PunkSpider: a real-world cybersecurity ethics case study

Part 1: The Case Study

PunkSpider is a mass-scale website monitoring tool that actively crawls through the entire web to find common vulnerabilities and exploits, the found vulnerabilities of the millions of websites will then be publicly disclosed on the tool's search engine where it can display or probe target URLs for its vulnerabilities. This tool is created with the purpose of forcing the site owners to fix these issues: the site administrators will be repeatedly "fuzzed" until the vulnerabilities are patched[1].

PunkSpider was initially created in 2013 and its first debut, people questioned the harmful side effects of this service, as it "was enabling blackhat hackers—and violating the Computer Fraud and Abuse Act in the process." It was able to anonymously elicit vulnerabilities on websites without authorization from the sites' owners, which treads the line of its legality. It was originally hosted by Amazon Web Services (AWS), but due to Amazon "repeatedly booting" PunkSpider from AWS as multiple abuse reports from web administrators are received, and the constant running cost of the service, it was shut down in 2015[2].

However, in 2021, the company and development team behind PunkSpider are acquired by QOMPLX, and PunkSpider has been re-released and improved. It allowed websites to detect PunkSpider's anonymous probing, and opt out of its search engine to not have their vulnerabilities publicly shown, however, the unconsented probing is still present. The new PunkSpider has been proven effective, finding massive security flaws in Kickstarter and LendingTree's websites, but its ethical issues are still in question[2].

Part 2: The Essay – "What should we do to reduce the negative impacts of this technology?"

Although PunkSpider has been improved to give the probed sites choices to opt out, there are still many negative impacts this product can cause unintentionally. In this report, a few of these issues will be discussed and potential solutions will be provided to attempt to reduce harm to the stakeholders.

Firstly, PunkSpider conducts unconsented vulnerability exploitation and penetration testing on websites and exposes them[2]. Although probed websites can opt out of the vulnerability search engine, the security rating and category of existing exploits are still shown with the Chrome browser extension, even if the results aren't entirely accurate[3]. This damages the reputation of the targeted website which leads to user distrust and causes potential users losses or revenue losses, which has happened in the case of Kickstarter and LendingTree. Additionally, many website owners don't have the corresponding capabilities to fix the exposed vulnerabilities themselves nor the budget to hire security professionals. PunkSpider intends to help push website owners to fix these issues[4], rather than leave incapable website owners stranded and exposed, or intentionally cause financial losses by publicly disclosing the vulnerabilities.

A measure to solve this problem could be requesting approval from the website owners before proceeding with the probing, if a website doesn't wish to engage, PunkSpider can show that website as "Unscanned" or "Unapproved by PunkSpider" to indicate to users the

potential danger for using this website. In this way, even if no vulnerability is exposed, security-cautious users of the website would still be driven away, hence pushing the website owners to either give consent to the security scanning or fix the underlying vulnerabilities, achieving the same goal as intended while being able to acquire the consent from website owners. This also doesn't put website owners incapable of fixing exposed issues at risk as they can simply reject the probing entirely.

Another glaring issue is that PunkSpider enables malicious users to use the PunkSpider search engine to find potentially vulnerable targets. Similar Internet of Things (IoT) scanning tools like Shodan and Censys have a reputation in some of the largest hacking forums as a great tool for locating vulnerable website domains and building botnets: a massive network of malware-infected and controlled devices to launch malicious attacks, such as DDoS (Distributed Denial of Service) attacks[5]. Shodan and similar services have also been used in gaining personally identifiable information and IP camera trolling, as they can "get the person's name and have a few people do a quick dox" and "social engineer someone into doing something, and we would get to see it happen live on cam."[5] Another case is that revealing specific vulnerabilities to the public effectively increases the likelihood that an already vulnerable website will be penetrated and exploited first before the web administrators can step in and patches these vulnerabilities, giving website owners insufficient time to remedy existing issues[2]. In these cases, the damage PunkSpider causes to internet security massively outweighs its benefits.

Currently, the malicious usages of similar IoT monitoring tools heavily rely on their public API (application programming interface), where customized malicious programs can be made using the API[5]. Hence, a potential solution to this problem is to restrict access and tighten user control of PunkSpider's API, making it entirely private or requiring personally identifiable information to gain access. This can be also achieved by implementing authentication for the API such as by allocating API keys and adding a limit on the number of website scan requests a user can make to make sure the API can't be used to do massive scanning for botnet building. This would effectively reduce the quantity and capability of malicious programs created using PunkSpider and to an extent prevent the unintentional harmful consequences of this tool. Regarding the issue that insufficient time is given to website owners to fix the vulnerabilities by directly releasing them to the public, PunkSpider can try to notify website owners first and provide them with a time limit before these vulnerabilities are revealed, hence reducing the potential negative impact to existing users on these websites.

In conclusion, PunkSpider is a powerful yet dangerous tool with good intentions yet many drawbacks that can cause massive unintended damage to internet security. Such a tool requires utmost attention when it can be freely used by the public as any client can use this tool for any kind of purpose. To ensure the success of PunkSpider, the unintended negative consequences should be seriously considered and potential solutions must be carefully implemented.

Bibliography

[1] Montalbano, E. (n.d.). *Reboot of punkspider tool at DEF CON stirs debate*. Threatpost English Global threatpostcom. Retrieved November 19, 2022, from https://threatpost.com/punkspider-def-con-debate/168223/

[2] Greenberg, A. (2021, July 27). *A controversial tool calls out thousands of hackable websites*. Wired. Retrieved November 19, 2022, from https://www.wired.com/story/punkspider-web-site-vulnerabilities/

[3] Punkspider. (n.d.). Retrieved November 19, 2022, from https://punkspider.io/wtv.html

[4] Raicu, I. (n.d.). *Making vulnerabilities visible*. Markkula Center for Applied Ethics. Retrieved November 19, 2022, from https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/making-vulnerabilities-visible-a-cybersecurity-ethics-case-study/

[5] Bada, M., & Pete, I. (2020). *An exploration of the cybercrime ecosystem around Shodan* (pp. 1–8). Cambridge, UK: University of Cambridge.