

# Gemeente Schildwaard

## Kwetsbaarhedenscan Burgerzaken

[Demonstratie: Dit is een demonstratie-rapport. Gemeente Schildwaard is een fictieve gemeente. Het rapport is gegenereerd door PDCS ter illustratie van een securityscan. Niets in dit rapport heeft betrekking op een werkelijke gemeente of werkelijk systeem.]

VERTROUWELIJK



<b>Versie</b>	1.0
<b>Auteur</b>	Remko Sikkema
<b>Datum</b>	26 April 2026

## Inhoudsopgave

1. Versiebeheer.....	3
2. Inleiding .....	4
2.1 Achtergrond.....	4
2.2 Doel.....	4
2.3 Scope .....	4
2.4 Aanpak .....	4
2.5 Methode .....	4
2.6 Disclaimer.....	4
3. Management Samenvatting .....	6
4. Bevindingen .....	9
4.1 Target: burgerzaken.gemeente-schildwaard.nl .....	9
4.2 Target: https://burgerzaken.gemeente-schildwaard.nl/.....	48
5. Addendum .....	53
5.1 Tools en techniek .....	53
6. Over PDCS .....	54

## 1. Versiebeheer

### Distributielijst

Naam	Ro1	Organisatie
Remko Sikkema	Security Consultant	PDCS
[Contact gemeente]	TISO	Gemeente Schildwaard

### Versie geschiedenis

Versie	Datum	Naam	Status
1.0	26 April 2026	Remko Sikkema	Definitief

## 2. Inleiding

### 2.1 Achtergrond

PDCS heeft met de Gemeente Schildwaard afgesproken om een kwetsbaarheidscans uit te voeren op de systemen van burgerzaken.

De securitytest is uitgevoerd op 25 April 2026.

### 2.2 Doel

Het doel van deze securitytest was om een eerste beoordeling te maken van de websites binnen scope vanuit securityperspectief en inzicht te krijgen in mogelijke kwetsbaarheden en het risico op misbruik door een externe aanvaller vanaf het internet.

### 2.3 Scope

De volgende systemen vielen in de scope van het onderzoek:

Target	Beschrijving
burgerzaken.gemeente-schildwaard.nl	Host burgerzaken
<a href="https://burgerzaken.gemeente-schildwaard.nl/">https://burgerzaken.gemeente-schildwaard.nl/</a>	Website burgerzaken

### 2.4 Aanpak

De test simuleerde een externe dreiging (hacker of malicious user) vanaf het internet die probeert kwetsbaarheden in de systemen te identificeren en – waar mogelijk – te misbruiken om ongeautoriseerde toegang te verkrijgen tot gevoelige informatie of de werking van systemen te beïnvloeden.

De test is uitgevoerd zonder authenticatie (er zijn geen inloggegevens verstrekt) en richt zich daarmee uitsluitend op publiek toegankelijke onderdelen van de systemen.

Hierdoor zijn kwetsbaarheden die alleen zichtbaar zijn na authenticatie of in interne componenten buiten beschouwing gebleven.

N.B. Alleen bevindingen met risico medium of hoger zijn benoemd in dit rapport, op aanvraag is het ook mogelijk om een overzicht te ontvangen van alle lage risico's.

### 2.5 Methode

De uitgevoerde testen zijn gebaseerd op professionele ervaring en sluiten aan bij algemeen geaccepteerde richtlijnen en methodologieën, zoals OWASP Top 10 en NIST 800-115.

### 2.6 Disclaimer

Houd er rekening mee dat het niet mogelijk is om netwerken, informatiesystemen en mensen volledig te testen op alle mogelijke security kwetsbaarheden. Dit rapport biedt geen garantie dat uw systemen beschermd zijn tegen alle dreigingen. De uitgevoerde testen en resultaten geven een momentopname weer op basis van de uitgevoerde werkzaamheden.

Delen van de tekst zijn door een geautomatiseerd vertaalprogramma vertaald.

Er kan geen garantie worden gegeven dat de systemen volledig veilig zijn tegen alle vormen van aanvallen, inclusief kwetsbaarheden die op het moment van testen nog niet bekend waren.

Daarnaast kunnen wijzigingen in de geteste systemen invloed hebben op het beveiligingsniveau, zowel in positieve als negatieve zin.

De testen zijn uitgevoerd binnen een beperkte tijd en op basis van een best-effort inspanning.

DEMONSTRATIE — FICTIEVE GEMEENTE — © PDACS

### 3. Management Samenvatting

In opdracht van Gemeente Schildwaard heeft PDCS een kwetsbaarhedenscan uitgevoerd op de website *burgerzaken.gemeente-schildwaard.nl*. Doel was om vanuit het perspectief van een externe aanvaller (zonder inloggegevens) inzicht te krijgen in welke kwetsbaarheden misbruikt zouden kunnen worden om gegevens van inwoners te bemachtigen of de dienstverlening te verstoren.

Het onderzoek heeft **20 kwetsbaarheden** aan het licht gebracht: **3 kritiek**, **11 hoog** en **6 middel**. Het beeld is zorgelijk. Op de server draait verouderde software (Apache, PHP, Redis, OpenSSL) waarvoor al jaren beveiligingsupdates beschikbaar zijn die niet zijn doorgevoerd. Drie van die kwetsbaarheden zijn met hoge zekerheid op afstand misbruikbaar zonder inloggen, waarmee een aanvaller volledige controle over de server kan krijgen. Daarnaast is een Redis-database direct vanaf het internet bereikbaar zonder enige toegangsbeveiliging, dit is in de praktijk een open deur. Tot slot bevat de webapplicatie zelf invoervalidatie-fouten waardoor SQL Injection en Cross-Site Scripting mogelijk zijn; via die weg kan een aanvaller ongeautoriseerd in de database kijken of namens een burger handelingen verrichten.

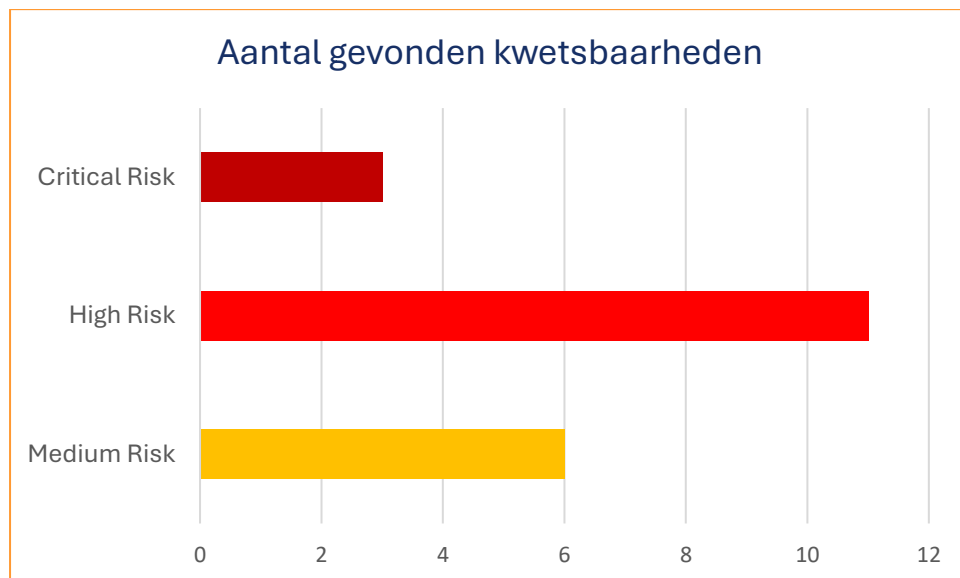
**De impact bij misbruik:** uitlekken of manipuleren van persoonsgegevens van inwoners (BRP-gerelateerde data), reputatieschade en mogelijk uitval van burgerzakendiensten. Gezien de aard van de gegevens vragen deze bevindingen om spoedige opvolging.

PDCS adviseert drie sporen, in deze volgorde:

1. **Onmiddellijk** — sluit de Redis-, MySQL- en SSH-services af van het publieke internet en verplaats deze achter de firewall of VPN. Dit kan vandaag.
2. **Zo spoedig mogelijk** — installeer de beschikbare beveiligingsupdates voor Apache, PHP, Redis en OpenSSL, of migreer naar een ondersteunde versie. Verwijder de op de server aangetroffen back-up- en configuratiebestanden uit de publiek toegankelijke mappen.
3. **Structureel** — voer patchmanagement, hardening en periodieke security-tests in als vast onderdeel van het beheer, in lijn met de BIO. Implementeer invoervalidatie en een Web Application Firewall vóór de publieke webapplicatie.

De technische details, het exacte risico per bevinding en concrete aanbevelingen vindt u in hoofdstuk 4 van dit rapport.

Onderstaand is een visuele weergave van de bevindingen en de bijbehorende risiconiveaus:



Onderstaande tabel geeft een samenvatting van de bevindingen die tijdens deze securitytest zijn geïdentificeerd<sup>1</sup>:

ID	Getroffen systeem	Finding name	Risk level	Verified
4.1	burgerzaken.gemeente-schildwaard.nl	Apache Server - Remote Code Execution (CVE-2021-42013)	Critical	✓
		Redis < 8.2.1 lua script - Integer Overflow (CVE-2025-46817)	Critical	✓
		Redis Lua Parser < 8.2.2 - Use After Free (CVE-2025-49844)	Critical	✓
		Kwetsbaarheden gevonden voor Apache Httpd 2.4.49	High	x
		Kwetsbaarheden gevonden voor OpenSSL 1.1.1d	High	x
		Kwetsbaarheden gevonden voor Redis Key-Value Store 7.0.15	High	x
		Apache Server - Remote Code Execution (CVE-2021-41773)	High	✓

<sup>1</sup> Alleen bevindingen met risico medium of hoger zijn benoemd in dit rapport, op aanvraag is het ook mogelijk om een overzicht te ontvangen van alle lage risico's.

		Redis Lua Sandbox < 8.2.2 - Cross-User Escape (CVE-2025-46818)	High	✓
		Redis < 8.2.1 Lua Long-String Delimiter - Out-of-Bounds Read (CVE-2025-46819)	High	✓
		Redis Server - Unauthenticated Access	High	✓
		Redis - weak password	High	✓
		Generic Env File Disclosure	High	✓
		SSH service exposed to the Internet	Medium	✓
		MySQL service exposed to the Internet	Medium	✓
		Redis service exposed to the Internet	Medium	✓
		Kwetsbaarheden gevonden voor PHP 7.4.33	Medium	x
		Compressed Backup File	Medium	✓
		Git Configuration	Medium	✓
4.2	<a href="https://burgerzaken.gemeenteschildwaard.nl/">https://burgerzaken.gemeenteschildwaard.nl/</a>	SQL Injection	High	✓
		Cross-Site Scripting	High	✓

✓ - geverifieerde finding

## 4. Bevindingen

### Uitleg prioritering van kwetsbaarheden in verouderde software

De prioriteit van kwetsbaarheden wordt bepaald op basis van impact (CVSS) en kans op misbruik (EPSS).

- CVSS geeft de impact aan (hoe ernstig is misbruik).
- EPSS Score geeft de kans op exploitatie.
- EPSS Percentile geeft aan hoe interessant de kwetsbaarheid is voor aanvallers t.o.v. andere kwetsbaarheden.

Richtlijn voor prioritering:

- CVSS < 7 → geen directe actie vereist
- EPSS Percentile < 80% → meestal geen directe actie vereist
- CVSS ≥ 7 én EPSS Percentile ≥ 80% → actief oppakken
- CVSS ≥ 9 → altijd direct oppakken (ongeacht EPSS)

Kwetsbaarheden die zowel een hoge impact als een aantoonbaar verhoogde kans op misbruik hebben (top 20%) krijgen prioriteit voor opvolging. Overige bevindingen kunnen worden meegenomen in regulier patch- en onderhoudsbeleid.

### 4.1 Target: [burgerzaken.gemeente-schildwaard.nl](http://burgerzaken.gemeente-schildwaard.nl)

#### 4.1.1 Apache Server - Remote Code Execution (CVE-2021-42013)

Getroffen systeem burgerzaken.gemeente-schildwaard.nl	<b>Critical</b> Status: <b>Open</b> Port: <b>443/tcp</b>
--	--

### Bewijs

We hebben deze kwetsbaarheid kunnen detecteren door middel van het volgende HTTP request, met het id commando als payload:

#### HTTP Request:

```
POST /cgi-bin/./%32%65/./%32%65/./%32%65/./%32%65/./%32%65/bin/sh HTTP/1.1  
Host: burgerzaken.gemeente-schildwaard.nl
```

```
echo Content-Type: text/plain; echo; id
```

#### HTTP Response:

```
HTTP 200
```

```
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```

## Kwetsbaarheid omschrijving

Wij hebben geconstateerd dat de target Apache-server kwetsbaar is voor CVE-2021-42013, een Remote Code Execution-kwetsbaarheid in het /cgi-bin endpoint. Als CGI (mod-cgi) expliciet is enabled op de server en bestanden buiten de document root niet beschermd zijn met de "require all denied"-configuratie, kan een unauthenticated remote attacker willekeurige binaries op het filesystem benaderen (bijv. /bin/sh) en commando's uitvoeren op de server.

De root cause van deze kwetsbaarheid is een wijziging in de path normalization-code in versies 2.4.49-2.4.50 van Apache Server. Alleen deze specifieke versies zijn affected.

## Risico omschrijving

Het risico bestaat dat een remote unauthenticated attacker de server volledig kan compromitteren om vertrouwelijke informatie te stelen, ransomware te installeren of te pivoten naar het interne netwerk.

## Aanbeveling

Wij adviseren de Apache Server te upgraden naar een versie gelijk aan of hoger dan 2.4.51.

## Referenties

<https://nvd.nist.gov/vuln/detail/CVE-2021-42013>

<https://www.exploit-db.com/exploits/50406>

<https://www.exploit-db.com/exploits/50512>

## Classificatie

Category	ID / Value
EPSS score	0.9441
EPSS percentile	0.99978
CISA KEV	True
CVE	<a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42013">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42013</a>
CVSS	10
CVSS V3	9.8

## Verificatie

✓ Deze finding is gevalideerd en is dus geen False Positive.

#### 4.1.2 Redis < 8.2.1 lua script - Integer Overflow (CVE-2025-46817)

Getroffen systeem burgerzaken.gemeente-schildwaard.nl	<div style="background-color: red; color: white; padding: 2px; font-weight: bold;">Critical</div> Status: <span style="background-color: #e0e0e0;">Open</span> Port: <b>6379/tcp</b>
--	---

#### Bewijs

We hebben deze kwetsbaarheid kunnen detecteren met behulp van de volgende Request / Response chain.

We hebben de volgende informatie uit het target gehaald: 7.0.15

Endpoint: burgerzaken.gemeente-schildwaard.nl:6379

#### Kwetsbaarheid omschrijving

Redis-versies 8.2.1 en eerder met Lua scripting enabled bevatten een integer overflow-kwetsbaarheid in het Lua script execution path. Een authenticated user kan een specially crafted Lua script indienen dat de integer overflow in de Lua execution-component triggert. Deze overflow kan de program state corrupten en kan leiden tot remote code execution op de Redis-server. Het issue is opgelost in Redis 8.2.2.

#### Risico omschrijving

Succesvolle exploitatie kan leiden tot arbitrary code execution als het Redis-proces, met risico op volledige system compromise en verlies van data integrity. De kwetsbaarheid is high severity en exploiteerbaar wanneer een aanvaller kan authenticeren bij een Redis-instance met Lua scripting enabled, waardoor de kans op exploitatie significant is in exposed of zwak beveiligde deployments.

#### Aanbeveling

Pas de vendor-patch toe door te upgraden naar Redis 8.2.2 of hoger, en beperk netwerktoegang en authenticatie tot Redis-instances om exposure te minimaliseren tot er gepatcht is.

#### Referenties

<https://github.com/dwiswant0/CVE-2025-46817/blob/master/README.md>

#### Classificatie

Category	ID / Value
EPSS score	0.132
EPSS percentile	0.94162
CISA KEV	False
CVE	<a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-46817">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-46817</a>

CVSS V3	7
---------	---

### Verificatie

- ✓ Deze finding is gevalideerd en is dus geen False Positive.

DEMONSTRATIE — FICTIEVE GEMEENTE — © PDACS

### 4.1.3 Redis Lua Parser < 8.2.2 - Use After Free (CVE-2025-49844)

Getroffen systeem burgerzaken.gemeente-schildwaard.nl	<div style="background-color: red; color: white; padding: 2px; font-weight: bold;">Critical</div> Status: <span style="background-color: #e0e0e0;">Open</span> Port: 6379/tcp
--	--

#### Bewijs

We hebben deze kwetsbaarheid kunnen detecteren met behulp van de volgende Request / Response chain.

We hebben de volgende informatie uit het target gehaald: 7.0.15

Endpoint: burgerzaken.gemeente-schildwaard.nl:6379

#### Kwetsbaarheid omschrijving

Redis-versies vóór 8.2.2 met Lua scripting bevatten een use-after-free-kwetsbaarheid in de interactie tussen de Lua parser en garbage collection. Een authenticated Redis client die Lua scripts kan uitvoeren (EVAL/EVALSHA) kan een specially crafted script indienen dat de Lua garbage collector manipuleert en een use-after-free in het serverproces triggert. Succesvolle exploitatie kan execution van arbitrary code toestaan in de context van het redis-server-proces, of een crash veroorzaken. Het issue treft alle Redis-builds met Lua scripting enabled en is opgelost in Redis 8.2.2.

#### Risico omschrijving

Een authenticated aanvaller met de mogelijkheid Lua scripts uit te voeren kan memory corruption triggeren die kan leiden tot remote code execution of denial-of-service, met een high-severity impact. De kwetsbaarheid is remote exploiteerbaar door elke user die EVAL/EVALSHA mag aanroepen, waardoor exploitatie relatief waarschijnlijk is in omgevingen die script execution toestaan.

#### Aanbeveling

Upgrade de getroffen Redis-installaties naar versie 8.2.2 of hoger; alternatief: schakel Lua script execution uit of beperk deze via ACL door EVAL en EVALSHA te weigeren voor untrusted accounts tot de patch is toegepast.

#### Referenties

<https://www.wiz.io/blog/wiz-research-redis-rce-cve-2025-49844>

<https://github.com/dwisiswant0/CVE-2025-49844>

#### Classificatie

Category	ID / Value
EPSS score	0.14172
EPSS percentile	0.94399

CISA KEV	False
CVE	<a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-49844">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-49844</a>
CVSS V3	9.9

### Verificatie

- ✓ Deze finding is gevalideerd en is dus geen False Positive.

DEMONSTRATIE — FICTIEVE GEMEENTE — © PDACS

#### 4.1.4 Kwetsbaarheden gevonden voor Apache Httpd 2.4.49

Getroffen systeem burgerzaken.gemeente-schildwaard.nl	<b>High</b>  Status: <b>Open</b> Port: <b>443/tcp</b>
--	--

#### Bewijs

CVE	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-38476">https://nvd.nist.gov/vuln/detail/CVE-2024-38476</a>
CVSS	9.8
EPSS Score	0.04673
EPSS Percentile	0.89356
CISA KEV	No
Summary	<p>Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution via backend applications whose response headers are malicious or exploitable.</p> <p>Users are recommended to upgrade to version 2.4.60, which fixes this issue.</p>
Exploit	N/A
CVE	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-38474">https://nvd.nist.gov/vuln/detail/CVE-2024-38474</a>
CVSS	9.8
EPSS Score	0.00994
EPSS Percentile	0.76994
CISA KEV	No
Summary	<p>Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts in directories permitted by the configuration but not directly reachable by any URL or source disclosure of scripts meant to only to be executed as CGI.</p> <p>Users are recommended to upgrade to version 2.4.60, which fixes this issue.</p> <p>Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.</p>
Exploit	N/A
CVE	<a href="https://nvd.nist.gov/vuln/detail/CVE-2023-25690">https://nvd.nist.gov/vuln/detail/CVE-2023-25690</a>

CVSS	9.8
EPSS Score	0.68183
EPSS Percentile	0.98609
CISA KEV	No
Summary	<p>Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.</p> <p>Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:</p> <pre>RewriteEngine on RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?\$1"; [P] ProxyPassReverse /here/ http://example.com:8080/</pre> <p>Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.</p>
Exploit	N/A
CVE	<a href="https://nvd.nist.gov/vuln/detail/CVE-2022-31813">https://nvd.nist.gov/vuln/detail/CVE-2022-31813</a>
CVSS	9.8
EPSS Score	0.00043
EPSS Percentile	0.13252
CISA KEV	No
Summary	<p>Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.</p>
Exploit	N/A
CVE	<a href="https://nvd.nist.gov/vuln/detail/CVE-2022-23943">https://nvd.nist.gov/vuln/detail/CVE-2022-23943</a>
CVSS	9.8
EPSS Score	0.60552

EPSS Percentile	0.98295
CISA KEV	No
Summary	Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.
Exploit	N/A

## Kwetsbaarheid omschrijving

Kwetsbaarheden gevonden voor Apache Httpd 2.4.49

## Risico omschrijving

Deze kwetsbaarheden stellen de getroffen applicaties bloot aan het risico van ongeautoriseerde toegang tot vertrouwelijke data en mogelijk denial-of-service-aanvallen. Een aanvaller kan een geschikt exploit zoeken (of zelf ontwikkelen) voor één van deze kwetsbaarheden en deze gebruiken om het systeem aan te vallen.

### Notes:

Omdat de kwetsbaarheden uitsluitend zijn vastgesteld op basis van version-based testing, zal het risiconiveau voor deze finding niet hoger zijn dan "high". Critical risico's worden alleen toegekend aan kwetsbaarheden die zijn vastgesteld via actieve en gevalideerde testmethoden.

- De kwetsbaarheden zijn geïdentificeerd op basis van de versie van de server.
- Voor elke poort worden alleen de eerste 5 kwetsbaarheden met het hoogste risico getoond.

## Aanbeveling

Wij adviseren de getroffen software te upgraden naar de laatste versie om de risico's van deze kwetsbaarheden te elimineren.

## Classificatie

Category	ID / Value
EPSS score	0.68183
EPSS percentile	0.98609
CISA KEV	False
CVE	<a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-38476">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-38476</a> , <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-38474">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-38474</a> , <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25690">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25690</a> , <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-</a>

	<a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23943">31813, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23943</a>
CVSS V3	9.8

**Verificatie**

x

DEMONSTRATIE — FICTIEVE GEMEENTE — © PDACS

#### 4.1.5 Kwetsbaarheden gevonden voor OpenSSL 1.1.1d

Getroffen systeem burgerzaken.gemeente-schildwaard.nl	<b>High</b>  Status: <b>Open</b> Port: <b>443/tcp</b>
--	--

#### Bewijs

CVE	<a href="https://nvd.nist.gov/vuln/detail/CVE-2021-3711">https://nvd.nist.gov/vuln/detail/CVE-2021-3711</a>
CVSS	9.8
EPSS Score	0.02373
EPSS Percentile	0.8501
CISA KEV	No
Summary	<p>In order to decrypt SM2 encrypted data an application is expected to call the API function <code>EVP_PKEY_decrypt()</code>. Typically an application will call this function twice. The first time, on entry, the "out" parameter can be NULL and, on exit, the "outlen" parameter is populated with the buffer size required to hold the decrypted plaintext. The application can then allocate a sufficiently sized buffer and call <code>EVP_PKEY_decrypt()</code> again, but this time passing a non-NULL value for the "out" parameter. A bug in the implementation of the SM2 decryption code means that the calculation of the buffer size required to hold the plaintext returned by the first call to <code>EVP_PKEY_decrypt()</code> can be smaller than the actual size required by the second call. This can lead to a buffer overflow when <code>EVP_PKEY_decrypt()</code> is called by the application a second time with a buffer that is too small. A malicious attacker who is able present SM2 content for decryption to an application could cause attacker chosen data to overflow the buffer by up to a maximum of 62 bytes altering the contents of other data held after the buffer, possibly changing application behaviour or causing the application to crash. The location of the buffer is application dependent but is typically heap allocated. Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k).</p>
Exploit	N/A
CVE	<a href="https://nvd.nist.gov/vuln/detail/CVE-2023-4807">https://nvd.nist.gov/vuln/detail/CVE-2023-4807</a>
CVSS	7.8
EPSS Score	0.00675
EPSS Percentile	0.71515
CISA KEV	No

<b>Summary</b>	<p>Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications on the Windows 64 platform when running on newer X86_64 processors supporting the AVX512-IFMA instructions.</p> <p>Impact summary: If in an application that uses the OpenSSL library an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences.</p>
<b>Exploit</b>	N/A

## Kwetsbaarheid omschrijving

Kwetsbaarheden gevonden voor OpenSSL 1.1.1d

## Risico omschrijving

Deze kwetsbaarheden stellen de getroffen applicaties bloot aan het risico van ongeautoriseerde toegang tot vertrouwelijke data en mogelijk denial-of-service-aanvallen. Een aanvaller kan een geschikt exploit zoeken (of zelf ontwikkelen) voor één van deze kwetsbaarheden en deze gebruiken om het systeem aan te vallen.

### Notes:

Omdat de kwetsbaarheden uitsluitend zijn vastgesteld op basis van version-based testing, zal het risiconiveau voor deze finding niet hoger zijn dan "high". Critical risico's worden alleen toegekend aan kwetsbaarheden die zijn vastgesteld via actieve en gevalideerde testmethoden.

- De kwetsbaarheden zijn geïdentificeerd op basis van de versie van de server.
- Voor elke poort worden alleen de eerste 5 kwetsbaarheden met het hoogste risico getoond.

## Aanbeveling

Wij adviseren de getroffen software te upgraden naar de laatste versie om de risico's van deze kwetsbaarheden te elimineren.

## Classificatie

Category	ID / Value
EPSS score	0.02373
EPSS percentile	0.8501
CISA KEV	False

CVE	<a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2026-28390">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2026-28390</a> , <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2026-28389">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2026-28389</a> , <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2026-28387">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2026-28387</a> , <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4807">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4807</a> , <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3711">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3711</a>
CVSS V3	9.8

### Verificatie

x

DEMONSTRATIE — FICTIEVE GEMEENTE — © PDACS

#### 4.1.6 Kwetsbaarheden gevonden voor Redis Key-Value Store 7.0.15

Getroffen systeem burgerzaken.gemeente-schildwaard.nl	<b>High</b>  Status: <b>Open</b> Port: <b>6379/tcp</b>
--	---

#### Bewijs

CVE	<a href="https://nvd.nist.gov/vuln/detail/CVE-2025-49844">https://nvd.nist.gov/vuln/detail/CVE-2025-49844</a>
CVSS	9.9
EPSS Score	0.14172
EPSS Percentile	0.94397
CISA KEV	No
Summary	Redis is an open source, in-memory database that persists on disk. Versions 8.2.1 and below allow an authenticated user to use a specially crafted Lua script to manipulate the garbage collector, trigger a use-after-free and potentially lead to remote code execution. The problem exists in all versions of Redis with Lua scripting. This issue is fixed in version 8.2.2. To workaround this issue without patching the redis-server executable is to prevent users from executing Lua scripts. This can be done using ACL to restrict EVAL and EVALSHA commands.
Exploit	N/A
CVE	<a href="https://nvd.nist.gov/vuln/detail/CVE-2025-48367">https://nvd.nist.gov/vuln/detail/CVE-2025-48367</a>
CVSS	7.5
EPSS Score	0.00126
EPSS Percentile	0.31639
CISA KEV	No
Summary	Redis is an open source, in-memory database that persists on disk. An unauthenticated connection can cause repeated IP protocol errors, leading to client starvation and, ultimately, a denial of service. This vulnerability is fixed in 8.0.3, 7.4.5, 7.2.10, and 6.2.19.
Exploit	N/A
CVE	<a href="https://nvd.nist.gov/vuln/detail/CVE-2025-21605">https://nvd.nist.gov/vuln/detail/CVE-2025-21605</a>
CVSS	7.5
EPSS Score	0.01547
EPSS Percentile	0.81464

<b>CISA KEV</b>	No
<b>Summary</b>	Redis is an open source, in-memory database that persists on disk. In versions starting at 2.6 and prior to 7.4.3, An unauthenticated client can cause unlimited growth of output buffers, until the server runs out of memory or is killed. By default, the Redis configuration does not limit the output buffer of normal clients (see client-output-buffer-limit). Therefore, the output buffer can grow unlimitedly over time. As a result, the service is exhausted and the memory is unavailable. When password authentication is enabled on the Redis server, but no password is provided, the client can still cause the output buffer to grow from "NOAUTH" responses until the system will run out of memory. This issue has been patched in version 7.4.3. An additional workaround to mitigate this problem without patching the redis-server executable is to block access to prevent unauthenticated users from connecting to Redis. This can be done in different ways. Either using network access control tools like firewalls, iptables, security groups, etc, or enabling TLS and requiring users to authenticate using client side certificates.
<b>Exploit</b>	N/A
<b>CVE</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2025-46817">https://nvd.nist.gov/vuln/detail/CVE-2025-46817</a>
<b>CVSS</b>	7.0
<b>EPSS Score</b>	0.132
<b>EPSS Percentile</b>	0.94159
<b>CISA KEV</b>	No
<b>Summary</b>	Redis is an open source, in-memory database that persists on disk. Versions 8.2.1 and below allow an authenticated user to use a specially crafted Lua script to cause an integer overflow and potentially lead to remote code execution The problem exists in all versions of Redis with Lua scripting. This issue is fixed in version 8.2.2.
<b>Exploit</b>	N/A
<b>CVE</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2025-46819">https://nvd.nist.gov/vuln/detail/CVE-2025-46819</a>
<b>CVSS</b>	6.3
<b>EPSS Score</b>	0.05046
<b>EPSS Percentile</b>	0.89793
<b>CISA KEV</b>	No
<b>Summary</b>	Redis is an open source, in-memory database that persists on disk. Versions 8.2.1 and below allow an authenticated user to use a specially crafted LUA script to read out-of-

	bound data or crash the server and subsequent denial of service. The problem exists in all versions of Redis with Lua scripting. This issue is fixed in version 8.2.2. To workaround this issue without patching the redis-server executable is to prevent users from executing Lua scripts. This can be done using ACL to block a script by restricting both the EVAL and FUNCTION command families.
Exploit	N/A

## Kwetsbaarheid omschrijving

Kwetsbaarheden gevonden voor Redis Key-Value Store 7.0.15

## Risico omschrijving

Deze kwetsbaarheden stellen de affected applicaties bloot aan het risico van ongeautoriseerde toegang tot vertrouwelijke data en mogelijk denial-of-service-aanvallen. Een aanvaller kan een geschikt exploit zoeken (of zelf ontwikkelen) voor één van deze kwetsbaarheden en deze gebruiken om het systeem aan te vallen.

### Notes:

Omdat de kwetsbaarheden uitsluitend zijn vastgesteld op basis van version-based testing, zal het risiconiveau voor deze finding niet hoger zijn dan "high". Critical risico's worden alleen toegekend aan kwetsbaarheden die zijn vastgesteld via actieve en gevalideerde testmethoden.

- De kwetsbaarheden zijn geïdentificeerd op basis van de versie van de server.
- Voor elke poort worden alleen de eerste 5 kwetsbaarheden met het hoogste risico getoond.

## Aanbeveling

Wij adviseren de affected software te upgraden naar de laatste versie om de risico's van deze kwetsbaarheden te elimineren.

## Classificatie

Category	ID / Value
EPSS score	0.14172
EPSS percentile	0.94397
CISA KEV	False
CVE	<a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-49844">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-49844</a> , <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-48367">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-48367</a> , <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-46819">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-46819</a> , <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-</a>

	<a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-21605">46817, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-21605</a>
CVSS V3	9.9

**Verificatie**

x

DEMONSTRATIE — FICTIEVE GEMEENTE — © PDACS

#### 4.1.7 Apache Server - Remote Code Execution (CVE-2021-41773)

Getroffen systeem burgerzaken.gemeente-schildwaard.nl	<b>High</b> Status: <b>Open</b> Port: <b>443/tcp</b>
--	--

#### Bewijs

We hebben deze kwetsbaarheid kunnen detecteren met behulp van de volgende request, waarin het id command in de payload is opgenomen:

#### HTTP Request:

```
POST /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/bin/sh HTTP/1.1  
Host: burgerzaken.gemeente-schildwaard.nl:443
```

```
A=|echo;id
```

#### HTTP Response:

```
HTTP 200
```

```
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```

#### Kwetsbaarheid omschrijving

Wij hebben geconstateerd dat de target Apache-server kwetsbaar is voor CVE-2021-41773, een Remote Code Execution-kwetsbaarheid in het /cgi-bin endpoint. Als CGI (mod-cgi) expliciet is enabled op de server en bestanden buiten de document root niet beschermd zijn met de "require all denied"-configuratie, kan een unauthenticated remote attacker willekeurige binaries op het filesystem benaderen (bijv. /bin/sh) en commando's uitvoeren op de server.

De root cause van deze kwetsbaarheid is een wijziging in de path normalization-code in versie 2.4.49 van Apache Server. Alleen deze specifieke versie is affected.

We hebben deze kwetsbaarheid vastgesteld door een HTTP POST request te sturen naar het exposed endpoint, met id in de body, en vervolgens de command response uit de output te lezen.

#### Risico omschrijving

Het risico bestaat dat een remote unauthenticated attacker de server volledig kan compromitteren om vertrouwelijke informatie te stelen, ransomware te installeren of te pivoten naar het interne netwerk.

#### Aanbeveling

Wij adviseren de Apache Server te upgraden naar een versie gelijk aan of hoger dan 2.4.51.

#### Referenties

<https://nvd.nist.gov/vuln/detail/CVE-2021-41773>

<https://www.exploit-db.com/exploits/50383>

<https://www.exploit-db.com/exploits/50512>

### Classificatie

Category	ID / Value
EPSS score	0.94391
EPSS percentile	0.99973
CISA KEV	True
CVE	<a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41773">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41773</a>
CVSS	4.3
CVSS V3	7.5

### Verificatie

✓ Deze finding is gevalideerd en is dus geen False Positive.

#### 4.1.8 Redis Lua Sandbox < 8.2.2 - Cross-User Escape (CVE-2025-46818)

Getroffen systeem  
burgerzaken.gemeente-schildwaard.nl

**High**

Status: **Open**  
Port: **6379/tcp**

#### Bewijs

We hebben deze kwetsbaarheid kunnen detecteren met behulp van de volgende Request / Response chain.

We hebben de volgende informatie uit het target gehaald: 7.0.15

Endpoint: burgerzaken.gemeente-schildwaard.nl:6379

#### Kwetsbaarheid omschrijving

Redis-serverinstallaties met Lua scripting enabled (EVAL/FUNCTION) in versies 8.2.1 en eerder bevatten een sandbox escape-kwetsbaarheid die een authenticated user toestaat een Lua script te crafted dat Lua-objecten manipuleert en de bedoelde script isolation ontsnapt. De flaw treft het Lua scripting-subsysteem en kan getriggerd worden via normale script execution-commands wanneer authenticatie beschikbaar is. Exploitatie laat de aanvaller code uitvoeren of acties uitvoeren met de privileges van een andere Redis user context. Het issue is opgelost in Redis 8.2.2.

#### Risico omschrijving

Een authenticated aanvaller kan deze kwetsbaarheid benutten om arbitrary code of commands uit te voeren in de context van een andere user, wat kan leiden tot data exposure, privilege escalation of bredere system compromise. Exploitatie vereist authenticated access en de mogelijkheid Lua scripts aan te roepen, waardoor de kans matig is in omgevingen die scripting access toestaan.

#### Aanbeveling

Upgrade Redis naar versie 8.2.2 of hoger. Als tijdelijke mitigatie kan Lua script execution worden uitgeschakeld of beperkt via ACL's om de EVAL- en FUNCTION-commandofamilies te blokkeren voor untrusted users.

#### Referenties

<https://github.com/dwisiswant0/CVE-2025-46818>

#### Classificatie

Category	ID / Value
EPSS score	0.03178
EPSS percentile	0.87002

CISA KEV	False
CVE	<a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-46818">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-46818</a>
CVSS V3	6

### Verificatie

- ✓ Deze finding is gevalideerd en is dus geen False Positive.

DEMONSTRATIE — FICTIEVE GEMEENTE — © PDACS

#### 4.1.9 Redis < 8.2.1 Lua Long-String Delimiter - Out-of-Bounds Read (CVE-2025-46819)

<p>Getroffen systeem burgerzaken.gemeente-schildwaard.nl</p>	<p><b>High</b></p> <p>Status: <b>Open</b> Port: <b>6379/tcp</b></p>
--	---

#### Bewijs

We hebben deze kwetsbaarheid kunnen detecteren met behulp van de volgende Request / Response chain.

We hebben de volgende informatie uit het target gehaald: 7.0.15

Endpoint: burgerzaken.gemeente-schildwaard.nl:6379

#### Kwetsbaarheid omschrijving

Redis-versies 8.2.1 en eerder met Lua scripting bevatten een out-of-bounds read-kwetsbaarheid in de afhandeling van de Lua long-string delimiter. Een authenticated client die Lua scripts kan uitvoeren kan een specially crafted script indienen dat de long-string delimiter-bug triggert, waarbij memory wordt gelezen buiten de bedoelde bounds, of de server crasht. Het issue treft alle Redis-builds met Lua scripting enabled en is opgelost in Redis 8.2.2. Exploitatie vereist de mogelijkheid EVAL/FUNCTION-style commands uit te voeren op de target-server.

#### Risico omschrijving

Succesvolle exploitatie kan memory-inhoud van het Redis-proces disclosen of een crash veroorzaken, wat leidt tot information leakage of denial-of-service. Omdat de flaw authenticated script execution vereist, hangt de kans af van access controls en exposure van accounts die Lua kunnen runnen, maar de impact kan hoog zijn op exposed of multi-tenant deployments.

#### Aanbeveling

Upgrade Redis naar versie 8.2.2 of hoger; als een directe upgrade niet mogelijk is, beperk dan het uitvoeren van Lua scripts door de EVAL- en FUNCTION-commandofamilies te verwijderen of uit te schakelen via ACL's voor untrusted accounts.

#### Referenties

<https://github.com/dwisiswant0/CVE-2025-46819>

#### Classificatie

Category	ID / Value
EPSS score	0.05046
EPSS percentile	0.89796

CISA KEV	False
CVE	<a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-46819">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-46819</a>
CVSS V3	6.3

### Verificatie

- ✓ Deze finding is gevalideerd en is dus geen False Positive.

DEMONSTRATIE — FICTIEVE GEMEENTE — © PDACS

#### 4.1.10 Redis Server - Unauthenticated Access

Getroffen systeem burgerzaken.gemeente-schildwaard.nl	<b>High</b> Status: <b>Open</b> Port: <b>6379/tcp</b>
--	---

#### Bewijs

We hebben vastgesteld dat de target server is geconfigureerd met een default credential pair.

We hebben de volgende informatie uit het target gehaald: burgerzaken.gemeente-schildwaard.nl:6379

Authenticatie werd uitgevoerd zonder credentials.

Username: ""

Password: ""

#### Kwetsbaarheid omschrijving

Deze kwetsbaarheid ontstaat wanneer een Redis-server geconfigureerd is om connecties te accepteren

zonder dat authenticatie vereist is. Standaard handhaaft Redis geen access control. Als de Redis-instance gebonden is aan een netwerkinterface die toegankelijk is

voor untrusted sources (bijv. het publieke internet of een onvoldoende gesegmenteerd intern netwerk), kunnen malicious actors een connectie opzetten en interacteren met de Redis-server zonder gebruikersnaam, wachtwoord of andere credentials.

Dit gebrek aan access control staat de uitvoering van elk willekeurig Redis-command toe.

#### Risico omschrijving

Het draaien van een Redis-server met unauthenticated access en exposed aan een netwerk vormt een kritieke security-kwetsbaarheid. Ongeautoriseerde gebruikers kunnen vrij interacteren met de Redis-instance, wat kan leiden tot ernstige consequenties zoals het lezen, wijzigen of verwijderen van alle data die opgeslagen is in de database, including sensitive application state or cached information.

Daarnaast kan Redis-functionaliteit misbruikt worden om remote command execution te bereiken op de onderliggende server, waarmee aanvallers controle krijgen over de

host. Dit kan via technieken zoals het schrijven van bestanden to arbitrary locations or executing Lua scripts with malicious intent.

Daarnaast kunnen aanvallers denial-of-service-aanvallen uitvoeren door de server te overspoelen met commando's of databases te flushen, wat applicaties die afhankelijk zijn

on Redis. In environments with insufficient network segmentation, a compromised Redis-instance kan ook fungeren als pivot point voor lateral movement naar andere

systems.

## Aanbeveling

Wij adviseren om het kritieke risico van unauthenticated Redis access te adresseren. Het is essentieel om authenticatie te enablen. Dit moet gedaan worden door een sterk en uniek wachtwoord te configureren met de `requirepass`-directive in de Redis-configuratiefile

(`redis.conf`). Na het wijzigen van deze instelling moet de Redis-server herstart worden om de wijzigingen door te voeren. Daarnaast is het belangrijk om ervoor te zorgen

dat de Redis-instance alleen toegankelijk is vanuit trusted networks of hosts door firewall rules te implementeren die toegang tot de Redis-poort (default 6379) beperken.

Idealiter is Redis alleen bereikbaar vanaf de applicatieservers die het nodig hebben, en niet direct exposed aan het publieke internet of breder intern netwerken. Review regelmatig netwerkconfiguraties en Redis-instellingen om de these security controls.

## Referenties

[https://redis.io/docs/latest/operate/oss\\_and\\_stack/management/security/](https://redis.io/docs/latest/operate/oss_and_stack/management/security/)

[https://owasp.org/www-project-top-ten/2017/A2\\_Broken\\_Authentication](https://owasp.org/www-project-top-ten/2017/A2_Broken_Authentication)

## Classificatie

Category	ID / Value
CVSS V3	7.2

## Verificatie

✓ Deze finding is gevalideerd en is dus geen False Positive.

#### 4.1.11 Redis - weak password

Getroffen systeem  
burgerzaken.gemeente-schildwaard.nl

**High**

Status: **Open**  
Port: **6379/tcp**

#### Bewijs

We managed to detect that the target server is set up with a default credential pair.  
We extracted the following information from the target: burgerzaken.gemeente-schildwaard.nl:6379

Username: ""  
Password: "admin"

#### Kwetsbaarheid omschrijving

De Redis data structure-server kan beschermd worden met een wachtwoord. Deze kwetsbaarheid ontstaat wanneer het geconfigureerde wachtwoord zwak, voorspelbaar of veelgebruikt is (bijv. "password", "123456", default credentials als deze ooit gezet zijn). Aanvallers kunnen brute-force-technieken, dictionary attacks of kennis van veelvoorkomende zwakke wachtwoorden inzetten om ongeautoriseerde toegang te krijgen tot de Redis-instance met deze eenvoudig te compromitteren credentials.

#### Risico omschrijving

Het gebruik van zwakke credentials voor een Redis-instance die exposed is aan een netwerk brengt

een significant security-risico met zich mee. Als een aanvaller het zwakke wachtwoord succesvol kraakt of raadt, krijgt hij hetzelfde niveau toegang als een authenticated user.

Deze ongeautoriseerde toegang kan leiden tot het kunnen lezen, wijzigen of verwijderen any data stored in Redis, potentially compromising sensitive application informatie. Bovendien kunnen aanvallers, net als bij lege credentials, misbruik maken van Redis-functionaliteit om remote command execution te bereiken op de onderliggende server. Het exploiteren van zwakke credentials kan dus leiden tot data breaches, system compromise, and denial-of-service attacks, making it a serious threat to the confidentiality, integrity, and availability of the affected systems.

#### Aanbeveling

Om de risico's van zwakke Redis-credentials te mitigeren, is het essentieel to replace any easily guessable passwords with strong, unique passwords that voldoende lang zijn en een mix bevatten van hoofd- en kleine letters, numbers, and symbols. Organizations should enforce strong password policies voor alle Redis-instances. Overweeg daarnaast om network-level restricties te implementeren om toegang tot de Redis-poort te beperken tot alleen trusted

hosts of  
netwerken. Het regelmatig auditen van het geconfigureerde Redis-wachtwoord en het  
gebruik van  
monitoring voor verdachte authenticatie-pogingen kan de security verder verhogen.

### Referenties

[https://redis.io/docs/latest/operate/oss\\_and\\_stack/management/security/](https://redis.io/docs/latest/operate/oss_and_stack/management/security/)

[https://owasp.org/www-project-top-ten/2017/A2\\_Broken\\_Authentication](https://owasp.org/www-project-top-ten/2017/A2_Broken_Authentication)

### Verificatie

✓ Deze finding is gevalideerd en is dus geen False Positive.

#### 4.1.12 Generic Env File Disclosure

Getroffen systeem burgerzaken.gemeente-schildwaard.nl	<b>High</b> Status: <b>Open</b> Port: <b>443/tcp</b>
--	--

#### Bewijs

We managed to detect a Generic Env File Disclosure, using the following Request / Response chain.

Endpoint: <https://burgerzaken.gemeente-schildwaard.nl:443/.env>

#### Kwetsbaarheid omschrijving

Deze kwetsbaarheid ontstaat wanneer gevoelige environment-bestanden, die vaak gebruikt worden door webapplicaties om configuratiedetails op te slaan, toegankelijk zijn voor ongeautoriseerde gebruikers. Dit kan ontstaan door verschillende oorzaken: onjuiste webserver-configuratie, verkeerd omgaan met statische bestanden, of deployment-fouten waardoor deze bestanden op publiek toegankelijke locaties blijven staan. Aanvallers kunnen deze bestanden ophalen via directe URL-toegang of andere middelen, en zo kritieke secrets blootleggen.

#### Risico omschrijving

De blootstelling van generic environment-bestanden vormt een hoog security-risico. Deze bestanden bevatten vaak zeer gevoelige informatie die nodig is voor de werking van de applicatie, zoals database credentials waarmee een aanvaller data kan lezen, wijzigen of verwijderen; API keys die toegang verschaffen tot externe services onder de identiteit van de applicatie; en secret keys voor cryptografische operaties, wat session hijacking of het forgen van security tokens mogelijk kan maken. Succesvolle retrieval van deze bestanden kan leiden tot een volledige compromise van de webapplicatie en de bijbehorende data, evenals potentiële toegang tot connected services en infrastructuur.

#### Aanbeveling

Om het risico van generic environment file disclosure te mitigeren is het essentieel te voorkomen dat deze bestanden door de webserver worden uitgeleverd. Dit kan door de webserver (bijv. Apache, Nginx) zo te configureren dat toegang tot bestanden met extensies zoals `.env` expliciet geweigerd wordt. Zorg er daarnaast voor dat applicatie-deploymentprocessen deze gevoelige bestanden niet naar publiek toegankelijke directories van de webserver kopiëren. Overweeg om gevoelige configuratie-informatie op te slaan in environment variables op OS-niveau of gebruik secure secret management-oplossingen in plaats van alleen op `.env`-bestanden te vertrouwen in productieomgevingen. Review regelmatig webserver-configuraties en deploymentscripts om te bevestigen dat deze gevoelige bestanden correct beschermd zijn en niet onbedoeld exposed.

#### Hoe te reproduceren

```
curl -X 'GET' \  
-H 'Accept: */*' \  
-H 'Accept-Language: en' \  
-H 'User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)  
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.4.1 Safari/605.1.24'  
'https://burgerzaken.gemeente-schildwaard.nl:443/.env'
```

## Referenties

[https://cheatsheetseries.owasp.org/cheatsheets/DotEnv\\_Security\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/DotEnv_Security_Cheat_Sheet.html)

<https://cwe.mitre.org/data/definitions/532.html>

## Verificatie

✓ Deze finding is gevalideerd en is dus geen False Positive.

#### 4.1.13 SSH service exposed to the Internet

Getroffen systeem burgerzaken.gemeente-schildwaard.nl	<b>Medium</b>  Status: <b>Open</b> Port: <b>22/tcp</b>
--	---

#### Bewijs

We hebben een publiek toegankelijke SSH service kunnen detecteren.

```
Starting Nmap ( https://nmap.org ) at 2026-04-25 16:54 EEST
Nmap scan report voor burgerzaken.gemeente-schildwaard.nl (178.105.3.89)
Host is up (0.0059s latency).
rDNS record voor 178.105.3.89: static.89.3.105.178.clients.your-server.de

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u9 (protocol 2.0)
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.63 seconds
```

#### Kwetsbaarheid omschrijving

Wij hebben geconstateerd dat de SSH-service met username/password-authenticatie publiek toegankelijk is. Netwerkbeheerders gebruiken remote administration-protocollen vaak om apparaten zoals switches, routers en andere essentiële systemen te beheren. Het via het internet bereikbaar maken van deze services verhoogt echter security-risico's en creëert potentiële aanvalsmogelijkheden tegen de organisatie.

#### Risico omschrijving

Het online exposen van deze service met username/password-authenticatie maakt het voor aanvallers mogelijk om authenticatie-aanvallen uit te voeren, zoals het raden van login credentials, en potentieel ongeautoriseerde toegang te verkrijgen. Kwetsbaarheden zoals unpatched software, protocol flaws of backdoors kunnen ook geëxploiteerd worden. Een voorbeeld is de CVE-2024-3094 (XZ Utils Backdoor)-kwetsbaarheid.

#### Aanbeveling

Wij adviseren SSH met username/password-authenticatie over het internet uit te schakelen en in plaats daarvan een Virtual Private Network (VPN) te gebruiken dat two-factor authentication (2FA) verplicht stelt. Als de SSH-service essentieel is voor bedrijfsdoeleinden, adviseren wij toegang te beperken tot designated IP-adressen via een firewall. Daarnaast is

het verstandig SSH Public Key Authentication te gebruiken, aangezien dit een key pair gebruikt om de identiteit van een gebruiker of proces te verifiëren.

### Hoe te reproduceren

```
nmap -p 22 -sV -n --script ssh-auth-methods --open burgerzaken.gemeente-schildwaard.nl
```

### Verificatie

✓ Deze finding is gevalideerd en is dus geen False Positive.

DEMONSTRATIE — FICTIEVE GEMEENTE — © PDACS

#### 4.1.14 MySQL service exposed to the Internet

Getroffen systeem  
burgerzaken.gemeente-schildwaard.nl

**Medium**

Status: **Open**  
Port: **3306/tcp**

#### Bewijs

We hebben een publiek toegankelijke MySQL service kunnen detecteren.

```
PORT STATE SERVICE VERSION  
3306/tcp open mysql MySQL 5.5.5-10.11.14-MariaDB-0+deb12u2
```

#### Kwetsbaarheid omschrijving

Wij hebben geconstateerd dat de MySQL-service publiek toegankelijk is. MySQL fungeert als veelgebruikte database voor talloze webapplicaties en services voor data storage, waardoor het een aantrekkelijk target is voor gemotiveerde aanvallers.

#### Risico omschrijving

Het risico bestaat dat een aanvaller dit issue exploiteert door een password-based attack uit te voeren op de MySQL-service. Daarnaast kan hij zero-day-kwetsbaarheden exploiteren om remote access te krijgen tot de MySQL database-server, en daarmee volledige controle krijgen over het besturingssysteem en bijbehorende services. Zo'n aanval kan leiden tot de blootstelling van vertrouwelijke of gevoelige informatie.

#### Aanbeveling

Wij adviseren publieke internettoegang tot MySQL uit te schakelen en een Virtual Private Network (VPN) te gebruiken dat two-factor authentication (2FA) afdwingt. Vermijd directe user authentication tot de MySQL-service via het internet, omdat dit aanvallers in staat stelt password-guessing uit te voeren en mogelijk aanvallen te initiëren die tot volledige controle leiden. Als de MySQL-service desondanks direct toegankelijk moet zijn vanaf het internet, adviseren wij deze te herconfigureren zodat hij alleen toegankelijk is vanaf bekende IP-adressen.

#### Hoe te reproduceren

```
nmap -p 3306 -sV -n --open burgerzaken.gemeente-schildwaard.nl
```

#### Verificatie

✓ Deze finding is gevalideerd en is dus geen False Positive.

#### 4.1.15 Redis service exposed to the Internet

Getroffen systeem  
burgerzaken.gemeente-schildwaard.nl

**Medium**

Status: **Open**  
Port: **6379/tcp**

#### Bewijs

We hebben een publiek toegankelijke Redis service kunnen detecteren.

```
PORT STATE SERVICE VERSION  
6379/tcp open redis Redis key-value store 7.0.15
```

#### Kwetsbaarheid omschrijving

Wij hebben geconstateerd dat de Redis-service publiek toegankelijk is. Deze service bevat vaak kritieke organisatiedata, waardoor het een aantrekkelijk target is voor gemotiveerde aanvallers.

#### Risico omschrijving

Het risico bestaat dat een aanvaller dit issue exploiteert door een password-based attack uit te voeren op de Redis-service. Als een aanvaller een correct set login-gegevens identificeert, kan hij toegang krijgen tot de database en beginnen met enumeration, wat mogelijk vertrouwelijke informatie blootlegt. Bovendien kunnen zulke kwetsbaarheden leiden tot andere aanvalsvormen, waaronder privilege escalation, waardoor aanvallers system commands kunnen uitvoeren en lateraal kunnen bewegen naar andere systemen in het interne netwerk.

#### Aanbeveling

Wij adviseren ervoor te zorgen dat de Redis-service niet publiek toegankelijk is. De Redis-service moet beschermd worden achter een firewall of alleen beschikbaar gesteld worden aan gebruikers die verbonden zijn via een Virtual Private Network (VPN). Als de Redis-service desondanks direct toegankelijk moet zijn vanaf het internet, adviseren wij deze te herconfigureren zodat hij alleen toegankelijk is vanaf bekende IP-adressen.

#### Hoe te reproduceren

```
nmap -p 6379 -sV -n --open burgerzaken.gemeente-schildwaard.nl
```

#### Verificatie

✓ Deze finding is gevalideerd en is dus geen False Positive.

#### 4.1.16 Kwetsbaarheden gevonden voor PHP 7.4.33

Getroffen systeem burgerzaken.gemeente-schildwaard.nl	<b>Medium</b>  Status: <b>Open</b> Port: <b>443/tcp</b>
--	--

#### Bewijs

CVE	<a href="https://nvd.nist.gov/vuln/detail/CVE-2022-4900">https://nvd.nist.gov/vuln/detail/CVE-2022-4900</a>
CVSS	6.2
EPSS Score	0.00065
EPSS Percentile	0.20003
CISA KEV	No
Summary	A vulnerability was found in PHP where setting the environment variable PHP_CLI_SERVER_WORKERS to a large value leads to a heap buffer overflow.
Exploit	N/A
CVE	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-5458">https://nvd.nist.gov/vuln/detail/CVE-2024-5458</a>
CVSS	5.3
EPSS Score	0.03579
EPSS Percentile	0.87768
CISA KEV	No
Summary	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs (FILTER_VALIDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly.
Exploit	N/A

#### Kwetsbaarheid omschrijving

Kwetsbaarheden gevonden voor PHP 7.4.33

## Risico omschrijving

Deze kwetsbaarheden stellen de affected applicaties bloot aan het risico van ongeautoriseerde toegang tot vertrouwelijke data en mogelijk denial-of-service-aanvallen. Een aanvaller kan een geschikt exploit zoeken (of zelf ontwikkelen) voor één van deze kwetsbaarheden en deze gebruiken om het systeem aan te vallen.

### Notes:

Omdat de kwetsbaarheden uitsluitend zijn vastgesteld op basis van version-based testing, zal het risiconiveau voor deze finding niet hoger zijn dan "high". Critical risico's worden alleen toegekend aan kwetsbaarheden die zijn vastgesteld via actieve en gevalideerde testmethoden.

- De kwetsbaarheden zijn geïdentificeerd op basis van de versie van de server.
- Voor elke poort worden alleen de eerste 5 kwetsbaarheden met het hoogste risico getoond.

## Aanbeveling

Wij adviseren de affected software te upgraden naar de laatste versie om de risico's van deze kwetsbaarheden te elimineren.

## Classificatie

Category	ID / Value
EPSS score	0.03579
EPSS percentile	0.87768
CISA KEV	False
CVE	<a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-5458">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-5458</a> , <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-4900">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-4900</a>
CVSS V3	6.2

## Verificatie

x

#### 4.1.17 Compressed Backup File

Getroffen systeem  
burgerzaken.gemeente-schildwaard.nl

**Medium**

Status: **Open**  
Port: **443/tcp**

#### Bewijs

We hebben een Compressed Backup File kunnen detecteren met behulp van de volgende Request / Response chain.

Endpoint: <https://burgerzaken.gemeente-schildwaard.nl:443/backup.tar.gz>

#### Kwetsbaarheid omschrijving

Web-toegankelijke compressed backup- en archive-bestanden (bijv. .zip, .tar.gz, .7z, .rar, .sql.gz, .war, .db) zijn gedetecteerd op voorspelbare HTTP-paden op de target-host. Deze bestanden bevatten vaak (gedeeltelijke) applicatiedata, configuratiebestanden, database dumps of source-artefacten, en zijn kwetsbaar wanneer ze direct over HTTP worden uitgeleverd zonder authenticatie of access controls. Een aanvaller kan deze archives ophalen door bekende filenames of automated directory-locaties op te vragen, en de gevoelige inhoud vervolgens offline extraheren. De kwetsbaarheid vereist alleen dat backup- of export-bestanden bestaan in de web root of bereikbare directories, en dat de server ze retourneert met HTTP 200-responses.

#### Risico omschrijving

Exposed archives kunnen gevoelige informatie blootleggen zoals credentials, API keys, database-inhoud en interne configuratie, wat verdere intrusion, data theft of privilege escalation mogelijk maakt. Exploitatie is straightforward en automatiseerbaar, waardoor succesvolle compromise waarschijnlijk is wanneer zulke bestanden aanwezig en toegankelijk zijn.

#### Aanbeveling

Verwijder onnodige backup- en archive-bestanden uit web-toegankelijke directories en handhaaf least-privilege access controls; als backups moeten blijven, sla ze op buiten de web root en restrict access via authenticatie en netwerk-controls. Implementeer daarnaast automated scans om exposed archives te detecteren en remediëren, en zorg dat backups versleuteld en veilig geroteerd worden.

#### Hoe te reproduceren

```
curl -X 'GET' \  
-H 'Accept: */*' \  
-H 'Accept-Language: en' \  
-H 'User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)  
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.4.1 Safari/605.2.20'  
'https://burgerzaken.gemeente-schildwaard.nl:443/backup.tar.gz'
```

### Classificatie

Category	ID / Value
CVSS V3	5.3

### Verificatie

- ✓ Deze finding is gevalideerd en is dus geen False Positive.

#### 4.1.18 Git Configuration

Getroffen systeem  
burgerzaken.gemeente-schildwaard.nl

**Medium**

Status: **Open**  
Port: **443/tcp**

#### Bewijs

We hebben een Git Configuratie kunnen detecteren met behulp van de volgende Request / Response chain.

Endpoint: <https://burgerzaken.gemeente-schildwaard.nl:443/.git/config>

#### Kwetsbaarheid omschrijving

Publiek toegankelijke Git repository-metadata is ontdekt door het ophalen van het /.git/config-bestand en gerelateerde log output. De exposed bestanden kunnen repository-configuratie bevatten zoals remote URLs, embedded credentials, en references naar branches of submodules. Een aanvaller kan repository-level informatie verkrijgen en, afhankelijk van de inhoud, credentials of URLs die andere interne hosts of services prijsgeven. Het issue ontstaat wanneer een webserver de .git-directory of bestanden van een werkende repository in de web document root uitlevert.

#### Risico omschrijving

Disclosure van .git-configuratie en logs kan gevoelige informatie prijsgeven inclusief embedded usernames, passwords of service endpoints, wat account compromise of lateral discovery mogelijk maakt. Aanvallers kunnen exposed repository-metadata gebruiken om source code te reconstrueren, secrets te bemachtigen of verdere aanvallen op te zetten tegen de applicatie of interne infrastructuur, waardoor exploitatie waarschijnlijk is als de bestanden beschikbaar zijn via HTTP.

#### Aanbeveling

Voorkom directe web-toegang tot .git en andere VCS-bestanden door repositories uit de document root te verwijderen of de webserver te configureren om 403/404 te returnen voor deze paden, en roteer alle credentials die in exposed bestanden gevonden zijn; als cloning heeft plaatsgevonden, overweeg dan affected keys en wachtwoorden te roteren en te auditen op ongeautoriseerde toegang.

#### Hoe te reproduceren

```
curl -X 'GET' \  
-H 'Accept: */*' \  
-H 'Accept-Language: en' \  
-H 'User-Agent: Mozilla/5.0 (Windows NT 10.0, Win64, x64, rv:128.0) Gecko/20100101 Firefox/128.0' 'https://burgerzaken.gemeente-schildwaard.nl:443/.git/config'
```

### Classificatie

Category	ID / Value
CVSS V3	5.3

### Verificatie

- ✓ Deze finding is gevalideerd en is dus geen False Positive.

## 4.2 Target: <https://burgerzaken.gemeente-schildwaard.nl/>

### 4.2.1 SQL Injection

Getroffen systeem <a href="https://burgerzaken.gemeente-schildwaard.nl/">https://burgerzaken.gemeente-schildwaard.nl/</a>	<b>High</b>  Status: <b>Open</b> Port: <b>443/tcp</b>
--	--

### Bewijs

URL	<a href="https://burgerzaken.gemeente-schildwaard.nl/admin.php">https://burgerzaken.gemeente-schildwaard.nl/admin.php</a>
Method	POST
Vulnerable Parameter	pass (Body Parameter)
Bewijs	<p>We injected payloads with 2 different time delays in the <b>pass body parameter</b> and all were successful.</p> <p>Injecting the value '+(SELECT*FROM(SELECT(SLEEP(8)))a)+'0 generated a time delay of <b>8.040608 s</b>.</p> <p>Injecting the value '+(SELECT*FROM(SELECT(SLEEP(22)))a)+'0 generated a time delay of <b>22.043913 s</b>.</p> <p>The original response time was <b>0.046764 s</b>.</p> <p>Tried exploiting for a MySQL database and failed.  <a href="https://ptt.eu-central-1.linodeobjects.com/ptt/6826ff11ad1802a2.txt">https://ptt.eu-central-1.linodeobjects.com/ptt/6826ff11ad1802a2.txt</a></p>
URL	<a href="https://burgerzaken.gemeente-schildwaard.nl/admin.php">https://burgerzaken.gemeente-schildwaard.nl/admin.php</a>
Method	POST
Vulnerable Parameter	user (Body Parameter)
Bewijs	<p>We injected payloads with 2 different time delays in the <b>user body parameter</b> and all were successful.</p> <p>Injecting the value '+(SELECT*FROM(SELECT(SLEEP(10)))a)+'0 generated a time delay of <b>10.041202 s</b>.</p> <p>Injecting the value '+(SELECT*FROM(SELECT(SLEEP(24)))a)+'0 generated a time delay of <b>24.040613 s</b>.</p> <p>The original response time was <b>0.040887 s</b>.</p> <p>Tried exploiting for a MySQL database and failed.  <a href="https://ptt.eu-central-1.linodeobjects.com/ptt/f72ad90a3ed4a0b5.txt">https://ptt.eu-central-1.linodeobjects.com/ptt/f72ad90a3ed4a0b5.txt</a></p>
URL	<a href="https://burgerzaken.gemeente-schildwaard.nl/zaak.php">https://burgerzaken.gemeente-schildwaard.nl/zaak.php</a>

Method	GET
Vulnerable Parameter	id (Query Parameter)
Bewijs	<p>Injecting the value " in the <b>id query parameter</b> generated the following error(s) in the response:</p> <pre>&lt;h2&gt;Zoekresultaat&lt;/h2&gt;&lt;p&gt;Database fout: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' at line 1&lt;/p&gt;&lt;p&gt;Query: &lt;code&gt;SELECT ID, post_title, post_date FROM wp_posts WHERE ID = 1d3d2d231d2dd4"&lt;/code&gt;&lt;/p&gt;</pre> <p><a href="https://ptt.eu-central-1.linodeobjects.com/ptt/543eea74e4f50fcd.txt">https://ptt.eu-central-1.linodeobjects.com/ptt/543eea74e4f50fcd.txt</a></p>
URL	<a href="https://burgerzaken.gemeente-schildwaard.nl/zoek.php">https://burgerzaken.gemeente-schildwaard.nl/zoek.php</a>
Method	GET
Vulnerable Parameter	naam (Query Parameter)
Bewijs	<p>Injecting the value ' in the <b>naam query parameter</b> generated the following error(s) in the response:</p> <pre>&lt;h2&gt;Resultaten voor: 1d3d2d231d2dd4'&lt;/h2&gt;&lt;p&gt;Database fout: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '%'' at line 1&lt;/p&gt;&lt;p&gt;Query: &lt;code&gt;SELECT user_login, user_email, user_registered FROM wp_users WHERE user_login LIKE '%1d3d2d231d2dd4'%'&lt;/code&gt;&lt;/p&gt;</pre> <p><a href="https://ptt.eu-central-1.linodeobjects.com/ptt/925efd707f62365.txt">https://ptt.eu-central-1.linodeobjects.com/ptt/925efd707f62365.txt</a></p>

### Kwetsbaarheid omschrijving

Wij hebben geconstateerd dat de webapplicatie kwetsbaar is voor SQL Injection-aanvallen in de afhandeling van database-queries. De kwetsbaarheid wordt veroorzaakt door onvoldoende input sanitization en stelt een aanvaller in staat willekeurige SQL-commando's te injecteren en deze direct op de database uit te voeren.

### Risico omschrijving

Het risico bestaat dat een aanvaller ongeautoriseerde toegang krijgt tot de informatie in de database van de applicatie. Hij kan informatie extraheren en wijzigen zoals: gebruikersnamen, wachtwoorden, klantgegevens en andere applicatie-specifieke data.

## Aanbeveling

Wij adviseren een validatiemechanisme te implementeren voor alle data die van gebruikers ontvangen wordt.

De beste manier om je te beschermen tegen SQL Injection is door prepared statements te gebruiken voor elke SQL-query die op de database wordt uitgevoerd.

Daarnaast kan user input ook worden gesanitized met dedicated methoden zoals: `mysqli_real_escape_string`.

## Referenties

[https://owasp.org/www-community/attacks/SQL\\_Injection](https://owasp.org/www-community/attacks/SQL_Injection)

[https://cheatsheetseries.owasp.org/cheatsheets/SQL\\_Injection\\_Prevention\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html)

## Classificatie

Category	ID / Value
CWE	<a href="https://cwe.mitre.org/data/definitions/89.html">https://cwe.mitre.org/data/definitions/89.html</a>
OWASP Top 10 - 2025	<a href="https://owasp.org/search/?searchString=A05-Injection%202025">https://owasp.org/search/?searchString=A05-Injection%202025</a>

## Verificatie

✓ Deze finding is gevalideerd en is dus geen False Positive.

#### 4.2.2 Cross-Site Scripting

<p>Getroffen systeem <a href="https://burgerzaken.gemeente-schildwaard.nl/">https://burgerzaken.gemeente-schildwaard.nl/</a></p>	<p><b>High</b></p> <p>Status: <b>Open</b> Port: <b>443/tcp</b></p>
--	--

#### Bewijs

URL	<a href="https://burgerzaken.gemeente-schildwaard.nl/zoek.php">https://burgerzaken.gemeente-schildwaard.nl/zoek.php</a>
Method	GET
Vulnerable Parameter	naam (Query Parameter)
Bewijs	<p>Injected the payload <code>&lt;svg/onload=document.body.append(`4a6bf02e`.repeat(2))&gt;</code> in the <b>naam query parameter</b> and the expected result <code>4a6bf02e4a6bf02e</code> was found in the response. The script inside the payload tries to repeat a random string. If the string <code>4a6bf02e</code> is doubled on the response page, we confirm that our script has been executed. This request was done using a Chrome browser.</p> <p>If available, the replay attack button uses a simpler <code>alert()</code> payload that may not work as expected. <a href="https://ptt.eu-central-1.linodeobjects.com/ptt/b71f28edc4f43d0c.txt">https://ptt.eu-central-1.linodeobjects.com/ptt/b71f28edc4f43d0c.txt</a></p>

#### Kwetsbaarheid omschrijving

Wij hebben geconstateerd dat de target-webapplicatie kwetsbaar is voor Cross-Site Scripting (XSS)-aanvallen. Deze kwetsbaarheid wordt veroorzaakt door onvoldoende input validation, waardoor een malicious actor JavaScript-code kan injecteren en uitvoeren in de context van een sessie van een andere gebruiker.

#### Risico omschrijving

Het risico is dat de door een aanvaller geïnjecteerde code kan leiden tot effecten zoals het stelen van session cookies, het aanroepen van applicatiefuncties namens een andere gebruiker, en het exploiteren van browser-kwetsbaarheden. Succesvolle exploitatie van Cross-Site Scripting-aanvallen vereist menselijke interactie (bijv. de gebruiker via social engineering een speciale link laten openen).

#### Aanbeveling

Er zijn meerdere manieren om XSS-aanvallen te mitigeren. Wij adviseren:

- never trust user input
- always encode and escape user input (using a Security Encoding Library)
- gebruik de HttpOnly cookie flag ter bescherming tegen cookie theft

- implement Content Security Policy
- gebruik de X-XSS-Protection response header.

### Referenties

<https://owasp.org/www-community/attacks/xss>

[https://cheatsheetseries.owasp.org/cheatsheets/Cross\\_Site\\_Scripting\\_Prevention\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html)

### Classificatie

Category	ID / Value
CWE	<a href="https://cwe.mitre.org/data/definitions/79.html">https://cwe.mitre.org/data/definitions/79.html</a>
OWASP Top 10 - 2025	<a href="https://owasp.org/search/?searchString=A05-Injection%202025">https://owasp.org/search/?searchString=A05-Injection%202025</a>

### Verificatie

- ✓ Deze finding is gevalideerd en is dus geen False Positive.

## 5. Addendum

### 5.1 Tools en techniek

Dit is een lijst met tools die zijn gebruikt tijdens de penetratietest:

Tool	Source IP	Target	Starttijd
Network Scanner	172.[REDACTED]	burgerzaken.gemeente-schildwaard.nl	Apr 25, 2026 - 15:52 UTC+02
Website Scanner	172.[REDACTED]	<a href="https://burgerzaken.gemeente-schildwaard.nl/">https://burgerzaken.gemeente-schildwaard.nl/</a>	Apr 25, 2026 - 18:50 UTC+02

## 6. Over PDCS

PDCS staat voor **Plan, Do, Check... Security**. De naam is afgeleid van de bekende kwaliteitscirkel: plannen, uitvoeren, controleren en bijstellen. Die gedachte vormt de kern van onze aanpak. Informatiebeveiliging is geen eenmalig project en geen papieren verplichting, maar een continu proces waarin beleid, uitvoering, controle en verbetering logisch op elkaar moeten aansluiten.

Bij PDCS geloven we dat lokale overheden zelf hun verantwoordelijkheid voor informatiebeveiliging goed kunnen waarmaken. Dat lukt het beste wanneer zij gebruikmaken van duidelijke standaarden, bewezen werkwijzen en ondersteuning van specialisten die de gemeentelijke praktijk begrijpen. Wij helpen gemeenten om informatiebeveiliging praktisch, bestuurlijk begrijpelijk en aantoonbaar te organiseren.

Voor bestuur en management maken wij digitale risico's inzichtelijk in heldere taal: wat zijn de grootste risico's, wat betekent dit voor de dienstverlening en welke maatregelen verdienen prioriteit? Voor CISO's en informatiebeveiligingsteams bieden wij ondersteuning bij beleid, risicoanalyses, plannen, verantwoording en uitvoering. Daarbij leveren we geen dikke rapporten om af te vinken, maar helpen we processen, eigenaarschap en verbetercycli echt in te richten.

Onze aanpak sluit aan op relevante kaders zoals de BIO, ENSIA en de Cyberbeveiligingswet/NIS2. Met praktische werkvormen, sjablonen, begeleiding en trainingen helpen we gemeenten om beleid sneller om te zetten in concrete acties en aantoonbare resultaten. Zo wordt kennis beter geborgd en blijft de organisatie minder kwetsbaar bij personeelwisselingen.

PDCS is in 2025 opgericht door **Kees Hintzbergen, Remco Groet, Remko Sikkema en Arjen Hartog**. Samen brengen zij tientallen jaren ervaring mee op het gebied van informatiebeveiliging, crisismanagement, CERT/CSIRT-werk, risicomanagement, governance, identity & accessmanagement, pentesting, awareness en bestuurlijke advisering. Hun ervaring is opgedaan bij onder meer ministeries, gemeenten, banken, verzekeraars, veiligheidsorganisaties en de Informatiebeveiligingsdienst voor gemeenten.