Incident handler's journal

Date: 15-01-2025	**Entry: 001** Website Compromise and Malware Delivery via JavaScript Injection
Description	The website yummyrecipesforme.com was compromised through a brute force attack on its administrative panel. An attacker injected malicious JavaScript code that prompted site visitors to download a fake "browser update" file, which upon execution redirected users to a second malicious site (greatrecipesforme.com) hosting malware. Multiple users reported slow system performance and suspicious activity following the download. DNS and HTTP traffic captured during analysis confirms this behavior.
Tool(s) used	tcpdump DNS lookup HTTP traffic inspection Manual browser testing in sandbox environment Source code review of yummyrecipesforme.com
The 5 W's	**Who** caused the incident? A former employee (insider threat) who still had knowledge of or access to default administrative credentials. **What** happened? The attacker performed a brute force attack on the admin panel, accessed the web server, injected JavaScript code that tricked users into downloading a malicious file, and redirected them to a malware-laden website. **When** did the incident occur? Initial malicious DNS queries and HTTP traffic occurred between 14:18 and 14:25 on the day of analysis. The exact time of compromise was likely several hours earlier, as multiple user reports were already received. **Where** did the incident happen? On the production web server of yummyrecipesforme.com. Secondary activity occurred on greatrecipesforme.com, hosted on a different IP. **Why** did the incident happen? The admin interface was left unprotected by multi-factor authentication and still used a default password, making it vulnerable to brute force attacks. There were no intrusion prevention or alerting systems in place to detect or stop the attack.

Additional notes	Immediate action was taken to take the site offline and begin forensic analysis. Users were notified of potential compromise and instructed not to run any downloads from the site. The malware file and redirect script were analyzed and isolated in a sandbox. DNS and traffic logs confirmed the flow from yummyrecipesforme.com to greatrecipesforme.com. Future remediation will include MFA enforcement, brute force detection, and source code integrity checks.