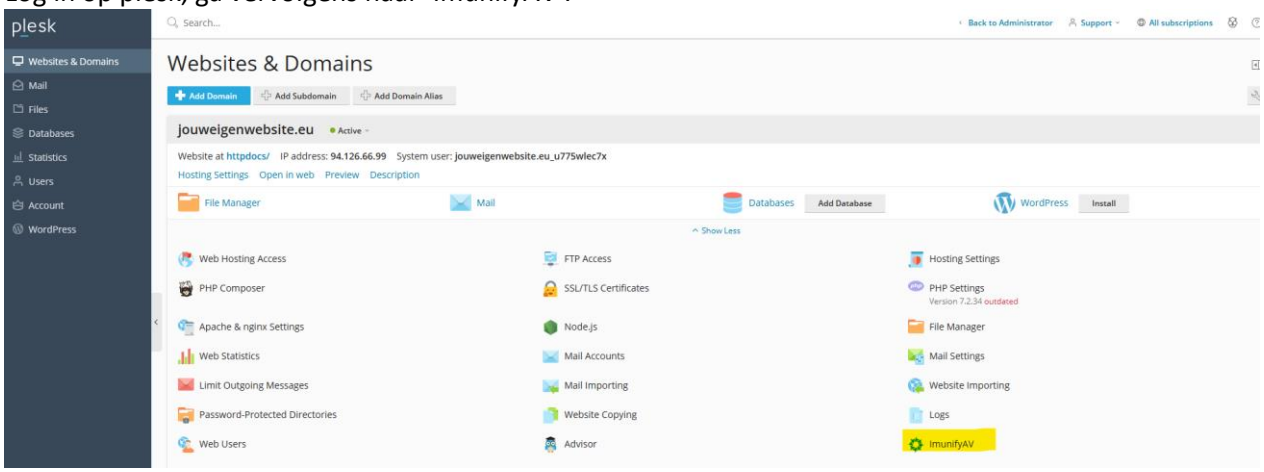
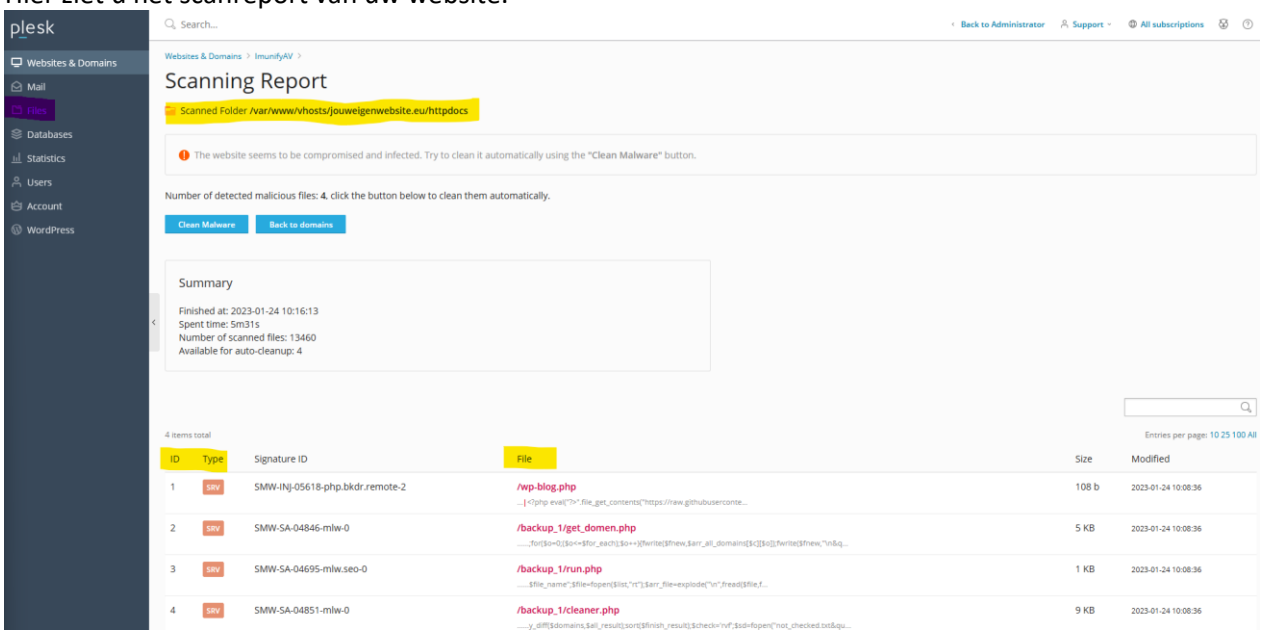
Indien er door ImunifyAV malware is gevonden op uw website, zult u uw webhosting omgeving moeten opschonen, en moeten zorgen dat enige kwetsbaarheden in de website gepatched of geupdate worden.

Om met behulp van ImunifyAV de website op te schonen zijn er 2 opties, wij raden sterk aan om de 1e optie te gebruiken, omdat hier minder risico aan vast zit dat uw website na het opschonen niet meer functioneert.

Optie 1:
Log in op plesk, ga vervolgens naar 'ImunifyAV'.



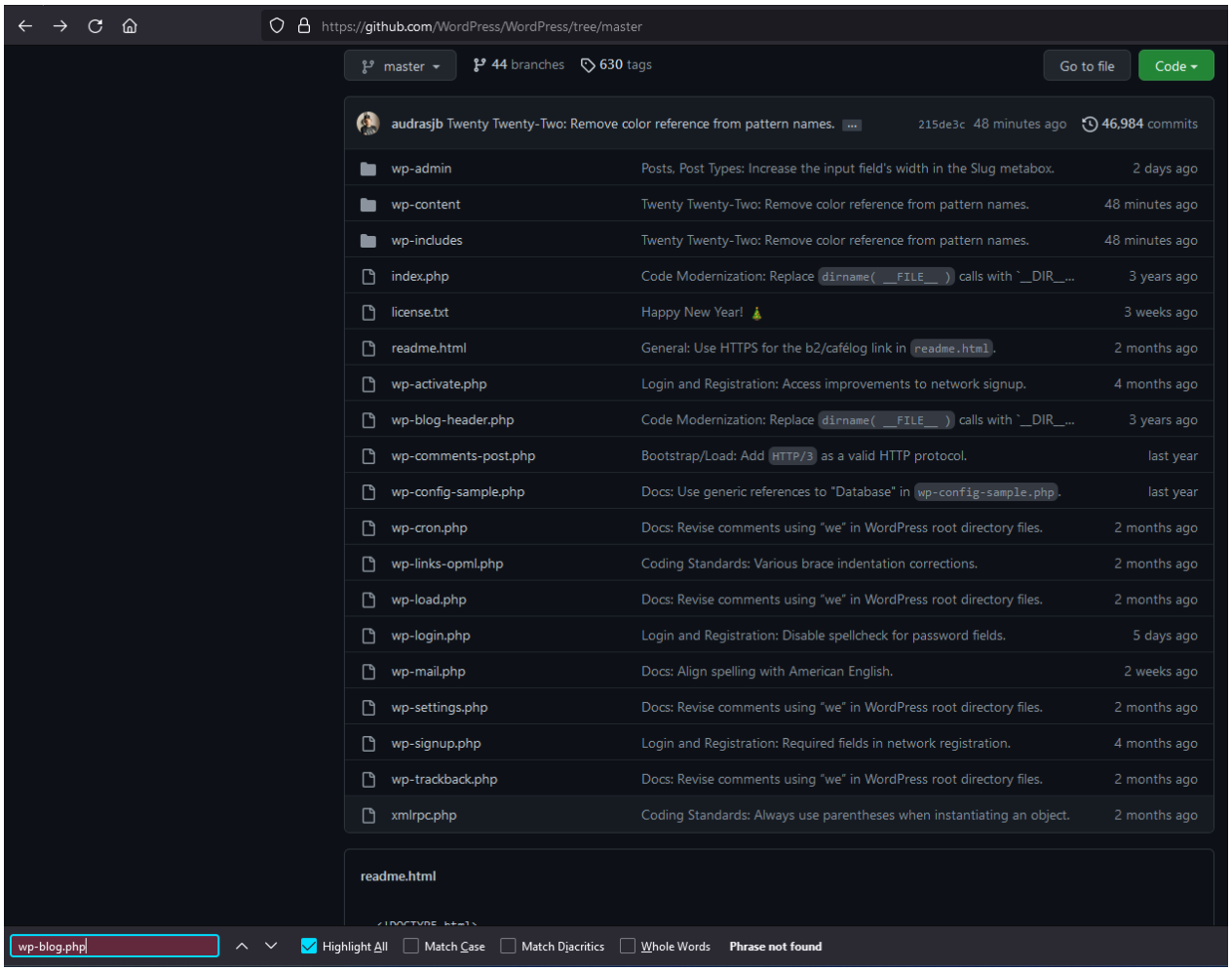
Hier ziet u het scanreport van uw website.



In de onderste tabel, ziet u welke bestanden er geinfecteerd zijn.
Alle bestanden zullen zich in de document root bevinden, welke na 'scanned Folder' staat (bovenaan).

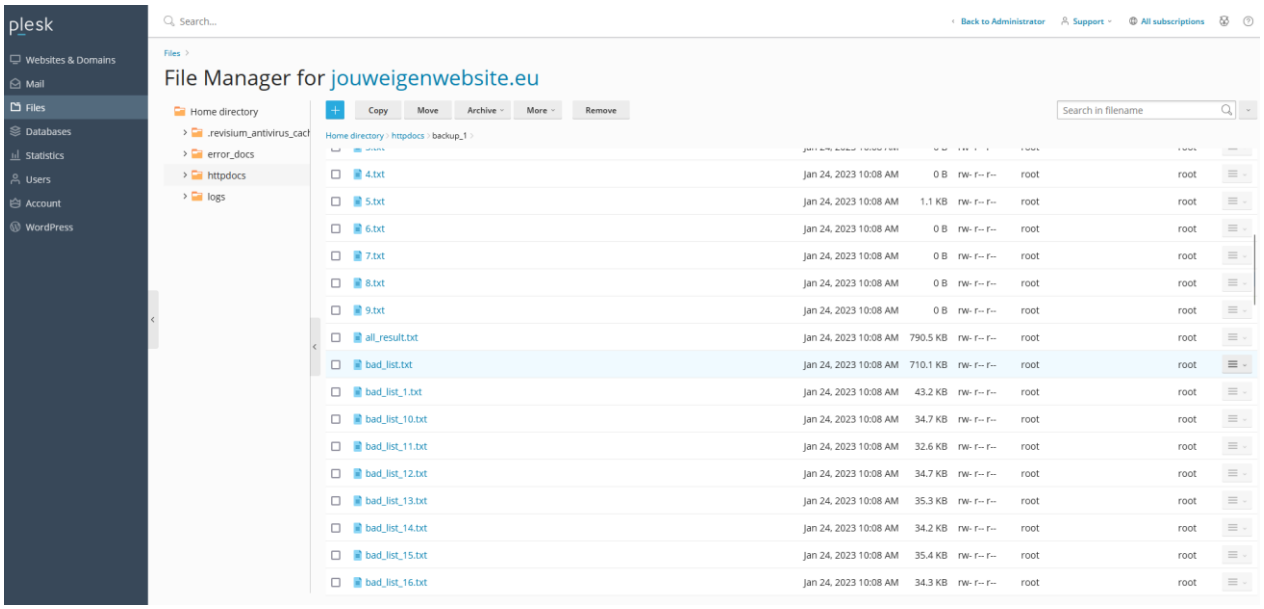
Ga vervolgens naar files (Links in het paars), en ga door alle bestanden heen die zich in de Imunify lijst bevinden.

In dit voorbeeld gebruik ik een gehackte wordpress website, ten alle tijden is het raadzaam om de orginele wordpress bestanden na te lopen om te zien of dit een orgineel bestand is, waar de content aangepast is door de hack, of dat het gehele bestand weg kan.



Zoals te zien is op de WordPress Github repo (https://github.com/WordPress/WordPress/) bestaat het bestand wp-blog.php niet.
Haal in deze dus het gehele bestand weg!

De volgende bestanden in de tabel staan in de map backup_1.



Zoals te zien is, staat deze gehele map vol met bestanden van de hackers.
Verwijder deze map dus gewoon in zijn geheel.

Optie 2:

Log in op plesk, en ga naar ‘ImunifyAV’.
Klik vervolgens op de ‘Clean Malware’ knop.
ImunifyAV zal hiermee proberen alle malafide code weg te halen uit de bestanden.
Let hier in wel op! Dit kan zorgen dat uw website niet meer naar behoren functioneert, u bent zelf geheel verantwoordelijk voor het geval dat uw website hier door kapot gaat, en zult dit dus ook zelf moeten repareren.

Vervolg stappen:
Het opschonen van de malafide bestanden is stap 1, echter zult u hierna ook stappen moeten ondernemen om te zorgen dat uw website niet weer direct gehackt word.
De kwetsbaarheid zit nog steeds in uw website, en deze zal in geen tijd weer gevonden en geëxploiteerd zijn door de hacker.

In het geval dat uw website na de automatische opschoning niet meer werkt, hebben wij eventueel backups! Let op, de kosten voor het terugzetten van de backup is €100,- exc BTW.

Zorg dus dat u;

- Uw CMS of andere software die draait op uw website up to date is.
- Uw software up to date houd in de toekomst! Kijk naar automatische update processen, of check geregeld zelf of er updates zijn.
- Installeer bepaalde beveiligings plugins op uw website, en neem verdere stappen om te zorgen dat uw website veilig is (https://www.wpbeginner.com/wordpress-security/)