

Veilige Websites



Wat is het?

- Iedere pagina met informatie of applicatie die je via een browser kunt vinden is een website, niet allen daarvan zijn veilige websites.
- Een veilige website maakt gebruik van een hoge:
 - confidentialiteit: versleuteling van de data zodat niemand daar inzage in heeft.
 - integriteit: het zeker zijn dat de website niet door anderen aangepast kan worden, dat de gebruiker weet dat dit de echte website is en vice versa.
 - beschikbaarheid: het zeker zijn dat de website gebruikt kan worden.
- Een website is voor iedereen ter wereld met een internetaansluiting bereikbaar.
- Wordt 24/7 aangevallen door kwaadaardige programma's en kwaadwillenden;
- Bij het bezoeken van een kwaadaardige of gehackte website kunnen er nare dingen gebeuren met het apparaat dat de pagina bezoekt.



Belang voor Nederland

- Vrijwel iedere vorm van informatievoorziening maakt gebruik van een website.
- Diverse interacties tussen burger en overheid verlopen via websites (bijvoorbeeld DigiD).
- Cruciaal voor de voortgang van, en het vertrouwen in, de digitale economie.



Gevolgen bij misbruik

- Legitieme pagina's kunnen ongezien veranderd worden in kwaadaardige pagina's die de apparatuur van gebruikers aanvallen.
- Illegale of onrust stokende beelden kunnen getoond worden, waarvan niet te bepalen is of het door de echte eigenaar geplaatst is of niet.
- Persoonsgegevens kunnen uitlekken die op lange termijn problemen veroorzaken zoals:
 - identiteitsdiefstal, vergrote kans om slachtoffer te worden van criminaliteit door bekend zijn van telefoonnummers, wachtwoorden, mailadressen, woonadressen of andere persoonsgegevens.
- Verstoring of aanpassing van de functie van de website, bijvoorbeeld:
 - betalingen in webshops naar een andere rekening laten gaan.
 - aankopen doen zonder te betalen.
 - onbruikbaar maken van de dienstverlening voor anderen.
- Verlies van vertrouwen met als gevolg het vermijden van digitale communicatie en middelen.



Is misbruik al eens voorgekomen?

- Ja, ontelbare keren over de hele wereld op kleine of middelgrote schaal.
- Ook op grote schaal zijn lekken bekend waar tienduizenden of zelfs honderduizenden websites kwetsbaar bleken te zijn.
 - Apache Struts (2018): een aanvaller kreeg volledige controle over de website door deze kwetsbaarheid. 2 dagen na publicatie van het lek, werd het gebruikt om een kwaadaardige code in tienduizenden kwetsbare sites te stoppen.
 - Heartbleed (2014): een lek in de versleutelde verbinding die veilige communicatie met websites mogelijk maakt, zorgde ervoor dat gevoelige informatie achterhaald kon worden op vrijwel iedere website.
 - Phishing aanvallen (doorlopend): mails worden gestuurd met links naar nagemaakte inlogportalen van bijvoorbeeld email of bancaire applicaties om gebruikers erin te luizen en vervolgens van hen te stelen (data of geld).
 - Nog veel meer voorbeelden te vinden.



Cybercrime specifieke relevante nationale wetgeving of andere richtlijnen

- Raakvlak met wetten zoals DGIA, TA, Wbni en DigiD normen;
- OWASP (Open Web Application Security Project)
 - Voornaamste vereniging op gebied van website beveiliging, wereldwijd erkend;
 - Onafhankelijk en grotendeels afhankelijk van vrijwilligers uit de securitywereld;
 - Creëert richtlijnen en oefenmateriaal voor veilig ontwikkelen (ASVS, MSVS) en stelt lijsten samen zoals de top 10 meest voorkomende fouten in webapplicaties.

Belangrijke webapplicatie hacks met concrete voorbeelden (6 min)

<https://www.youtube.com/watch?v=lj1Us6UWK74>



Uitleg van de verschillende OWASP top 10 kwetsbaarheden (10 min per stuk)

https://www.youtube.com/watch?v=rWHvp7rUka8&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD

