IngramMicro
FlexibleServices

INGRAM MICRO

Web Application Scanning (WAS)

Het Ingram Micro Cyber Security Center of Excellence team is opgericht met de visie om te helpen het Cyber Security potentieel te ontsluiten. Het team, dat gevestigd is in Utrecht, biedt een reeks gespecialiseerde Cyber Security consultancy- en trainingsoplossingen aan onze Business en Channel Partners.

Met een services portfolio bestaande uit technische assessments, consultancy en managed security services zijn we in een zeer sterke positie om onze channel partners te helpen om elke cyber security deal te winnen. We doen dit door onze partners volledig te ondersteunen bij complexe security vraagstukken en de mogelijkheid te bieden om zelf cyber security diensten (door) te ontwikkelen en verder te laten groeien om zo lucratieve white-labelled beveiligingsdiensten aan te bieden aan eindklanten.

INGRAM MICRO

Cyber Security Center

Web Application Scanning (WAS), ook wel vulnerability scanning van webapplicaties genoemd, is een automatisch beveiligings-programma dat zoekt naar softwarekwetsbaar-heden binnen webapplicaties. De software crawlt eerst en bouwt een softwareconstructie van de gehele website. Dit geeft de scanner inzicht in de applicatie, de scanner voert vervolgens een automatische audit uit op veelvoorkomende beveiligingslekken door |een reeks webaanvallen uit te voeren. De consultants verifiëren deze beveiligingslekken vervolgens handmatig.

De doelstellingen van Web Application Scanning (WAS) zijn:

- Het identificeren van beveiligingslekken en -problemen in de website van de klant met behulp van een kwetsbaarhedenscanner.
- Problemen die worden geïdentificeerd door de kwetsbaarheidsscanner worden hand-matig geïnspecteerd en gerapporteerd.

Dit type beoordeling omvat de hieronder beschreven stappen:

- Scannen en crawlen: informatie verzamelen over de draaiende webapplicatie, inclusief netwerkpoorten, webserverversie, geïnstal-leerde modules, versienummers, en door alle mappen en bestanden die op de website kunnen bestaan crawlen.
- Identificeer kwetsbaarheden: voortbouwend op de informatie die in de vorige fase is verzameld, zal de consultant handmatig het bestaan van webkwetsbaarheden of be-veiligingsfouten beoordelen door speciaal geconstrueerde verzoeken naar de webap-plicatie te sturen om kwetsbaarheden en beveiligingszwakheden te identificeren.
- Resultaatanalyse: beoordeling van de reacties van de applicatie op webverzoeken die in de vorige fase zijn gedaan, en het handmatig verifiëren van de geïdentificeerde webkwetsbaarheden en het elimineren van valspositieven.
- Rapportage: rapporteren van de geïdentifi-ceerde webkwetsbaarheden inclusief de im-pact rating en de aanbevolen actie om deze te verminderen. Ingram Micro maakt gebruik van de door de industrie aanbevolen kwets-baarheidsbeoordelingstools om kwetsbaar-heden in webapplicaties te identificeren. De consultant verifieert vervolgens handmatig de resultaten en consolideert een rapport met de relevante bevindingen.

Na afronding van de beoordeling wordt een gedetailleerd rapport naar de klant gestuurd met daarin het volgende:

- Managementsamenvatting: samenvatting van het doel van deze beoordeling, evenals een korte uitleg van de bedreigingen waar-

IngramMicro
FlexibleServices
INGRAM MICRO

aan de organisatie wordt blootgesteld vanuit een zakelijk perspectief.

- Bevindingen: een gedetailleerde, technische uitleg van de bevindingen van de beoordeling, samen met stappen en bewijzen van de bevindingen.
- Conclusie & aanbevelingen: in dit hoofdstuk vindt u de laatste aanbevelingen en een samenvatting van de kwesties die tijdens de beveiligingsbeoordeling zijn gevonden.

Meer weten over onze Cyber Security Assessment services?
Neem contact op met het Ingram Micro Cyber Security Center of Excellence (COE) via cs-coe-weur@ingrammicro.com of met uw Account Manager.

IngramMicro
FlexibleServices
INGRAM MICRO