Security incident report

Section 1: Identify the network protocol involved in the incident
• **DNS:** Attacker used it to find the fake website's address. • **HTTP:** How normal people browsed the website, and how the bad code got sent to their computers. • **TCP:** Made sure all the website data and the malware got through properly.

Section 2: Document the incident
Someone hacked our site, yummyrecipesforme.com. Looks like they used the admin panel, which still had the easy default password. We think it might be a pissed-off ex-employee. They put in sneaky code (JavaScript) that tricked visitors into downloading a bad file when they came to the site. This file was malware that sent them to a fake website (greatrecipesforme.com) that probably stole their info or messed with their computers.

Section 3: Recommend one remediation for brute force attacks
IMMEDIATELY change the admin password to something strong!! This should NEVER have been left as the default. Also, we need to get some kind of two-factor verification set up on the admin panel, so even if someone guesses the password, they can't get in without another code or something.