

Rapport

Pentestrapport Voorbeeld B.V.

Fictief voorbeeld

Dit rapport is volledig verzonnen om te laten zien hoe een rapport van Blackbox Cyber eruitziet. Voorbeeld B.V. en uw-webshop.nl bestaan niet; er is geen echt systeem getest.

Opdrachtgever

Voorbeeld B.V.

Dienst

Pentest Website

Kenmerk

BC-2026-014

Scope

uw-webshop.nl, zonder inlog

Testperiode

2 testdagen

Methode

OWASP WSTG

1. Samenvatting voor de ondernemer

We vonden **1 bevinding met een hoog risico**, 1 met een middelmatig risico en 1 met een laag risico. De belangrijkste: de kortingscode voor nieuwe klanten kan onbeperkt opnieuw worden gebruikt. Dat kost direct omzet. **Los die als eerste op.** Alle drie de punten zijn met beperkte moeite door uw bouwer op te lossen.

	Hoog	Middel	Laag
Aantal bevindingen	1	1	1

2. Overzicht

Nr.	Bevinding	Ernst	Hertest
BC-01	Kortingscode kan onbeperkt opnieuw gebruikt worden	Hoog	opgelost
BC-02	Beheerpagina zonder limiet op inlogpogingen	Middel	opgelost
BC-03	Foutmelding toont de versie van de software	Laag	opgelost

3. Bevindingen in detail

BC-01 Hoog Kortingscode kan onbeperkt opnieuw gebruikt worden

Wat we vonden	De code WELKOM10 is bedoeld voor één keer per klant. Door de bestelling af te breken en opnieuw te beginnen, werkt de code steeds opnieuw, ook op andere accounts.
Bewijs	1) Code invoeren in de winkelwagen. 2) Betaalstap afbreken. 3) Nieuwe bestelling: de code wordt opnieuw geaccepteerd. (In een echt rapport: schermafbeeldingen en verzoeken.)
Waarom het ertoe doet	Klanten of bots kunnen onbeperkt korting krijgen. Directe omzetschade.
Oplossing	Controleer het gebruik van de code op de server bij het afronden van de bestelling, niet alleen bij het invoeren. Koppel de code aan het klantaccount én het e-mailadres.
Referentie	OWASP Top 10: A04 Insecure Design · WSTG-BUSL

BC-02 Middel Beheerpagina zonder limiet op inlogpogingen

Wat we vonden	De inlogpagina voor beheerders accepteert onbeperkt wachtwoordpogingen en heeft geen tweestapsverificatie.
Bewijs	Met een beperkt aantal geautomatiseerde pogingen (binnen de afgesproken grens) bleef de pagina pogingen accepteren.
Waarom het ertoe doet	Een aanvaller kan automatisch wachtwoorden raden. Lukt dat, dan heeft hij volledige toegang tot de webshop.
Oplossing	Zet tweestapsverificatie aan voor alle beheerders en blokkeer tijdelijk na 5 mislukte pogingen.
Referentie	OWASP Top 10: A07 Identification and Authentication Failures · WSTG-ATHN

BC-03 Laag Foutmelding toont de versie van de software

Wat we vonden	Een niet-bestaande pagina toont een foutmelding met de naam en versie van de webshopsoftware.
Bewijs	Een willekeurig adres opvragen geeft een foutpagina met de versie.
Waarom het ertoe doet	Een aanvaller weet direct welke bekende lekken hij kan proberen.
Oplossing	Toon bezoekers een algemene foutpagina zonder technische details.
Referentie	OWASP Top 10: A05 Security Misconfiguration · WSTG-ERRH

4. Belangrijk om te weten

Een test is een momentopname met de afgesproken technieken en tijd. Dat betekent niet dat er geen andere zwakke plekken zijn of later ontstaan. Daarom adviseren wij een hertest na herstel en regelmatige controle. Wij testen alleen na schriftelijke toestemming van de eigenaar van het systeem.

Uitgevoerd door: Enes, Blackbox Cyber · +31 485 234 002 · info@blackboxservice.nl