Ethical Review on Making Vulnerabilities Visible Analysis (Punk-Spider)

Vikrant Singh, Student id: 21262315, vikrant.singh3@mail.dcu.ie, Msc in computing (Secure Software Engineering), CA640, 22/11/2021, word-count: 2496

Disclaimer

An essay submitted to Dublin City University, School of Computing for module CA640 Professional and Research Skills in Computing.

I understand that the University regards breaches of academic integrity and plagiarism as grave and serious. I have read and understood the DCU Academic Integrity and Plagiarism Policy. I accept the penalties that may be imposed should I engage in practice or practices that breach this policy.

I have identified and included the source of all facts, ideas, opinions, viewpoints of others in the assignment references. Direct quotations, paraphrasing, discussion of ideas from books, journal articles, internet sources, module text, or any other source whatsoever are acknowledged and the sources cited are identified in the assignment references.

I declare that this material, which I now submit for assessment, is entirely my own work and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work.

By signing this form or by submitting this material online I confirm that this assignment, or any part of it, has not been previously submitted by me or any other person for assessment on this or any other course of study. By signing this form or by submitting material for assessment online I confirm that I have read and understood DCU Academic Integrity and Plagiarism Policy.

Name: Vikrant Singh
Date: 22-11-2021

Introduction

Punk-Spider is a vulnerability scanning tool, this tool automatically scans the hackable vulnerabilities in websites and then allows to search anyone those results using keywords or by name or level of vulnerability. Punk-spider makes a list of unsecured or unpatched vulnerabilities on the website and makes them public.

The developers of Punk-Spider believes that this tool helps in enrolling fast security patches, because administrators of websites know that the vulnerabilities are public, so they must take fast actions to stop any severe consequences. However, the developers knew there is a high possibility that people with bad intentions can exploit these weaknesses. Also, Alejandro Caceres which is one of the creators of Punk-spider says that these exploitable vulnerabilities are there for decades and many other scanners are doing the same work, the only difference is that Punk-Spider makes them public so that everyone including customers and even your investors will be able to see those vulnerabilities and it creates a sense of pressure on the organization to fix these problems fast and make their websites secure.

According to wired, the previous version of the Punk-Spider was removed from Amazon Web Service many times, because of the continuous reports against the tool by several unhappy web administrators, who are angry about the disclosure of the vulnerabilities publicly and now the newer version contains few features to provide a bit more flexibility to the admins and developers a feature which allows probing on user agent so that they can identify the visitors on the websites and another option named as opt-out is provided that allows websites remove themselves from searches of the tool if they want.

Cyber security experts like Jeremiah Grossman for instance said that the type of test Punk-spider is performing without the permissions for the website owner is a legal concern, but when it comes to the ethics of revealing a vulnerability Katie Moussouris CEO of Luta Security and a respected voice in hacker community debates over vulnerability research and disclosure said

that these are weaknesses themselves that lead to attacks on websites, Punk-Spider is just making vulnerabilities visible to others.

And Alejandro Caceres says, he doesn’t know about the legal concerns they are just trying to do the right things and some things, because after the years of warning about these vulnerabilities are continuing to be ignored.

Analysis Summary according to ACM code of ethics

The new Punk-spider follows many ethical principles as per policy. The motive of the developers of this extension is to safeguard the attacks that happen through the internet by revealing them and making people aware of potential threats which aim principal 2.7 to spread foster public awareness about computing and its effects. They also understand their responsibility to safeguard the data and protect it from malicious use which follows principal 3.1 in the code of ethics which is the public good is the main concern during professional computing. They are also taking legal issues and regulations very seriously, so they are following principal 2.3 means they know and respect legal concerns. They are using stepwise disclosure, they created a process that applies, and support policies and processes that reflect the principles of the Code according to principal 3.4 and this process have rules which follow many other codes of ethics like 1.2 principal which is to avoid harm by revealing only that about the security of website but doesn’t disclose specific details to exploit the vulnerability and their team also suggest the organization how to secure the potential thread and also suggest third party security resources means they are following principal 2.5 which is comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks and also following principal 2.4 which is accepted and provide an appropriate professional review.

But they are still some problems with public disclosure of information, and they are still figuring out better methods to provide controlled access of subsets of the information. It’s still a difficult task as even if there is a small information disclosure to the user there is still a large possibility that smart users or attackers can use that information to implement some attacks on a website. Because it's like providing a starting point to an attacker because they can just turn on extension while surfing over the internet and can find many vulnerabilities and can use the information provided by Punk-Spider for the advancement of the attack.

Liffick’s analysis of the case

1. Participants

Developers of punk spider named Alejandro Caceres and Jason Hopper and websites administrators are because admins who are worried about the vulnerability repealing methods of the punk-spider, which includes the general public, or we can say the end-user to account because they are people getting information about the weaknesses on the website and can try to exploit these bugs.

Other participants are industry people who are commenting or giving their views on the release of punk-spider again in the market. Electronic Frontier Foundation (EFF) state wired that there will be very severe effects of punk-spider and one of the EFF's analysts Karen Gullo said that it's hard to fix vulnerabilities fast as compared to the speed of breaches and this tool only promotes more breaches by providing a starting point to the attackers. Also, a well-known hacker, Jeremiah Grossman, commented that the test punk-spider is using is illegal and this type of malicious testing can be illegal under the Computer Fraud and Abuse Act.

Katie Moussouris, a known voice in the security industry speaks in favour of this tool and said that these are vulnerabilities that lead to breaches and a tool like this is just revealing them.

Reduced List of Participants

Potentially, Punk-Spider's developers, websites administrators and the general public including attackers mean people with bad intentions are the main participants. As, in this case, the Punk-spiders revealing method affects the admins and attackers as end-users can benefit from these things. So, these are the main participants of this case study.

Reasonable Assumption and legal Consideration

The things we know about the Punk-spider is revealing the nature of Punk-Spider, the developers of Punk-Spider said that are trying to make the internet safer by putting pressure on admins to fix vulnerabilities, which shows the motive of Punk-Spider developers.

Also, in a new version of Punk-Spider they are considering ethical issues and responsive disclosure very seriously, but still, they are not considering their testing methods. As Jeremiah Grossman said, Punk-Spider's methods are not legitimate and even the

developer Alejandro Caceres said that they don't know about the legal considerations, they are only trying to do the right things.

Some laws allow to act against the disclosure parties, but disclosure consequences are not clear in these laws. Laws like CFAA (Computer Fraud and Abuse Act of 1984 (CFAA)) and State Anti-Hacking Laws and DMCA (the Digital Millennium Copyright Act of 1998) from the United States of America and even the CEPS task force also try to implement a policy called CVD (coordinated vulnerability) disclosure in Europe and also they are trying to Implementing government disclosure decision processes (GDDP) throughout Europe, but still, these Laws are not concrete and even sometimes they can vary from country to country and even state to state. And in this case, there is no legal action against Punk-Spider this time because of their improved disclosure policy of disclosure. Features in the newer version allow administrators to probe visitors and even remove their website from search, even now they start reporting admins along with assistants to resolve the problem and even are trying to disclose less information to the general public. So, small features and improvements in the newer version saved Punk-Spider from legal consequences till now. But still, there is a debate in the industry about the revealing nature of Punk-Spider.

Ethical Questions

Some ethical questions that come into mind are related to the disclosure of a vulnerability because this case study is all about the public disclosure of a vulnerability and it's a big issue in the cyber-security sector not only for the Punk-Spider, even independent researchers working in the security industry are part to this matter. In addition to that, other vulnerability scanners in the market may follow a bit different approach they don't reveal things publicly, but still, they are publicly available and anyone use one can use them and a great example is burp-suite and it's a great vulnerability scanner and just put the URL and it will scan the whole website, which means the concern is about the disclosure of the vulnerability. Even a small leakage of information will lead to high-end breaches and can cause financial losses and even loss of privacy.

Analogy

An analogy that perfectly fits in this situation is the security jobs means jobs like a police officer, security personnel, army officers or any other security jobs in which information confidentiality plays a very vital role and events lead to severe consequences. Suppose, the military has some secret mission and they want to destroy a terrorist camp so the information about the mission is only shared among top officers and after the completion of the mission information is provided to the general public but still, the information provided is very limited and they only tell about the mission and process not how they accomplish the mission and it remains secret.

Similarly, it goes when it comes to the disclosure of a vulnerability, researchers must report the vulnerability to the organization and even to the high-level official of the organization so that they know the situation and put some pressure on the admins to fix them as soon as possible. After the vulnerability will be fixed then the researcher or organization can reveal the details about the vulnerability in the public and even the publication of vulnerability must be in a controlled way means just by providing the limited information. The organization and researcher can sign a legal agreement where the company can ask the researcher for a non-disclosure agreement and the researcher should ask for some bounty or even a hall of fame sometime.

Alternative Proposals

There can be potentially few differences to solve the ethical problem and let’s say them optimistic, pessimistic and compromise. So, let's see them one by one.

Let’s talk about the worst-case scenario first, which is getting rid of the Punk-spider means just removing this tool or putting some ban on the tool so no one can use it. It’s is the worst scenario or we can say the worst thing we can do to solve the case because by doing so every participant, in this case, got affected developers of Punk-Spider got affected because they won’t get any profits from the tool because no one uses it and if they removed it from stores online and banned its usage which means no revenue for them. The administrators/organizations got affected because they aren’t able to discover vulnerabilities in their websites and later these can be exploited which leads to huge losses to the company and they can even lose their userbase. Even the general public got

affected because they will not be able to know the security of a website and even those breaches lead to loss of data that belongs to end-users and they can lose their privacy.

The best-case scenario is to make such a path pay which allow administrators to fix the problem as soon as Punk-Spider find it. It’s even better can’t reveal anything to the user until the vulnerability is fixed by the admins of those websites and the Punk-Spider can build a dedicated team with contact and assist admins to fix the problem as fast as they can, until then they can warn the user that there are some security issues on a page rather than just providing them with the nature of the vulnerability.

But, both these scenarios are a bit inefficient, as the first like denying a technological advancement and the second one is very hard to implement, so we need a policy that provides the necessary information to the end-user without compromising the security of a website. So, the best pay is to limit the information provided to the end-user that even if some attacker wants to attack the website it will take some and in this time admins should repair the problem. For example, suppose there is a cross-site scripting vulnerability in a website Punk-spider can only display that there is possible XSS possible but don’t describe the nature of the attack and the payloads used for the attack then if the attacker wants to test the page it will take some time to get correct payload and in meantime, website team can repair it and Punk-Spider team can assist them in resolving the problem. The developer of Punk-Spider is working on the best methods to provide a subset of information to a user via a searchable database.

The ethical theory that influenced the choices proposed

These types of tools are always a part of the controversial topic of vulnerability disclosure and there are many norms and policies which are needed to be worked on, the thought process I used to process this case providing solutions and the conclusion is based on the Consequence-based ethical theory means that my decisions are purely based on the benefit of public or we can say for the betterment of the public and I am not considering the results based on Utilitarian ethical theories even utilitarianism is similar to consequentialism but it says that advantages outweigh disadvantages but I believe in this case it's not true because with vulnerabilities their comes to a risk of exploiting that’s why I am only considering my results based on a consequentialism.

Conclusion

To conclude, I would say that tools like Punk-Spider may be very efficient in finding or searching for vulnerabilities and even they are using better methods to scan the web and have better payloads and methods to find weaknesses in a website than their counter-parts and helping in making the web secure. Still, they are no proper policies and methods for disclosure methods available and even the organizations are not ready for these tools because of a lack of security experts in these firms and even with the availability of experts, there are many chances of breaches. So, in my belief and taking into consideration consequentialism theory I would say these tools can only be beneficial for society when proper policies and laws should be implemented about the consequences of using these tools, it's better to use tools like Punk-Spider after proper implementation of vulnerability disclosure laws and policies.

References

1. "ACM Ethics." ACM Ethics, ethics.acm.org/.
2. "responsible disclosure and ethics." Punk Spider, punkspider.org/disclosure.html.
3. "Case: Making Vulnerabilities Visible." SCU.EDU, https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/making-vulnerabilities-visible-a-cybersecurity-ethics-case-study/.
4. "Article: A Controversial Tool Calls Out Thousands of Hackable Websites." WIRED, https://www.wired.com/story/punkspider-web-site-vulnerabilities/#intcid=_wired-homepage-right-rail_ccc01eef-4405-4b6c-99ec-6b49d3c40e41_popular4-1
5. "Article Law: To Disclose or Not Disclose: The Ethics of Vulnerability Disclosure", medium, https://medium.com/@ptcrews/to-disclose-or-not-disclose-the-ethics-of-vulnerability-disclosure-aaf09c1ab4b0**.**
6. "Article Law: Protecting Europe against software vulnerabilities.", CEPS, https://www.ceps.eu/ceps-publications/protecting-europe-against-software-vulnerabilities-its-time-act/