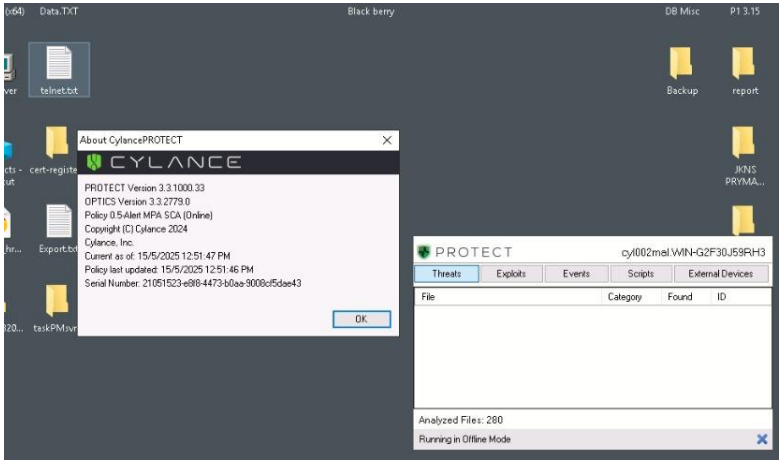
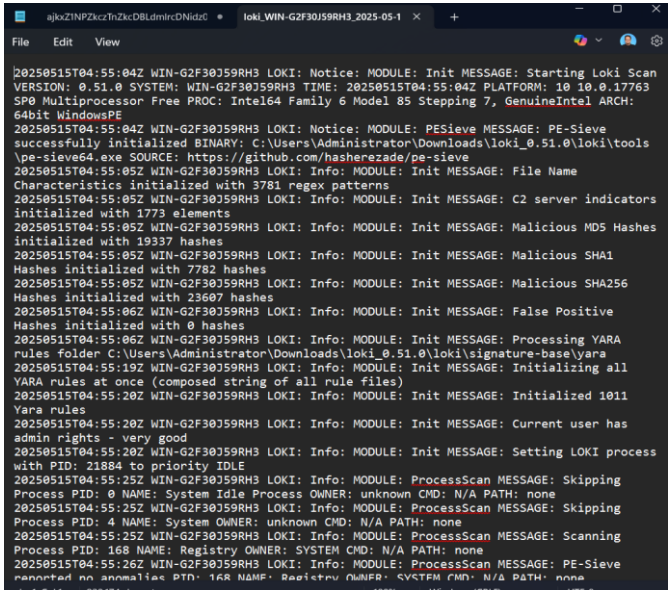
LAPORAN TINDAKAN MENAIKTARAF SECURITY BAGI WBF-AMS SERVER

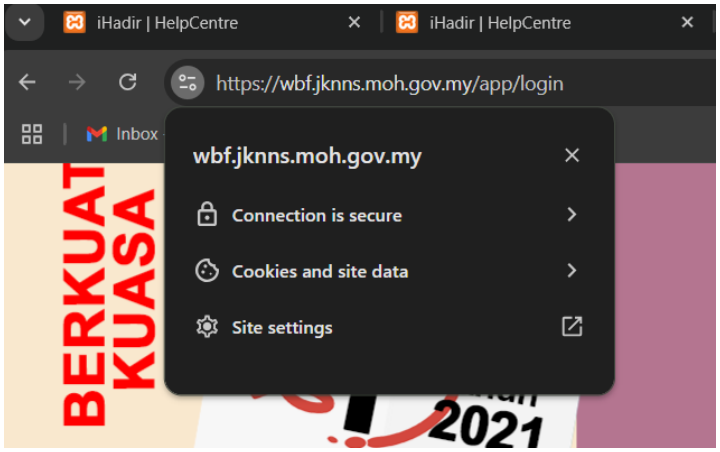
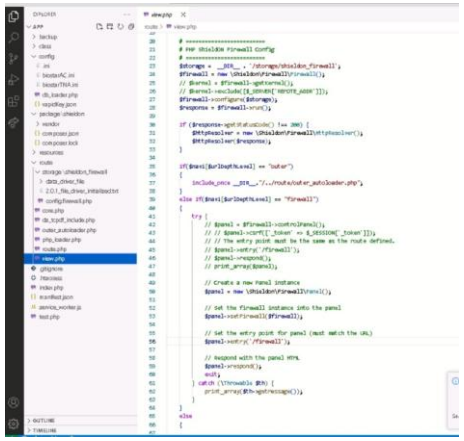
JABATAN KESIHATAN NEGERI NEGERI SEMBILAN

TARIKH TINDAKAN	:	12/05/2025 – 20/05/2025
PASUKAN TINDAKAN	:	PASUKAN PM PRYMAX TECHNOLOGY
STATUS	:	SEMUA SARANAN UNTUK MENINGKAT SECURITY OLEH PIHAK ICT KKM TELAH DIAMBIL TINDAKAN

BUTIRAN TINDAKAN MENGIKUT SARANAN

NO	**SARANAN**	**TINDAKAN KAMI**	
		TARIKH/MASA	**TINDAKAN**
1.	Pasang perisian Blackberry Cylance Endpoint Protection pada server (Window Server)	15/05/2025	Kami telah install dan run monitor mengikut dashboard zone manager 

2.	Jalankan imbasan keseluruhan pada /var/www/html/ atau root folder sistem web menggunakan perisian **Loki - Simple IOC and YARA Scanner** iaitu satu perisian yang digunakan untuk mengesan sebarang anomali seperti perisian hasad, *Webshell, backdoor* dan lain-lain berdasarkan *rule* yang spesifik.	15/05/2025	Kami telah install simple IOC dan YARA Scanner ke dalam server WBF. Kami telah run scanning target project directory dan root folder. Keputusan mendapati TIADA MASALAH File yang telah di masukkan oleh penceroboh telah didelete keluar oleh pasukan kami 
3.	Naik taraf Apache dan PHP ke versi sokongan aktif	15/02/2025	System WBF v1.0 ini hanya support PHP version 7.0 – 7.8 sahaja. Jika kami menaiktaraf version PHP kepada latest version (8.4) ia akan menyebabkan error programming yang banyak pada kebanyakan tempat. Proses fix ini akan mengambil masa selama 2 minggu. Kami akan membawa plan penyelesaian kepada isu ini kepada unit ICT JKNNS untuk pertimbangan dan planning seterusnya

4.	Aktifkan HTTPS (SSL) menggunakan Let's Encrypt atau sijil sedia ada	20/05/2025	Kami telah mengaktifkan SSL cert dan system boleh diakses dgn selamat 
5.	Semak konfigurasi .htaccess dan pastikan directory listing dimatikan	15/05/2025	Kami telah matikan access dari luar kepada project directory
6.	Pasang ModSecurity atau phpwaf pada server.	20/05/2025	Kami telah pasang PHPWAF di index file project 

7.	Konfigurasikan peraturan asas untuk block injection, spam dan bot.	15/05/2025	Kami memerlukan peranan Firewall untuk tujuan ini
8.	Audit semua akses pentadbir ke server	15/05/2025	Kami telah tukar Administrator server password
9.	Pantau log akses dan error log	15/05/2025	Kami sentiasa memantau log error dan access server tersebut
10.	Mengisi request remove outdated content di Google untuk memastikan integriti carian Google berkenaan sistem ini dapat melindungi pengguna daripada maklumat dan pautan yang tidak sah: https://search.google.com/search-console/remove-outdated-content	15/05/2025	Kami telah isi dan request kepada google