SiteSafe

Rapportage

Security Audit voor CFConsultancy

Rapport Basic Security Audit Plus voor CFConsultancy

Introductie

In opdracht voor CFConsultancy zal SiteSafe het CMS “MiniCMS” controleren op beveiligingsrisico’s. Het gekozen “pakket” is Basic Security Audit Plus.

De Basic Security Audit Plus (kortweg BSA+) is een snelle Audit op de front-end van de website. De front-end is de website die de bezoekers te zien krijgen. De website is met behulp van de Security Checklist gecontroleerd op de beveiliging.

Op de volgende pagina’s zal worden vermeld welke kwetsbaarheden zich bevinden op de website. Tevens zal worden vermeld wáár deze kwetsbaarheden zich bevinden. Met behulp van de Security Checklist en de resultaten op de volgende pagina’s, kunt u de gevonden kwetsbaarheden laten oplossen door een erkend bedrijf.

Algemene indruk

Het CMS ziet er netjes en overzichtelijk uit. De code waarin het CMS is geschreven (PHP) is iets verouderd, dat zou problemen kunnen opleveren in de nieuwere versies van PHP. Er is echter wel aan SQL-injecties gedacht, dat is dus een pluspunt.

Er is expliciet gekozen om niet naar de back-end van het systeem te kijken.

In Bijlage A is de Security Checklist bijgesloten. Deze checklist bevat een aantal criteria die wel of juist niet aanwezig moet zijn in het CMS. In het volgende onderdeel wordt deze checklist bekeken.

Constateringen

Hieronder staan, in de volgorde zoals deze te vinden is in de Security Checklist (Bijlage A) de constateringen

Het CMS voldoet aan alle gecontroleerde punten uit de Security Checklist.

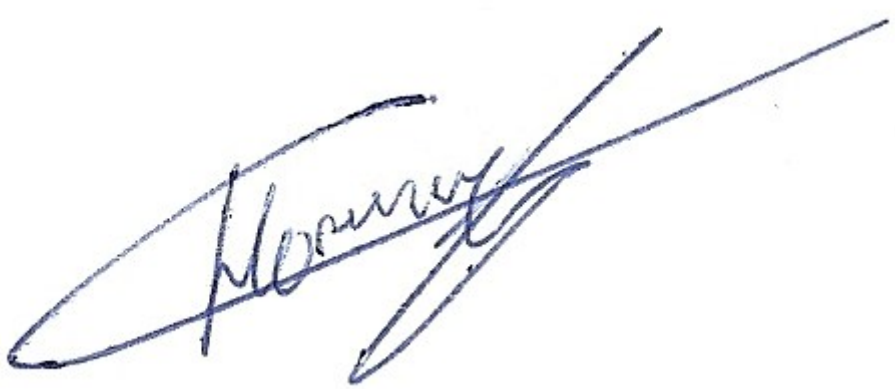
De overige punten zijn niet opgenomen omdat deze niet zijn gevonden binnen de website, of omdat deze zich in de back-end van de website bevinden.

Conclusie

De beoordeling van de Security Audit op het CMS is optimaal.

Doordat aan alle punten uit de Security Checklist is voldaan, is het CMS optimaal beveiligd.
Het is niet mogelijk om door middel van een SQL-injectie data uit de database op te halen.
Het is niet mogelijk om lokale of externe bestanden in te laden in de website.
Het is niet mogelijk om door middel van een XSS-injectie de inhoud van de website te veranderen.
De administratie is beveiligd tegen een brute-force aanval, het wachtwoord kan niet worden geraden.

Deze audit is uitgevoerd door Chris Horeweg, eigenaar SiteSafe.



Bijlage A: Security Checklist

De bijlage bevind zich in de e-mail en heeft de naam “SiteSafe Security Checklist.pdf”

Bijlage B: Verwijzingen naar de website

Er zijn geen verwijzingen naar de website.

Bijlage C: Technische informatie over constateringen

- Front-end: Het zichtbare gedeelte van de website waar een bezoeker en/of klant mee te maken heeft.
- Back-end: De achterkant/administratie van een website, waar de eigenaar zijn/haar website kan beheren.
- Inladen/Includen: Het inladen van een specifiek bestand
- PHP: Programmeertaal waar de website in is gemaakt
- SQL-injectie: Via de browser extra informatie uit de database halen, waaronder bijvoorbeeld inlog-gegevens van klanten.
- XSS-injectie: Via de browser de inhoud op de website aanpassen, waardoor de inhoud niet authentiek is.