Security incident report DNS

Section 1: Identify the network protocol involved in the incident

The network protocol involved is the DNS protocol.

Section 2: Document the incident

Ex-employee used a brute force attack to obtain access to the website's source code. From there the threat actor tampered with the code and had the website be redirected to a different page that prompted visitors to download a file embedded with malware.

Section 3: Recommend one remediation for brute force attacks

A security control that could be easily implemented is stronger password policies and segmentation. The reason this attack was successful was due to the ex-employee's knowledge of default passwords. If the admin account had stronger password protections a large amount of damage would've been avoided.