

# Security incident report

## Section 1: Identify the network protocol involved in the incident

The network protocol was Hypertext transfer protocol (HTTP).

## Section 2: Document the incident

A disgruntled baker made multiple attempts to log in to the admin side of the website and eventually succeeded. They then edited the JavaScript of the page, causing users to download a file to their computers. This file has been slowing down their computers and redirecting them to a fake website similar to the original, where leaked recipes are posted. The cyber security analyst on our end used a sandbox environment to examine more of what occurred and looked at the logs.

## Section 3: Recommend one remediation for brute force attacks

Based on how this problem arose I would recommend implementing a limit to how many passwords a user may try. Because of the ample amount of unmonitored login attempts from the baker they eventually were able to guess the password.