Security Incident Report

Section 1: Network protocol involved in the incident

Layer	Evidence in capture	Purpose in this incident
DNS (53/ UDP)	dns.google.domain queries (35084+ A? yummyrecipesforme.com) and replies (A 203.0.113.22)	Converted the human-readable host-names `yummyrecipesforme.com` and later greatrecipesforme.com into IP addresses so the browser could connect to the servers.
TCP (Transmission Control Protocol)	SYN / SYN-ACK / ACK three-way handshakes on ephemeral ports 36086, 56378	Provided reliable transport for the HTTP sessions that followed.
HTTP (80/ TCP)	`GET / HTTP/1.1` requests and flows labelled `.http`	Carried both the legitimate page request to yummyrecipesforme.com *and* the forced redirect and malware download that sent the victim to greatrecipesforme.com.

Note: No encrypted traffic (e.g., HTTPS) appears—everything occurs in clear-text HTTP, which made it easy for the attacker to tamper with the site and for us to observe the compromise.

Section 2: Document the incident

14:18:32 — DNS Resolution for yummyrecipesforme.com

```
14:18:32.192571 IP your.machine.52444 > dns.google.domain: 35084+ A? yummyrecipesforme.com. (24)
```

```
14:18:32.204388 IP dns.google.domain > your.machine.52444: 35084 1/0/0 A 203.0.113.22 (40)
```

What's happening:
Your machine asks Google's DNS for the IP of yummyrecipesforme.com.

Google replies with 203.0.113.22.

This is the first contact—before HTTP starts—indicating the browser is trying to load the site.

14:18:36 — TCP 3-Way Handshake and HTTP Request

```
14:18:36.786501 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [S], seq 2873951608, win 65495, options [mss 65495,sackOK,TS val 3302576859 ecr 0,nop,wscale 7], length 0
```

```
14:18:36.786517 IP yummyrecipesforme.com.http > your.machine.36086: Flags [S.], seq 3984334959, ack 2873951609, win 65483, options [mss 65495,sackOK,TS val 3302576859 ecr 3302576859,nop,wscale 7], length 0
```

```
14:18:36.786529 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [.], ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 0
```

```
14:18:36.786589 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 73: HTTP: GET / HTTP/1.1
```

What's happening:
The browser establishes a TCP connection to the website on port 80 (HTTP) using a three-way handshake:

[S] = SYN
[S.] = SYN-ACK
[.] = ACK

Then it immediately sends a **GET /** request.

This means the browser is loading the homepage over HTTP.

Attack Starts – Malware Delivered

...<a lot of traffic on the port 80>…

What's implied here:
The packet capture notes high traffic following the initial GET request.

This implies the site sent a large payload, including:
JavaScript prompting a malware file download.
A redirect script pointing to the second domain: greatrecipesforme.com.

14:20:32 — DNS Lookup for the Second Domain (Redirect)

```
14:20:32.192571 IP your.machine.52444 > dns.google.domain: 21899+ A? greatrecipesforme.com. (24)

14:20:32.204388 IP dns.google.domain > your.machine.52444: 21899 1/0/0 A 192.0.2.17 (40)
```

What's happening:
The browser executes the JavaScript redirect, asking for the IP of the malicious redirect domain.
DNS resolves greatrecipesforme.com to 192.0.2.17.

14:25:29 — New Connection to the Malware Site

```
14:25:29.576493 IP your.machine.56378 > greatrecipesforme.com.http: Flags [S], seq 1020702883, win 65495, options [mss 65495,sackOK,TS val 3302989649 ecr 0,nop,wscale 7], length 0

14:25:29.576510 IP greatrecipesforme.com.http > your.machine.56378: Flags [S.], seq 1993648018, ack 1020702884, win 65483, options [mss 65495,sackOK,TS val 3302989649 ecr 3302989649,nop,wscale 7], length 0

14:25:29.576524 IP your.machine.56378 > greatrecipesforme.com.http: Flags [.], ack 1, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649], length 0

14:25:29.576590 IP your.machine.56378 > greatrecipesforme.com.http: Flags [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649], length 73: HTTP: GET / HTTP/1.1
```

What's happening:
Same TCP handshake + HTTP request pattern now repeats for the second site, confirming that:
The redirect script from yummyrecipesforme.com worked.
The browser has now landed on a new site hosting more malware or a phishing page.

What we see in the timeline

Log Line	Meaning
DNS for yummyrecipesforme.com	Start of page load
TCP + HTTP GET	Initial request to legitimate site
High port 80 traffic	Malicious code and payload delivered
DNS for greatrecipesforme.com	Triggered by JavaScript
TCP + HTTP GET to new domain	Victim fully redirected to attacker-controlled server

Section 3: Root cause, impact and Indicators of Compromise (IoC)

Root cause
A former employee carried out a brute-force attack against the web-host's admin interface (still using its default password).

After gaining access they inserted malicious JavaScript that weaponised every visit to yummyrecipesforme.com.

Impact
Customers who accepted the download executed malware, experienced system slow-downs, and unknowingly visited a phishing domain.

Trust in the brand and website integrity has been damaged; incident is classed as
High severity.

Indicators of Compromise (IoCs)
Domains: greatrecipesforme.com, any other sub-domains seen in future variants.

IPs: 192.0.2.17, 203.0.113.22 (until verified clean).

Hash of the dropped executable (see malware sandbox report).

Inserted JavaScript snippet (saved in forensic copy of index.html).

Section 4: Key remediation against brute-force attacks

Introduce MFA (Multi-Factor Authentication)—require something the user knows (password) plus something they have (TOTP code, hardware token, or FIDO2 key) for every administrative login.

Even if a weak or default password remains in place, the second factor blocks automated password-guessing attacks.

Combine MFA with rate-limiting / account lock-out, mandatory strong-password policy, and server-side logging with alerting for repeated failures to create layered protection.

Implementing MFA (Multi-Factor Authentication) is the single most effective safeguard and aligns with current best-practice guidance from NIST 800-63 and OWASP ASVS.

Apendix A: Frameworks

1. NIST Cybersecurity Framework (NIST CSF 2.0)

Relevance: Full-lifecycle support for detecting, responding to, and recovering from this type of incident.

NIST CSF Function	Relevant Activities in This Scenario
Identify	Understand critical assets (e.g., admin panel, website code), user roles, and security gaps like weak passwords.
Protect	Implement MFA, password policies, and security hardening of web servers.
Detect	Use intrusion detection systems (IDS), logs, and anomaly detection to spot brute-force attempts and code changes.
Respond	Conduct incident analysis (like with tcpdump), isolate affected systems, and communicate with users.
Recover	Restore a clean backup of the site, reset credentials, and apply lessons learned through improved policies.

---

2. MITRE ATT&CK Framework

Relevance: Maps adversary tactics, techniques, and procedures (TTPs) used in this attack.

Tactic	Technique Example Used
Initial Access	Brute Force (T1110)
Execution	User Execution: Malicious file (T1204.002)
Persistence	Account Manipulation (T1098) – attacker changed admin password
Command & Control	Web Service: Malicious domain (greatrecipesforme.com)
Defense Evasion	Masquerading the malware as a browser update

---

3. OWASP Top 10

Relevance: Since this is a **web application compromise**, OWASP helps prioritize weaknesses in the app.

OWASP Risk	Scenario Relevance
A01:2021 – Broken Access Control	Admin login using default credentials without brute-force prevention.
A05:2021 – Security Misconfiguration	No MFA, no lockout after failed logins, default credentials.
A06:2021 – Vulnerable and Outdated Components	Possible outdated CMS or plugins enabled the JavaScript injection.
A08:2021 – Software and Data Integrity Failures	Malicious changes to the site's source code.

———————————————————————————————

4. ISO/IEC 27001 / 27002

———————————————————————————————

Relevance: Governance and operational security for information security management systems (ISMS).

Control Domain	Relevance
Access Control (A.9)	Weak admin credentials and no access restrictions.
Operations Security (A.12)	Lack of logging, monitoring, and change detection.
Information Security Incident Management (A.16)	This journal and tcpdump analysis are part of A.16.1.5 "Response to information security incidents".

———————————————————————————————

5. CIS Controls v8

———————————————————————————————

Relevance: Practical implementation recommendations to prevent or detect the same attack.

CIS Control	Description
Control 4: Secure Configuration of Enterprise Assets	Disable default credentials and enforce password complexity.
Control 5: Account Management	Remove old accounts, enforce MFA.
Control 7: Continuous Vulnerability Management	Scan for misconfigurations and JavaScript injection vectors.
Control 13: Network Monitoring and Defense	tcpdump used here; IDS/IPS should be deployed proactively.