# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The protocol involved in the incident is the Hypertext transfer protocol (HTTP). Since the issue was with accessing the web server for yummyrecipesforme.com, we know that requests to web servers for web pages involve http traffic. Also, when we ran tcpdump and accessed the yummyrecipesforme.com website the corresponding tcpdump log file showed the usage of the http protocol when contacting the . The malicious file is observed being transported to the users’ computers using the HTTP protocol at the application layer. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| A ex-employee used there knowledge of system to gain access to website by logging in as admin and loading in a java script to the web page to redirect traffic to none host site. The tcpdump shows traffic being diverted. The websites source code was reviewed and seen to be edit to move data from host site. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| My recommendation to avoid attacks like this is to use a password manager. Another thing to remember is to change your password often. |