Out-of-Scope Bounty

Chris Fullerton case study week 3

In this scenario a student performing a bounty found a critical flaw and was out of scope when the student found it. What the student should do is to make sure not to further exploit the flaw which would hold the student as a threat actor and hold them liable for an attack. The student then should not submit the bounty because it's out of scope so they would not get credit and would possibly be held as unauthorized access causing more issues. The student would need to find another route to contacting the company such as an email or phone call to security outputs in the company. If none existed the student could reach out to CERT or platforms assistant to handle the situation more professionally and legally. The student should keep the report to minimum information such as just showing proof and not personal or important information that could further cause harm.

What not to include in the report would be things like the actual exploit code, this could cause harm if it became leaked through the contact between you and the business. The student should not include important data if the flaw has access to sensitive information such as medical records, passwords, billing information, etc. If medical records were shared even as proof of a flaw the student would then be violating the HIPPA act causing serious legal troubles. The student should not include any public data links because that further increases risk of the flaw becoming public. The student should also wait and not contain payment information because then it may look like an attacker using ransome rather than an out of scope bounty.

Public disclosure should only happen if the student has contacted the business several times and has not had a single reply. They should wait for at least 90 to 120 days. The public disclosure should help protect the student but only if they followed guidelines not to harm the business physically by posting the exploit code.