Websitetest: adagia.eu

Gefeliciteerd, je domeinnaam wordt spoedig in de **Hall of Fame** opgenomen!

100%

Bereikbaar via moderne internetadres (IPv6)

Domeinnaam ondertekend (DNSSEC)

Verbinding voldoende beveiligd (HTTPS)

Alle applicatie-beveiligingsopties ingesteld (Beveiligingsopties)

Modern adres (IPv6)

Goed gedaan! Je website is bereikbaar voor bezoekers die een moderne internetadres (IPv6) gebruiken, en daardoor volledig onderdeel van het moderne internet.

Nameservers

IPv6-adressen voor nameservers

Uitslag:
Twee of meer nameservers van je domeinnaam hebben een IPv6-adres.

Technische details:

Nameserver	IPv6-adres	IPv4-adres
ns3.firstfind.nl.	2a01:b940:1057::53	5.157.86.222
ns5.firstfind.net.	2a03:b0c0:1:e0::639:7001	178.128.167.58
ns4.firstfind.nl.	2a01:b940:1058::53	5.157.87.222

Testuitleg:
We testen of je domeinnaam tenminste twee nameservers met een IPv6-adres heeft. Dit sluit aan bij de eis van SIDN (beheerder van het .nl-domein) dat iedere .nl-domeinnaam tenminste twee nameservers moeten hebben.

IPv6-bereikbaarheid van nameservers

Uitslag:
Alle nameservers die een IPv6-adres hebben zijn bereikbaar via IPv6.

Testuitleg:
We testen of alle nameservers, die een AAAA-record met IPv6-adres hebben, bereikbaar zijn via IPv6.

Webserver

IPv6-adressen voor webserver

Uitslag:
Tenminste één van je webservers heeft een IPv6-adres.

Technische details:

Webserver	IPv6-adres	IPv4-adres
adagia.eu	2001:985:7ebb:1:211:32ff:fe8e:8bc3	212.238.211.4

Testuitleg:
We testen of er tenminste één AAAA-record met IPv6-adres voor je webserver is.

IPv6-bereikbaarheid van webserver

Uitslag:
Al je webservers met een IPv6-adres zijn bereikbaar via IPv6.

Testuitleg:
We testen of we je webserver(s) kunnen bereiken via IPv6 op alle beschikbare poorten (80 en/of 443). We testen alle IPv6-adressen die we ontvangen van je nameservers. Een deelscore wordt gegeven als niet alle IPv6-adressen bereikbaar zijn. Als een IPv6-adres (syntactisch) ongeldig is, dan beschouwen we dat als onbereikbaar.

Gelijke website op IPv6 en IPv4

Uitslag:
Je website op IPv6 lijkt gelijk aan je website op IPv4.

Testuitleg:
We vergelijken de webcontent die we van je webserver ontvangen via zowel IPv6 als IPv4 op alle beschikbare poorten (80 en/of 443). In het geval er meerdere IPv6-adressen en IP4-adressen zijn, dan pakken we één IPv6-adres en één IPv4-adres. Als het contentverschil niet groter is dan 10%, dan gaan we ervanuit uit dat de primaire webcontent gelijk is. Daardoor zullen ook websites met kleine verschillen (bijvoorbeeld door wisselende advertenties) slagen voor dit testonderdeel.

Ondertekende domeinnaam (DNSSEC)

Goed gedaan! Je domeinnaam is ondertekend met een geldige handtekening (DNSSEC). Daardoor zijn bezoekers die controle van domein-handtekeningen geactiveerd hebben, beschermd tegen gemanipuleerde vertaling van jouw domeinnaam naar kwaadaardige internetadressen.

DNSSEC aanwezigheid

Uitslag:
Je domein is met DNSSEC ondertekend.

Technische details:

Domein	Registrar
adagia.eu	Realtime Register B.V.

Testuitleg:
We testen of je domeinnaam ondertekend is met DNSSEC.

Als een domein via `CNAME` doorverwijst naar een ander domein, dan checken we (conform de DNSSEC-standaard) ook of het CNAME-domein ondertekend is met DNSSEC. Als het CNAME-domein niet ondertekend is, dan zal deze subtest een negatief resultaat tonen.

Let op: de geldigheid van de ondertekening wordt niet getest in deze subtest maar wel in de volgende subtest.

DNSSEC geldigheid

Uitslag:
Je domeinnaam is veilig oftewel 'secure', omdat zijn DNSSEC-handtekening geldig is.

Technische details:

Domein	Status
adagia.eu	secure

Testuitleg:
We testen of je domeinnaam is ondertekend met een geldige DNSSEC- handtekening.

Als een domein via `CNAME` verwijst naar een ander ondertekend domein, dan checken we (conform de DNSSEC-standaard) ook of de ondertekening van het CNAME-domein geldig is. Als de ondertekening CNAME-domein niet geldig is, dan zal deze subtest een negatief resultaat tonen.

Beveiligde verbinding (HTTPS)

Goed gedaan! De verbinding met je website is voldoende beveiligd (HTTPS). Gegevens die onderweg zijn tussen je website en haar bezoekers, zijn daardoor beschermd tegen afluisteren en manipulatie.

HTTP

HTTPS beschikbaar

Uitslag:
Je website biedt HTTPS aan.

Technische details:

Webserver-IP-adres	HTTPS aanwezig
2001:985:7ebb:1:211:32ff:fe8e:8bc3	ja
212.238.211.4	ja

Testuitleg:
We testen of je website bereikbaar is via HTTPS.

Als dat het geval is, dan testen we in de navolgende subtesten of HTTPS ook veilig is geconfigureerd conform de 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0'.

HTTPS garandeert de vertrouwelijkheid en integriteit van uitgewisselde informatie. Omdat het van de situatie afhangt hoe (privacy-)gevoelig en waardevol informatie is, een bezoeker van je website bepaalt hoe (privacy-) gevoelig en waardevol informatie is, is een veilige HTTPS-configuratie voor iedere website van belang. Ook triviale, publieke informatie kan door omstandigheden voor de gebruiker zeer gevoelig en waardevol zijn. Let op: vanwege performance-redenen wordt de HTTPS-deeltest alleen uitgevoerd voor het eerst beschikbare IPv6- en IPv4-adres.

HTTPS-doorverwijzing

Uitslag:
Je webserver verwijst bezoekers automatisch door van HTTP naar HTTPS op dezelfde domeinnaam.

Technische details:

Webserver-IP-adres	HTTPS-doorverwijzing
2001:985:7ebb:1:211:32ff:fe8e:8bc3	ja
212.238.211.4	ja

Testuitleg:
We testen of je webserver bezoekers automatisch doorverwijst van HTTP naar HTTPS op dezelfde domeinnaam (m.b.v. 301/302 redirect), óf dat deze ondersteuning biedt voor alleen HTTPS en niet voor HTTP.

In geval van doorverwijzing moet de domeinnaam eerst zelf 'upgraden' door een redirect naar zijn HTTPS-versie, voordat deze eventueel doorverwijst naar een andere domeinnaam. Dit zorgt er ook voor dat een webbrowser de HSTS-policy kan accepteren. Voorbeelden van correcte redirect-volgorde:

- `http://example.nl ⇒ https://example.nl ⇒ https://www.example.nl`
- `http://www.example.nl ⇒ https://www.example.nl`

Zie 'Webapplicatie-richtlijnen, Verdieping' van NCSC, richtlijn U/WA.05.

HTTP-compressie

Uitslag:
Je webserver ondersteunt HTTP-compressie, wat een beveiligingsrisico kan vormen.

Technische details:

Webserver-IP-adres	HTTP-compressie
2001:985:7ebb:1:211:32ff:fe8e:8bc3	ja
212.238.211.4	ja

Testuitleg:
We testen of je webserver HTTP-compressie ondersteunt.

Bij het HTTP-protocol wordt compressie vaak gebruikt om de beschikbare bandbreedte efficiënter te gebruiken. HTTP-compressie maakt de beveiligde verbinding met je webserver echter kwetsbaar voor de BREACH-aanval. Weeg de voors en tegens van HTTP-compressie zorgvuldig tegen elkaar af. Wanneer u kiest voor het gebruik van HTTP-compressie, ga dan na of het mogelijk is om hieruit voortvloeiende potentiële applicatie-aanvallen te beperken. Een voorbeeld van een dergelijke maatregel is het beperken van de mate waarin een aanvaller de respons van de server kan beïnvloeden.

Dit testonderdeel controleert of de webserver op rootdirectory-niveau HTTP-compressie ondersteunt, maar controleert geen andere websitebronnen zoals plaatje en scripts.

Zie 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0' van NCSC, richtlijn B7-1 en tabel 11.

Niveau van vereistheid: Optioneel

HSTS

Uitslag:
Je webserver biedt een HSTS-policy aan.

Technische details:

Webserver-IP-adres	HSTS-policy
2001:985:7ebb:1:211:32ff:fe8e:8bc3	max-age=31536000; includeSubDomains; preload
212.238.211.4	max-age=31536000; includeSubDomains; preload

Testuitleg:
We testen of je webserver HSTS ondersteunt.

Browsers onthouden HSTS per (sub-)domein. Het niet toevoegen van HSTS voor ieder (sub-)domein (in een redirect-keten) kan gebruikers kwetsbaar maken voor MITM-aanvallen. Om die reden testen we HSTS bij het eerste contact, d.w.z. voordat een eventuele doorverwijzing plaatsvindt.

HSTS dwingt af dat een webbrowser direct via HTTPS verbindt bij terugkerend bezoek. Dit helpt man-in-the-middle-aanvallen te voorkomen. Een HSTS-geldigheidsduur (`max-age`) van tenminste zes maanden achten we voldoende veilig. Een lange geldigheidsduur heeft als voordeel dat ook infrequente bezoekers beschermd zijn. Het nadeel is dat wanneer je wil stoppen met HTTPS, je langer moet wachten totdat de geldigheid van de HSTS-policy in alle browsers die je website bezochten, is verlopen.

Zie 'Webapplicatie-richtlijnen, Verdieping' van NCSC, richtlijn U/WA.05.

TLS

TLS-versie

Uitslag:
Je webserver ondersteunt alleen veilige TLS-versies.

Technische details:

Webserver-IP-adres	Getroffen TLS-versie
2001:985:7ebb:1:211:32ff:fe8e:8bc3	Geen
212.238.211.4	Geen

Testuitleg:
We testen of je webserver alleen veilige TLS-versies ondersteunt.

Een webserver kan meer dan één TLS-versie ondersteunen.

Let op: browsermakers hebben aangekondigd dat ze in het eerste kwartaal van 2020 zullen stoppen met de ondersteuning van TLS 1.1 en 1.0. Daardoor zullen websites die geen TLS 1.2 en/of 1.3 ondersteunen onbereikbaar worden.

Zie 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0' van NCSC, richtlijn B1-1 en tabel 1

- Goed: TLS 1.3 en 1.2
- Uit te faseren: TLS 1.1 en 1.0
- Onvoldoende: SSL 3.0, 2.0 and 1.0

Ciphers (Algoritmeselecties)

Uitslag:
Je webserver ondersteunt alleen veilige ciphers.

Technische details:

Webserver-IP-adres	Getroffen ciphers
2001:985:7ebb:1:211:32ff:fe8e:8bc3	Geen
212.238.211.4	Geen

Testuitleg:
We testen of je webserver alleen veilige ciphers (algoritmeselecties) ondersteunt.

Een algoritmeselectie bestaat uit ciphers voor vier cryptografische functies: 1) sleuteluitwisseling, 2) certificaatverificatie, 3) bulkversleuteling, en 4) hashing. Een webserver kan meer dan één algoritmeselectie ondersteunen.

- Vanaf TLS 1.3 omvat de term 'cipher suite' alleen ciphers voor bulkversleuteling en hashing. Als TLS 1.3 gebruikt wordt dan zijn de ciphers voor sleuteluitwisseling en certificaatverificatie onderhandelbaar en niet langer onderdeel van de naam van de cipher suite. Omdat dit de term 'cipher suite' ambigu maakt, gebruikt NCSC de term 'algoritmeselectie' om alle vier de functies aan te duiden.

- NCSC gebruikt de IANA-naamgeving voor algoritmeselecties. Internet.nl hanteert de OpenSSL-naamgeving. Vanaf TLS 1.3 volgt OpenSSL de IANA-naamgeving. Een vertaling tussen beide is onderdeel van de OpenSSL-documentation.

Zie 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0' van NCSC, richtlijn B2-1 t/m B2-4 en tabel 2, 4, 6 en 7.

Hieronder staan 'Goede', 'Voldoende' en 'Uit te faseren' algoritmeselecties in de door NCSC voorgeschreven volgorde, gebaseerd op bijlage C van de 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0'. Achter iedere algoritmeselectie noemen we de minimale TLS-versie (bijv. [1.2]) die deze algoritmeselectie ondersteunt en die tenminste 'Uit te faseren' is.

Goed:

- `ECDHE-ECDSA-AES256-GCM-SHA384` (`TLS_AES_256_GCM_SHA384` in 1.3) [1.2]
- `ECDHE-ECDSA-CHACHA20-POLY1305` (`TLS_CHACHA20_POLY1305_SHA256` in 1.3) [1.2]
- `ECDHE-ECDSA-AES128-GCM-SHA256` (`TLS_AES_128_GCM_SHA256` in 1.3) [1.2]
- `ECDHE-RSA-AES256-GCM-SHA384` (`TLS_AES_256_GCM_SHA384` in 1.3) [1.2]
- `ECDHE-RSA-CHACHA20-POLY1305` (`TLS_CHACHA20_POLY1305_SHA256` in 1.3) [1.2]
- `ECDHE-RSA-AES128-GCM-SHA256` (`TLS_AES_128_GCM_SHA256` in 1.3) [1.2]

Voldoende:

- `ECDHE-ECDSA-AES256-SHA384` [1.2]
- `ECDHE-ECDSA-AES256-SHA` [1.0]
- `ECDHE-ECDSA-AES128-SHA256` [1.2]
- `ECDHE-ECDSA-AES128-SHA` [1.0]
- `ECDHE-RSA-AES256-SHA384` [1.2]
- `ECDHE-RSA-AES256-SHA` [1.0]
- `ECDHE-RSA-AES128-SHA256` [1.2]
- `ECDHE-RSA-AES128-SHA` [1.0]
- `DHE-RSA-AES256-GCM-SHA384` [1.2]
- `DHE-RSA-CHACHA20-POLY1305` [1.2]
- `DHE-RSA-AES128-GCM-SHA256` [1.2]
- `DHE-RSA-AES256-SHA256` [1.2]
- `DHE-RSA-AES256-SHA` [1.0]
- `DHE-RSA-AES128-SHA256` [1.2]
- `DHE-RSA-AES128-SHA` [1.0]

Uit te faseren:

- `ECDHE-ECDSA-DES-CBC3-SHA` [1.0]
- `ECDHE-RSA-DES-CBC3-SHA` [1.0]

- DHE-RSA-DES-CBC3-SHA [1.0]
- AES256-GCM-SHA384 [1.2]
- AES128-GCM-SHA256 [1.2]
- AES256-SHA256 [1.2]
- AES256-SHA [1.0]
- AES128-SHA256 [1.2]
- AES128-SHA [1.0]
- DES-CBC3-SHA [1.0]

Cipher-volgorde

Uitslag:
Je webserver dwingt zijn eigen cipher-voorkeur af ('I'), en biedt ciphers aan conform de voorgeschreven volgorde ('II').

Technische details:

Webserver IP-adres	Eerst gevonden getroffen cipher-paren
2001:985:7ebb:1:211:32ff:fe8e:8bc3	Geen
212.238.211.4	Geen

Testuitleg:
We testen of je webserver zijn eigen cipher-voorkeur afdwingt ('I'), en ciphers aanbiedt conform de voorgeschreven volgorde ('II').

Als je webserver alleen 'Goede'ciphers ondersteunt, dan is deze test niet van toepassing aangezien de volgorde geen significant beveiligingsvoordeel oplevert.

I. *Server afgewongen cipher-volgorde*: De webserver dwingt zijn cipher-voorkeur af tijdens de onderhandeling met een webbrowser, en accepteert geen voorkeur van de webbrowser. (*Niveau van vereistheid: Vereist*);

II. *Voorgeschreven volgorde*: Ciphers worden aangeboden door de webserver in overeenstemming met de volgende voorgeschreven volgorde die de voorkeur geeft aan veilig en snelle ciphers.

A. Prefereer *Goede* boven *Voldoende* en dan pas *Uit te faseren* ciphers (*Niveau van vereistheid: Vereist*);

B. Ga binnen een bepaald veiligheidsniveau als volgt te werk:

1. Kies ciphers die de sleuteluitwisseling uitvoeren op basis van elliptische krommen

en als dat niet mogelijk is, dan pas de ciphers die finite fields gebruiken. Beide verdienen de voorkeur boven ciphers voor statische sleuteluitwisseling (*Niveau van vereistheid: Aanbevolen*);

2. Ciphers die bulkversleutelingen uitvoeren op basis van AEAD-algoritmes verdienen de voorkeur boven andere ciphers (*Niveau van vereistheid: Aanbevolen*);
3. De voorkeur gaat uit naar algoritmes die de certificaatverificatie uitvoeren op basis van ECDSA boven algoritmes die RSA gebruiken (*Niveau van vereistheid: Aanbevolen*);
4. Ciphers moeten gekozen worden op basis van een aflopende volgorde van hun sleutellengte en dan pas op basis van hun hash-grootte (*Niveau van vereistheid: Aanbevolen*);
5. AES-256 heeft de voorkeur boven ChaCha20 (*Niveau van vereistheid: Optioneel*).

In de tabel met technische details staan **alleen de eerst gevonden algoritmeselecties die niet voldoen aan de voorgeschreven volgorde**, met de overtreden volgorde-regel ernaast.

Zie 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0' van NCSC, richtlijn B2-5.

Sleuteluitwisselingsparameters

Uitslag:
Je webserver ondersteunt veilige parameters voor Diffie-Hellman-sleuteluitwisseling.

Technische details:

Webserver-IP-adres	Getroffen parameters
2001:985:7ebb:1:211:32ff:fe8e:8bc3	Geen
212.238.211.4	Geen

Testuitleg:
We testen of de publieke parameters, die in de Diffie-Hellman sleuteluitwisseling worden gebruikt door je webserver, veilig zijn.

De veiligheid van de ECDHE-sleuteluitwisseling is afhankelijk van de geselecteerde elliptische kromme. We testen of de bitlengte van de gebruikte kromme tenminste 224 bits is. Op dit moment kunnen we niet de naam van de elliptische kromme testen.

De veiligheid van de Diffie-Hellman Ephemeral (DHE) sleuteluitwisseling is afhankelijk van de lengte van de publieke en geheime sleutels die in de geselecteerde finite field-groep wordt gebruikt. We testen of je publieke DHE-sleutelmateriaal gebruikmaakt van

een van de gepredefinieerde finite field-groepen die zijn gespecificeerd in RFC 7919. Zelf-gegenereerde groepen zijn 'Onvoldoende'.

De grotere sleutellengtes die noodzakelijk zijn voor het gebruik van DHE gaan ten koste van de prestaties. Maak een zorgvuldige afweging en gebruik waar mogelijk ECDHE in plaats van DHE.

Naast ECDHE en DHE, kan RSA gebruikt worden voor sleuteluitwisseling. RSA loopt het risico om onvoldoende veilig te worden (huidige status 'Uit te faseren'). De publieke RSA-parameters worden getest in de subtest 'Handtekening-parameters van certificaat'. Overigens heeft RSA voor certificaatverificatie wel de status 'Goed'.

Zie 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0' van NCSC, richtlijn B5-1 en tabel 9 voor ECDHE, en richtlijn B6-1 en tabel 10 voor DHE.

Elliptische krommen voor ECDHE

- Goed: `secp384r1`, `secp256r1`, `x448`, en `x25519`
- Uit te faseren: `secp224r1`
- Onvoldoende: Andere krommen

Finite field-groepen voor DHE

Voldoende:

- ffdhe4096 (RFC 7919)
  sha256 checksum:
  `64852d6890ff9e62eecd1ee89c72af9af244dfef5b853bcedea3dfd7aade22b3`
- ffdhe3072 (RFC 7919)
  sha256 checksum:
  `c410cc9c4fd85d2c109f7ebe5930ca5304a52927c0ebcb1a11c5cf6b2386bbab`

Uit te faseren:

- ffdhe2048 (RFC 7919)
  sha256 checksum:
  `9ba6429597aeed2d8617a7705b56e96d044f64b07971659382e426675105654b`

Onvoldoende: Andere groepen

Hashfunctie voor sleuteluitwisseling

Uitslag:
Je webserver ondersteunt een veilige hashfunctie voor sleuteluitwisseling.

Technische details:

Webserver-IP-adress	SHA-2-ondersteuning voor handtekeningen
2001:985:7ebb:1:211:32ff:fe8e:8bc3	ja
212.238.211.4	ja

Testuitleg:
We testen of je webserver ondersteuning biedt voor veilige hashfuncties om tijdens sleuteluitwisseling de digitale handtekening te maken.

De webserver maakt tijdens de sleuteluitwisseling gebruik van een digitale handtekening om het eigenaarschap te bewijzen van de geheime sleutel die bij het certificaat hoort. De webserver creëert deze digitale handtekening door het ondertekenen van de output van een hashfunctie.

Zie 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0' van NCSC, tabel 5.

Niveau van vereistheid: Aanbevolen

SHA2-ondersteuning voor handtekeningen

- Goed: Ja (ondersteuning van SHA-256, SHA-384 of SHA-512)
- Uit te faseren: Nee (*geen* ondersteuning van SHA-256, SHA-384 of SHA-512)

TLS-compressie

Uitslag:
Je webserver ondersteunt geen TLS-compressie.

Technische details:

Webserver-IP-adres	TLS-compressie
2001:985:7ebb:1:211:32ff:fe8e:8bc3	nee
212.238.211.4	nee

Testuitleg:
We testen of je webserver TLS-compressie ondersteunt.

Het gebruik van compressie kan een aanvaller informatie bieden over geheime delen van versleutelde communicatie. Een aanvaller die in staat is om een deel van de verzonden data te achterhalen of te beïnvloeden, kan door middel van een groot aantal verzoeken stukje bij beetje de oorspronkelijke data reconstrueren. TLS-compressie

wordt zo weinig gebruikt dat het geen kwaad kan om deze optie uit te schakelen.

Zie 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0' van NCSC, richtlijn B7-1 en tabel 11.

Secure renegotiation

Uitslag:
Je webserver ondersteunt secure renegotiation.

Technische details:

Webserver-IP-adres	Secure renegotiation
2001:985:7ebb:1:211:32ff:fe8e:8bc3	ja
212.238.211.4	ja

Testuitleg:
We testen of je webserver secure renegotiation ondersteunt.

In de oudere versies van TLS (vóór TLS 1.3) is het tot stand brengen van een nieuwe handshake toegestaan. Dit zogeheten 'opnieuw onderhandelen' (renegotiation) was in het oorspronkelijke ontwerp onveilig. Inmiddels is de standaard gerepareerd en is er een veiliger renegotiation-mechanisme beschikbaar. De oude versie wordt sindsdien als insecure renegotiation aangeduid en deze moet derhalve uitgeschakeld worden.

Zie 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0' van NCSCL, richtlijn B8-1 en tabel 12.

Client-initiated renegotiation

Uitslag:
Je webserver staat geen client-initiated renegotiation toe.

Technische details:

Webserver-IP-adres	Client-initiated renegotiation
2001:985:7ebb:1:211:32ff:fe8e:8bc3	nee
212.238.211.4	nee

Testuitleg:
We testen of een client (doorgaans een webbrowser) een renegotiation kan initiëren met jouw webserver.

In het algemeen is het niet nodig om clients de mogelijkheid te bieden om een renegotiation te initiëren (client-initiated renegotiation). Bovendien komt een webserver hierdoor binnen een TLS-verbinding bloot te staan aan DoS-aanvallen. Een

aanvaller kan ook zonder renegotiation op initiatief van een client soortgelijke DoS-aanvallen uitvoeren door veel parallelle TLS-verbindingen te openen. Dergelijke aanvallen zijn echter eenvoudiger te traceren en met de standaardmaatregelen te migiteren. Merk op dat client-initiated renegotiation impact heeft op de beschikbaarheid en niet op de vertrouwelijkheid.

Zie 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0' van NCSC, richtlijn 8-1 en tabel 13.

0-RTT

Uitslag:
Deze subtest is niet van toepassing aangezien je webserver TLS 1.3 niet ondersteunt.

Technische details:

Webserver-IP-adres	0-RTT
2001:985:7ebb:1:211:32ff:fe8e:8bc3	nee
212.238.211.4	nee

Testuitleg:
We testen of je webserver Zero Round Trip Time Resumption (0-RTT) ondersteunt.

0-RTT is een optie in TLS 1.3 waarmee applicatiedata wordt getransporteerd tijdens het eerste handshake-bericht. 0-RTT biedt echter geen bescherming tegen replay-aanvallen op de TLS-laag en dient daarom uitgezet te worden. Alhoewel het risico gemitigeerd kan worden door 0-RTT niet toe te staan voor non-idempotent requests, is een dergelijke configuratie vaak niet triviaal, afhankelijk van applicatielogica en daardoor foutgevoelig.

Als je webserver geen TLS 1.3 ondersteunt, dan is deze test niet van toepassing. Voor webservers die TLS 1.3 ondersteunen, wordt de indexpagina `/` opgehaald via TLS 1.3 en daarbij wordt de omvang van de ondersteuning voor early data zoals aangegeven door de webserver gecontroleerd. Indien deze groter is dan nul, dan wordt een tweede verbinding gemaakt waarbij de TLS-sessiedetails van de eerste connectie worden hergebruikt maar de HTTP opvraging *vóór* de TLS handshake plaatsvindt (d.w.z. geen round trips (0-RTT) nodig voordat applicatiedata naar de server gaat). Als de TLS handshake slaagt en de webserver antwoordt met een non-HTTP 425 Too Early, dan wordt aangenomen dat de webserver 0-RTT ondersteunt.

Zie 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0' van NCSC, richtlijn B9-1 en tabel 14.

OCSP stapling

Uitslag:
Je webserver ondersteunt OCSP *niet*.

Technische details:

Webserver-IP-adres	OCSP stapling
2001:985:7ebb:1:211:32ff:fe8e:8bc3	nee
212.238.211.4	nee

Testuitleg:
We testen of je webserver de TLS Certificate Status extension of te wel OCSP stapling ondersteunt.

De webbrowser kan de geldigheid van het certificaat van de webserver via het OCSP-protocol controleren bij de certificaatleverancier. Dat OCSP-protocol verschaft de certificaatleverancier informatie over browsers die met de betreffende webserver communiceren. Dit kan een privacy-risico vormen. Een server kan de OCSP-informatie ook zelf verstrekken (OCSP stapling). Dit lost niet alleen het privacy-risico op, maar vereist ook geen connectiviteit tussen de webbrowser en certificaatleverancier en dit gaat dan ook sneller.

Als we verbinden met je webserver dan verzoeken we via de TLS Certificate Status extension om OCSP-data op te nemen in het antwoord van de webserver. Als je webserver OCSP-data heeft opgenomen in het antwoord, dan verifiëren we of de OCSP-data valide is, d.w.z. correct ondertekend door een bekende certificaatleverancier. Let op: we gebruiken de OCSP-data niet om de geldigheid van het certificaat te controleren.

Zie 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0' van NCSC, tabel 15.

OCSP stapling

- Goed: Aan
- Voldoende: Uit

Certificaat

Vertrouwensketen van certificaat

Uitslag:
De vertrouwensketen van je websitecertificaat is compleet en ondertekend door een

vertrouwde certificaatautoriteit.

Technische details:

Webserver-IP-adres	Onvertrouwde certificaatketen
2001:985:7ebb:1:211:32ff:fe8e:8bc3	Geen
212.238.211.4	Geen

Testuitleg:
We testen of we een geldige vertrouwensketen voor je websitecertificaat kunnen opbouwen.

Er is sprake van een geldige vertrouwensketen, als je certificaat is uitgegeven door een publiekelijk vertrouwde certificaatautoriteit én je webserver alle noodzakelijke tussenliggende certificaten presenteert.

Zie 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0' van NCSC, richtlijn B3-4.

Publieke sleutel van certificaat

Uitslag:
De digitale handtekening van je websitecertificaat gebruikt veilige parameters.

Technische details:

Webserver-IP-adres	Getroffen handtekening-parameters
2001:985:7ebb:1:211:32ff:fe8e:8bc3	Geen
212.238.211.4	Geen

Testuitleg:
We testen of de (ECDSA of RSA) digitale handtekening van je websitecertificaat veilige parameters gebruikt.

Bij de verificatie van certificaten wordt gebruik gemaakt van digitale handtekeningen. Om de authenticiteit van de verbinding te garanderen, moet een betrouwbaar algoritme voor certificaatverificatie gekozen worden. Het algoritme dat gebruikt wordt om een certificaat te ondertekenen, wordt door de certificaatleverancier geselecteerd.

Het certificaat specificeert het algoritme voor digitale handtekeningen dat tijdens de sleuteluitwisseling door zijn eigenaar wordt gebruikt. Het is mogelijk om meerdere certificaten te configureren, zodat er ook meer dan één algoritme ondersteund kan worden.

De veiligheid van de ECDSA-digitale-handtekeningen is afhankelijk van de geselecteerde kromme. De veiligheid van RSA voor de versleuteling en digitale

handtekeningen houdt verband met de sleutellengte van de publieke sleutel.

Zie 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0' van NCSC, richlijn B5-1 en tabel 9 voor ECDSA, en richtlijn B3-3 en tabel 8 voor RSA.

Elliptische krommen voor ECDSA

- Goed: `secp384r1`, `secp256r1`, `x448`, and `x25519`
- Uit te faseren: `secp224r1`
- Onvoldoende: Andere krommen

Lengte van RSA-sleutels

- Goed: Minimaal 3072 bit
- Voldoende: 2048 – 3071 bit
- Onvoldoende: Minder dan 2048 bit

Handtekening van certificaat

Uitslag:
Je websitecertificaat is ondertekend met een voldoende algoritme voor hashing.

Technische details:

Webserver-IP-adres	Getroffen hashing-algoritme
`2001:985:7ebb:1:211:32ff:fe8e:8bc3`	`Geen`
`212.238.211.4`	`Geen`

Testuitleg:
We testen of de ondertekende fingerprint van het websitecertificaat is gemaakt met een veilig algoritme voor hashing.

Zie 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0' van NCSC, richtlijn B3-2 en tabel 3.

Hashfuncties voor certificaatverificatie

- Goed: SHA-512, SHA-384, SHA-256
- Onvoldoende: SHA-1, MD5

Domeinnaam op certificaat

Uitslag:

De domeinnaam van je website komt overeen met de domeinnaam op je websitecertificaat.

Technische details:

Webserver-IP-adres	Niet-overeenkomende domeinen op certificaat
2001:985:7ebb:1:211:32ff:fe8e:8bc3	Geen
212.238.211.4	Geen

Testuitleg:
We testen of de domeinnaam van je website overeenkomt met de domeinnaam op het certificaat.

Het kan handig zijn om meerdere domeinnamen (bijvoorbeeld de domeinnaam met en zonder www) als Subject Alternative Name (SAN) in het certificaat op te nemen.

Zie 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0' van NCSC, richtlijn B3-1.

DANE

DANE aanwezigheid

Uitslag:
Je websitedomein bevat *geen* TLSA-record voor DANE.

Technische details:

Webserver-IP-adres	DANE TLSA-record aanwezig
2001:985:7ebb:1:211:32ff:fe8e:8bc3	nee
212.238.211.4	nee

Testuitleg:
We testen of de nameserver van je websitedomein een correct ondertekend TLSA-record voor DANE bevat.

Aangezien DNSSEC een noodzakelijke randvoorwaarde is voor DANE, zal een domeinnaam niet slagen voor de test als DNSSEC ontbreekt op het websitedomein, of als er DANE-gerelateerde DNSSEC-issues zijn (bijv. geen bewijs voor 'Denial of Existence').

Zie 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0' van NCSC, Appendix A, onder 'Certificate pinning en DANE'.

Niveau van vereistheid: Optioneel

DANE geldigheid

Uitslag:
Deze subtest is niet uitgevoerd, omdat een bovenliggende test waarvan deze subtest afhankelijk is een negatief testresultaat gaf, of omdat onvoldoende informatie beschikbaar was om de subtest uit te kunnen voeren.

Technische details:

Webserver-IP-adres	DANE TLSA-record geldig
2001:985:7ebb:1:211:32ff:fe8e:8bc3	niet getest
212.238.211.4	niet getest

Testuitleg:
We testen of de DANE-fingerprint die je domein presenteert geldig is voor je websitecertificaat.

Met DANE kan je informatie over jouw websitecertificaat publiceren in een speciaal DNS-record, een TLSA-record. Clients, zoals webbrowsers, kunnen het certificaat nu niet alleen via de certificaatautoriteit, maar ook via het TLSA-record controleren op authenticiteit. Een client kan het TLSA-record ook als signaal gebruiken om alleen via HTTPS (en niet via HTTP) te verbinden. DNSSEC is een noodzakelijke randvoorwaarde voor DANE. Helaas ondersteunen nog niet veel webbrowsers DANE-validatie.

Niveau van vereistheid: Aanbevolen (alleen als subtest voor 'DANE aanwezigheid' is geslaagd)

Beveiligingsopties

Goed gedaan! Alle applicatie-beveiligingsopties zijn ingesteld voor je website (Beveiligingsopties). Met deze opties kan je browsermechanismen activeren die bezoekers beschermen tegen aanvallen met bijvoorbeeld cross-site scripting (XSS) of framing. Let erop dat we HTTPS beschouwen als een vereiste voor deze testcategorie, en dat de beveiligingsopties *niet* relevant zijn voor domeinen die doorverwijzen (m.b.v. 301/302 redirect).

HTTP security headers

X-Frame-Options

Uitslag:
Je webserver biedt veilig ingestelde X-Frame-Options aan.

Technische details:

Webserver-IP-adres	X-Frame-Options waarde
2001:985:7ebb:1:211:32ff:fe8e:8bc3	SAMEORIGIN
212.238.211.4	SAMEORIGIN

Testuitleg:
We testen of je webserver een HTTP header voor `X-Frame-Options` aanbiedt die een voldoende veilige instelling heeft. Met deze HTTP header kan je webbrowsers laten weten of het toegestaan is om jouw website te 'framen'. Het voorkomen van 'framen' beschermt bezoekers tegen aanvallen zoals clickjacking. We beschouwen de volgende waarden als voldoende veilig:

- `DENY` ('framen' niet toegestaan);
- `SAMEORIGIN` ('framen' alleen door je eigen website toegestaan); of
- `ALLOW-FROM https://example.nl/` (alleen genoemde websites mogen jouw website 'framen').

`Content-Security-Policy` (CSP) biedt vergelijkbare bescherming en nog veel meer voor bezoekers met moderne webbrowsers. `X-Frame-Options` biedt hoe dan ook bescherming aan bezoekers van oudere browsers die geen CSP ondersteunen. Bovendien kan `X-Frame-Options` waardevolle bescherming aan alle bezoekers bieden, indien CSP niet (goed) is ingesteld voor de desbetreffende website.

Zie ook 'Webapplicatie-richtlijnen van NCSC, Verdieping', richtlijn U/PW.03.

Niveau van vereistheid: Aanbevolen

X-Content-Type-Options

Uitslag:
Je webserver biedt X-Content-Type-Options aan.

Technische details:

Webserver-IP-adres	X-Content-Type waarde
2001:985:7ebb:1:211:32ff:fe8e:8bc3	nosniff
212.238.211.4	nosniff

Testuitleg:
We testen of je webserver een HTTP header voor `X-Content-Type-Options` aanbiedt. Met deze HTTP header kan je webbrowsers laten weten dat zij geen 'MIME type sniffing' mogen uitvoeren en altijd het `Content-Type` zoals gedeclareerd door jouw webserver moeten volgen. De enige geldige waarde voor deze HTTP header is `nosniff`. Indien actief, dan zal een browser verzoeken voor `style` en `scipt`

blokkeren als deze geen corresponderende `Content-Type` (dat wil zeggen `text/css` of een 'Javascript MIME type' zoals `application/javascript`) hebben.

'MIME type sniffing' is een techniek waarbij de browser de inhoud van een bestand scant om te bepalen wat het formaat van het bestand is, ongeacht het door de webserver gedeclareerde `Content-Type`. Deze techniek is kwetsbaar voor de zogenaamde 'MIME confusion attack' waarbij de aanvaller de content van een bestand zodanig manipuleert dat de browser deze behandelt als een andere `Content-Type`, zoals een executeerbaar bestand.

Niveau van vereistheid: Aanbevolen

Content-Security-Policy aanwezigheid

Uitslag:
Je webserver biedt Content-Security-Policy (CSP) aan.

Technische details:

Webserver-IP-adres	CSP-waarde
2001:985:7ebb:1:211:32ff:fe8e:8bc3	`script-src 'self'; script-src-elem 'self' 'unsafe-inline'; object-src 'none'; frame-ancestors 'self'; base-uri 'none'; frame-src https://widgetscode.com https://www.youtube.com; font-src https://fonts.gstatic.com https://fonts.googleapis.com https://s.w.org 'self' data:; img-src 'self' https: data:; report-uri https://adagia.report-uri.com/r/d/csp/enforce; connect-src 'self' https://*.amazonaws.com; form-action 'self'; upgrade-insecure-requests; block-all-mixed-content`
212.238.211.4	`script-src 'self'; script-src-elem 'self' 'unsafe-inline'; object-src 'none'; frame-ancestors 'self'; base-uri 'none'; frame-src https://widgetscode.com https://www.youtube.com; font-src https://fonts.gstatic.com https://fonts.googleapis.com https://s.w.org 'self' data:; img-src 'self' https: data:; report-uri https://adagia.report-uri.com/r/d/csp/enforce; connect-src 'self' https://*.amazonaws.com; form-action 'self'; upgrade-insecure-requests; block-all-mixed-content`

Testuitleg:
We testen of je webserver een HTTP header voor `Content-Security-Policy` (CSP) aanbiedt. CSP beschermt een website tegen aanvallen via cross-site scripting (XSS). Door met CSP bronnen van goedgekeurde content in te stellen, voorkom je dat browsers kwaadaardige content van aanvallers laden. Momenteel beoordelen we niet de effectiviteit van de CSP-configuratie. We bevelen wel aan om:

- de HTTP header voor `Content-Security-Policy-Report-Only` te gebruiken om te experimenteren met CSP-policies door hun effecten te monitoren zonder dat deze effecten worden afgedwongen;
- `frame-ancestors` te gebruiken om het laden van de webpagina in een frame te beperken;
- een `default-src` policy te definiëren, die dient als een fallback voor andere brontypen als die geen eigen policy hebben;
- zeer terughoudend te zijn met het gebruik van `unsafe-inline` en `data:`, omdat deze aanvallen via cross-site scripting (XSS) mogelijk maken;
- `https://` te gebruiken als met een URL naar een bron wordt verwezen.

Zie ook 'Webapplicatie-richtlijnen van NCSC, Verdieping', richtlijn U/PW.03.

Niveau van vereistheid: Optioneel

Referrer-Policy aanwezigheid

Uitslag:
Je webserver biedt Referrer-Policy aan.

Technische details:

Webserver-IP-adres	Referrer-Policy waarde
2001:985:7ebb:1:211:32ff:fe8e:8bc3	strict-origin
212.238.211.4	strict-origin

Testuitleg:
We testen of je webserver een HTTP header voor `Referrer-Policy` aanbiedt. Met deze HTTP header kan je browsers laten weten welke zogenoemde referer-informatie, die wordt verzonden in de `Referer` header, onderdeel mag zijn van de website-opvraging. De `Referer` header bevat het adres van de vorige webpagina waarop de bezoeker een link volgde naar de opgevraagde pagina.

De informatie in de `Referer` header wordt meestal gebruikt voor analytics en logging. Er kunnen echter privacy- and beveiligingsrisico's aan kleven. De informatie kan bijvoorbeeld gebruikt worden voor user tracking en de informatie kan lekken naar derden die de verbinding afluisteren. Met de HTTP header voor `Referrer-Policy` kan je deze risico's mitigeren.

Momenteel beoordelen we *niet* de effectiviteit van de ingestelde `Referrer-Policy` waarde. We adviseren wel om een geïnformeerde beslissing te nemen, met privacy- en beveiligingsrisico's in gedachte, over het gebruik van één van de policy-waarden uit de

onderstaande eerste twee categorieën.

Aanbevolen policy-waarden:

1. Geen gevoelige informatie naar derde-partijen
   - `no-referrer`
   - `same-origin`
2. Gevoelige informatie naar derde-partijen alleen via beveiligde verbindingen (HTTPS)
   - `strict-origin`
   - `strict-origin-when-cross-origin`

Niet aanbevolen policy-waarden:

1. Gevoelige informatie naar derde-partijen mogelijkerwijs via onbeveiligde verbindingen (HTTP)
   - `no-referrer-when-downgrade` (default policy van browsers)
   - `origin-when-cross-origin`
   - `origin`
   - `unsafe-url`

Niveau van vereistheid: Aanbevolen
