

## Open deur of gecontroleerde toegang?\*

Uw werknemer of klant wil gebruik maken van uw diensten op alle mogelijke tijdstippen, vanaf alle mogelijke locaties. Om aan deze behoefte in de markt te kunnen voldoen heeft u als onderneming steeds meer applicaties via het web toegankelijk gemaakt. Misschien vraagt u zich af hoeveel risico u daarbij loopt. Een webapplicatie kan immers vanuit de hele wereld worden benaderd. Kunnen kwaadwillende personen via uw webapplicatie toegang krijgen tot bedrijfsgevoelige informatie? Kunt u garanderen dat de persoonlijke gegevens van klanten of medewerkers veilig zijn? Kunnen kwaadwillende personen misschien de beschikbaarheid van uw applicatie schaden ten koste van uw omzet? Kortom, hoe veilig is uw applicatie?

Om dit soort vragen in deze groeiende markt te kunnen beantwoorden biedt PwC Advisory de Web Application Security Assessment (WASA).

### De Web Application Security Assessment bij klanten

#### Een online applicatie voor klanten van een financiële dienstverlener

Een financiële dienstverlener heeft ons gevraagd een onderzoek uit te voeren naar de beveiliging van klantgegevens binnen zijn webapplicatie. Tijdens de Web Application Security Assessment zijn onze professionals er in geslaagd om alle klantgegevens van de financiële dienstverlener te downloaden. De klant heeft het rapport van PwC gebruikt om de gevonden zwakheden samen met een derde partij op te lossen.

De zwakte werd veroorzaakt door het opslaan van login-gegevens in een cookie aan de kant van de gebruiker. Hierdoor was het mogelijk om deze login-gegevens aan te passen en zodoende zonder gebruik te maken van een geldige gebruikersnaam en wachtwoord combinatie als een willekeurige gebruiker in te loggen. Daarnaast werden in de scans op de infrastructuur en firewall verschillende zwakheden aangetroffen, waaronder ontbrekende patching en overbodige firewall regels.

Tijdens deze assessment hebben wij de volledige site in kaart gebracht door middel van een recursieve scan. Na beoordeling van de resultaten zijn gerichte aanvallen uitgevoerd op de dynamische delen van de website. Deze aanvallen hadden onder andere betrekking op "SQL injection", "brute force login" en "parameter tampering".

#### De website van een organisatie in de entertainment & media sector

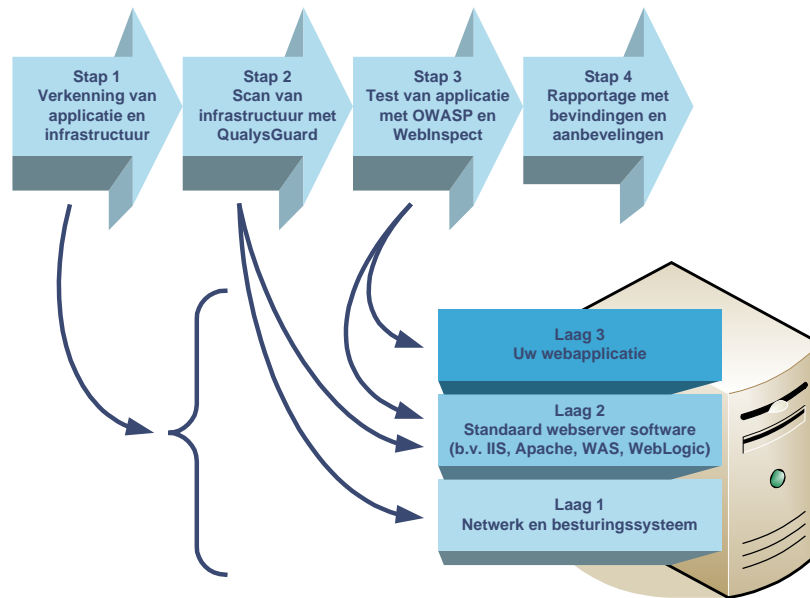
In verband met een negatief bericht op een security website over zwakheden in de website van een bekende organisatie in de entertainment & media sector heeft deze organisatie PwC gevraagd een security assessment uit te voeren op de applicatie. Uit de tests zijn geen aanwijzingen gebleken van zwakheden in de website. Het management van de organisatie heeft met het rapport van PwC uiteindelijk besloten een grote mailing-campagne te laten doorgaan.

#### Een online aangeboden applicatie in ontwikkeling

Een aanbieder van een online applicatie voor bedrijven (een "application service provider") heeft ons gevraagd een Web Application Security Assessment op deze applicatie uit te voeren, alvorens deze in productie zou gaan. Uit de assessment kwamen een groot aantal zwakheden naar voren. Zo konden gebruikers in gegevens van andere bedrijven kijken. Ook kon een lijst van gegevens van alle bedrijven in het systeem worden opgevraagd. De ontwikkelaar heeft het rapport van PwC gebruikt om de gaten te dichten en wil in een vervolgtraject de applicatie laten certificeren.

Er bleek zwakke encryptie gebruikt te worden, waardoor af luisteren van communicatie mogelijk werd. De inhoud van de achterliggende database kon worden gewist door een "SQL injection" aanval. Gegevens tussen verschillende gebruikers (in dit geval dus bedrijven) bleken niet goed gescheiden. Door sessie parameters te manipuleren konden gegevens van andere gebruikers worden opgevraagd.

## De Web Application Security Assessment aanpak



De Web Application Security Assessment (WASA) is een penetratietest die efficiëntie combineert met een hoge kwaliteit. Dit doen wij op de volgende manier:

- Wij zoeken naar kwetsbaarheden in alle lagen van een website: in het netwerk en besturingssysteem, in de software die gebruikt wordt om de webapplicatie in te draaien en in de webapplicatie zelf.
- Wij gebruiken QualysGuard als tool om kwetsbaarheden op infrastructuurniveau op te sporen. Dit is een volledig geautomatiseerd proces. Op deze manier testen wij altijd op de laatst bekend geworden kwetsbaarheden.
- Op applicatieniveau testen wij juist niet volledig automatisch. Onze professionals zullen de beveiliging op applicatieniveau handmatig testen. Om tot kwalitatieve, herhaalbare resultaten te komen wordt daarbij de steeds belangrijker wordende OWASP checklist gebruikt. Onze professionals maken gebruik van WebInspect als gereedschapsset om deze evaluatie efficiënt uit te kunnen voeren.
- Wij schrijven een rapportage met bevindingen en aanbevelingen. Hierin beogen wij de zuiver technische feiten in verband te brengen met de échte beveiligingsrisico's en concrete aanbevelingen te doen om de risico's te verminderen.

Voor de meeste webapplicaties kunnen wij de WASA uitvoeren voor een vaste prijs van EUR 8.000,-.

## Meer informatie

Indien u behoefte heeft aan meer informatie of vragen heeft over deze dienstverlening, neemt u dan contact op met Otto Vermeulen of Arjan Zwikker, beiden bereikbaar via telefoonnummer 020 568 1660. Naast de standaard Web Application Security Assessment leveren wij ook security reviews op maat, bijvoorbeeld security scans van een gehele infrastructuur. Ook kunnen wij uw Internet omgeving testen op zwakheden die door kwaadwillende websites kunnen worden uitgebuit (denk hierbij bijvoorbeeld aan spyware).