SiteSafe Website Audit Checklist

Inhoud

De inhoud van dit document bevat een lijst met punten die zijn afgewerkt en extra uitleg bij deze punten.

Resultaten uitleg

Icoon	Uitleg
	De test is uitgevoerd en de resultaten waren goed
	De test is uitgevoerd en de resultaten waren niet goed
	De test is niet uitgevoerd

#	Omschrijving	Resultaat	Referentie
1.0	**Software**		
1.1	Apache heeft een veilige versie		
1.2	MySQL heeft een veilige versie		
1.3	PHP heeft een veilige versie		
1.4	PHP is veilig geconfigureerd		
2.0	**Authenticatie**		
2.1	Bruteforce-login is niet mogelijk		
2.2	Wachtwoorden worden niet per mail verstuurd, of slechts eenmalig		
2.3	Wachtwoord opgeven bij wijzigen instellingen/gegevens		
2.4	Oude wachtwoord opgeven bij wijzigen wachtwoord		
2.5	Geen gegevens in cookies		
2.6	Wachtwoord vergeten niet op basis van geheime vraag		
2.7	Bij iedere pagina wordt gekeken naar de authenticatie		
2.8	Sessies zijn gekoppeld aan IP-adres (geen Sessie Hijacking mogelijk)		
3.0	**User input**		
3.1	User input wordt altijd “puur” opgeslagen, bij het ophalen “sanitized”		
3.2	XSS-Injectie is niet mogelijk		
3.3	SQL-Injectie is niet mogelijk		
3.4	Geuploade bestanden staan niet in publieke map		
3.5	Geuploade bestanden worden niet gecontroleerd op MIME-type		
3.6	Bij validatie, is er altijd server-side validatie		
4	**Algemeen**		
4.1	Foutmeldingen (debug) worden niet getoond aan de gebruiker		
4.2	Robots.txt bevat geen gevoelige informatie		
4.3	Er zijn geen oude/tijdelijke bestanden aanwezig		
4.4	Er zijn geen oude/tijdelijke gebruikers aanwezig		
4.5	Wachtwoord wordt ge-encodeerd opgeslagen		
4.6	E-mail formulier kan niet worden misbruikt door spammers		
4.7	Local File Inclusion is niet mogelijk		
4.8	Remote File Inclusion is niet mogelijk		
4.9	Cross Site Request Forgery is niet mogelijk		