

# UK Domain, Email Authentication & PHP2Shell Remediation Playbook

Zero-downtime implementation guide for strict SPF (-all), staged DMARC enforcement (p=reject), 2048-bit DKIM, MTA-STS, TLS 1.3 security headers, and emergency hardening for October 2026 PHP runtime advisories (CVE-2026-109618 & CVE-2026-109619).

## 01 // UK REGULATORY ALIGNMENT

Mapped directly to UK Cyber Essentials v3.2 (2026), NCSC Email Security Guidance, UK GDPR Article 32, SRA, ICAEW, and FCA operational resilience standards.

## 02 // ZERO-DOWNTIME MAIL ROLLOUT

Protect Microsoft 365, Google Workspace, Xero, Sage, SendGrid, HubSpot, and Mailchimp flows while transitioning from p=none to strict p=reject.

## 03 // PHP2SHELL RCE LOCKDOWN

Immediate version verification, OS patching (ondrej/php, remi, IIS), php.ini SAPI isolation, WAF rules, and read-only forensic log triage.

## 04 // BOARD & AUDIT EVIDENCE

Backed by our October 2026 UK North West Professional Services Benchmark and automated CLI verification via `faultypacket_uk_auditor.py`.

## INCLUDED AUTOMATION & TEMPLATES IN THIS PACK

`tools/faultypacket_uk_auditor.py` • `tools/php2shell_local_triage.sh` •  
`templates/cloudflare-email-security-dns.zone` • `templates/nginx-hardening-and-headers.conf` • `templates/apache-htaccess-security.conf` • `templates/iis-web-config-hardening.xml` • `templates/php-ini-production-lockdown.ini` • `templates/mta-sts-policy.txt`

## Table of Contents & Executive Overview

| SECTION | TOPIC & PRACTITIONER DELIVERABLES                                                                    | PAGE    |
|---------|------------------------------------------------------------------------------------------------------|---------|
| Sec 1.1 | UK Executive Summary & Regulatory Mapping (Cyber Essentials v3.2, NCSC, GDPR Art. 32, SRA/ICAEW/FCA) | Page 2  |
| Sec 1.2 | Oct 2026 UK North West Benchmark: Why 73% of Surveyed Firms Are Spoofable                            | Page 3  |
| Sec 2.1 | Zero-Downtime SPF & Third-Party Sender Audit (M365, Google, Xero, Sage, HubSpot, Mailchimp)          | Page 4  |
| Sec 2.2 | Staged DMARC Enforcement (p=none → p=quarantine → p=reject) & 7 Registrar Syntax Guide               | Page 5  |
| Sec 2.3 | 2048-Bit DKIM Rotation, Inbound SMTP TLS (MTA-STS & TLS-RPT) & CAA Certificate Locks                 | Page 6  |
| Sec 3.1 | Emergency PHP2Shell (CVE-2026-109618 & CVE-2026-109619) Patch Matrix & OS Upgrade Paths              | Page 7  |
| Sec 3.2 | Production php.ini Lockdown & Perimeter WAF Rules (Cloudflare, Nginx, Apache, Windows IIS)           | Page 8  |
| Sec 3.3 | Defensive Incident Triage & Read-Only Access Log Hunting (Linux & Windows IIS)                       | Page 9  |
| Sec 4.0 | HTTP Security Header & TLS 1.3 Baseline + Final Go-Live Verification Checklist                       | Page 10 |

### 1.1 UK Regulatory & Insurer Compliance Mapping

Across the United Kingdom, domain spoofing and unpatched edge web servers remain the two primary entry vectors for Business Email Compromise (BEC), conveyancing/invoice diversion fraud, and ransomware initial access. Relying on default registrar DNS records or default php.ini distributions leaves organisations exposed to both direct financial loss and regulatory enforcement.

| UK FRAMEWORK / REGULATOR                              | SPECIFIC TECHNICAL REQUIREMENT                                                                                                                                                | FAULTYPACKET REMEDIATION CONTROL                                                                         |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| NCSC Email Security & Anti-Spoofing Guidance          | Mandates outbound SPF, 2048-bit DKIM signing, enforced DMARC (p=reject), and inbound/outbound TLS encryption via MTA-STS.                                                     | Section 2 Playbook + cloudflare-email-security-dns.zone & mta-sts-policy.txt.                            |
| UK Cyber Essentials v3.2 (IASME 2026 Baseline)        | Requires all internet-facing services to run supported, patched software within 14 days of high/critical CVEs and disable unnecessary OS execution features.                  | Section 3 PHP Patch Matrix ( ≥ 8.5.12 / 8.4.27 / 8.3.36 / 8.2.35) + php-ini-production-lockdown.ini.     |
| UK GDPR Article 32 (ICO Security of Processing)       | Requires "appropriate technical and organisational measures" including encryption in transit (TLS 1.2/1.3, HSTS) and protection against spoofing of data controller identity. | Strict DMARC p=reject + HSTS preload + MTA-STS enforcement + automated HTML audit evidence.              |
| SRA (Solicitors Regulation Authority) & Law Society   | Conveyancing & client account protection: firms failing to implement DMARC p=reject face severe scrutiny if client bank details are spoofed via lookalike/exact-domain email. | Strict -all SPF + p=reject; sp=reject DMARC + wildcard *.domain anti-spoofing TXT records.               |
| ICAEW / ACCA & FCA (SYSC 13 / Operational Resilience) | Accountancy & financial practices handling HMRC, payroll, and client tax data must prevent unauthorized impersonation and web portal clickjacking/credential harvesting.      | Full DMARC enforcement + Content-Security-Policy (frame-ancestors 'self') + X-Frame-Options: SAMEORIGIN. |

#### Key Takeaway for UK IT Managers & Partners:

A DMARC policy of v=DMARC1; p=none; provides

## 1.2 October 2026 UK North West Professional Services Benchmark

In October 2026, FaultyPacket conducted an unintrusive, public DNS and HTTP response header baseline study across **15 established legal, accountancy, and property practices** operating across Liverpool, Manchester, Warrington, Preston, and Wigan. The findings illustrate why automated posture verification is critical:

**73.3% Lacked DMARC Reject Enforcement (11 of 15 Firms)**

5 firms had no `_dmarc` record whatsoever, and 6 firms were stuck on `p=none` (monitoring only), leaving clients vulnerable to exact-domain invoice and conveyancing spoofing.

**93.3% Lacked HSTS & Clickjacking Headers (14 of 15 Firms)**

14 of 15 websites lacked Strict-Transport-Security (HSTS) and Content-Security-Policy / X-Frame-Options headers, and 3 sites failed TLS validation outright.

| BENCHMARK FIRM / SECTOR (UK NORTH WEST)     | MAIL GATEWAY       | SPF POLICY      | DMARC STATUS              | HTTPS & HEADERS        |
|---------------------------------------------|--------------------|-----------------|---------------------------|------------------------|
| JF Law Solicitors (jflaw.co.uk)             | Cloud Spam Gateway | Strict (-all)   | p=reject                  | No HSTS / No CSP       |
| Bell Lamb & Joynson (bljsolicitors.co.uk)   | MiCloud Gateway    | Strict (-all)   | p=reject                  | No HSTS / No CSP       |
| Stephensons Solicitors (stephensons.co.uk)  | Mimecast           | SoftFail (~all) | p=reject                  | No HSTS / No CSP       |
| FDR Law Solicitors (fdrlaw.co.uk)           | Mimecast           | SoftFail (~all) | p=reject                  | No HSTS / No CSP       |
| MSB Solicitors (msbsolicitors.co.uk)        | Hornetsecurity     | SoftFail (~all) | sp=none (Subdomains Open) | No HSTS / X-Powered-By |
| Ashtons Legal (ashtonslegal.co.uk)          | Mimecast           | Strict (-all)   | p=none (No Enforce)       | No HSTS / No CSP       |
| Williamson & Croft (williamsoncroft.co.uk)  | Microsoft 365      | Strict (-all)   | p=none (No RUA)           | No HSTS / No CSP       |
| AC Accountancy (ac-accountancy.co.uk)       | Microsoft 365      | Strict (-all)   | p=none (No Enforce)       | No HSTS                |
| Tax Driven Accountants (taxdriven.co.uk)    | Microsoft 365      | SoftFail (~all) | p=none (No Enforce)       | No HSTS / No CSP       |
| Sapphire Homes (sapphirehomes.co.uk)        | Sophos Hydra       | Weak (?all)     | p=none (No Enforce)       | No HSTS / No CSP       |
| Styles & Co Accountants (stylesandco.co.uk) | Mimecast / M365    | Strict (-all)   | MISSING (_dmarc)          | Headers Present        |
| WatkinsonBlack (watkinsonblack.co.uk)       | None Published     | MISSING         | MISSING                   | No HSTS / No CSP       |
| Watson Solicitors (watsonsolicitors.co.uk)  | None Published     | MISSING         | MISSING                   | TLS Handshake Fail     |
| Haltons Accountants (haltons.co.uk)         | None Published     | MISSING         | MISSING                   | TLS Handshake Fail     |
| Hamlet Homes (hamletwarrington.co.uk)       | Google Workspace   | MISSING         | MISSING                   | SSL Cert Mismatch      |

### Common Failure Patterns Identified in the Field

- The "Set and Forget" p=none Trap:** External IT providers often add `v=DMARC1; p=none`; during initial M365 migration and never return to advance the policy to `p=quarantine` or `p=reject`.

## 2.1 Auditing Senders & Strict SPF (-all) Architecture

Before switching SPF to -all or DMARC to p=reject, you must inventory every legitimate cloud service that sends mail as @yourdomain.co.uk. However, per **RFC 7208 Section 4.6.4**, an SPF record must not trigger more than **10 DNS-querying mechanisms** (include, a, mx, ptr, exists, redirect). Exceeding 10 lookups causes receiving mail servers to return PermError and reject or spam-folder your email.

UK B2B SaaS Sender Reference Table (SPF & DKIM Alignment)

| PLATFORM / SAAS               | OFFICIAL SPF MECHANISM                                           | DNS LOOKUPS          | DKIM & ALIGNMENT NOTES                                                                                              |
|-------------------------------|------------------------------------------------------------------|----------------------|---------------------------------------------------------------------------------------------------------------------|
| Microsoft 365                 | include:spf.protection.outlook.com                               | 2 lookups            | Enable 2048-bit CNAMEs selector1._domainkey & selector2._domainkey in Defender portal.                              |
| Google Workspace              | include:_spf.google.com                                          | 3-4 lookups          | Generate 2048-bit RSA key in Admin Console → Apps → Gmail → Authenticate email.                                     |
| Xero Accounting               | Uses custom DKIM + Return-Path CNAMEs (No root SPF bloat needed) | 0 lookups (via DKIM) | In Xero → Email Settings, add the 2 DKIM CNAMEs so invoices align via DKIM without burning SPF lookups.             |
| Sage 50 / Sage Business Cloud | include:spf.sage.com (or M365 SMTP relay connector)              | 1-2 lookups          | Prefer routing Sage outbound mail through an authenticated M365 SMTP relay or verifying custom DKIM in Sage portal. |
| SendGrid / Twilio             | include:sendgrid.net (or sub-domain em1234.yourdomain.co.uk)     | 1 lookup             | Enable "Automated Security" in SendGrid to delegate s1._domainkey and s2._domainkey CNAMEs.                         |
| Mailchimp (Intuit)            | Authenticate via DKIM CNAMEs (k2._domainkey & k3._domainkey)     | 0 lookups            | Do <b>not</b> add include:servers.mcsv.net to root SPF—Mailchimp uses its own bounce domain and aligns via DKIM.    |
| HubSpot CRM                   | include:1234567.spf01.hubspotemail.net                           | 1 lookup             | Connect Email Sending Domain in HubSpot Settings to provision hs1- and hs2-_domainkey CNAMEs.                       |

### How to Stay Under the 10-Lookup SPF Limit (Without Paid SPF Flattening)

- Remove Redundant a and mx Mechanisms:** If your website server does not send email directly via local Postfix/Exim, remove a from your SPF record. If your outbound mail is already covered by include:spf.protection.outlook.com, remove mx as well—each saves 1-2 DNS lookups.
- Drop Legacy DKIM-Aligned Marketing Includes:** Platforms like Mailchimp, Brevo, and Postmark authenticate DMARC via DKIM or a dedicated custom Return-Path subdomain (e.g. bounces.yourdomain.co.uk). Removing their include: from your apex domain saves 3-5 lookups immediately.
- Segregate Bulk Marketing onto a Subdomain:** Send newsletters from news.yourdomain.co.uk with its own isolated 10-lookup SPF budget, keeping your primary corporate root domain clean:

```
# Clean Production Root SPF Record (Microsoft 365 + Mimecast Outbound Example - Only 3 Lookups)
yourdomain.co.uk. 3600 IN TXT "v=spf1 include:spf.protection.outlook.com include:eu._netblocks.mimecast.com -all"

# Dedicated Subdomain SPF for Marketing / Transactional Billing
billing.yourdomain.co.uk. 3600 IN TXT "v=spf1 include:sendgrid.net -all"
```

## 2.2 Staged DMARC Enforcement Rollout (Zero Email Disruption)

Follow this 4-stage progression to reach full p=reject compliance without dropping a single legitimate invoice, CRM email, or copier scan-to-email message:

| ROLLOUT PHASE              | DURATION            | EXACT _DMARC TXT VALUE & OPERATIONAL OBJECTIVE                                                                                                                                                                                           |
|----------------------------|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Stage 1: Observation       | Days 1 – 7          | v=DMARC1; p=none; sp=none; pct=100; rua=mailto:dmarc-reports@yourdomain.co.uk; fo=1; ri=86400<br>Collect daily XML aggregate reports (rua) with zero impact on mail flow. Verify M365/Google and SaaS DKIM alignment.                    |
| Stage 2: Canary Quarantine | Days 8 – 14         | v=DMARC1; p=quarantine; sp=quarantine; pct=25; rua=mailto:dmarc-reports@yourdomain.co.uk; fo=1<br>Quarantines 25% of unauthenticated messages to recipient Junk folders. Confirm no legitimate internal department senders are flagged.  |
| Stage 3: Full Quarantine   | Days 15 – 21        | v=DMARC1; p=quarantine; sp=quarantine; pct=100; rua=mailto:dmarc-reports@yourdomain.co.uk; fo=1<br>Enforces quarantine across 100% of unaligned traffic on both the root domain and all subdomains (sp=quarantine).                      |
| Stage 4: Strict Reject     | Day 22+ (Permanent) | v=DMARC1; p=reject; sp=reject; pct=100; adkim=r; aspf=r; rua=mailto:dmarc-reports@yourdomain.co.uk; fo=1<br>Instructs all receiving gateways (Gmail, Outlook, Mimecast, Proofpoint) to block spoofed messages outright at the SMTP edge. |

### UK Registrar DNS Configuration Matrix (Exact Host/Name Syntax)

A frequent cause of broken DMARC or DKIM deployments in the UK is registrar-specific zone apex formatting (some registrars automatically append .yourdomain.co.uk to the Host field, while others require the full FQDN):

| DNS PROVIDER / REGISTRAR | ROOT SPF HOST FIELD     | DMARC HOST FIELD | DKIM SELECTOR 1 HOST FIELD | QUOTING & TTL GOTCHAS                                                                               |
|--------------------------|-------------------------|------------------|----------------------------|-----------------------------------------------------------------------------------------------------|
| Cloudflare DNS           | @                       | _dmarc           | selector1._domainkey       | Set DKIM CNAMEs to <b>DNS Only (Grey Cloud)</b> — never proxy (Orange Cloud) DKIM CNAMEs.           |
| 123-Reg                  | @                       | _dmarc           | selector1._domainkey       | Do not wrap TXT value in outer quotes in the 123-Reg UI; it adds quotes automatically.              |
| GoDaddy UK               | @                       | _dmarc           | selector1._domainkey       | Avoid pasting trailing .yourdomain.co.uk in the Name field or GoDaddy creates _dmarc.domain.domain. |
| IONOS (1&1 UK)           | @                       | _dmarc           | selector1._domainkey       | Use TTL 3600 (1 hour) during rollout so stage transitions propagate within 60 minutes.              |
| Namecheap                | @                       | _dmarc           | selector1._domainkey       | In Advanced DNS, select TXT Record for DMARC/SPF and CNAME Record for M365 DKIM.                    |
| Fasthosts UK             | @ (or leave blank)      | _dmarc           | selector1._domainkey       | Fasthosts requires leaving the Host Name blank for root @ TXT records in standard panels.           |
| AWS Route 53             | Leave record name blank | _dmarc           | selector1._domainkey       | Route 53 <b>requires</b> double quotes "v=DMARC1; ..." around TXT record values in the console.     |

**External DMARC Report Authorisation (\_report.\_dmarc):**  
If you send DMARC aggregate reports (rua=mailto:dmarc@thirdparty.co.uk) to an address outside your own domain, you must also publish a DMARC-Report-To record.

## 2.3 2048-Bit DKIM Rotation, MTA-STS & SMTP TLS Reporting

While SPF and DMARC verify sender identity, **MTA-STS (RFC 8461)** and **SMTP TLS Reporting (RFC 8460)** prevent active man-in-the-middle (MitM) downgrade attacks on inbound SMTP connections by requiring sending mail servers to validate your MX certificate and use TLS 1.2/1.3.

### Step 1: Upgrade Microsoft 365 & Google Workspace DKIM Keys to 2048-Bit

Legacy 1024-bit DKIM keys no longer meet NCSC baseline recommendations. In Microsoft 365 (Exchange Online PowerShell or Defender Portal → Email Authentication → DKIM), publish the two CNAME records and rotate to 2048-bit:

```
# 1. Publish CNAMEs in DNS (Replace 'yourtenant' and 'yourdomain-co-uk'):  
selector1._domainkey.yourdomain.co.uk. 3600 IN CNAME selector1-yourdomain-co-uk._domainkey.yourtenant.onmicrosoft.com.  
selector2._domainkey.yourdomain.co.uk. 3600 IN CNAME selector2-yourdomain-co-uk._domainkey.yourtenant.onmicrosoft.com.  
  
# 2. Enable & Rotate to 2048-Bit in Exchange Online PowerShell:  
Connect-ExchangeOnline  
New-DkimSigningConfig -DomainName "yourdomain.co.uk" -KeySize 2048 -Enabled $true  
Rotate-DkimSigningConfig -KeySize 2048 -Identity "yourdomain.co.uk"
```

### Step 2: Deploy Inbound SMTP TLS Enforcement (MTA-STS & TLS-RPT)

MTA-STS requires two components: (a) a static HTTPS policy file hosted at `https://mta-sts.yourdomain.co.uk/.well-known/mta-sts.txt` (template provided in `templates/mta-sts-policy.txt`), and (b) two DNS TXT records:

```
# File: https://mta-sts.yourdomain.co.uk/.well-known/mta-sts.txt (Content-Type: text/plain)  
version: STSv1  
mode: enforce  
mx: *.mail.protection.outlook.com  
max_age: 604800  
  
# DNS TXT Records for MTA-STS & SMTP TLS Reporting (Update id= timestamp whenever policy changes):  
_mta-sts.yourdomain.co.uk. 3600 IN TXT "v=STSv1; id=2026102501"  
_smtp._tls.yourdomain.co.uk. 3600 IN TXT "v=TLSRPTv1; rua=mailto:tls-reports@yourdomain.co.uk"
```

### Step 3: Lock Certificate Issuance with DNS CAA Records (RFC 8659)

Certification Authority Authorization (CAA) DNS records restrict which Certificate Authorities (CAs) are permitted to issue TLS certificates for your domain, preventing unauthorized certificate issuance:

```
yourdomain.co.uk. 3600 IN CAA 0 issue "letsencrypt.org"  
yourdomain.co.uk. 3600 IN CAA 0 issue "sectigo.com"  
yourdomain.co.uk. 3600 IN CAA 0 issuewild ";"  
yourdomain.co.uk. 3600 IN CAA 0 iodef "mailto:security@yourdomain.co.uk"
```

#### Verification Command (Included CLI Tool):

Run `python3 tools/faultypacket_uk_auditor.py yourdomain.co.uk --html report.html` immediately after publishing these records to verify live DoH resolution across Cloudflare and Google DNS.

## 3.1 Emergency PHP2Shell (CVE-2026-109618 & CVE-2026-109619) Remediation

The October 2026 PHP Security Advisory addresses two high-severity Remote Code Execution (RCE) and SAPI argument/stream handling vulnerabilities tracked as **CVE-2026-109618** and **CVE-2026-109619** (informally referred to as *PHP2Shell*). Automated internet scanners actively fingerprint web servers exposing X-Powered-By: PHP/ ... response headers to identify unpatched installations.

### October 2026 PHP Branch Vulnerability & Patch Threshold Matrix

| PHP RELEASE BRANCH | AFFECTED VERSIONS    | MINIMUM PATCHED RELEASE | SUPPORT STATUS & RECOMMENDED ACTION                            |
|--------------------|----------------------|-------------------------|----------------------------------------------------------------|
| PHP 8.5.x          | 8.5.0 through 8.5.11 | PHP 8.5.12+             | Active support — upgrade minor packages immediately.           |
| PHP 8.4.x          | 8.4.0 through 8.4.26 | PHP 8.4.27+             | Active support — upgrade minor packages immediately.           |
| PHP 8.3.x          | 8.3.0 through 8.3.35 | PHP 8.3.36+             | Security support — upgrade minor packages immediately.         |
| PHP 8.2.x          | 8.2.0 through 8.2.34 | PHP 8.2.35+             | Security support — upgrade and plan migration to 8.4.          |
| PHP <= 8.1.x / 7.x | All releases         | End-of-Life (Unpatched) | Apply immediate WAF/Nginx lockdown and migrate to PHP 8.3/8.4. |

### Safe Zero-Downtime Upgrade Commands by Operating System

#### 1. Ubuntu 22.04 / 24.04 LTS & Debian 12 (via ppa:ondrej/php or Sury Repo):

```
# Verify current PHP CLI and FPM versions:
php -v && systemctl list-units --type=service | grep php

# Refresh package index and upgrade only PHP packages without altering web server configs:
sudo apt-get update
sudo apt-get install --only-upgrade -y 'php8.*'

# Validate PHP-FPM configuration syntax before graceful reload:
sudo php-fpm8.3 -t && sudo systemctl reload php8.3-fpm
```

#### 2. RHEL 8/9, AlmaLinux & Rocky Linux (via Remi Modular Repository):

```
# Upgrade PHP packages from Remi modular stream and reload php-fpm:
sudo dnf update -y 'php*'
sudo php-fpm -t && sudo systemctl reload php-fpm
```

#### 3. Windows Server IIS (FastCGI PHP Handler):

```
# PowerShell: Check installed PHP CGI binary version in C:\PHP:
& "C:\PHP\php-cgi.exe" -v

# Download latest Thread-Safe/Non-Thread-Safe (NTS) x64 zip (≥ 8.4.27 or ≥ 8.3.36) from windows.php.net,
# extract to C:\PHP-8.4.27-nts, copy hardened php.ini, update IIS FastCGI handler mapping, and recycle AppPool:
Restart-WebAppPool -Name "DefaultAppPool"
```

## 3.2 Production php.ini Hardening & Perimeter WAF Rules

Patching PHP binaries must be paired with strict SAPI configuration hardening so that even if a third-party WordPress/Laravel/Drupal plugin introduces a flaw, the PHP runtime cannot spawn OS shells or disclose version banners. Copy templates/php-ini-production-lockdown.ini to /etc/php/<ver>/fpm/conf.d/99-faultypacket-hardening.ini:

```
; /etc/php/8.3/fpm/conf.d/99-faultypacket-hardening.ini
expose_php = Off
allow_url_include = Off
enable_dl = Off
cgi.force_redirect = 1
cgi.fix_pathinfo = 0
display_errors = Off
display_startup_errors = Off
log_errors = On
disable_functions = exec,passthru,shell_exec,system,proc_open,popen,pcntl_exec,pcntl_fork,dL,show_source,highlight_file,posix_kill,posix_mkfifo,posix_setpgid,posix_setsid,posix_setuid
open_basedir = /var/www/html:/tmp:/var/lib/php/sessions
```

### Perimeter Mitigation 1: Cloudflare WAF Custom Rule Expression

If you host legacy PHP applications behind Cloudflare, deploy this Custom WAF Rule (**Security → WAF → Custom rules → Create rule → Edit expression**) with action set to **Block** to stop CGI flag injection and stream wrapper exploitation at the Cloudflare edge before traffic reaches your origin server:

```
(http.request.uri.query contains "auto_prepend_file") or
(http.request.uri.query contains "allow_url_include") or
(http.request.uri.query contains "php://input") or
(http.request.uri.query contains "%2dd") or
(http.request.uri.query contains "-d+") or
(http.request.uri.path contains "/vendor/phpunit/") or
(http.request.uri.path contains ".env")
```

### Perimeter Mitigation 2: Nginx & Apache Origin Hardening

Even when behind a CDN, configure your origin web server (full files in templates/nginx-hardening-and-headers.conf and templates/apache-htaccess-security.conf) to strip X-Powered-By and reject suspicious query strings:

```
# Nginx (Inside server {} block):
server_tokens off;
fastcgi_hide_header X-Powered-By;
if ($query_string ~* "(?:^|&)(?:-[dnas]|auto_prepend_file|allow_url_include|php://input)") {
    return 403;
}

# Apache 2.4 (.htaccess or VirtualHost):
ServerSignature Off
Header always unset X-Powered-By
RewriteEngine On
RewriteCond %{QUERY_STRING} (?:^|&)(?:-[dnas]|%2d[dnas]|auto_prepend_file|allow_url_include|php://input) [NC]
RewriteRule .* - [F,L]
```

#### Why Hiding X-Powered-By Matters:

Mass exploitation campaigns filter Shodan and HTTP scan targets by reading the X-Powered-By: PHP/8.x.y header. Setting `expose_php = Off` and `fastcgi_hide_header X-Powered-By` removes your server from automated version-fingerprinting sweeps.

## 3.3 Defensive Incident Triage & Forensic Log Inspection

If a server ran an unpatched PHP version prior to remediation, perform a read-only forensic inspection of web access logs, webroot modification times, and process trees to confirm no unauthorized webshells or scheduled tasks were planted. You can run `bash tools/php2shell_local_triage.sh` or execute the one-liners below:

### 1. Nginx & Apache Access Log Hunting One-Liners (Linux)

```
# Hunt for CGI argument injection (-d / %2dd), stream wrappers (php://input), and prepend probes:
grep -Eirn 'auto_prepend_file|allow_url_include|php://input|%2d[dnas][+%20]|invokefunction|call_user_func_array' /var/log/nginx/ /var/log/apache2/ 2>/dev/null

# Identify POST requests to unusual .php files inside upload or static asset directories:
grep -E 'POST /(wp-content/uploads|uploads|assets|images|storage)/.*\.php' /var/log/nginx/*access*.log /var/log/apache2/*access*.log 2>/dev/null

# Summarize top external IP addresses generating HTTP 403/500 responses on PHP endpoints:
awk '$7 ~ /\.\php/ && ($9 == 403 || $9 == 500) {print $1}' /var/log/nginx/*access*.log 2>/dev/null | sort | uniq -c | sort -nr | head -n 20
```

### 2. Windows Server IIS W3SVC Log Hunting (PowerShell)

```
# Scan IIS W3SVC access logs for suspicious PHP CGI query string parameters:
Get-ChildItem -Path "C:\inetpub\logs\LogFiles\W3SVC*" -Filter "*.log" -Recurse |
    Select-String -Pattern "auto_prepend_file|allow_url_include|php://input|%2dd|-d\+" |
    Select-Object Filename, LineNumber, Line
```

### 3. Read-Only Webroot Integrity & Persistence Check

```
# List any .php files modified in the last 14 days inside /var/www:
find /var/www -type f -name "*.php" -mtime -14 -ls 2>/dev/null

# Scan recent .php files in public upload directories for obfuscated base64/gzipinflate payloads:
find /var/www -type f -name "*.php" -exec grep -El 'base64_decode\s*\(|gzipinflate\s*\(|eval\s*\(|\s*\$_' {} + 2>/dev/null

# Verify no unexpected child processes or crontabs are running under the www-data / nginx user:
ps -ef | awk '$1 == "www-data" || $1 == "nginx" || $1 == "apache"'
crontab -u www-data -l 2>/dev/null
```

#### Incident Escalation Protocol (UK GDPR 72-Hour Notification Rule):

If log inspection reveals HTTP 200 OK responses to `auto_prepend_file / php://input` requests or unauthorized .php files in upload directories: (1) snapshot the VM disk for forensic preservation, (2) isolate the host from production networks, (3) rotate all database, API, and SMTP credentials stored in .env or wp-config.php, and (4) assess whether personal data was accessed under UK GDPR Article 33.

## 4.0 Production HTTP Security Header & TLS 1.3 Baseline

As demonstrated in our UK North West Benchmark (Page 3), 93% of surveyed firms failed basic HTTP response header checks even when HTTPS was active. Implementing the six headers below brings any corporate website or client portal to an immediate **Grade A+** posture:

| HTTP RESPONSE HEADER      | RECOMMENDED PRODUCTION VALUE                                                                                                                                                                            | SECURITY CONTROL PURPOSE                                                              |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Strict-Transport-Security | max-age=63072000; includeSubDomains; preload                                                                                                                                                            | Enforces HTTPS for 24 months and blocks SSL-stripping attacks.                        |
| Content-Security-Policy   | default-src 'self' https;; script-src 'self' 'unsafe-inline' https;; style-src 'self' 'unsafe-inline' https;; img-src 'self' data: https;; frame-ancestors 'self'; base-uri 'self'; form-action 'self'; | Restricts cross-site scripting (XSS) sources and blocks third-party iframe embedding. |
| X-Frame-Options           | SAMEORIGIN                                                                                                                                                                                              | Legacy browser clickjacking defense alongside frame-ancestors.                        |
| X-Content-Type-Options    | nosniff                                                                                                                                                                                                 | Prevents MIME-sniffing execution of uploaded assets.                                  |
| Referrer-Policy           | strict-origin-when-cross-origin                                                                                                                                                                         | Strips sensitive URL paths/tokens when navigating to external sites.                  |
| Permissions-Policy        | camera=(), microphone=(), geolocation=(), payment=()                                                                                                                                                    | Disables browser hardware APIs not required by the site.                              |

### Cloudflare Pages / Static Hosting \_headers File

If your corporate site runs on Cloudflare Pages or Netlify, place a file named `_headers` in your web root:

```
/*
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: camera=(), microphone=(), geolocation=(), payment=()
Content-Security-Policy: default-src 'self' https;; script-src 'self' 'unsafe-inline' https;; style-src 'self' 'unsafe-inline' https;; img-src 'self' data: https;; connect-src 'self' https;; frame-ancestors 'self'; base-uri 'self'; form-action 'self';
```

### Final Implementation Sign-Off Checklist

| DONE | VERIFICATION STEP                                                                       | TARGET / EXPECTED RESULT                             |
|------|-----------------------------------------------------------------------------------------|------------------------------------------------------|
| [ ]  | Single SPF TXT record published with $\leq 10$ lookups                                  | Ends with strict -all                                |
| [ ]  | 2048-bit DKIM signing enabled for M365 / Google + SaaS senders                          | selector1 / selector2 CNAMEs resolving               |
| [ ]  | DMARC record progressed to enforcement on root & subdomains                             | v=DMARC1; p=reject; sp=reject; rua=...               |
| [ ]  | MTA-STS policy & SMTP TLS-RPT TXT records published                                     | _mta-sts & _smtp._tls active                         |
| [ ]  | PHP patched to $\geq 8.5.12$ / 8.4.27 / 8.3.36 / 8.2.35 & <code>expose_php = Off</code> | Zero X-Powered-By leakage                            |
| [ ]  | HSTS, CSP, XFO, XCTO headers active on port 443                                         | Verified via <code>faultypacket_uk_auditor.py</code> |