# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| The incident involved the compromise of the Hypertext Transfer Protocol (HTTP). By running tcpdump and visiting the website yummyrecipesforme.com, the issue was identified. The evidence, gathered in a DNS and HTTP traffic log file, indicated that the malicious file was delivered to users' computers through the HTTP protocol at the application layer. | |
|

| **Section 2: Document the incident** |
| --- |
| Several customers contacted the website owner, reporting issues where they were prompted to download a file for a supposed browser update, resulting in their computers slowing down. The website owner faced difficulty logging into the web server and found their account locked.  To investigate, a cybersecurity analyst used a safe environment to check the website, capturing data using tcpdump. The analyst downloaded a file, thinking it was a browser update, and got redirected to a fake site resembling the real one (yummyrecipesforme.com).  Analyzing the data, the analyst noticed the browser initially connecting to yummyrecipesforme.com and then, after downloading the file, switching to the fake site (greatrecipesforme.com). A senior cybersecurity professional examined the website code and the downloaded file, finding added code that tricked users into downloading a harmful file, disguised as a browser update. The team suspects the attacker used a brute force attack to access the website owner's account, leading to a compromised admin password and the harmful file affecting users' computers. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| To make things safer, the team suggest to use two-factor authentication (2FA) to stop hackers from guessing passwords. Users will need to prove they're the real deal by entering a one-time code (OTP) sent to their email or phone. Only after confirming both their usual login info and the OTP will they get into the system. This makes it hard for attackers trying to guess passwords because they need more than just that. |