

Analysis of Making Vulnerabilities Visible

What is the main ethical dilemma?

Show the vulnerabilities of a site without your consent. Well, anyone can exploit them without prior notice.

Who are the actors involved in this case?

PunkSpider developers, people who use the site and the owners of the sites analyzed.

What ethical issues do you spot in this scenario?

Leaking of vulnerabilities to the general public.

Consider the case through the ethical lenses of rights, justice, utilitarianism, virtue, and the common good; what aspects of the ethical landscape do they highlight?

Due to the scope of the rights of the people who use the analyzed site, it could be said that the privacy of their data is being violated. Since anyone who exploits the security breach could have access to said data.

Regarding utilitarianism, it would have to be taken into consideration for users who exploit vulnerabilities for their own benefit, without informing the company. This is an activity punishable by law. There should be a framework in which the use of found vulnerabilities is restricted to members of the company during an admissible time interval. This grace period would allow the company in question to resolve the vulnerability.

Does the inclusion of an opt-out feature change your ethical analysis of the project? If so, how?

It would make a difference if a reasonable response time is given to such an exclusion, and if the vulnerability data is not published until the company patches the problem. The ethical exchange position would be respecting the data protection laws.

What could be the possible consequences of disclosing vulnerabilities?

- Violation of data protection laws, for users of the exposed site.
- Damage to the public image of the company to which the vulnerability analysis was carried out.
- Multiple attacks on the services offered by the site of the analyzed company.

Which principles of the ACM's Code of Ethics are violated in this case? Why?

- The "respect for privacy", because data protection laws could be violated.
- "Access to information and communication resources only when authorized, or when necessary to protect the public good" since the analyzed page does not consent to such analysis, and the information possibly disclosed may not be in the public domain.
- "Avoid harm" since the information obtained from exploiting the vulnerabilities could be used for malicious purposes.

Which local laws (from Ecuador) could control this type of business practice?

The Organic Reformatory Law of the Organic Integral Penal Code to Prevent and Combat Digital Sexual Violence and Strengthen the Fight Against Computer Crimes.