# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The network protocol that was involved in this incident was the Application layer, in the TCP/IP model. The problem within the incident occurred directly from the Hyper Text transfer protocol. The malicious file can be observed being transported to the users’ computers using the HTTP protocol at the application layer. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Firstly, we were notified about this incident due to several customers contacting us about our website needing them to download and run a file, and for them to update their browsers. Since downloading the file, their computers were running noticeably slower.  The incident occurred due to a brute force attack on an admin password. There is evidence of JavaScript code written into the transport layer of our website. Communication between the source and the intended destination of our website shows a blocked DNS request, and is redirected to a separate malicious website. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| To prevent this attack in the future, please use a stronger admin password, enforce two-factor authentication, and set a number of login attempts so that it may not be continuously attacked. |