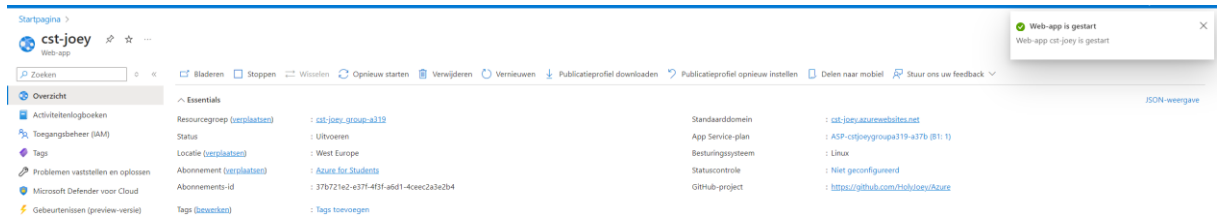


CST2 Practicum Azure Webapp 1

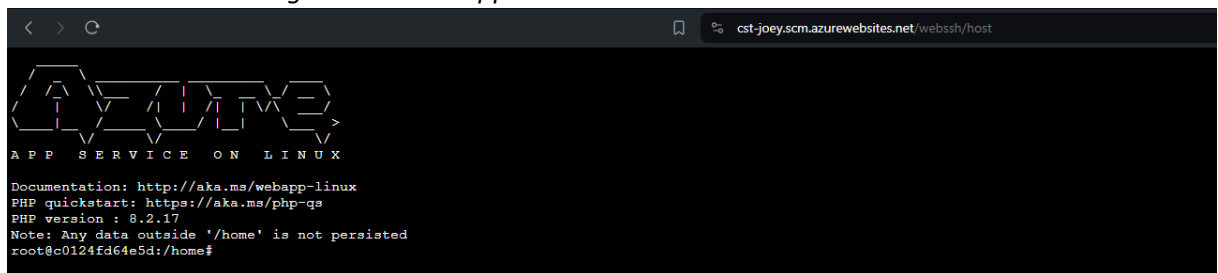
Practicum opdrachten

Maak de volgende opdrachten en beantwoordt de vragen:

1. Start de Azure web app uit het vorige practicum weer en test of deze weer werkt

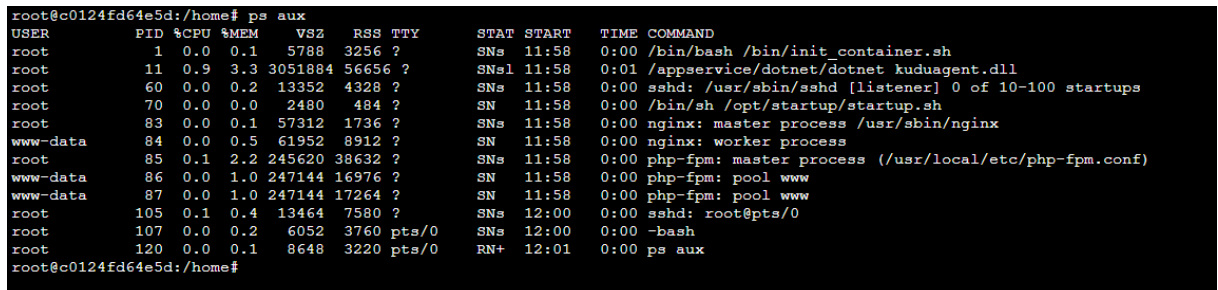


2. Maak een ssh verbinding naar de web app



3. Bekijk de proces list van de Linux container. Welke processen onder welk account draaien er?

Ik heb het commando "ps aux" gebruikt. Hierbij zie ik 3 processen die onder www-data draaien en de rest draait onder root.



4. *Test zowel via ssh als via echo.html (via de browser) of het commando “cat /etc/shadow” en “cat /etc/timezone” werkt. Verklaar ook je antwoord. (Bedenk wat je bij vraag 14 uit het vorige practicum hebt geantwoord)*

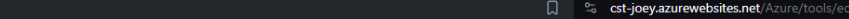
Door het commando “whoami” uit te voeren kan je zien met welk commando je bent ingelogd. Met de SSH verbinding ben je verbonden met het root account.

```
< > ↺
cst-joeyscm.azurewebsites.net/webssh/host
Last login: Tue Apr 30 12:03:52 2024 from 169.254.131.3

APP SERVICE ON LINUX

Documentation: http://aka.ms/webapp-linux
PHP quickstart: https://aka.ms/php-qs
PHP version : 8.2.17
Note: Any data outside '/home' is not persisted
root@c0124fd64e5d:/home# whoami
root
root@c0124fd64e5d:/home#
```

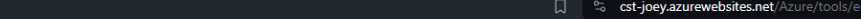
Zodra je echo.php gebruikt, voor je een commando uit via de website. Hier heb ik ook het commando “whoami” uitgevoerd. Hierbij wordt het resultaat gegeven dat je bent ingelogd onder www-data.



The screenshot shows a web browser window with the address bar displaying `cst-joeey.azurewebsites.net/Azure/tools/echo.php`. The main content area is divided into two sections. The top section, labeled "Output of:", contains the text `whoami`. The bottom section, labeled `www-data`, shows the output of the command.

Het 2^e commando: “cat /etc/timezone” kan door iedereen uitgevoerd worden. Dit is te bevestigen door het simpelweg uit te voeren.

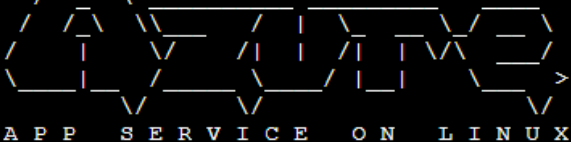
Via `echo.php`:



The screenshot shows a web browser window with the address bar displaying `cst-joeey.azurewebsites.net/Azure/tools/echo.php`. The main content area is divided into two sections. The top section, labeled "Output of:", contains the text `cat /etc/timezone`. The bottom section contains the output `Etc/UTC`.

Met ssh verbinding:

```
Last login: Tue Apr 30 12:04:22 2024 from 169.254.131.3
```

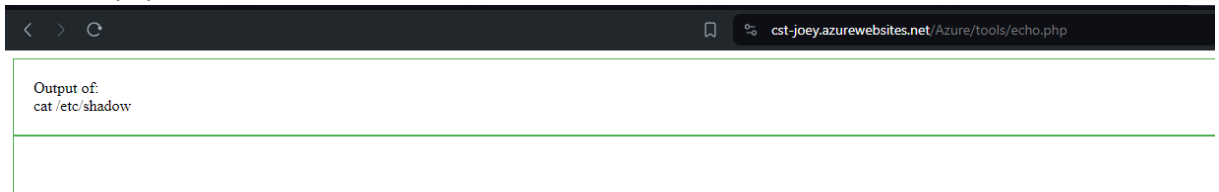


```
A P P   S E R V I C E   O N   L I N U X
```

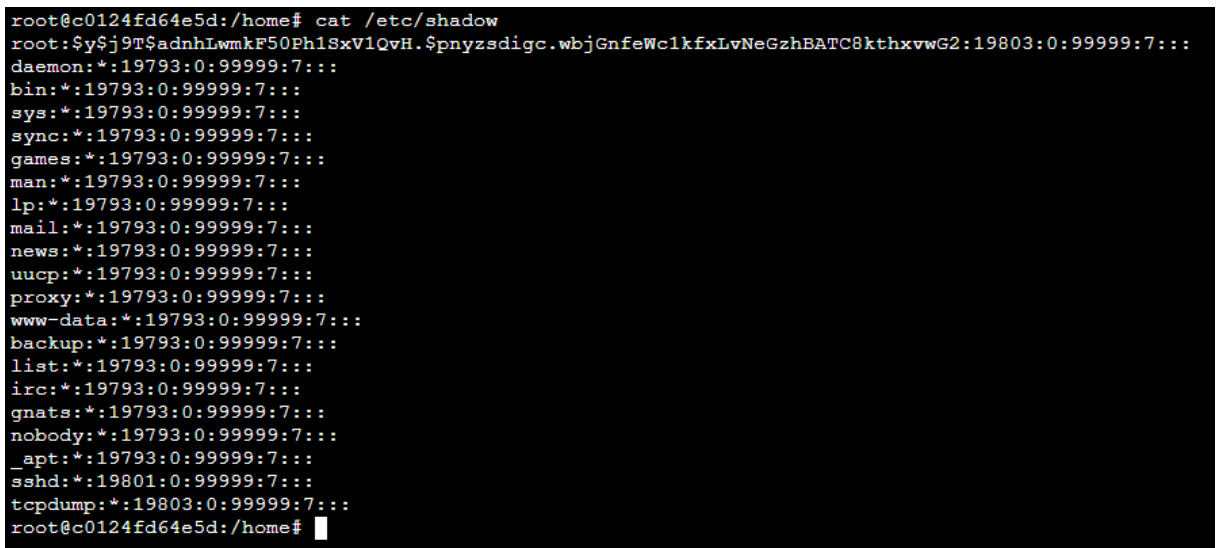
```
Documentation: http://aka.ms/webapp-linux  
PHP quickstart: https://aka.ms/php-qs  
PHP version : 8.2.17  
Note: Any data outside '/home' is not persisted  
root@c0124fd64e5d:/home# cat /etc/timezone  
Etc/UTC  
root@c0124fd64e5d:/home#
```

De file “shadow” kan alleen uitgelezen worden door accounts met root privileges. Het commando “cat /etc/shadow” zal hierdoor niet werken via echo.php, maar zal wel werken via SSH.

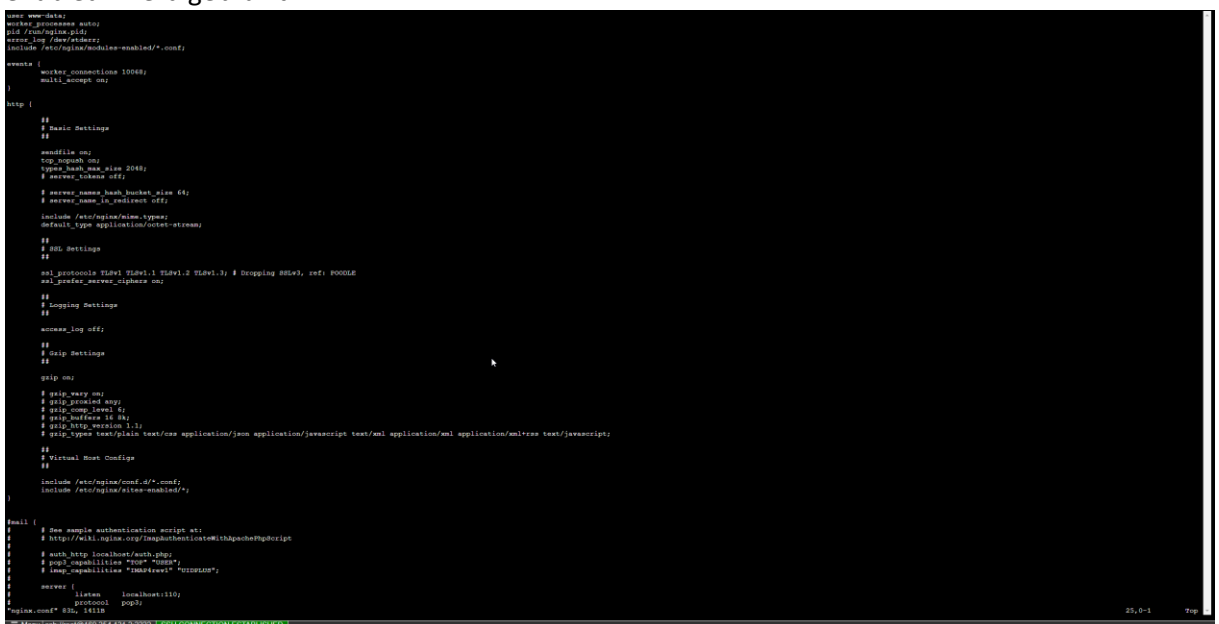
Via echo.php:



Via ssh:



5. Open de nginx configuratie. Welke default pagina’s zijn er ingesteld?
Ik heb /etc/nginx geopend. Hierin stond “nginx.conf”. Na dit uit te lezen zag ik dat “sites-enabled” werd gebruikt.



Ik heb sites-enabled bekeken. Hierin stond een default bestand. Na dit uit te lezen zag ik dat er in /home/site/wwwroot (de directory van de webpagina) wordt gekeken voor “index, index.php, index.html en index.htm”. Dit zijn dan de default pagina’s.

```
root@c0124fd64e5d:/etc/nginx# ls
conf.d fastcgi_params koi-utf koi-win mime.types modules-available modules-enabled nginx.conf proxy_params scgi_params sites-available sites-enabled snippets uwsgi_params win-utf
root@c0124fd64e5d:/etc/nginx# cd sites-enabled
root@c0124fd64e5d:/etc/nginx/sites-enabled# ls
default
root@c0124fd64e5d:/etc/nginx/sites-enabled# cat default
server {
    #proxy_cache cache;
    #proxy_cache_valid 200 1s;
    listen 8080;
    listen [::]:8080;
    root /home/site/wwwroot;
    index index.php index.html index.htm;
    server_name example.com www.example.com;
    port_30_redirect off;

    location / {
        index index.php index.html index.htm hostingstart.html;
    }

    # redirect server error pages to the static page /50x.html
    #
    error_page 500 502 503 504 /50x.html;
    location = /50x.html {
        root /html/;
    }

    # Disable .git directory
    location ~ /\.git {
        deny all;
        access_log off;
        log_not_found off;
    }

    # Add locations of phpmadmin here.
    location ~ ^/\.php(/|$) {
        fastcgi_split_path_info ^(.+?\.php)(?:([/]|\.)*);
        fastcgi_pass 127.0.0.1:9000;
        include fastcgi_params;
        fastcgi_param HTTP_PROXY "";
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
        fastcgi_param PATH_INFO $fastcgi_path_info;
        fastcgi_param QUERY_STRING $query_string;
        fastcgi_intercept_errors on;
        fastcgi_connect_timeout 300;
        fastcgi_send_timeout 3600;
        fastcgi_read_timeout 3600;
        fastcgi_buffer_size 128k;
        fastcgi_buffers 4 256k;
        fastcgi_busy_buffers_size 256k;
        fastcgi_temp_file_write_size 256k;
    }
}
root@c0124fd64e5d:/etc/nginx/sites-enabled#
```

Dit klopt ook aangezien index.php wordt gebruikt als default bij de site. Als ik mijn website zonder of met /index.php in de link zet, krijg ik dezelfde pagina te zien, namelijk de index.php pagina.



6. Zet directory listing aan en toon het resultaat. Deze verandering hoeft niet persistent te zijn. Ik heb via de SSH verbinding met nano /etc/nginx/sites-enabled directory listing toegevoegd. Vervolgens heb ik deze aanpassing doorgevoerd door nginx te herstarten.

```
nginx.conf (show)
#user www-data;
worker_processes auto;
pid /run/nginx.pid;
include /usr/share/nginx/modules/*.conf;

events {
    worker_connections 1024;
}

http {
    # Main configuration of the http module
    include /etc/nginx/mime.types;
    default_type application/octet-stream;

    # Logging
    access_log /var/log/nginx/access.log;
    error_log /var/log/nginx/error.log;

    # Gzip
    gzip on;

    # Virtual Hosts
    include /etc/nginx/sites-enabled/*;
}

# Additional location block for serving files from /home
location /test/ {
    alias /home/;
    autoindex on;
}
```

Index of /azure/

..	24-Apr-2024 16:15	-
bestandenvraag/	26-Apr-2024 14:16	-
tools/		

7. Welke heeft voorrang de default pagina of directory listing?
De default pagina heeft voorrang.
8. Maak een directive met location die verwijst naar een directory buiten de websiteroot
Ik heb in de default file “/test/” toegevoegd als alias voor “/home/”.

```
# Additional location block for serving files from /home
location /test/ {
    alias /home/;
    autoindex on;
}
```

Zodra ik nu deze pagina bezoek, kan ik bestanden zien binnen de home folder, een directory buiten de websiteroot

```
< > cst-joe.azurewebsites.net/test/
```

Index of /test/

..	24-Apr-2024 15:47	-
ASP.NET/	01-May-2024 07:21	-
DeploymentLogStream/	01-May-2024 07:13	-
LogFiles/	30-Apr-2024 14:03	-
data/	26-Apr-2024 14:42	-
site/	24-Apr-2024 16:13	-
uebaf8f4d28215824ad1336/		

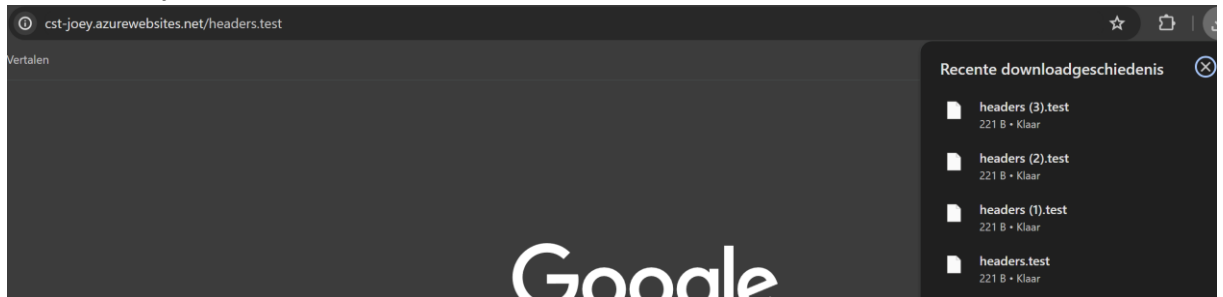
9. *Welke directive zorgt ervoor dat een php op de server wordt uitgevoerd? Wat maakt de configuratie van deze directive bijzonder?*

Dit stuk in de default file zorgt ervoor dat php wordt uitgevoerd op de server. Wat deze configuratie bijzonder maakt, is dat het direct de uitvoering van PHP-scripts mogelijk maakt wanneer de server een verzoek ontvangt voor een bestand met de extensie .php. Dit is een essentieel onderdeel van het hosten van dynamische webpagina's, omdat het de mogelijkheid biedt om PHP-code te verwerken en de gegenereerde HTML terug te sturen naar de webbrowser van de gebruiker.

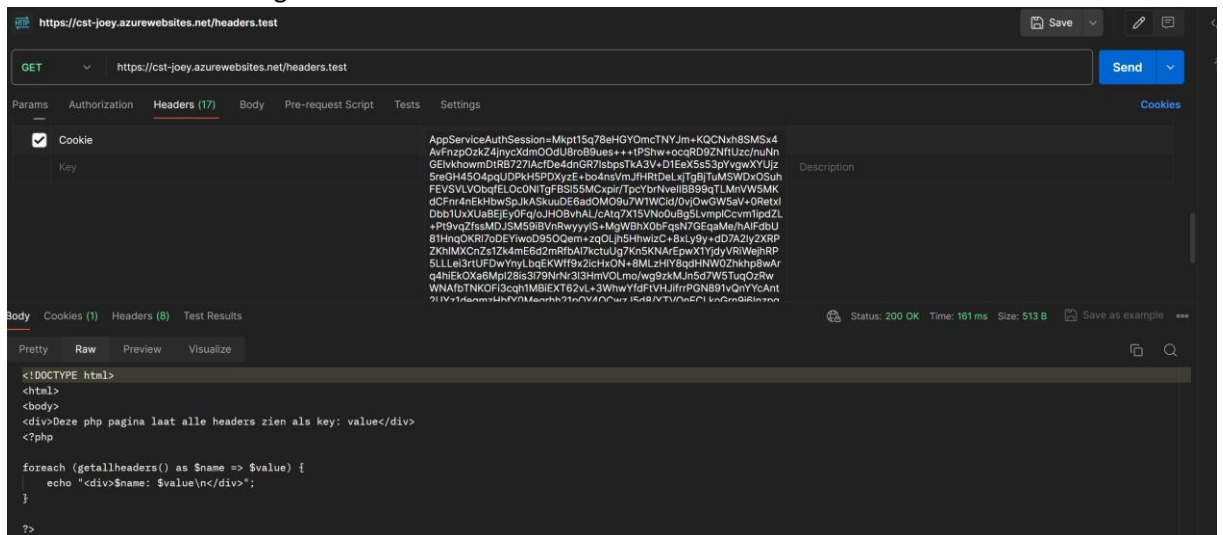
```
# Add locations of phpmyadmin here.
location ~* [^/]\.php(/|$) {
    fastcgi_split_path_info ^(.+?\. [Pp] [Hh] [Pp]) (|/.*)$;
    fastcgi_pass 127.0.0.1:9000;
    include fastcgi_params;
    fastcgi_param HTTP_PROXY "";
    fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
    fastcgi_param PATH_INFO $fastcgi_path_info;
    fastcgi_param QUERY_STRING $query_string;
    fastcgi_intercept_errors on;
    fastcgi_connect_timeout        300;
    fastcgi_send_timeout          3600;
    fastcgi_read_timeout          3600;
    fastcgi_buffer_size 128k;
    fastcgi_buffers 4 256k;
    fastcgi_busy_buffers_size 256k;
    fastcgi_temp_file_write_size 256k;
}
```

10. Verander de bestandsextensie. Wat gebeurt er nu als je een PHP bestand via de browser of Postman opvraagt?

Ik heb "headers.php" aangepast naar "headers.test". Zodra ik dit aanvraag in mijn browser, download mijn browser het bestand.



Zodra ik de pagina opvraag via postman, krijg ik de inhoud van de file te zien. Het php bestand wordt niet uitgevoerd.



11. Voeg via de nginx een Content Security Policy toe. Test of je kan dat er nu voor de hele website de CSP policy is doorgevoerd.

Ik heb via de SSH verbinding met nano /etc/nginx/sites-enabled CSP toegevoegd. Vervolgens heb ik deze aanpassing doorgevoerd door nginx te herstarten.

```
server {
    listen 80;
    listen [::]:80;
    root /var/www/html;
    index index.php index.html index.htm;
    server_name example.com www.example.com;
    port_in_redirect off;

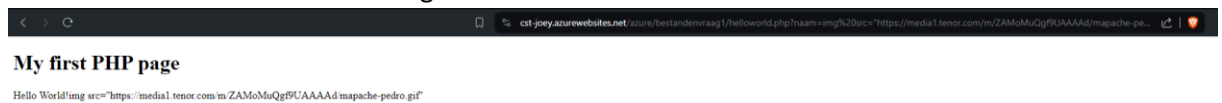
    location / {
        index index.php index.html index.htm;
        autoindex on; # Enable directory browsing
        add_header Content-Security-Policy "default-src 'self'"; # enable CSP
    }

    # Redirect server error pages to the static page /50x.html
    error_page 500 502 503 504 /50x.html;
    location = /50x.html {
        root /var/www/html;
    }

    # Disable .git directory
    location ~ /\.git {
        deny all;
        ssi off;
        log_not_found off;
    }

    # Add locations of phpmyadmin here.
    location ~* ^/(.*)php/(.*)$ {
        fastcgi_pass 127.0.0.1:9000;
        include fastcgi_params;
        fastcgi_param HTTP_PROXY "";
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
        fastcgi_param PATH_INFO $fastcgi_path_info;
        fastcgi_param QUERY_STRING $query_string;
        fastcgi_intercept_errors on;
        fastcgi_connect_timeout 300;
        fastcgi_send_timeout 3600;
        fastcgi_read_timeout 3600;
        fastcgi_buffer_size 128k;
        fastcgi_buffers 8 256k;
        fastcgi_busy_buffers_size 256k;
        fastcgi_max_lio_size 256k;
    }
}
```

Ik zie nu dat een externe afbeelding niet meer inlaad.



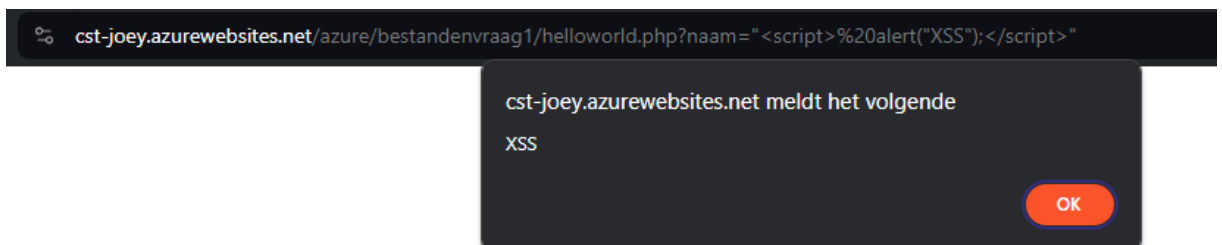
12. Kan je nu nog de XSS kwetsbaarheid uit het vorige practicum demonstreren? De code van php bestanden is niet aangepast.

In het vorige practicum heb ik een externe afbeelding weergegeven. Die werkt zoals bij vraag 11 te zien is niet meer. Echter is er nogsteeds een reflected XSS aanwezig. Alleen nu kan er niet gebruik gemaakt van externe locaties. Het is bijvoorbeeld nogsteeds mogelijk om bold tags te gebruiken of een script alert te genereren.



My first PHP page

Hello World!"test"



Om volledig XSS te stoppen zou in dezelfde config nog een line kunnen worden toegevoegd:
add_header X-XSS-Protection "1; mode=block";

13. Zet authentication aan via de Azure portal. Kies Microsoft als provider en kies de default redirect. Alle verder instellingen kunnen default zijn

[Home](#) > [cst-joeey | Authentication](#) >

Add an identity provider ...

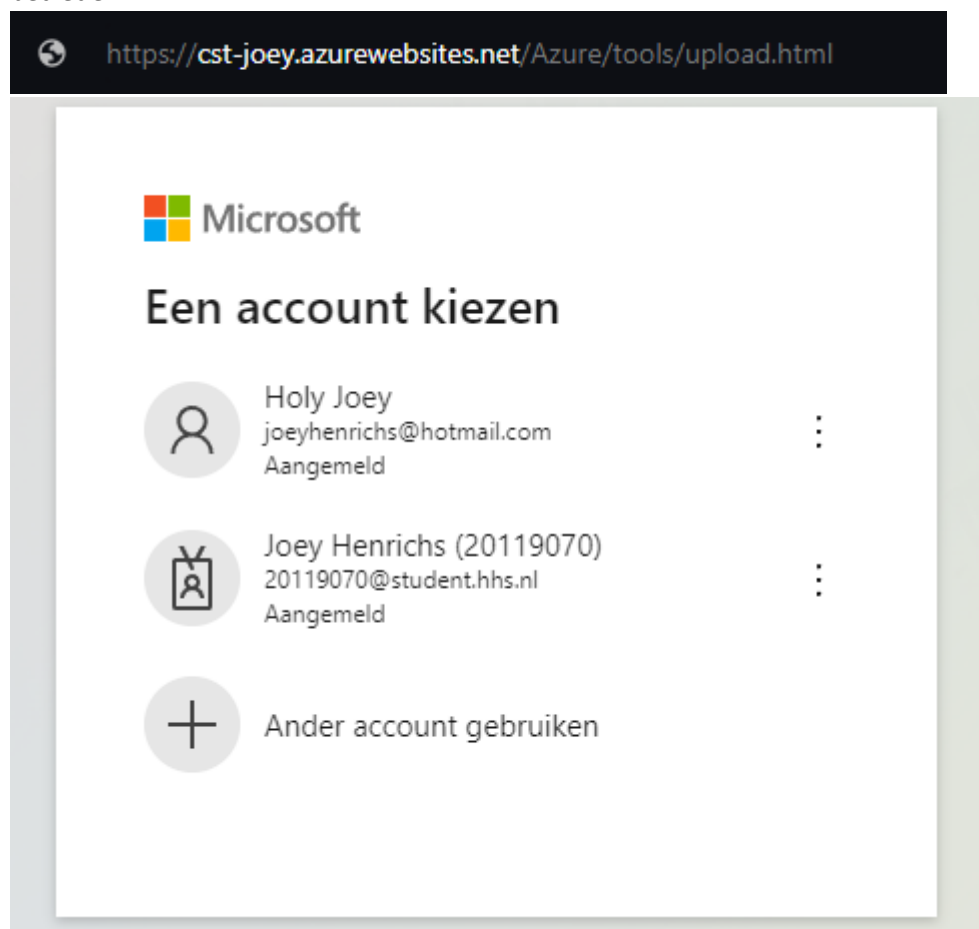
Basics Permissions

Identity provider *

Microsoft

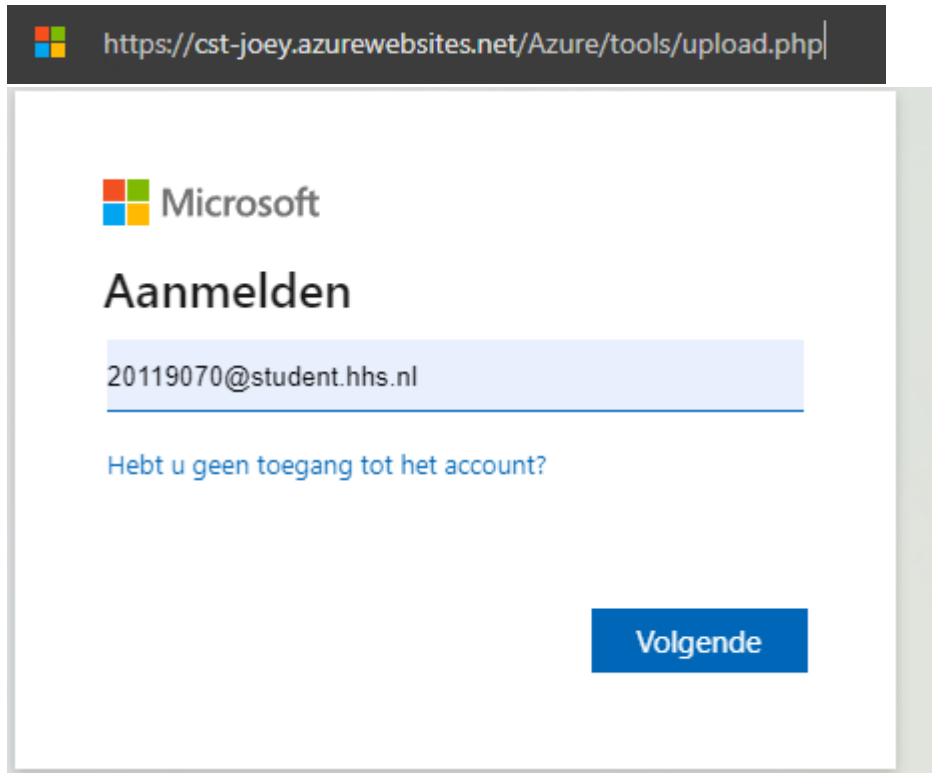
14. Vraag nu een html pagina van de website op via de browser.

Je wordt gevraagd om in te loggen. Pas zodra je bent ingelogd kan je de website verder betreden.



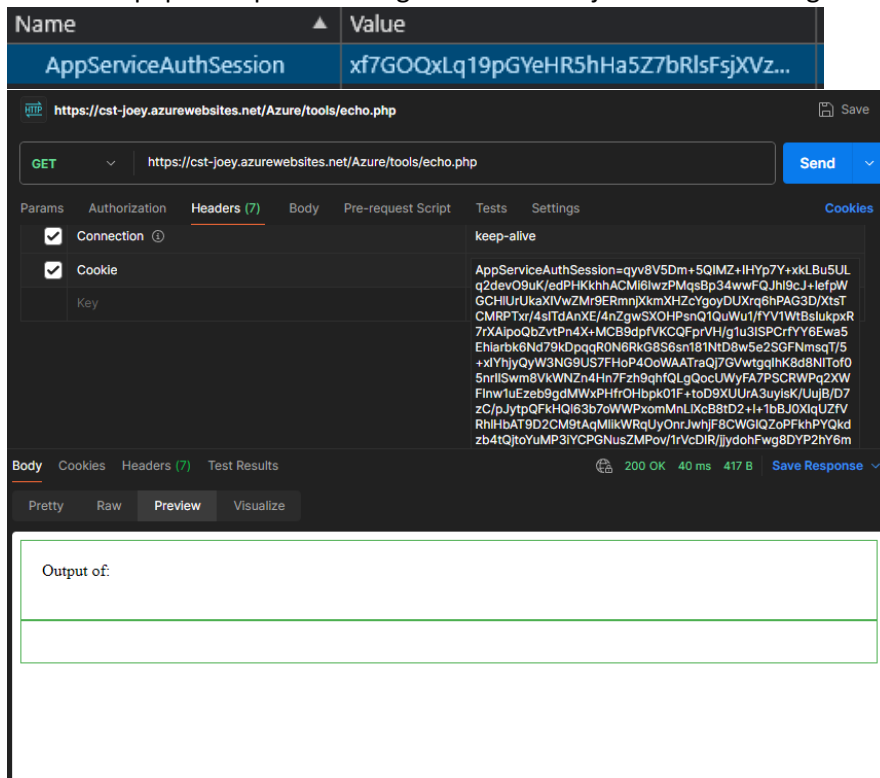
15. Idem voor een php bestand

Er gebeurt exact hetzelfde als bij vraag 14 (het ziet er nu alleen iets anders uit aangezien ik van browsers ben geswitched).



16. Vraag nu echo.php met een commando op via Postman. Wat moet je nu toevoegen in het request?

Om “echo.php” met postman te gebruiken moet je de cookies meegeven.



Name	Value
AppServiceAuthSession	xf7GOQxLq19pGYeHR5hHa5Z7bRIsFsjXVz...

GET https://cst-joeey.azurewebsites.net/Azure/tools/echo.php

Params Authorization Headers (7) Body Pre-request Script Tests Settings Cookies

☒ Connection ☒ Cookie

Key Value

keep-alive

AppServiceAuthSession=qyv8V5Dm+5QIMZ+IHYP7Y+xxkLBu5ULq2devO9uK/edPHKkhhACMI6lwzPMqs8p34wwFQJhI9cJ+lefpWGCIIUrUkaXIVwZMr9ERmnjXkmXHZcYgoyDUXrq6hPAG3D/XtsTCMRP Txr/4sITdAnXE/4nZgwSXOHPsnQ1QuWu1/fYV1WtBslukpxR7rXAlpoQbZvtPh4X+MCB9dpfVKCQFprVH/g1u3ISPCrfYY6Ewa5Ehlarbk6Nd79kDppqR0N6RkG8S6sn181ND8w5e2SGFNmsqT/5+xlYhjyQyW3NG9US7FH0P4OoAAATraQJ7GVwtgqlhK8d8NITof05nrlISwm8VkvWNZn4Hn7Fzh9qhtQLgQocUWyFA7PSCRWPq2XWFlnw1uEzeb9gdMWxPHfrOHbpk01F+toD9XUUIrA3uyisK/UujB/D7zC/pJytpQFkHQI63b7oWWPxmMnLXcB8tD2+1+1bBJ0XlqUZfVRhHbAT9D2CM9taqMlikWRqUyOnrJwhjF8CWGIQZoPFknPYQkdzb4tQtoYuMP3IYCPGNusZMPov1rVcDIR/jjydoHFWg8DY2hY6m

Body Cookies Headers (7) Test Results

200 OK 40 ms 417 B Save Response

Pretty Raw Preview Visualize

Output of:

17. Wat heb je nu aan dit aanzetten van authenticatie? Is er nu toegang voor een beperkt aantal gebruikers. NB Kan een medestudent nu nog bij jouw website?

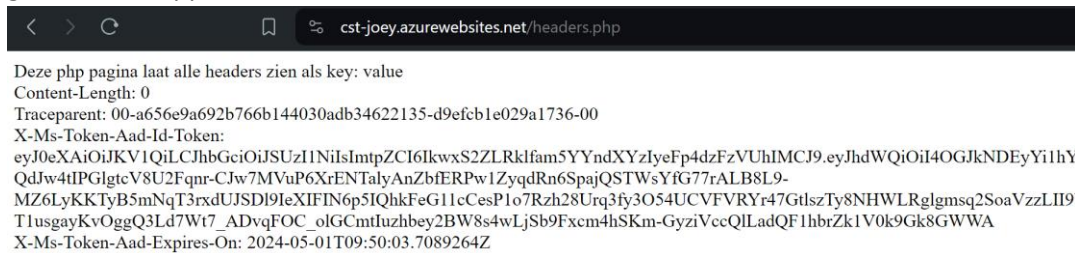
Zodra ik met een ander account inlog op de pagina krijg ik hetvolgende te zien:



Je moet nu toegevoegd zijn aan de resource in Azure met je microsoft account om bij de website te komen. Een medestudent of een wild vreemde kan zo niet zomaar bij mijn website.

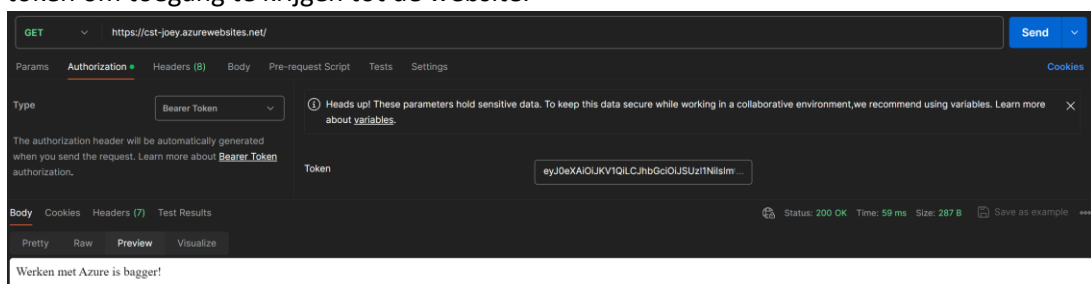
18. Deploy nu het bestand headers.php. Welke interessant header kan de PHP applicatie nu gebruiken voor de autorisatie?

De header "X-Ms-Token-Aad-Id-Token" kan worden gebruikt voor authenticatie. Deze header bevat een Azure Active Directory (AAD) acces token, die kan worden gebruikt om een gebruiker of applicatie te verifiëren.



19. Kan je via Postman deze header aanpassen als hacker?

Je kan de waarde van de token gebruiken onder de authorization pagina met het type bearer token om toegang te krijgen tot de website.



20. Vraag de volgende pagina op < domein >/.auth/me

