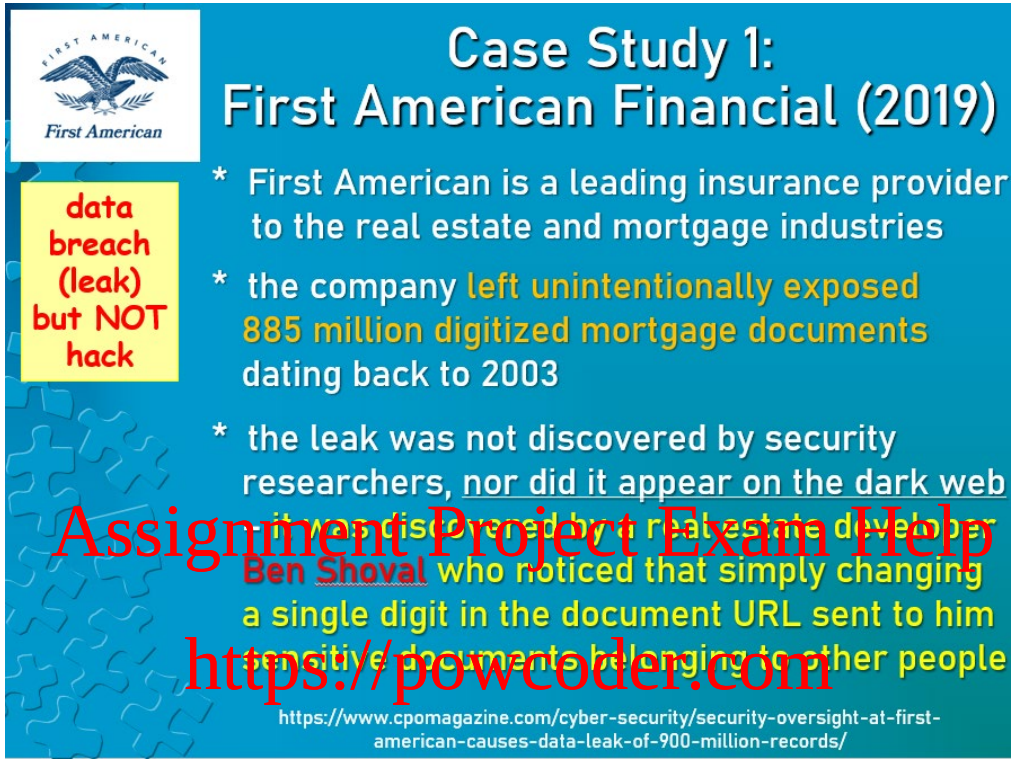


01:23:49 BO: In Ben Shovals case, does he have the right to ask for a reward?

01:24:03 BO: Or do they just fix the issue and move on

01:25:35 Aly Wakif: Even though they approached the bank quickly, were they still at risk legally for disclosing it? (ie the bank's lawyers could come after them anyways?)

Internet and its components:

Internet community would like software & network vulnerabilities to be discovered by 'good' and not by 'bad' guys.

security researchers

vulnerability disclosure

organization

Security researchers should keep looking for various vulnerabilities in various 'components' of the Internet.

Security researchers should know that poking around a software or software system could put them in trouble.

'Smart' organization should know that it is impossible to build a bulletproof software or software-system.

'Smart' organization should incentivize security researchers to discover and report vulnerabilities in their software products and systems.

OWASP (Open Web Application Security Project): Vulnerability Disclosure Cheat Sheet

https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html

Organisations should:

- Provide a clear method for researchers to securely report vulnerabilities.
- Clearly establish the scope and terms of any bug bounty programs.
- Respond to reports in a reasonable timeline.
- Communicate openly with researchers.
- Not threaten legal action against researchers.
- Request CVEs where appropriate.
- Publish clear security advisories and changelogs.
- Offer rewards and credit.

https://www.securitymagazine.com/articles/89372-bug-bounty-programs-an-emerging-best-practice

Cyber Security News | Cyber Tactics | Cyber

Bug Bounty Programs: An Emerging Best Practice

OWASP (Open Web Application Security Project): Vulnerability Disclosure Cheat Sheet

https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html

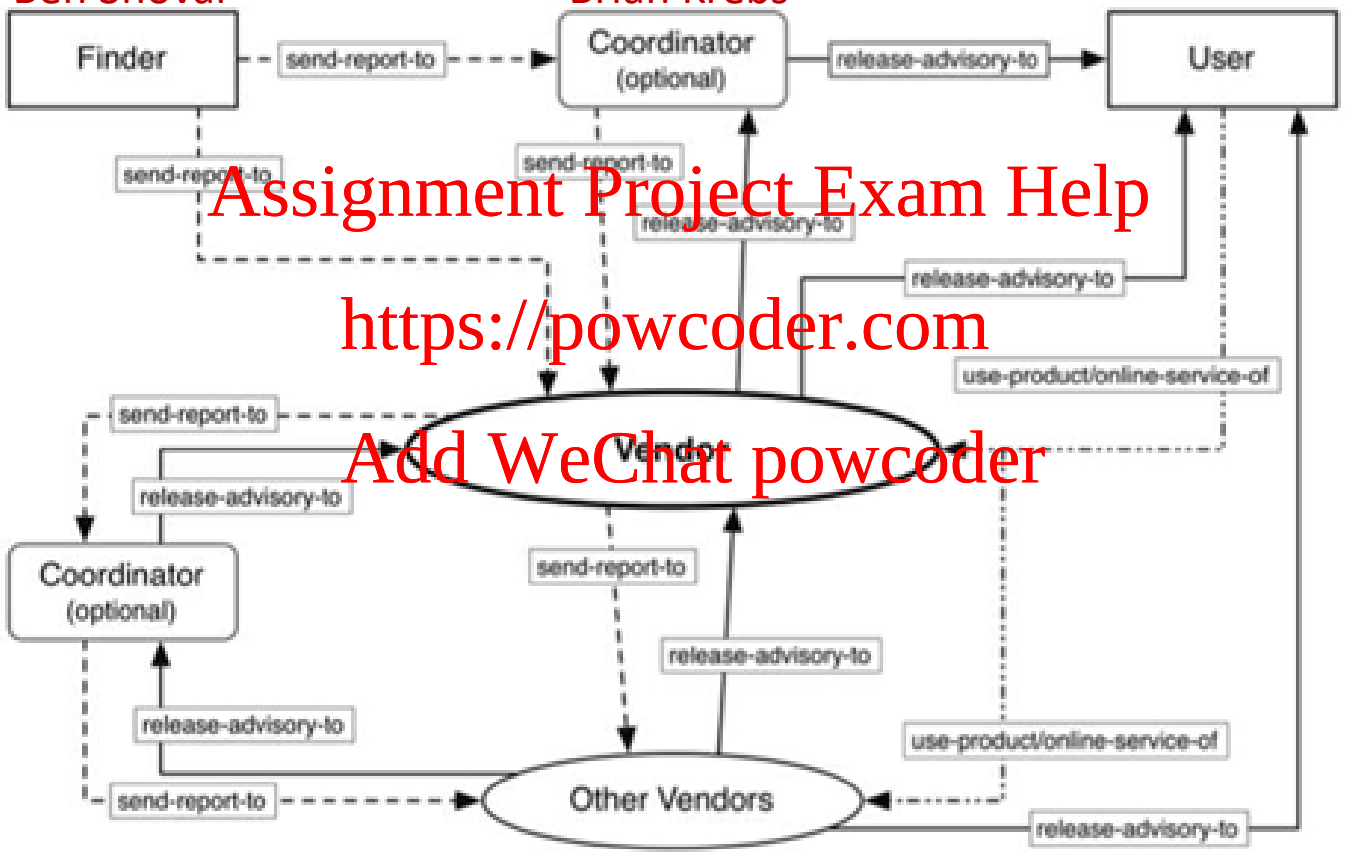
Researchers should:

- Ensure that any testing is legal and authorised.
- Respect the privacy of others.
- Make reasonable efforts to contact the security team of the organisation.
- Provide sufficient details to allow the vulnerabilities to be verified and reproduced.
- Not demand payment or rewards for reporting vulnerabilities outside of an established bug bounty program.

ISO/IEC 29147 and ISO/IEC 30111: Vulnerability Disclosure & Handling Standards for Vendors

Ben Shoval

Brian Krebs



https://www.first.org/global/sigs/vulnerability-coordination/multiparty/FIRST-Multiparty-Vulnerability-Coordination.pdf

OWASP (Open Web Application Security Project): Vulnerability Disclosure Cheat Sheet

Methods of Disclosure

Private Disclosure

In the private disclosure model the vulnerability is reported privately to the organisation. The organisation may choose to publish the details of the vulnerabilities, but this is done at the discretion of the organisation, not the researcher, meaning that many vulnerabilities may never be made public. The majority of bug bounty programs require that the researcher follows this model.

Full Disclosure

With the full disclosure approach, the full details of the vulnerability are made public as soon as they are identified. This means that the full details (sometimes including exploit code) are available to attackers, often before a patch is available. The full disclosure approach is primarily used in response of organisations ignoring reported vulnerabilities, in order to put pressure on them to develop and publish a fix.

Question:

Is ‘private disclosure’ the best way to go??

Think of:

- Past hacks that have not been explained …
- Companies/individuals that do not apply every patch …

Methods of Disclosure

Responsible or Coordinated Disclosure

Responsible disclosure attempts to find a reasonable middle ground between these two approaches. With responsible disclosure, the initial report is made privately, but with the full details being published once a patch has been made available (sometimes with a delay to allow more time for the patches to be installed).

In many cases, the researcher also provides a deadline for the organisation to respond to the report, or to provide a patch. If this deadline is not met, then the researcher may adopt the full disclosure approach, and publish the full details.

Google's Project Zero adopts a similar approach, where the full details of the vulnerability are published after 90 days regardless of whether or not the organisation has published a patch.