PENTEST RAPPORT DIGID-AUDIT

MBO voorzieningen

In opdracht van: Newtone

Surelock B.V.
Korenmolenlaan 1E
3447GG – Woerden
www.surelock.nl

Contact
Koen van der Sijs
31 (0)6 21 48 30 53

Versie geschiedenis

Versie	Datum	Auteur	Beschrijving
0.1	25/04/2024	Koen van der Sijs	Initiële versie
0.2	25/04/2024	Dim Gerssen	Interne review
1.0	25/04/2024	Koen van der Sijs	Opgeleverde versie

Verzendlijst

Naam
Björn Roskott

INHOUD

Managementsamenvatting

Newtone heeft Surelock gevraagd een DigiD onderzoek uit te voeren op de Test/acceptatie omgeving van MBO voorzieningen.
De aanleiding van de test is de door de overheid verplicht gestelde beveiligingsassessment (DigiD audit) welke jaarlijks moet worden uitgevoerd. Dit assessment wordt door Newtone uitgevoerd op de MBO voorzieningen omgeving.

Bevindingen DigiD onderzoek

Tijdens het onderzoek zijn de volgende normen meegenomen, hierbij zijn deze getoetst aan de hand van de richtlijnen opgenomen in de Norea Handreiking.
Op basis van het onderzoek kan worden vastgesteld dat er wordt voldaan aan de meeste richtlijnen/aandachtspunten die in de handreiking zijn toegelicht. De applicatie lijkt bij norm u/pw.03 niet volledig te voldoen aan de richtlijn voor een specifieke security-header, het risico is echter beperkt gezien het feit dat de betreffende header wel is geconfigureerd.

Norm	Oordeel	Opmerking
U/WA.03 + U/WA.04	Geen afwijkingen waargenomen.	
U/PW.02	Beperkte afwijking binnen de test omgeving aangetroffen/Geen afwijkingen binnen de productie omgeving.	In de test omgeving werd niet volledig voldaan aan één van de in totaal 6 aandachtspunten. De applicatie lijkt te veel informatie vrij te geven bij foutmeldingen. Na navraag te hebben gedaan bij de beheer partij 'Topicus' bleek dat de testomgeving meer informatie in foutmeldingen weergeeft dan bij de productie omgeving het geval is. Vanuit Topicus is bewijs aangeleverd waaruit dit blijkt. Hiermee is aangetoond dat binnen de productie omgeving geen afwijkingen aanwezig zijn.
U/PW.03	Beperkte afwijking*	Er wordt niet volledig voldaan aan één van de in totaal 7 aandachtspunten. De applicatie heeft een security-header (Referrer-policy) minder strikt ingesteld dan de richtlijn voorschrijft. Doordat de header wel is geconfigureerd is het risico zeer beperkt. **Aanbeveling**

		Wijzig de instellingen van de 'Referrer Policy' naar de 'Same origin' instelling zodat bij doorverwijzingen de 'base-url' niet wordt meegestuurd naar externe websites.
C.06	Geen afwijkingen waargenomen	

* : De applicatie voldoet strikt genomen niet aan alle aandachtspunten/richtlijnen maar de afwijking is zeer beperkt en vormt geen praktisch risico.

1. Opdrachtomschrijving

Door Surelock is een pentest uitgevoerd op de MBO voorzieningen applicatie in opdracht van 'Newtone' met als doel om te kunnen toetsen of de applicatie voldoet aan de gestelde DigiD normen.

1.1.Scope

Voor het huidige onderzoek zijn de volgende onderdelen aangeduid als 'in scope':

- test.inschrijvenmbo.nl

Om de kans op impact als gevolg van de test op de productie omgeving te mitigeren is er voor gekozen om het onderzoek op de test omgeving uit te voeren. Deze omgeving is qua functionaliteit vergelijkbaar aan de productie omgeving.

1.2.Tijdslijn

De test is uitgevoerd in de periode van dinsdag 23 april 2024 en woensdag 24 april 2024 in totaal bestond deze test uit 2 werkdagen.

1.3.Test vorm

De test werd uitgevoerd als een Grey-Box onderzoek, wat inhoudt dat tijdens het onderzoek basisinformatie zoals referenties, locatie en inloggegevens beschikbaar zijn gesteld aan de onderzoeker.
Richtlijnen
Gedurende de uitvoering van de securitytest is er gebruik gemaakt van de volgende Richtlijnen:

- OWASP Top 10 [1]
- OWASP Web Security Testing Guide (WSTG)[2]
- Normen DigiD beveiligingsassessment[3]

[1] Zie: https://owasp.org/www-project-top-ten/
[2] Zie: https://owasp.org/www-project-web-security-testing-guide/v41/
[3] Zie: https://www.norea.nl/uploads/bfile/d870b9bf-759c-40cc-a4a3-67ec8f7cee69

2. Aanpak

Surelock maakt bij het uitvoeren van een pentest gebruik van state of the art tooling, maar zal de resultaten hiervan altijd handmatig verifiëren. De pentest geeft een overzicht van alle huidige (technische) kwetsbaarheden die in de gegeven timebox zijn gevonden. De securityspecialisten kijken daarnaast ook naar de 'best practices' en of het doel voldoet aan deze globaal gestelde normen. De belangrijkste standaarden die tijdens de test zijn meegenomen zijn de OWASP Web Security Testing Guide (WSTG) en Penetration Execution Standard (PTES).

Tijdens het uitvoeren van het Grey-Box onderzoek zullen de volgende onderdelen worden meegenomen:

- Toegang tot het systeem met inloggegevens/toegangsrechten
- Controle Autorisatie en authenticatie
- Sessiebeheer
- Invoer validatie, sanering en encodering
- Foutafhandeling
- Encryptie (van verkeer en data)
- Wachtwoordbeveiligingsvereisten
- Digid normen op basis van de Norea Handreiking-ICT beveiligingsassessment DigiD[4]

[4] Zie: https://www.norea.nl/uploads/bfile/d870b9bf-759c-40cc-a4a3-67ec8f7cee69

3. Resultaten

3.1.Beoordeling DigiD normen

De onderzochte DigiD normen zijn getoetst op basis van de 'NOREA Handreiking ICTbeveiligingsassessment DigiD 4.0' hierin wordt per DigiD norm verder gespecificeerd waaraan moet worden voldaan en hoe dit moet worden getoetst. Onderstaande tabel geeft de beoordeling per norm weer. Uit deze tabel valt op te maken dat er aan de meeste aandachtspunten wordt voldaan. Bij de normen 'U/PW.02' & U/PW.03 wordt niet volledig aan deze punten voldaan hierom zijn er aanbevelingen voor verbetering opgenomen in onderstaande tabel. De volledige test resultaten om de richtlijnen/aandachtspunten te toetsten zijn in hoofdstuk 4 opgenomen.

Norm	Richtlijn/aandachtspunt	Oordeel	Opmerking
U/WA.03 + U/WA.04 (Deze normen zijn samengevoegd aangezien de richtlijnen op dezelfde wijze worden getest)	1. HTTP request voor alle invoermethodes zoals gespecificeerd in de ICT-Beveiligingsrichtlijnen van NCSC moeten worden gevalideerd (testen op type, lengte, formaat en karakters van invoer en speciale tekens (bv. <, >, ', ", & , /, --, etc.).	Voldoet	
	2. De webapplicatie codeert dynamische onderdelen in de uitvoer waarbij mogelijke gevaarlijke tekens (bv. <, >, ', ", & , /, --, etc.) worden genormaliseerd.	Voldoet	
U/PW.02	1. Behandel alleen HTTP-requests waarvan de gegevens een correct type, lengte, formaat, tekens en patronen hebben	Voldoet	
	2. Behandel alleen HTTP-requests van initiators met een correcte authenticatie en autorisatie.	Voldoet	
	3. Sta alleen de voor de ondersteunde webapplicaties benodigde HTTP-requestmethoden (GET, POST, etc.) toe en blokkeer de overige niet noodzakelijke HTTP-requestmethoden	Voldoet	

	4. Verstuur alleen HTTP-headers die voor het functioneren van HTTP van belang zijn.	Voldoet	
	5. Bij het optreden van een fout wordt de informatie in een HTTP-response tot een minimum beperkt. Een eventuele foutmelding zegt wel dat er iets is fout gegaan, maar niet hoe het is fout gegaan.	Voldoet binnen productie	De applicatie geeft in de test omgeving meer informatie vrij dan strikt noodzakelijk. Zo geeft de foutmelding ook informatie vrij over hoe de fout is ontstaan. Vanuit Topicus werd aangegeven dat dit binnen de productie omgeving niet het geval is.
U/PW.03	1. Directory listings worden niet ondersteund.	Voldoet	
	2. Cookie flags staan op 'HttpOnly' en 'Secure'.	Voldoet	
	3. De X-Frame-Options header voorkomt dat de pagina in een iFrame wordt geladen, waarmee gegevens kunnen worden gestolen, pagina's worden aangepast of gebruikers worden misleid. Te configureren waarden: deny of sameorigin	Voldoet	
	4. HTTP Strict Transport Security (HSTS) zorgt ervoor dat browsers alleen over TLS communiceren met de webapplicatie. Door het forceren van HTTPS beschermt deze header gebruikers tegen afluisteren en Man-in-the-Middle (MitM)-aanvallen. Minimaal te configureren waarde: max-age=31536000	Voldoet	
	5. X-Content-Type-Options De X-Content-Type-Options header voorkomt dat de browser het MIME-type van een	Voldoet	

	bestand bepaalt op basis van kenmerken (sniffing). Te configureren waarde: nosniff		
	6. Content-Security-Policy De Content-Security-Policy (CSP) geeft de browser instructies over welke resources vanaf welke locatie mogen worden ingeladen en hoe deze mogen worden gebruikt. Te configureren waarden: default-src 'self'; frame-src 'self'; frame-ancestors 'self'; Sta	Voldoet	
	7. Referrer-Policy De Referrer-Policy beperkt het ongevraagd delen van privacygevoelige informatie bij het doen van verzoeken aan, en bij het doorsturen van de gebruiker naar, een andere website. Gebruik de instelling 'same-origin', zodat de referrer-header alleen wordt meegestuurd bij verzoeken binnen het eigen domein.	Beperkte Afwijking	De huidige instellingen van de 'Referrer policy' header voldoen niet volledige aan de gestelde richtlijn. De huidige instelling staat toe dat de base-URL kan worden doorgestuurd. naar een externe website. Het risico is echter zeer beperkt aangezien de informatie die kan worden doorgestuurd ook zeer beperkt is. **Aanbeveling:** Wijzig de instellingen van de 'Referrer Policy' naar de 'Same origin' instelling zodat bij doorverwijzingen de 'base-url' niet wordt meegestuurd naar externe websites.
C.06	1. In de webapplicatie zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.	Voldoet	Gedurende het onderzoek is vastgesteld dat de applicatie bekende aanvallen kan detecteren en voorkomen, hierbij is ook gevalideerd dat een 'Webapplicatie firewall'(WAF) aanwezig is die dit soort aanvallen blokkeert voordat ze bij de daadwerkelijk applicatie terechtkomen.

4. Bewijs DigiD Normen

4.1.Bewijs U/WA.03 + U/WA.04

ID	**U/WA.03 + U/WA.04**
Betreft	Test.inschrijvenmbo.nl
Norm	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer en uitvoer te normaliseren en te valideren, voordat deze invoer of uitvoer wordt verwerkt.

Details

De betreffende norm is op basis van onderstaande eisen gevalideerd:

- HTTP request voor alle invoermethodes zoals gespecificeerd in de ICT-Beveiligingsrichtlijnen van NCSC moeten worden gevalideerd (testen op type, lengte, formaat en karakters van invoer en speciale tekens (bv. <, >, ', ", & , /, --, etc.).
- De webapplicatie codeert dynamische onderdelen in de uitvoer waarbij mogelijke gevaarlijke tekens (bv. <, >, ', ", & , /, --, etc.) worden genormaliseerd

Gedurende de test is gevalideerd of in en uitvoer juiste wordt gevalideerd, om dit te kunnen controleren zijn de volgende zaken onderzocht:

- Controle op Invoer validatie + normalisatie als ook XSS validatie waarbij wordt onderzocht of de applicatie niet vatbaar is voor XSS aanvallen. Zie: '**Invoer validatie + normalisatie validatie'**
- Controle op SQL injecties, dit toont mede aan dat gebruikersinvoer op een juiste manier worden gevalideerd en genormaliseerd. Zie: '**SQL injectie validatie'**
- Foutieve invoer/karakters. Zie: '**Validatie ongeldige invoer'**

Invoer validatie + normalisatie

Onderstaande afbeelding toont onder andere aan dat de applicatie niet vatbaar lijkt te zijn voor XSS aanvallen aangezien de uitvoer door de browser niet als geldige HTML/JavaScript code wordt gezien. Dit toont aan dat gebruikersinvoer op een juiste manier wordt genormaliseerd en niet als uitvoerbare code wordt geïnterpreteerd.

Afbeelding 1 – XSS validatie

SQL injectie validatie

```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent
is illegal. It is the end user's responsibility to obey all applicable local, state and
federal laws. Developers assume no liability and are not responsible for any misuse or
damage caused by this program

[*] starting @ 13:50:51 /2024-04-23/

[13:50:51] [INFO] parsing HTTP request from 'sql-test-req'
[13:50:51] [INFO] testing connection to the target URL
[13:50:56] [INFO] checking if the target is protected by some kind of WAF/IPS
[13:50:56] [CRITICAL] WAF/IPS identified as 'CloudFlare'
are you sure that you want to continue with further target testing? [Y/n] Y
[13:51:04] [WARNING] please consider usage of tamper scripts (option '--tamper')
[13:51:04] [INFO] testing if the target URL content is stable
[13:51:04] [INFO] target URL content is stable
[13:51:04] [INFO] testing if POST parameter
'fieldSet:fieldSetMarkup:inputFields:0:controlGroup:controlGroup_body:formField' is
dynamic
[13:51:04] [INFO] POST parameter
'fieldSet:fieldSetMarkup:inputFields:0:controlGroup:controlGroup_body:formField' appears
to be dynamic
[13:51:05] [WARNING] heuristic (basic) test shows that POST parameter
'fieldSet:fieldSetMarkup:inputFields:0:controlGroup:controlGroup_body:formField' might not
be injectable
[13:51:05] [INFO] testing for SQL injection on POST parameter
'fieldSet:fieldSetMarkup:inputFields:0:controlGroup:controlGroup_body:formField'
[13:51:05] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:51:05] [WARNING] reflective value(s) found and filtering out
[13:51:06] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[13:51:06] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP
BY clause (EXTRACTVALUE)'
[13:51:06] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
```

```
[13:51:07] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING
clause (IN)'
[13:51:07] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[13:51:07] [INFO] testing 'Generic inline queries'
[13:51:07] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[13:51:08] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[13:51:08] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[13:51:08] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[13:51:09] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[13:51:09] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[13:51:09] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other
(potential) technique found. Do you want to reduce the number of requests? [Y/n] Y
[13:51:14] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[13:51:14] [WARNING] POST parameter
'fieldSet:fieldSetMarkup:inputFields:0:controlGroup:controlGroup_body:formField' does not
seem to be injectable
[13:51:14] [INFO] testing if POST parameter
'fieldSet:fieldSetMarkup:inputFields:1:controlGroup:controlGroup_body:formField' is
dynamic
[13:51:14] [INFO] POST parameter
'fieldSet:fieldSetMarkup:inputFields:1:controlGroup:controlGroup_body:formField' appears
to be dynamic
[13:51:14] [WARNING] heuristic (basic) test shows that POST parameter
'fieldSet:fieldSetMarkup:inputFields:1:controlGroup:controlGroup_body:formField' might not
be injectable
[13:51:15] [INFO] testing for SQL injection on POST parameter
'fieldSet:fieldSetMarkup:inputFields:1:controlGroup:controlGroup_body:formField'
[13:51:15] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:51:16] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[13:51:16] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP
BY clause (EXTRACTVALUE)'
[13:51:16] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[13:51:16] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING
clause (IN)'
[13:51:16] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[13:51:17] [INFO] testing 'Generic inline queries'
[13:51:17] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[13:51:17] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[13:51:18] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[13:51:18] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[13:51:18] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[13:51:18] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[13:51:19] [INFO] testing 'Oracle AND time-based blind'
[13:51:19] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[13:51:20] [WARNING] POST parameter
'fieldSet:fieldSetMarkup:inputFields:1:controlGroup:controlGroup_body:formField' does not
seem to be injectable
[13:51:20] [INFO] testing if POST parameter
'fieldSet:fieldSetMarkup:inputFields:2:controlGroup:controlGroup_body:formField' is
dynamic
[13:51:20] [INFO] POST parameter
'fieldSet:fieldSetMarkup:inputFields:2:controlGroup:controlGroup_body:formField' appears
to be dynamic
```

```
[13:51:20] [WARNING] heuristic (basic) test shows that POST parameter
'fieldSet:fieldSetMarkup:inputFields:2:controlGroup:controlGroup_body:formField' might not
be injectable
[13:51:20] [INFO] testing for SQL injection on POST parameter
'fieldSet:fieldSetMarkup:inputFields:2:controlGroup:controlGroup_body:formField'
[13:51:20] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:51:21] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[13:51:21] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP
BY clause (EXTRACTVALUE)'
[13:51:22] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[13:51:22] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING
clause (IN)'
[13:51:22] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[13:51:22] [INFO] testing 'Generic inline queries'
[13:51:22] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[13:51:23] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[13:51:23] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[13:51:23] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[13:51:24] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[13:51:24] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[13:51:24] [INFO] testing 'Oracle AND time-based blind'
[13:51:25] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[13:51:25] [WARNING] POST parameter
'fieldSet:fieldSetMarkup:inputFields:2:controlGroup:controlGroup_body:formField' does not
seem to be injectable
[13:51:25] [INFO] testing if POST parameter
'bottomRowPanel:rightContainer:rightButtons:1:link' is dynamic
[13:51:26] [WARNING] POST parameter 'bottomRowPanel:rightContainer:rightButtons:1:link'
does not appear to be dynamic
[13:51:26] [WARNING] heuristic (basic) test shows that POST parameter
'bottomRowPanel:rightContainer:rightButtons:1:link' might not be injectable
[13:51:26] [INFO] testing for SQL injection on POST parameter
'bottomRowPanel:rightContainer:rightButtons:1:link'
[13:51:26] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:51:27] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[13:51:27] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP
BY clause (EXTRACTVALUE)'
[13:51:27] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[13:51:27] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING
clause (IN)'
[13:51:28] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[13:51:28] [INFO] testing 'Generic inline queries'
[13:51:28] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[13:51:28] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[13:51:29] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[13:51:29] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[13:51:29] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[13:51:30] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[13:51:30] [INFO] testing 'Oracle AND time-based blind'
[13:51:31] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[13:51:32] [WARNING] POST parameter 'bottomRowPanel:rightContainer:rightButtons:1:link'
does not seem to be injectable
[13:51:32] [CRITICAL] all tested parameters do not appear to be injectable. Try to
increase values for '--level'/'--risk' options if you wish to perform more tests. If you
```

```
suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you
could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--
random-agent'
[13:51:32] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 261 times

[*] ending @ 13:51:32 /2024-04-23/
```

Validatie ongeldige invoer

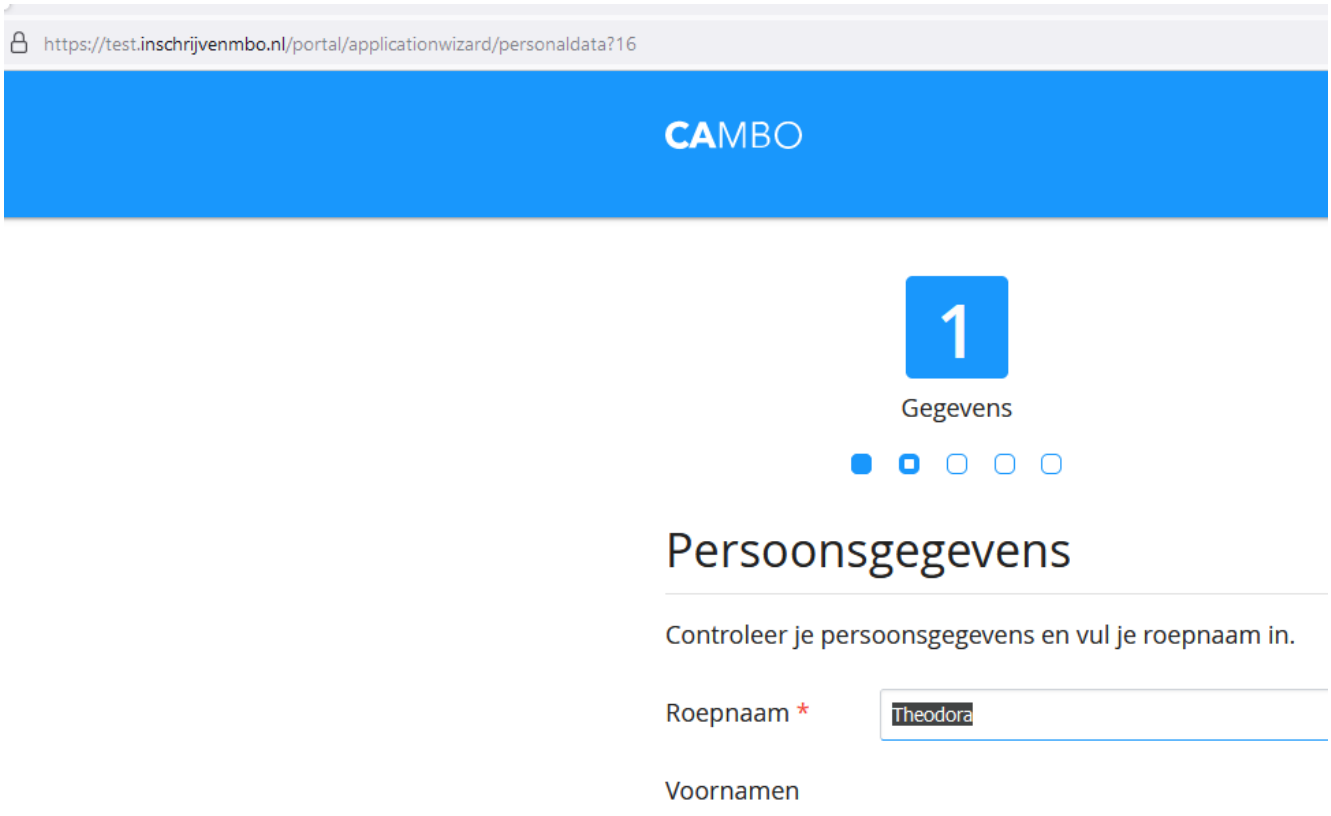
Tijdens het onderzoek is ook gevalideerd of de applicatie ongeldige invoer juist afhandelt.

Met onderstaand verzoek is een niet printbare karakter(%00) aan de roepnaam toegevoegd,

```
POST /portal/applicationwizard/personaldata?14-1.0-bottomRowPanel-rightContainer-rightButtons-1-link
HTTP/2
Host: test.inschrijvenmbo.nl
Cookie: JSESSIONID=p1~aTdMRwtYCjqr9QMFJ9gIlCNtFCqqaO7mdHF6kxXW.test
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:125.0) Gecko/20100101 Firefox/125.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://test.inschrijvenmbo.nl/portal/applicationwizard/personaldata?14
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Wicket-Ajax: true
Wicket-Ajax-Baseurl: applicationwizard/personaldata?14
Wicket-Focusedelementid: id175
X-Requested-With: XMLHttpRequest
Content-Length: 244
Origin: https://test.inschrijvenmbo.nl
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Pragma: no-cache
Cache-Control: no-cache
Te: trailers

fieldSet%3AfieldSetMarkup%3AinputFields%3A0%3AcontrolGroup%3AcontrolGroup_body%3AformField=Theodora%
00&extraSupportControlGroup%3AextraSupportControlGroup_body%3AextraSupportChoice=0&bottomRowPanel%3A
rightContainer%3ArightButtons%3A1%3Alink=1
```

Deze karakters lijken aan de server kant niet te worden geaccepteerd en worden door de server automatisch uit de invoer weg gefilterd, onderstaande afbeelding toont aan dat de ongeldige karakter niet aan de roepnaam is toegevoegd.

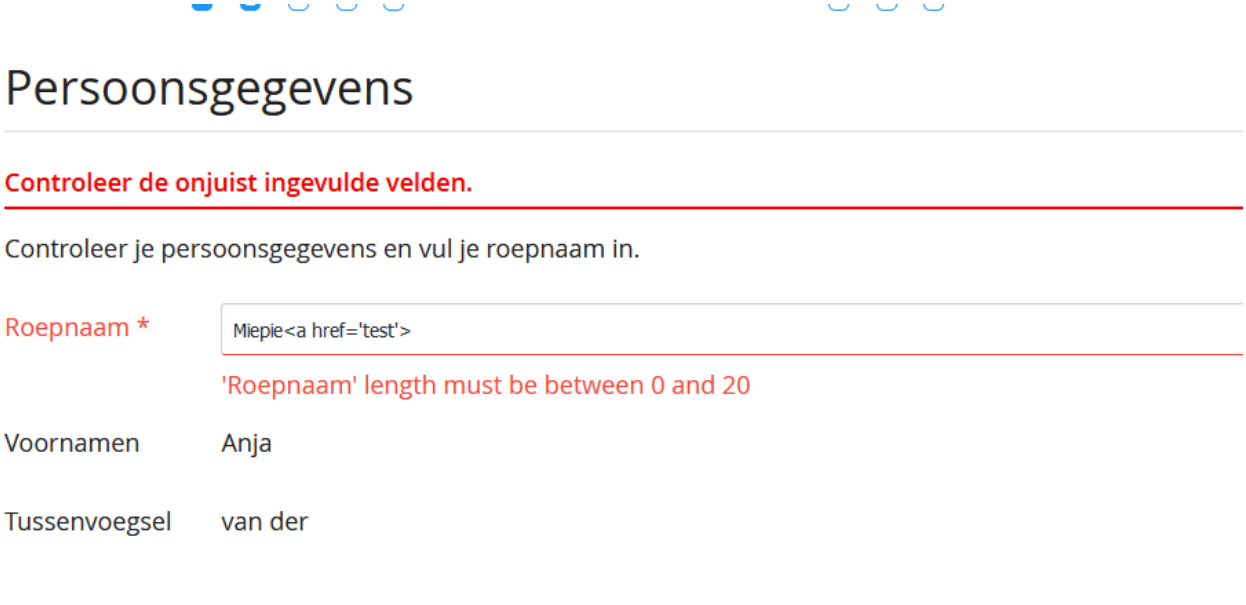


Afbeelding 2 – Invoervalidatie

Naast dat ongeldige tekens niet worden geaccepteerd vindt er ook validatie plaats op de lengte van de naam, hierbij worden namen langer dan 20 karakters niet geaccepteerd. Het is dus niet mogelijk om de lengte van het roepnaam veld te overschrijven.

Request

```
POST /portal/applicationwizard/personaldata?19-1.0-bottomRowPanel-rightContainer-rightButtons-1-link
HTTP/2
Host: test.inschrijvenmbo.nl
Cookie: JSESSIONID=p1~5ZfeSNYcGPeT7s4NL48MJtsOR2MX-GvDYxIwijLl.test
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:125.0) Gecko/20100101 Firefox/125.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://test.inschrijvenmbo.nl/portal/applicationwizard/personaldata?19
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Wicket-Ajax: true
Wicket-Ajax-Baseurl: applicationwizard/personaldata?19
Wicket-Focusedelementid: id177
X-Requested-With: XMLHttpRequest
Content-Length: 256
Origin: https://test.inschrijvenmbo.nl
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
```

<table>
<tr><td colspan="2"><pre>fieldSet%3AfieldSetMarkup%3AinputFields%3A0%3AcontrolGroup%3AcontrolGroup_body%3AformField=Miepie%3Ca+href%3D'test'>&extraSupportControlGroup%3AextraSupportControlGroup_body%3AextraSupportChoice=0&bottomRowPanel%3ArightContainer%3ArightButtons%3A1%3Alink=1</pre></td></tr>
<tr><td colspan="2">Het versturen van een te lange roepnaam resulteert in onderstaande foutmelding, dit toont aan dat de invoerlengte zowel aan de browser (client) kant als bij de server juist wordt gevalideerd.
 
</td></tr>
<tr><td>AANBEVELING</td><td>Er zijn geen aanbevelingen gezien de applicatie aan de gestelde richtlijnen voldoet..</td></tr>
</table>

4.2.Bewijs U/PW.02

ID	**U/PW.02**
BETREFT	Test.Inschrijvenmbo.nl
NORM	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.

DETAILS

De betreffende norm is op basis van onderstaande richtlijnen/aandachtspunten gevalideerd:

- Behandel alleen HTTP-requests waarvan de gegevens een correct type, lengte, formaat, tekens en patronen hebben. Zie : '**Validatie HTTP lengtes/formaat'**
- Behandel alleen HTTP-requests van initiators met een correcte authenticatie en autorisatie. Zie : '**Validatie HTTP Authenticatie'**
- Sta alleen de voor de ondersteunde webapplicaties benodigde HTTP-requestmethoden
- (GET, POST, etc.) toe en blokkeer de overige niet noodzakelijke HTTP-requestmethoden. Zie : '**Validatie HTTP methods'**
- Verstuur alleen HTTP-headers die voor het functioneren van HTTP van belang zijn. Zie: '**Validatie HTTP headers'**
- Toon in HTTP-headers alleen de hoogst noodzakelijke informatie die voor het functioneren van belang is. Zie : '**Validatie HTTP headers'**
- Bij het optreden van een fout wordt de informatie in een HTTP-response tot een minimum beperkt. Een eventuele foutmelding zegt wel dat er iets is fout gegaan, maar niet hoe het is fout gegaan. Zie : '**Validatie foutmeldingen'**

Validatie HTTP lengtes/formaat

De server reageert met verschillende foutmeldingen wanneer afwijkende 'Content-Length' headers worden meegegeven. Het wijzigen van de Content-Length is een bekende manier om HTTP verzoeken te 'smokkelen' tussen frontend(proxy) en backend servers . Het smokkelen van HTTP-verzoeken is een beveiligingsexploit op het HTTP-protocol dat misbruik maakt van een inconsistentie tussen de interpretatie van Content-Length- en Transfer-Encoding-headers tussen HTTP-serverimplementaties in een HTTP-proxyserverketen.
Onderstaand verzoek toont een voorbeeld van een afwijkende 'Content-lenght' header.

Request

```
POST /portal/profile HTTP/1.1
Host: test.inschrijvenmbo.nl
Cookie: JSESSIONID=p1~6Xdoy3oBdoPGYqmSYQ0YDdU6m8oh2riefHTVstes.test
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:125.0) Gecko/20100101
Firefox/125.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://test.inschrijvenmbo.nl/portal/profile?7
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
```

```
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Origin: https://kamnp6.com
Via: kamnp6
Content-Type: application/x-www-form-urlencoded
Content-Length: 36, 0

GET /favicon.ico HTTP/1.1
X-YzBqv:
```

De server lijkt verzoeken met foutieve/malafide lengtes niet te accepteren, bovenstaand verzoek resulteert in onderstaande foutmelding. Dit toont aan dat de server niet lijkt te accepteren

Foutmelding Response

```
HTTP/1.1 400 Bad Request
Server: cloudflare
Date: Wed, 24 Apr 2024 13:20:30 GMT
Content-Type: text/html
Content-Length: 557
Connection: close
CF-RAY: 8796641d0ef993be-AMS

<html>
<head><title>400 Bad Request</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<hr><center>cloudflare</center>
</body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

Validatie HTTP Authenticatie

De applicatie negeert alle verzoeken afkomstig van niet geauthentiseerde gebruikers en verwijst ze door naar de inlogpagina. Onderstaande requests toont het verschil tussen een geauthentiseerde gebruiker en niet geauthentiseerde gebruiker die de 'overview' pagina probeert te openen. Hetzelfde geldt voor alle wijzigingsverzoeken die binnen de applicatie kan worden gedaan, deze worden alleen geaccepteerd indien de gebruiker is ingelogd en over een geldige sessie-token beschikt.

Request geauthentiseerde gebruiker

```
GET /portal/profile?7 HTTP/2
Host: test.inschrijvenmbo.nl
Cookie: JSESSIONID=p1~6Xdoy3oBdoPGYqmSYQ0YDdU6m8oh2riefHTVswMH.test
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:125.0) Gecko/20100101
Firefox/125.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
Accept-Encoding: gzip, deflate, br
Referer: https://test.inschrijvenmbo.nl/portal/profile?7
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
```

Respone

```
HTTP/2 200 OK
Date: Wed, 24 Apr 2024 13:12:53 GMT
Content-Type: text/html;charset=UTF-8
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cross-Origin-Opener-Policy: same-origin
Cache-Control: no-cache, no-store
X-Xss-Protection: 1; mode=block
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Cross-Origin-Embedder-Policy-Report-Only: require-corp
Referrer-Policy: strict-origin-when-cross-origin
Content-Security-Policy: default-src 'none'; script-src 'strict-dynamic' 'nonce-L4aFNf6bn-
81TJA1XxalIiqC'; style-src 'nonce-L4aFNf6bn-81TJA1XxalIiqC' 'self'; img-src 'self' data:;
connect-src 'self'; font-src 'self'; manifest-src 'self'; child-src 'self'; frame-
ancestors none; base-uri 'self'; frame-src 'self'; report-uri cspviolation
Vary: sec-fetch-dest, sec-fetch-site, sec-fetch-mode
X-Content-Type-Options: nosniff
Feature-Policy: sync-xhr 'none';
Permissions-Policy: sync-xhr 'none';
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Cf-Cache-Status: DYNAMIC
Server: cloudflare
Cf-Ray: 879658f569216686-AMS
```

Request niet geauthentiseerde gebruiker

```
GET /portal/profile?7 HTTP/2
Host: test.inschrijvenmbo.nl
Cookie: JSESSIONID=p1~6Xdoy3oBdoPGYqmSYQ0YDdU6m8oh2riefHTVstes.test
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:125.0) Gecko/20100101
Firefox/125.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://test.inschrijvenmbo.nl/portal/profile?7
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
```

Response

```
HTTP/2 302 Found
Date: Wed, 24 Apr 2024 13:13:05 GMT
Content-Length: 0
```

```
Location:
https://test.inschrijvenmbo.nl/login/oauth2/authorize?scope=openid+profile&response_type=c
ode&redirect_uri=https%3A%2F%2Ftest.inschrijvenmbo.nl%2Fportal%2Foauth-
callback&state=f8fc30c434&code_challenge_method=S256&client_id=2279f19f-d5c5-4d3c-b704-
a499a83f7239&code_challenge=fHbk0oTAbOp_PEWrNHtIG2m6g2mjW0oy7M9RVKIopGQ
Expires: Thu, 01 Jan 1970 00:00:00 GMT
```

Dit toont aan dat alleen verzoeken met een geldige sessie token worden behandeld, dit betekent dat alleen geauthentiseerde gebruikers acties binnen de applicatie kunnen uitvoeren.

Validatie HTTP headers

Tijdens het onderzoek is nagegaan of de applicatie alleen HTTP-headers terugstuurt die voor het functioneren van belang zijn.

Op basis van onderstaande request/response is gevalideerd dat de server aan deze gestelde richtlijn voldoet. De server geeft **geen** informatie vrij over de achterliggende technologieën via de HTTP response headers en heeft alleen de noodzakelijke HTTP headers geconfigureerd.

Request

```
GET /portal/profile?7 HTTP/2
Host: test.inschrijvenmbo.nl
Cookie: JSESSIONID=p1~6Xdoy3oBdoPGYqmSYQ0YDdU6m8oh2riefHTVswMH.test
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:125.0) Gecko/20100101
Firefox/125.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://test.inschrijvenmbo.nl/portal/profile?7
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
```

Response

```
HTTP/2 200 OK
Date: Wed, 24 Apr 2024 13:12:53 GMT
Content-Type: text/html;charset=UTF-8
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cross-Origin-Opener-Policy: same-origin
Cache-Control: no-cache, no-store
X-Xss-Protection: 1; mode=block
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Cross-Origin-Embedder-Policy-Report-Only: require-corp
Referrer-Policy: strict-origin-when-cross-origin
Content-Security-Policy: default-src 'none'; script-src 'strict-dynamic' 'nonce-L4aFNf6bn-
81TJA1XxalIiqC'; style-src 'nonce-L4aFNf6bn-81TJA1XxalIiqC' 'self'; img-src 'self' data:;
connect-src 'self'; font-src 'self'; manifest-src 'self'; child-src 'self'; frame-
ancestors none; base-uri 'self'; frame-src 'self'; report-uri cspviolation
Vary: sec-fetch-dest, sec-fetch-site, sec-fetch-mode
X-Content-Type-Options: nosniff
Feature-Policy: sync-xhr 'none';
```

```
Permissions-Policy: sync-xhr 'none';
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Cf-Cache-Status: DYNAMIC
Server: cloudflare
Cf-Ray: 879658f569216686-AMS
```

Validatie HTTP methods

Onderstaande verzoeken tonen aan dat de applicatie de potentieel gevaarlijke TRACE en CONNECT HTTP methodes blokkeert, hiermee is aangetoond dat de server de HTTP methodes die verstuurd mogen worden beperkt.

Request

```
CONNECT /portal/overview?0-2.0-applications HTTP/2
Host: test.inschrijvenmbo.nl
Cookie: JSESSIONID=p1~mRG4VUrX2C0aGVK-sUZEvftQSrQ9FHijHjUjprsw.test
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:125.0) Gecko/20100101 Firefox/125.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://test.inschrijvenmbo.nl/portal/overview?0
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Wicket-Ajax: true
Wicket-Ajax-Baseurl: overview?0
X-Requested-With: XMLHttpRequest
Content-Length: 73
Origin: https://test.inschrijvenmbo.nl
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: keep-alive
```

Response

```
HTTP/2 400 Bad Request
Date: Wed, 24 Apr 2024 08:58:13 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 5750
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-
check=0
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Vary: Accept-Encoding
Server: cloudflare
Cf-Ray: 8794e3e77cf5a016-AMS
```

Request

```
TRACE /portal/overview?0-2.0-applications HTTP/2
Host: test.inschrijvenmbo.nl
Cookie: JSESSIONID=p1~mRG4VUrX2C0aGVK-sUZEvftQSrQ9FHijHjUjprsw.test
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:125.0) Gecko/20100101
Firefox/125.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: en-US,en;q=0.5
```

```
Accept-Encoding: gzip, deflate, br
Referer: https://test.inschrijvenmbo.nl/portal/overview?0
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Wicket-Ajax: true
Wicket-Ajax-Baseurl: overview?0
X-Requested-With: XMLHttpRequest
Content-Length: 73
Origin: https://test.inschrijvenmbo.nl
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: keep-alive
```

Response

```
HTTP/2 405 Method Not Allowed
Server: cloudflare
Date: Wed, 24 Apr 2024 08:58:12 GMT
Content-Type: text/html
Content-Length: 155
Cf-Ray: -
```

Validatie foutmeldingen

Wanneer er bij het ophalen van de overzicht pagina een onverwachte waarde (%00) wordt opgegeven in de server request valt op te merken dat de server reageert met een 500 foutmelding.

Server request

```
POST /portal/overview?0-2.0-applications HTTP/2
Host: test.inschrijvenmbo.nl
Cookie: JSESSIONID=p1~mRG4VUrX2C0aGVK-sUZEvftQSrQ9FHijHjUjprsw.test
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:125.0) Gecko/20100101 Firefox/125.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://test.inschrijvenmbo.nl/portal/overview?0
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Wicket-Ajax: true
Wicket-Ajax-Baseurl: overview?0
X-Requested-With: XMLHttpRequest
Content-Length: 76
Origin: https://test.inschrijvenmbo.nl
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

arg0=%00%5B%22id43%22%5D&arg1=%5B%5D&argCount=2&methodName=onScroll&callId=1
```

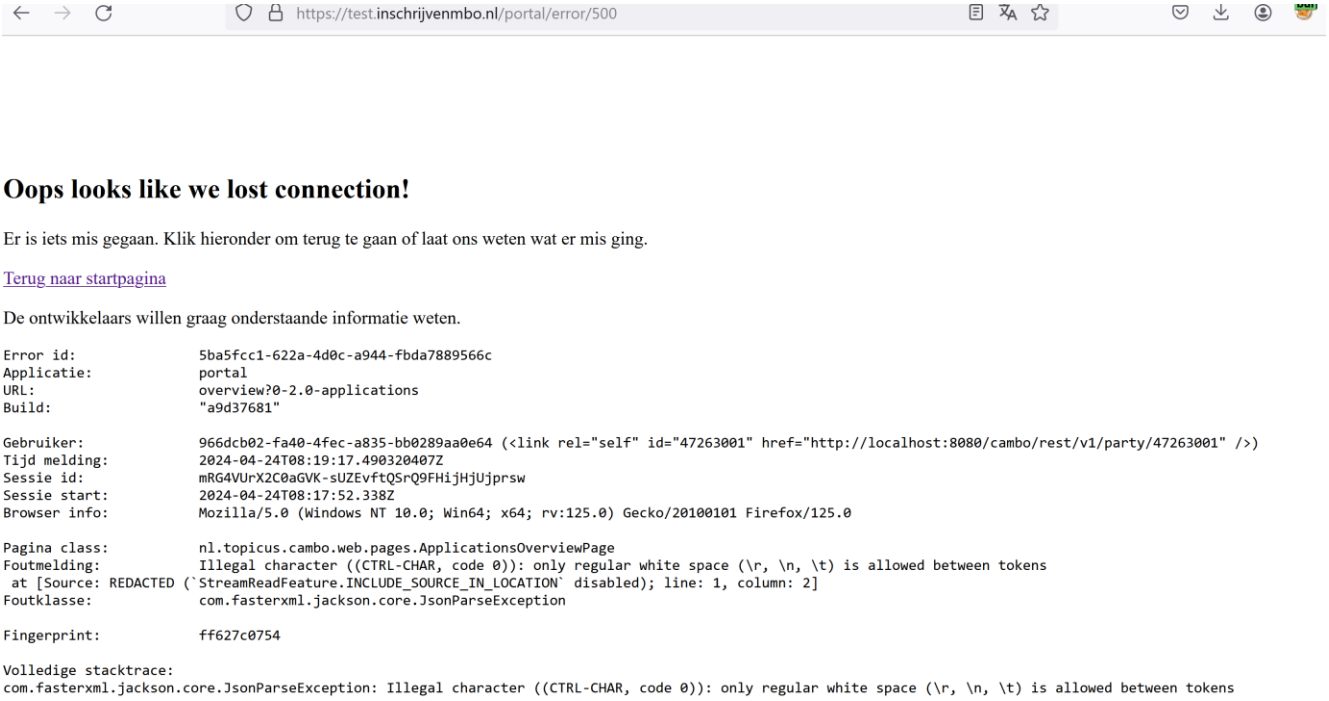
Response

```
HTTP/2 500 Internal Server Error
Date: Wed, 24 Apr 2024 08:19:24 GMT
Content-Type: text/html;charset=UTF-8
Cross-Origin-Opener-Policy: same-origin
X-Xss-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
```

```
Cross-Origin-Embedder-Policy-Report-Only: require-corp
Referrer-Policy: strict-origin-when-cross-origin
Content-Security-Policy: default-src 'none'; script-src 'strict-dynamic' 'nonce-
8GY4iZEk5mP6g8HdZoSxCqnN'; style-src 'nonce-8GY4iZEk5mP6g8HdZoSxCqnN' 'self'; img-src 'self' data:;
connect-src 'self'; font-src 'self'; manifest-src 'self'; child-src 'self'; frame-ancestors none;
base-uri 'self'; frame-src 'self'; report-uri cspviolation
Vary: sec-fetch-dest, sec-fetch-site, sec-fetch-mode
X-Content-Type-Options: nosniff
Feature-Policy: sync-xhr 'none';
Permissions-Policy: sync-xhr 'none';
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Cf-Cache-Status: DYNAMIC
Server: cloudflare
Cf-Ray: 8794ab0de8320a6d-AMS
```

Resulterende foutmelding:

Het versturen van bovenstaand verzoek resulteert in onderstaande foutmelding, hierbij wordt stacktrace informatie getoond



Afbeelding 3 – Foutmelding met stack trace informatie

De richtlijn stelt dat de informatie die in foutmeldingen getoond worden tot een minimum worden beperkt. In dit geval wordt er naast een globale foutmelding ook informatie vrijgegeven over de oorzaak van de fout. Deze informatie kan mogelijk verder worden beperkt.

Productie omgeving

Vanuit Topicus kon worden vastgesteld dat op de productie omgeving foutmeldingen als volgt worden weergegeven:

CAMBO
Centraal Aanmelden MBO en VAVO

Oops looks like we lost connection!

Er is iets mis gegaan. Klik hieronder om terug te gaan of laat ons weten wat er mis ging.

Terug naar startpagina

De fout is opgeslagen onder de referentie abb3a242-1a50-4c85-906d-d1b38c5392f1.

Hierbij valt op te merken dat er alleen een melding-ID wordt weergegeven zonder informatie over de achterliggende fout. Dit is zoals de richtlijn voorschrijft, hierdoor kan worden gesteld dat de applicatie op de productie voldoet.

AANBEVELING	Het is wellicht raadzaam om ook binnen de test omgeving dezelfde foutmelding te tonen als op productie, dus dat binnen de test omgeving alleen een fout-code in de meldingen worden weergegeven zonder additionele informatie te verstrekken.

4.3.Bewijs U/PW.03

ID	**U/PW.03**
BETREFT	Test.inschrijvenmbo.nl
NORM	De webserver is ingericht volgens een configuratie-baseline.

DETAILS

Deze norm is op basis van onderstaande eisen getest:

- Directory listings, zie '**Directory Listing'**
  Te configureren waarde: Directory listings worden niet ondersteund.
- Cookie flags, zie '**cookie flags'**
  Te configureren waarde: Cookie flags staan op 'HttpOnly' en 'Secure'.
- X-Frame-Options, zie '**HTTP security headers**'
  De X-Frame-Options header voorkomt dat de pagina in een iFrame wordt geladen, waarmee gegevens kunnen worden gestolen, pagina's worden aangepast of gebruikers worden misleid. Te configureren waarden: deny of sameorigin
- Strict-Transport-Security (HSTS), zie '**HTTP security headers**'
  HTTP Strict Transport Security (HSTS) zorgt ervoor dat browsers alleen over TLS communiceren met de webapplicatie. Door het forceren van HTTPS beschermt deze header gebruikers tegen afluisteren en Man-in-the-Middle (MitM)-aanvallen. HSTS voorkomt het gebruik van gemengde HTTP en HTTPS inhoud, beschermt tegen fouten van webservers zoals het laden van JavaScript via een onveilige verbinding en voorkomt dat gebruikers waarschuwingen over ongeldige certificaten kunnen negeren.
  Minimaal te configureren waarde: max-age=31536000
- X-Content-Type-Options, zie '**HTTP security headers**'
  De X-Content-Type-Options header voorkomt dat de browser het MIME-type van een bestand bepaalt op basis van kenmerken (sniffing). Wanneer deze header is ingesteld op nosniff, vertrouwt de browser het MIME-type dat door de server wordt meegegeven en zal de browser de bron blokkeren als deze fout is. Dit voorkomt spoofing van resources zoals CSS stylesheets en Javascript-bestanden die over HTTP worden verstuurd.
  Te configureren waarde: nosniff
- Content-Security-Polic, zie '**HTTP security headers**'
  De Content-Security-Policy (CSP) geeft de browser instructies over welke resources vanaf welke locatie mogen worden ingeladen en hoe deze mogen worden gebruikt. Een CSP kan fijnmazige instructies bevatten per soort resource, zoals afbeeldingen, stylesheets en scripts. Bij het gebruik van een CSP zijn standaard de uitvoering van inline scripts en de eval()-functie uitgeschakeld
  Te configureren waarden: default-src 'self'; frame-src 'self'; frame-ancestors 'self'; Sta geen onveilige configuratie toe door het gebruik van 'unsafe-inline' (tenzij gebruik wordt gemaakt van een nonce) en 'unsafe-eval'. Het is niet toegestaan bronnen beginnend met http:// te whitelisten.

- Referrer-Policy, zie '**HTTP security headers**'
  De Referrer-Policy beperkt het ongevraagd delen van privacygevoelige informatie bij het doen van verzoeken aan, en bij het doorsturen van de gebruiker naar, een andere website.
  Gebruik de instelling 'same-origin', zodat de referrer-header alleen wordt meegestuurd bij verzoeken binnen het eigen domein. Dit voorkomt het lekken van privacygevoelige informatie bij omleiden naar externe domeinen. De striktere instelling 'no-referrer' kan ook worden gebruikt, zodat de referrer-header nooit wordt meegestuurd.

Directory listing

Directory listing was op alle aangetroffen eindpunten (endpoints) uitgeschakeld, dit betekent dat de inhoud van de web mappen niet kon worden ingezien.

Cookie flags

Tijdens het onderzoek werden cookie met de in de norm verplicht gestelde 'HTTPOnly' en 'Secure' flags in de browser opgeslagen. Onderstaande request response geeft een voorbeeld van de manier hoe de cookies binnen de geteste omgeving worden ingesteld.

Request

```
GET /portal/oauth-initlogin?iss=https://test.inschrijvenmbo.nl HTTP/2
Host: test.inschrijvenmbo.nl
Cookie: JSESSIONID=p1~MoykY5xpbXeeXRjBz6QzO9dwjcFn4SjaERVI1He5.test
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:125.0) Gecko/20100101
Firefox/125.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://digistub-test.inschrijvenmbo.nl/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-site
Sec-Fetch-User: ?1
Te: trailers
```

Response

```
HTTP/2 302 Found
Date: Tue, 23 Apr 2024 10:24:47 GMT
Content-Length: 0
Location:
https://test.inschrijvenmbo.nl/login/oauth2/authorize?scope=openid+profile&response_type=c
ode&redirect_uri=https%3A%2F%2Ftest.inschrijvenmbo.nl%2Fportal%2Foauth-
callback&state=a13a2b8bc1&code_challenge_method=S256&client_id=2279f19f-d5c5-4d3c-b704-
a499a83f7239&code_challenge=mxBgVCK_oqXUGXhWltq1OIDRFkA_8n5wB25WK99FHkQ
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache, no-store
-> Set-Cookie: JSESSIONID=p1~RYYCYesvznT8_Rc0DBlDWMx-f2r-Z77V5VGX7mTz.test; path=/portal;
secure; HttpOnly
```

HTTP security headers

De webserver maakt gebruik van de in de norm verplicht gestelde HTTP security headers, de headers verplicht gesteld in de norm zijn als volgt:

- X-Frame-Options (met de optie: 'deny' of 'sameorigin')
- Frame-Ancestors (met de optie: 'none' of 'self')
- HTTP Strict Transport Security (HSTS) (met minimaal de 'max-age=31536000' optie)
- X-Content-Type-Options (met de optie: 'nosniff')
- Content-Security-Policy (met minimaal de opties 'default-src: self,
- Referrer-Policy (met de optie: 'Same-origin')

Onderstaande uitvoer toont alle configuratie instellingen van de betreffende applicatie:

```
=======================================================
[*] Analyzing headers of
https://test.inschrijvenmbo.nl/login/
[*] Effective URL:
https://test.inschrijvenmbo.nl/login/
[*] Header X-XSS-Protection is present! (Value: 1;
mode=block)
[*] Header X-Frame-Options is present! (Value:
DENY)
[*] Header X-Content-Type-Options is present! (Value: nosniff)
[*] Header Strict-Transport-Security is present! (Value: max-age=31536000;
includeSubDomains; preload)
[*] Header Content-Security-Policy is present! (Value: default-src 'none'; script-src
'strict-dynamic' 'nonce-wZChVpho9XsfQa5epkzx8GE7'; style-src 'nonce-
wZChVpho9XsfQa5epkzx8GE7' 'self'; img-src 'self' data:; connect-src 'self'; font-src
'self'; manifest-src 'self'; child-src 'self'; frame-ancestors none; base-uri
 'self'; frame-src 'self'; report-uri cspviolation)
[*] Header Referrer-Policy is present! (Value: strict-origin-when-cross-origin)
[*] Header Permissions-Policy is present! (Value: sync-xhr 'none';)
[!] Missing security header: Cross-Origin-Embedder-Policy
[!] Missing security header: Cross-Origin-Resource-Policy
[*] Header Cross-Origin-Opener-Policy is present! (Value: same-origin)
-------------------------------------------------------
[!] Headers analyzed for https://test.inschrijvenmbo.nl/login/
[+] There are 8 security headers
[-] There are not 2 security headers
```

Hierbij valt op te merken dat alleen de instellingen van de 'Referrer-Policy' niet volledig voldoet aan de gestelde, norm.

Huidige instelling:

- X-Frame-Options: Deny
- Content-Security-Policy Value: default-src 'none', frame-ancestors none;
- X-Content-Type-Options: nosniff
- -> Referrer-Policy: strict-origin-when-cross-origin

De richtlijn stelt dat minimaal de instelling 'Same-origin' dient te worden gebruikt, dit zorgt er voor dat de referrer-header alleen wordt meegestuurd bij verzoeken binnen het eigen domein.

De huidige instellingen maken het mogelijk dat de referrer ook wordt meegestuurd naar verzoeken die buiten het huidige domein liggen. Het risico kan als laag worden geclassificeerd aangezien deze situatie zich alleen voordoet wanneer de webserver gebruikers naar externe domeinen doorverwijst, daarnaast is de informatie die in dat geval via de referrer header wordt meegestuurd beperkt tot de base URL. Dit betekent dat alleen '`test.inschrijvenmbo.nl`' bij een doorverwijzing zal worden meegegeven naar een externe website. De huidige instellingen zijn al restrictiever dan wanneer deze header niet zou zijn geïmplementeerd lettend op de doelstelling van de norm kan worden	
AANBEVELING	Wijzig de huidige instellingen van de Referrer-Policy naar de volgende waarde : • Referrer-Policy: 'Same-origin'

4.4.Bewijs C.06

ID	**C.06**
BETREFT	Test.inschrijvenmbo.nl
NORM	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.

DETAILS

Deze norm is op basis van onderstaande richtlijn getest:

- In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.

Om dit te kunnen valideren is tijdens het onderzoek een zogenoemde 'Cross Site Scripting' aanval gesimuleerd, hierbij is gekeken of de betreffende aanval werd gedetecteerd en geblokkeerd/voorkomen.

Op basis van onderstaande verzoeken kan worden geconcludeerd dat de aanval werd gedetecteerd en geblokkeerd. Deze aanval lijkt de web applicatie niet te bereiken, dit toont aan dat dit soort aanvallen tijdig worden gesignaleerd.

Request XSS simulatie

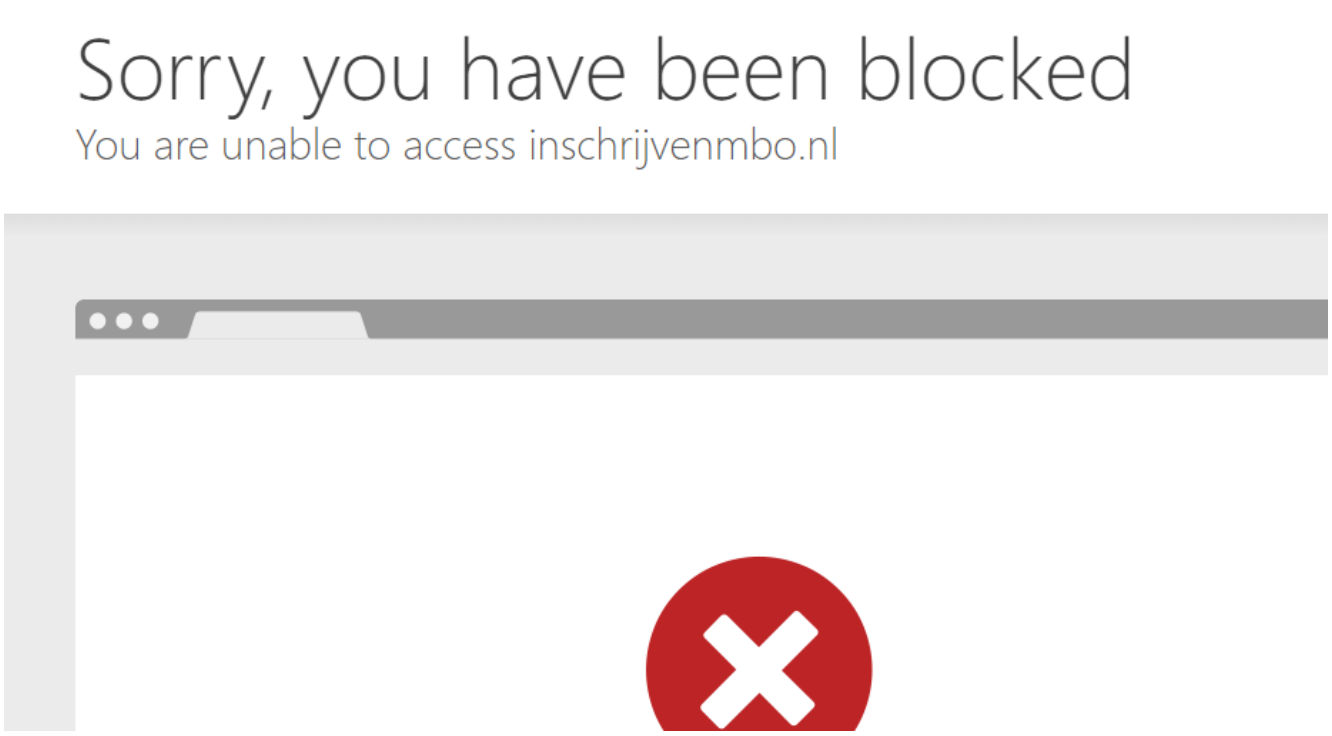
```
POST /portal/applicationwizard/contactdata?1-1.0-bottomRowPanel-rightContainer-rightButtons-1-link
HTTP/2
Host: test.inschrijvenmbo.nl
Cookie: JSESSIONID=p1~CR4qnUKd4L1ifV6Q_u0M-G5yoM8jswNGhvsX1RQc.test
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:125.0) Gecko/20100101 Firefox/125.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://test.inschrijvenmbo.nl/portal/applicationwizard/contactdata?1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Wicket-Ajax: true
Wicket-Ajax-Baseurl: applicationwizard/contactdata?1
Wicket-Focusedelementid: id15
X-Requested-With: XMLHttpRequest
Content-Length: 413
Origin: https://test.inschrijvenmbo.nl
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Pragma: no-cache
Cache-Control: no-cache
Te: trailers

fieldSet%3AfieldSetMarkup%3AinputFields%3A0%3AcontrolGroup%3AcontrolGroup_body%3AformField=pentest%4
0surelock.nl%3Cscript%3Ealert(1)%3C%2Fscript%3E&fieldSet%3AfieldSetMarkup%3AinputFields%3A1%3Acontro
lGroup%3AcontrolGroup_body%3AformField=06-
55556666&fieldSet%3AfieldSetMarkup%3AinputFields%3A2%3AcontrolGroup%3AcontrolGroup_body%3AformField=
06-77778888&bottomRowPanel%3ArightContainer%3ArightButtons%3A1%3Alink=1
```

Response

```
HTTP/2 403 Forbidden
```

```
Date: Tue, 23 Apr 2024 12:32:48 GMT
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Cache-Control: max-age=15
Expires: Tue, 23 Apr 2024 12:33:03 GMT
Server: cloudflare
Cf-Ray: 878de0dbf8d8a006-AMS
```



Afbeelding 4 – Foutmelding

Op basis van dit onderzoek kan worden vastgesteld dat XSS aanvallen worden geblokkeerd. Dit wordt vermoedelijk door een zogenoemde 'Web Application Firewall' (WAF) gedaan. Een WAF helpt webapplicaties te beschermen door HTTP-verkeer tussen een webapplicatie en internet te filteren en detecteert potentiële aanvallen. Om vast te stellen of de applicatie daadwerkelijk door een Web applicatie firewall wordt beveiligd is onderstaande tool gebruikt (WAFW00F). Op basis van onderstaande uitvoer kan worden vastgesteld dat de applicatie hoogstwaarschijnlijk door middel van een CloudFlare WAF wordt beschermd.

```
                    ~ WAFW00F : v2.2.0 ~
      The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://test.inschrijvenmbo.nl
[+] The site https://test.inschrijvenmbo.nl is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```

AANBEVELING	Er zijn geen aanbevelingen gezien de applicatie aan de gestelde richtlijnen voldoet.

5. House cleaning

In dit hoofdstuk worden de zaken beschreven die na de test nog moeten worden aangepast of verwijderd zodat de omgeving weer in originele staat is.

Gebruikers:

Voor het uitvoeren van het onderzoek zijn de volgende testaccounts aangemaakt:

- koen@surelock.nl
- pentest@surelock.nl

Het is aanbevolen om deze test-accounts te verwijderen.