# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The incident involved the Hypertext Transfer Protocol (HTTP). Since the issue pertained to accessing the web server for yummyrecipesforme.com, we can determine that web page requests to servers involve HTTP traffic. Additionally, when we ran `tcpdump` and accessed the yummyrecipesforme.com website, the corresponding `tcpdump` log confirmed HTTP protocol usage. The malicious file was observed being transmitted to users' computers via HTTP at the application layer. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| A former employee/s decided to lure users to a fake website with malware. They perform a brute force attack to obtain the password of an admin user. They were able to access the admin panel and change the website’s source code. After this, they changed the password of the admin account. Users complained to the company that they are prompted to download a file. The downloaded file redirects the website of yummyrecipesforme.com to a fake website greatrecipesforme.com. After downloading the file, their personal computers began running more slowly. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| * Implement secure password formats. Include one capital letter, one small letter, numbers, and special characters with at least 8 characters in length. * Implement two-factor authentication to prevent unauthorized access. * Have a forgot password module to recover the changed password. |