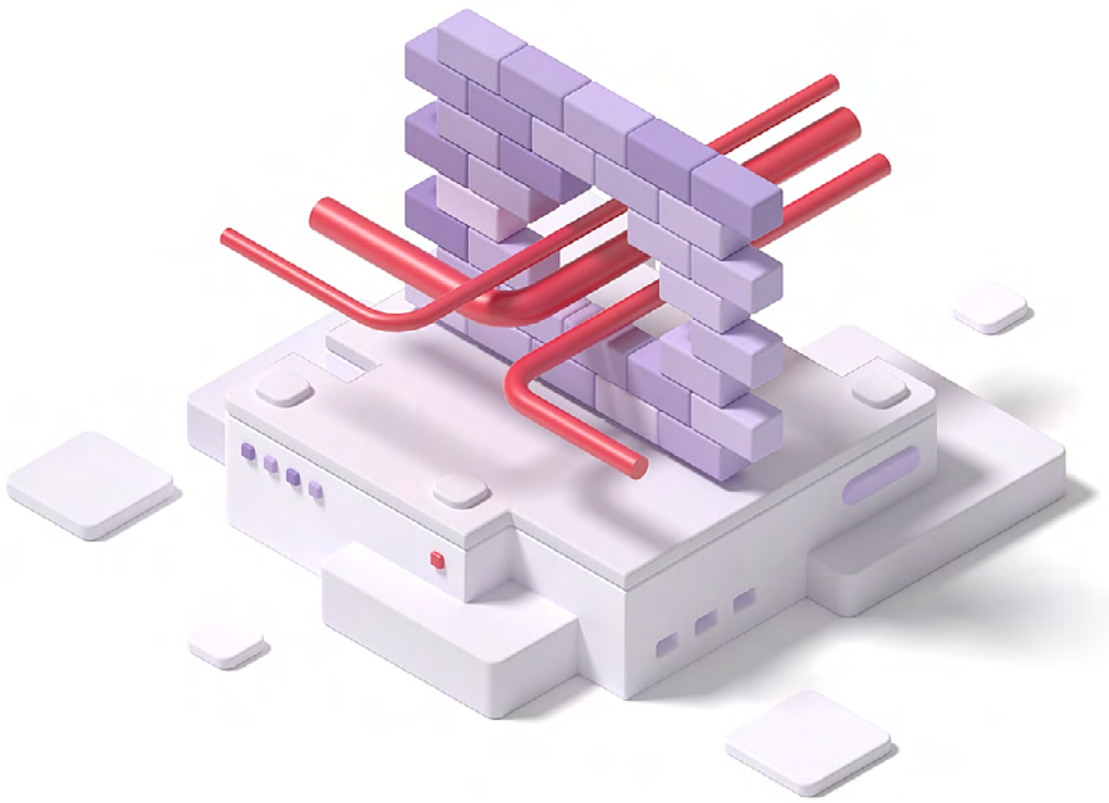
WebSec

Penetratietests door WebSec

Let us in to keep them out



Vulnerability Assessment / Penetration Testing (VAPT)

In het hedendaagse digitale tijdperk is robuuste cybersecurity essentieel voor elke organisatie. Gezien de snel evoluerende aard van cyberdreigingen, vormt het adequaat beschermen van persoonlijke gegevens en bedrijfsdata een aanzienlijke uitdaging voor vele ondernemingen. WebSec biedt gespecialiseerde beveiligingsdiensten aan die essentieel zijn om deze uitdagingen het hoofd te bieden.

Onze diensten richten zich op het uitvoeren van grondige controles op kwetsbaarheden in computersystemen, code en software, om potentiële risico's proactief te identificeren en te adresseren voordat ze kunnen worden uitgebuit door kwaadwillenden.

Bij WebSec personaliseren we onze penetratietestdiensten om nauw aan te sluiten bij de unieke vereisten van elke organisatie waarmee we samenwerken. U kunt vertrouwen op onze expertise en toewijding om de veiligheid en integriteit van uw informatiesystemen te waarborgen.

Onze diensten

Bij WebSec bieden wij een breed scala aan geavanceerde penetratietestdiensten om de kritieke activa van uw organisatie te beveiligen.

Soorten penetratietests die wij uitvoeren:

☑ Pentest voor webapplicaties

Onze pentests voor webapplicaties zijn gericht op het identificeren van beveiligingskwetsbaarheden in webgebaseerde software en applicaties. Dit zorgt ervoor dat klantgegevens en bedrijfskritische informatie optimaal beschermd zijn tegen cyberaanvallen.

☑ Pentest voor mobiele applicaties

Deze pentest richt zich op het waarborgen van de veiligheid van uw mobiele applicaties, waarbij we streven naar een veilige en betrouwbare gebruikservaring voor uw eindgebruikers.

☑ Pentest voor infrastructuur

Onze infrastructuurpentests evalueren uw netwerkinfrastructuur, inclusief servers, firewalls en routers, om zwakke plekken en mogelijke kwetsbaarheden te identificeren en te verhelpen.

☑ Pentest voor netwerk & test voor netwerksegmentering

Deze service is gericht op het detecteren van beveiligingslacunes in uw netwerk en de segmentatie ervan, wat bijdraagt aan effectievere en robuustere beveiligingsstrategieën.

☑ Pentest voor IoT

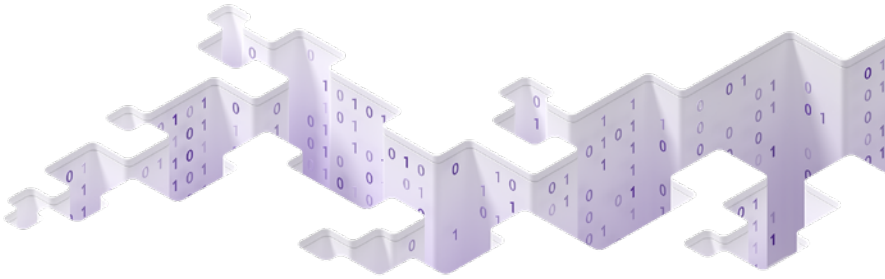
Onze IoT-pentests zijn ontworpen om de veiligheid van uw Internet of Things-apparaten te verifiëren, waarbij we zorgen dat uw slimme apparaten en netwerken bestand zijn tegen hedendaagse cyberdreigingen.

☑ Pentest voor SCADA/ICS

Deze pentest focust op het waarborgen van de veiligheid van industriële besturingssystemen (ICS), door te verzekeren dat deze systemen zijn getest en geconfigureerd volgens de beste beveiligingsnormen in de industrie.

☑ Pentest voor API/endpoints

Onze pentests voor API's en endpoints zijn bedoeld om mogelijke kwetsbaarheden te ontdekken, waarbij de integriteit en veiligheid van uw gegevens vooropstaan.



Pentest voor compliance

WebSec begrijpt dat compliance met de wettelijke vereisten in het huidige digitale landschap cruciaal is. Daarom bieden we meerdere pentests voor compliance om u te helpen aan branchespecifieke normen en voorschriften te voldoen.

Pentest voor NEN-7510 (voor medische instellingen)

De pentests voor NEN-7510 zorgen ervoor dat uw organisatie aan de strengste normen voor informatiebeveiliging in de gezondheidszorg voldoet.

Pentest voor ISO 27001 (voor kwaliteitsborging)

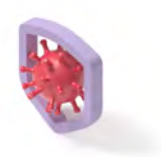
De pentests voor ISO 27001 helpen u bij het evalueren van uw managementsysteem voor informatiebeveiliging en zorgen ervoor dat u aan de internationale normen voldoet.

Pentest voor BIO (voor Nederlandse overheidsinstellingen)

Deze pentest helpt aan de Baseline Informatiebeveiliging Overheid (BIO)-vereisten te voldoen, zodat uw gevoelige gegevens veilig blijven.

Pentest voor PCI-DSS (voor financiële instellingen)

De pentests voor PCI-DSS evalueren de compliance met de Payment Card Industry Data Security Standard (PCI-DSS) van uw organisatie en garanderen de veiligheid van de financiële gegevens van uw klanten.



Pentest voor CoronaCheck-app (voor Nederlandse centra/laboratoria voor coronatests)

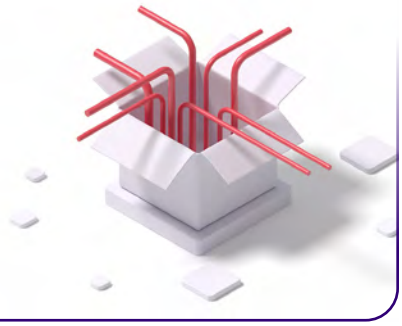
Deze pentest is ontworpen om u te helpen aan de strenge eisen voor het beveiligen van gevoelige persoonlijke gezondheidsinformatie te voldoen.

Verschillende Aanpakken in Pentesting

Bij WebSec begrijpen we dat elke organisatie unieke eisen stelt aan penetratietests. Daarom bieden wij diverse aanpakken aan, afgestemd op verschillende pentestscenario's, om precies aan de specifieke behoeften van onze klanten te voldoen.

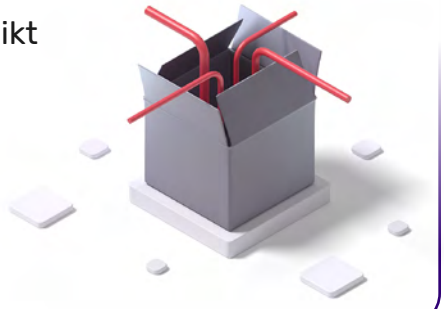
White Box

Onze white box pentest is ideaal voor organisaties die een diepgaande evaluatie van hun systemen of applicaties wensen. Met volledige toegang tot en kennis van de broncode, zijn onze beveiligingsexperts in staat om nauwkeurig kwetsbaarheden en zwakke plekken te identificeren.
Voordelen: Gedetailleerde inzichten in de beveiligingsstatus.
Nadelen: Minder representatief voor externe aanvalsscenario's.



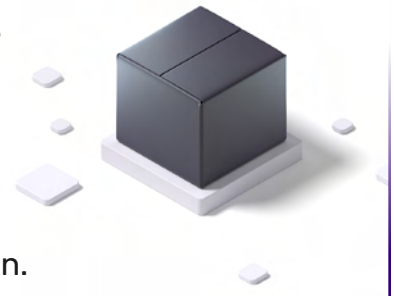
Grey Box

Onze grey box pentest biedt een evenwichtige aanpak, geschikt voor organisaties die zowel uitgebreide tests als realistische aanvalsscenario's wensen. Met beperkte voorkennis van uw systemen simuleren we realistische aanvallen om potentiële beveiligingsfouten in uw infrastructuur te identificeren.
Voordelen: Evenwicht tussen diepgang en realisme.
Nadelen: Mogelijk minder gedetailleerd dan white box tests.



Black Box

Onze black box pentest is perfect voor organisaties die hun detectie- en responsvermogen op cyberaanvallen willen testen. Zonder voorkennis van uw systemen of applicaties, simuleren we realistische aanvalsscenario's om potentiële beveiligingsrisico's te ontdekken en te helpen bij het verbeteren van uw verdedigingsmechanismen.
Voordelen: Test het vermogen van uw organisatie om onbekende aanvallen te detecteren.
Nadelen: Lager risico om specifieke kwetsbaarheden te ontdekken.

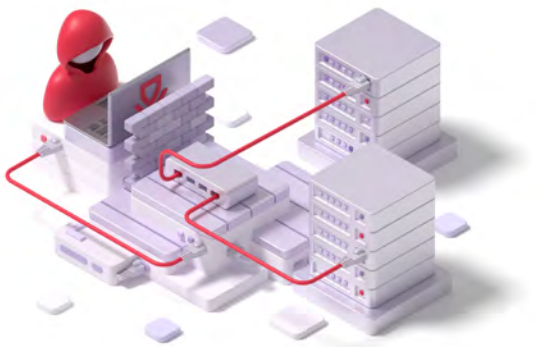


Onderzoeksgebied van pentests

Een effectieve penetratietest begint met een duidelijk inzicht in de onderzoeksgebieden. Of het nu gaat om externe of interne systemen, het identificeren van kwetsbaarheden is essentieel voor de bescherming van de kritieke bedrijfsmiddelen van een organisatie.

Externe pentest

Met onze externe pentests evalueren we de beveiliging van de naar buiten gerichte systemen, applicaties en netwerken van uw organisatie. Deze tests, uitgevoerd op uw IP-adressen of domeinen, zijn gericht op het detecteren van kwetsbaarheden die kunnen worden uitgebuit door externe aanvallers.



Interne pentest

Onze interne pentest is ideaal voor organisaties met uitgebreide interne systemen en netwerken. Uitgevoerd door onze ervaren beveiligingsexperts, hetzij op afstand via een VPN of fysiek op locatie, richt deze test zich op het opsporen van kwetsbaarheden binnen uw interne infrastructuur.

Ons proces voor pentests

1. Intake
2. Vrijwaringsverklaring en contract voor pentest
3. Planning
4. Pentests
5. Rapportage
6. Nazorg

WebSec heeft een systematische en grondige aanpak om pentests uit te voeren. Hieronder kunt u ons volledige proces voor penetratietests vinden.

1. Intake: De intakefase omvat een diepgaand gesprek om de unieke behoeften en specifieke eisen van uw organisatie voor de penetratietest te begrijpen.

2. Vrijwaringsverklaring en Pentestcontract: We garanderen naleving van wettelijke vereisten en volledige transparantie door het verstrekken van een vrijwaringsverklaring en een gedetailleerd pentestcontract. Dit document omvat de scope, het tijdsbestek, en de levering van producten en diensten.

3. Planningsfase: In de planningsfase ontwikkelen we een gedetailleerd strategieplan, waarin de te onderzoeken kwetsbaarheden, de gebruikte testmethoden, en de tijdlijn van de pentest zijn opgenomen.

4. Uitvoering van Pentests: Ons team van deskundige ethische hackers voert de pentest uit met de meest geavanceerde hulpmiddelen en technieken, gericht op het identificeren van potentiële beveiligingszwakheden.

5. Rapportage: Na afronding van de pentest leveren we een uitvoerig en gedetailleerd rapport, inclusief een analyse van de gevonden kwetsbaarheden en aanbevelingen voor effectieve herstelstrategieën.

6. Nazorg: Onze betrokkenheid eindigt niet bij de afronding van de pentest. We bieden uitgebreide nazorg, waaronder monitoring en ondersteuning, om de beveiliging van uw bedrijfsmiddelen continu te waarborgen.

Hoe Wij de Kwaliteit van Onze Pentests Waarborgen

Bij WebSec streven we naar de hoogste kwaliteit in onze pentests en rapportages. We hanteren daarom een scala aan geavanceerde beveiligingstechnieken en -normen, waaronder:

OWASP: We volgen de OWASP-normen, waaronder ASVS, WSTG en TOP 10 om een grondige aanpak voor het opsporen van kwetsbaarheden te garanderen.

PTES-norm: We houden ons aan de Penetration Testing Execution Standard (PTES) om consistentie en volledigheid van onze testmethodologie te waarborgen.

CCV-pentest: Het wereldwijde keurmerk voor CCV-pentests geeft aan dat we een geverifieerde aanbieder van penetratietests zijn. Deze certificering betekent dat we de normen volgens NEN en ISO/IEC 17065 naleven en garandeert dat we naadloze pentestdiensten leveren.

Ons team bestaat uit ervaren en OSCP-gecertificeerde beveiligingsexperts, met elk 2 tot 5 jaar ervaring in pentests of aanverwante specialismen. Wij zijn trots op onze expertise en de kwaliteit die we leveren aan onze klanten.

WebSec Penetratietests: Deliverables

Bij WebSec gaan onze penetratietests verder dan alleen het uitvoeren van de tests; we focussen op het leveren van concrete resultaten en hulpmiddelen voor uw organisatie.
Na voltooiing van een penetratietest ontvangt u de volgende deliverables:

Belangrijkste producten en diensten:

Technisch rapport

Een gedetailleerde analyse van de resultaten van de penetratietest, inclusief opgespoorde kwetsbaarheden en aanbevolen oplossingen.

Managementrapport

Samenvatting die speciaal voor leidinggevenden op managementniveau is opgesteld en is gericht op strategische inzichten en de gevolgen van risicobeheer.

Extra optie

VAPT-certificering (Vulnerability Assessment and Penetration Testing Certificate)

Een officiële certificering voor de succesvolle afronding van grondige tests en het voldoen aan vereisten voor veiligheid.

Digitale badge

Straal uw beveiliging uit naar uw klanten met een Digitale Badge. Dit digitale embleem kan op uw platforms worden weergegeven om uw toewijding aan krachtige beveiliging te tonen.


WebSec

CERTIFICATE

OF SECURITY AUDIT

No. _____

This is to acknowledge that

Has successfully conducted and passed the in-depth security audit by remediating the found vulnerabilities during the penetration test.

Assessment Approach: Date of Certification:

Assessment Type: Expiration Date:

Managing director of WebSec BV