# **Security incident report**

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| **DNS (Domain Name System)**: This protocol was used to resolve the domain names "yummyrecipesforme.com" and "greatrecipesforme.com" into their respective IP addresses. DNS is a foundational Internet service that translates human-readable domain names (like "yummyrecipesforme.com") into machine-readable IP addresses.  **HTTP (Hypertext Transfer Protocol)**: This is the primary protocol used for transmitting web pages over the Internet. It was utilized in the incident for several purposes:  The browser initiated HTTP requests to "yummyrecipesforme.com" to retrieve the webpage.  The malicious JavaScript embedded in the webpage used HTTP to initiate the download of the malware to the user's device.  After the malware was installed, it redirected the browser to initiate another HTTP request to "greatrecipesforme.com". | |
|

| **Section 2: Document the incident** |
| --- |
| A former employee executed a brute force attack on the administrative panel of Yummyrecipesforme.com by exploiting the use of a default password. Upon gaining access, they embedded malicious JavaScript in the website’s source code. This script automatically prompted visitors to download and execute a file that redirected them to a fake, malware-infested version of the site hosted at greatrecipesforme.com. This attack resulted in unauthorized software installation and potential compromise of visitor's systems.  **Key Events**:  Brute Force Attack: Attacker gained access to the admin panel using a default password.  Malicious Code Injection: Embedded JavaScript prompted a malware download.  Redirection: Users were redirected to a malicious site, potentially compromising their devices.  User Complaints: Customers reported unusual prompts to download files for accessing recipes.  Loss of Access: The legitimate website owner was unable to access the admin panel.  **Network Protocols Involved:**  DNS (Domain Name System): Used for resolving the domain names to IP addresses.  HTTP (Hypertext Transfer Protocol): Used to retrieve web pages and initiate malware downloads.  Impact:  Privacy Risk: Potential theft of personal and financial information from users.  System Integrity: User systems may be compromised and used for further malicious activities.  Reputational Damage: Loss of trust in Yummyrecipesforme.com among customers and partners.  **Immediate Actions Taken:**  Site Takedown: Temporarily disabled access to the site to prevent further downloads.  Password Reset: Admin credentials were reset with the help of the hosting provider.  Malware Analysis: Conducted in a sandbox environment to understand behavior and impact.  Code Cleanup: Malicious JavaScript was removed from the source code.  **Recommendations:**  Implement stronger password policies and change default credentials before deployment.  Introduce account lockout and rate limiting to mitigate brute force attacks.  Regular security audits and penetration testing should be scheduled.  Adopt multi-factor authentication (MFA) for administrative and sensitive accounts.  Increase security awareness training for employees focusing on cybersecurity best practices |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| **Assessment of Needs**: Identify critical systems that need MFA, such as administrative panels.  **Selection of MFA Solution:** Choose an appropriate MFA method (e.g., SMS codes, authenticator apps, hardware tokens, biometrics).  **System Integration**: Integrate MFA with existing IT systems and authentication processes.  **User Enrollment and Education:** Enroll users into the MFA system and educate them on its use and benefits.  **Regular Monitoring**: Continuously monitor the effectiveness of the MFA and make adjustments as necessary.  **Policy Updates**: Revise security policies to include MFA requirements and compliance. |