notifications. In: The 2019 Workshop on the Economics of Information Security (2019). Boston, MA, pp. 1–19, 2019, URL: https://www.semanticscholar.org/paper/Fixing-HTTPS-Misconfigurations-at-Scale%5C%3A-An-with-Zeng-Li/b22c522c6201f8545e1626deaf6ca43db52444d7.