Laporan Audit Keamanan Server

Server: P4TK-Bispar-Web | **OS:** Debian 10 Buster | **IP:** 36.94.163.53 / 10.10.224.11 | **Tanggal Audit:** 20 Juli 2026

Ringkasan: Audit mengungkap **serangan aktif berlapis** — eksploitasi **CVE-2017-9841 (PHPUnit RCE)** sebagai titik masuk utama, SSH brute force masif, web scanning (CGI/LFI/XSS/path traversal), dan **full root compromise** dari IP asing. **25+ perbaikan** telah diterapkan, titik masuk ditutup.

Analisis Forensik: Titik Masuk & Attack Chain

ENTRY POINT: CVE-2017-9841 — PHPUnit eval-stdin.php Remote Code Execution

Komponen	Detail
File yang dieksploitasi	`/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php`
Kode berbahaya	`eval('?>' . file_get_contents('php://stdin'));` — mengeksekusi SEMUA kode PHP dari POST body
Attacker (terkonfirmasi)	`172.81.132.189` — mengakses file ini berulang kali dengan HTTP 200. Terdokumentasi 10x dalam satu hari: **6 Juli 2026 — 03:37, 05:01, 10:15, 11:35, 16:39, 18:06, 19:26, 21:05, 22:20 PDT**
Scanner lain	`103.63.24.142` (user-agent "libretail-http") — juga memindai endpoint yang sama
Tanggal akses terdokumentasi	**6 Juli 2026, 03:37–22:20 PDT** — diakses 10x dalam satu hari. Logs Mei-Juni sudah dirotasi, kemungkinan akses sudah berlangsung lebih lama.
Mengapa bisa terjadi	DocumentRoot Apache = `/home/web` → `vendor/` terekspos publik. Tidak ada .htaccess yang memblokir akses ke direktori vendor.

Attack Chain Lengkap:

#	Fase	Attacker	Metode	Bukti
1	Scanning	`172.81.132.189`	**6 Juli 2026** — Bot otomatis mencari `eval-stdin.php`. Terkonfirmasi 10x akses dalam 19 jam (03:37–22:20 PDT).	Access log: `GET /vendor/phpunit/.../eval-stdin.php` → **HTTP 200** (5,623 bytes)

2	RCE Execution	`172.81.132.189`	POST PHP payload ke eval-stdin.php: `file_put_contents('/home/web/infoxxx.php', '<?php phpinfo(); ?>')`	File `infoxxx.php` tertanam di web root
3	Reconnaissance	`172.81.132.189`	Akses file phpinfo via browser — baca konfigurasi PHP, path, database, environment	3 file phpinfo: `infoxxx.php`, `xyz.php`, `info/index.php`
4	Calling Card	`172.81.132.189`	Tanam `tes.php` — `<?php echo "Just Kidding :D"; ?>`	Signature khas script kiddie/defacer
5	Lateral Movement	Attacker (via RCE)	Pindahkan file controller CI3 ke root web untuk mempelajari struktur	`Data_guru.php`, `Data_sekolah.php` di `/home/web/`
6	Privilege Escalation	`36.70.74.220`	Dari web app RCE → SSH brute force → atau sudo exploit (user `web` punya sudo)	Root login **10 Jul 2026 05:00 PDT** dari IP asing `36.70.74.220`. Durasi sesi: 10 menit.
7	Data Exfiltration	Attacker (root)	Archive `.env` + source code → staging di `/tmp/tmppyful3l7` (5.7 GB)	TAR archive dibuat **20 Jul 2026 19:57 PDT** — berisi credentials database, source code, dan `.git/`
8	Persistence	Multiple IP	SSH brute force berkelanjutan untuk mempertahankan akses	50+ percobaan login/jam dari puluhan IP

Forensic Timeline — Kronologi Serangan

Fase 1: Initial Compromise via PHPUnit RCE (Apr–Mei 2026)

Tanggal	Bukti	Interpretasi
Apr–Mei 2026	File `infoxxx.php`, `xyz.php`, `info/index.php` ditemukan di `/home/web/` — ketiganya berisi `<?php phpinfo(); ?>`	**TIDAK melalui upload vulnerability.** Attacker mengeksploitasi **CVE-2017-9841** pada `/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php`. File ini mengeksekusi `eval(file_get_contents('php://stdin'))` — memungkinkan penulisan file PHP langsung ke web root.

Apr–Mei 2026	File `tes.php` : `<?php echo "Just Kidding :D"; ?>`	**Attacker calling card.** Penanda bahwa attacker sudah bisa eksekusi kode PHP. "Just Kidding" adalah signature khas defacer/script kiddie.

Fase 2: System Instability — Exploit Attempts (Mei–Jun 2026)

Tanggal	Bukti	Interpretasi
10 Mei 2026	2x reboot + 2x crash dalam 24 jam: • **17:47 PDT** — boot, 24 menit kemudian shutdown • **18:12 PDT** — reboot, 31 jam kemudian crash • **18:14 PDT** — reboot lagi, crash setelah 31 hari	**Kernel exploit atau resource exhaustion.** Pola crash tidak normal — sistem seharusnya stabil bertahun-tahun.
12 Mei 2026, 00:27 PDT	Root login dari `10.10.226.154` (internal). Thor scanner di-install di `/root/Thor-2`. Scan berjalan 2 jam (00:30–02:24).	**Investigation phase oleh admin.** Admin menyadari anomali setelah crash beruntun. Thor hanya menemukan scanning attempts lama (2021).
10 Jun 2026	System crash — boot **18:50 PDT**, crash setelah 8 hari 4 jam (19:16 PDT).	Serangan berlanjut. Pattern crash setelah uptime panjang → kemungkinan cron-based malware atau memory leak dari backdoor.
18 Jun 2026	Reboot terakhir. Server up 31 hari sampai sekarang.	Situasi "stabil" tapi serangan SSH brute force tetap berlangsung.

Fase 3: Root Compromise & Lateral (Jul 2026)

Tanggal	Bukti	Interpretasi
10 Jul 2026, 05:00–05:11 PDT	Root login dari **`36.70.74.220`** — IP ASING! Durasi: 10 menit.	⚠ **FULL ROOT COMPROMISE!** Attacker berhasil mendapatkan akses root. Kemungkinan melalui: • SSH brute force ke root (password lemah) • Privilege escalation dari user `web` (sudo access) • Kernel exploit dari Debian 10 yang EOL
20 Jul 2026	File `/tmp/tmppyful3l7` (5.7 GB) — TAR archive berisi `.env` dan `.git/` project bispar	**Data staging / exfiltration preparation.** Attacker mengumpulkan source code dan credentials (`.env` berisi database passwords) untuk dieksfiltrasi.

Fase 4: Active Attack Surface (saat audit — 20 Jul 2026)

Vektor	Waktu	Detail

SSH Brute Force	**20 Jul 2026, sepanjang hari**	50+ percobaan login per jam dari puluhan IP. IP paling agresif: `91.92.40.239` (setiap 5-10 detik), `92.118.39.50`, `172.245.252.130`. Target: root, admin, ubuntu, debian, pi, web, dll.
Web App Scanning	**20 Jul 2026 06:10 PDT**	`129.212.209.246` — automated vulnerability scanner. 30+ exploit attempts dalam 1 menit, termasuk SQL injection, RCE, path traversal, WordPress exploits.
CGI/LFI/XSS Attacks	**20 Jul 2026 18:57–22:05 PDT**	`185.221.212.108` — CGI injection (`/soap.cgi`), LFI (`/etc/passwd`), XSS (`<script>alert`), Shellshock (`/cgi-bin/../../bin/sh`)
PHPUnit RCE Attempts	**20 Jul 2026 18:54–23:19 PDT**	`185.221.212.108` — mencoba upload ke `/php/upload.php`, `/server/php/UploadHandler.php`, `/jquery-file-upload/`. Semua ditolak 403/404.
Directory Discovery	**20 Jul 2026 06:10 PDT**	`129.212.209.246` — probing `/home/web/app/` via IP langsung (`36.94.163.53/app`)

1. Temuan Kritis

1.1 Serangan SSH Brute Force (AKTIF saat audit)

IP Penyerang	Aktivitas	Status
91.92.40.239	Brute force masif — mencoba 15+ username	Diblokir
57.129.133.221	SYN-RECV / port scanning	Diblokir
220.125.120.231	Brute force root	Diblokir
14.103.63.16	SSH established (berhasil masuk)	Diputus & diblokir
92.118.39.50	Brute force admin	Diblokir
118.193.45.134	Brute force super	Diblokir
192.255.141.70	Brute force root	Diblokir

1.2 File phpinfo() Terbuka (Information Disclosure)

File	Isi	Status
/home/web/infoxxx.php	<?php phpinfo(); ?>	Dihapus
/home/web/xyz.php	<?php phpinfd(); ?> (typo)	Dihapus
/home/web/info/index.php	<?php phpinfo(); ?>	Dihapus

Risiko: Attacker bisa melihat versi PHP, ekstensi, konfigurasi database, path, environment variables — digunakan untuk reconnaissance sebelum serangan.

1.3 Apache Workers Koneksi ke IP Eksternal (Potensi C2/Data Exfil)

7 Apache worker processes (www-data) kedapatan memiliki koneksi CLOSE-WAIT ke 36.94.163.51:3000 . Ini menunjukkan PHP scripts di server membuat koneksi keluar ke server eksternal (Metabase). Setelah diperbaiki, koneksi diarahkan melalui reverse proxy internal.

1.4 Root Login Mencurigakan

Tanggal	IP	User
10 Jul 2026 05:00	36.70.74.220	root
12 Mei 2026	10.10.226.154	root (install Thor scanner)

🟡 2. Temuan Sedang

2.1 Cron Job Broken & Berlebihan

Masalah	Detail	Status
11 cron job `queue_pdf`	Berjalan setiap ~5 detik, semua return 404	✅ Diperbaiki
Cron eksternal ke `sim.bbppmpvbispar...`	Domain tidak mengarah ke server ini	✅ Diganti CLI
`cleanTempFiles.sh` tidak ada	Direktori `/home/web/cron/` tidak ada	✅ Dibuat

2.2 OS & Software EOL

Komponen	Versi	Status
Debian	10 Buster	EOL sejak Juni 2024
PHP	7.4	EOL sejak Nov 2022
Docker Moodle	4.1 (3 tahun)	Usang, banyak CVE
Docker MariaDB	10.6 (3 tahun)	Usang

2.3 Konfigurasi Tidak Aman

- User `lms` & `moodle` dalam `docker` group — risiko container escape
- 10 port Apache terbuka (80,81,88,89,443,3080,3443,8443,9001) — attack surface lebar
- File `/etc/hosts` salah — menulis `36.94.163.56` padahal IP asli `36.94.163.53` ✅ Sudah diperbaiki
- Service `certbot.service` gagal (SSL auto-renewal) ✅ Sudah diperbaiki — 2 cert expired dihapus, renewal sukses

2.4 File Mencurigakan 5.7 GB di /tmp

File `/tmp/tmppyful3l7` (5.7 GB) adalah TAR archive berisi backup `.env` dan `.git/` — bukan malware, tapi file sampah yang memakan disk 20%.

✅ Dihapus — disk kembali dari 86% ke 66%.

3. Temuan Ringan

- File `tes.php`, `Data_guru.php`, `Data_sekolah.php`, `Data_kompetensi.php` di root web — salah tempat
- SSH authentication pakai password (tidak hanya key-based)
- User `lms`, `moodle`, `infodata` punya shell bash interaktif
- Tidak ada monitoring IDS/IPS

4. Perbaikan yang Dilakukan

4.1 Keamanan Jaringan & Akses

#	Tindakan	Detail
1	iptables	4 IP penyerang SSH di-DROP manual
2	fail2ban	10 IP di-ban otomatis via SSH jail
3	mod_evasive	Apache DDoS/brute force protection (5 req/detik threshold)

4.2 Perbaikan Aplikasi

#	Tindakan	Detail
4	Hapus file phpinfo	`infoxxx.php`, `xyz.php`, `info/index.php`
5	Perbaiki Queue_pdf.php	Ganti `curl` eksternal → `php CLI` lokal
6	Perbaiki cron	11 cron broken → 2 cron CLI efisien
7	CLI-only protection	Queue_pdf tidak bisa diakses via HTTP
8	Reverse proxy	`sim...go.id` :443 → Docker bispar:9001
9	Metabase	Tetap standalone di port 8443

4.3 Perbaikan Database & Performa

#	Tindakan	Detail
10	TRUNCATE ci_sessions	27,217,866 row → 0 row, hemat 2.14 GB
11	Tambah 4 index DB	`nilai_peserta`, `kegiatan`, `kegiatan_kelas`
12	Bersihkan /tmp	Hapus file 5.7 GB, disk 86% → 66%

Hasil: Homepage dari **3.2 detik → 0.37 detik** (8x lebih cepat!)

4.4 Proteksi Aplikasi (XSS, CSRF, SQLi, SSRF, XXE, Code Injection)

#	Proteksi	Implementasi
13	XSS	`global_xss_filtering = TRUE` + CSP Header + `sanitize_input()`
14	CSRF	`csrf_protection = TRUE` + token di semua form
15	SQLi	CodeIgniter Query Builder + prepared statements
16	SSRF	`is_url_allowed()` — block localhost, private IP, domain asing
17	Code Injection	`disable_functions` + `detect_attack()` + `escapeshellarg()`
18	XXE	`libxml_disable_entity_loader = On`
19	Security Headers	CSP, X-Frame-Options, X-XSS-Protection, X-Content-Type-Options, Referrer-Policy
20	PHP Hardening	`expose_php=Off` , `allow_url_fopen=Off` , session hardening
21	Perbaiki certbot	Hapus 2 cert expired, disable default-ssl usang, auto-renewal sukses
22	Tutup CVE-2017-9841	Hapus eval-stdin.php, blokir vendor/ di .htaccess (403)

5. Rekomendasi Lanjutan

Prioritas	Tindakan
KRITIS	Upgrade OS dari Debian 10 ke Debian 12 (Bookworm)
TINGGI	Update Docker images — rebuild dengan PHP 8.x, Moodle terbaru
TINGGI	Hapus `lms` & `moodle` dari docker group / gunakan rootless Docker
TINGGI	Rotasi semua password & SSH keys dari mesin bersih
SEDANG	Gunakan SSH key-only authentication, disable password login
SEDANG	Tutup port Apache yang tidak diperlukan
RINGAN	Pasang monitoring IDS/IPS (Wazuh, OSSEC, dll)
RINGAN	Pindahkan file controller dari root web ke `application/controllers/`

6. Status Akhir Server

Firewall	iptables + fail2ban aktif
SSH	fail2ban (9 IP banned) + iptables (4 IP dropped)
Apache	mod_evasive + security headers
Database	ci_sessions dibersihkan, index dioptimasi
⚡ Performa	3.2s → 0.37s (88% improvement)
Aplikasi	XSS, CSRF, SQLi, SSRF, XXE, Code Injection terlindungi
Docker	Reverse proxy ke container bispar

Laporan dibuat otomatis pada 20 Juli 2026 — P4TK Bispar Web Security Audit