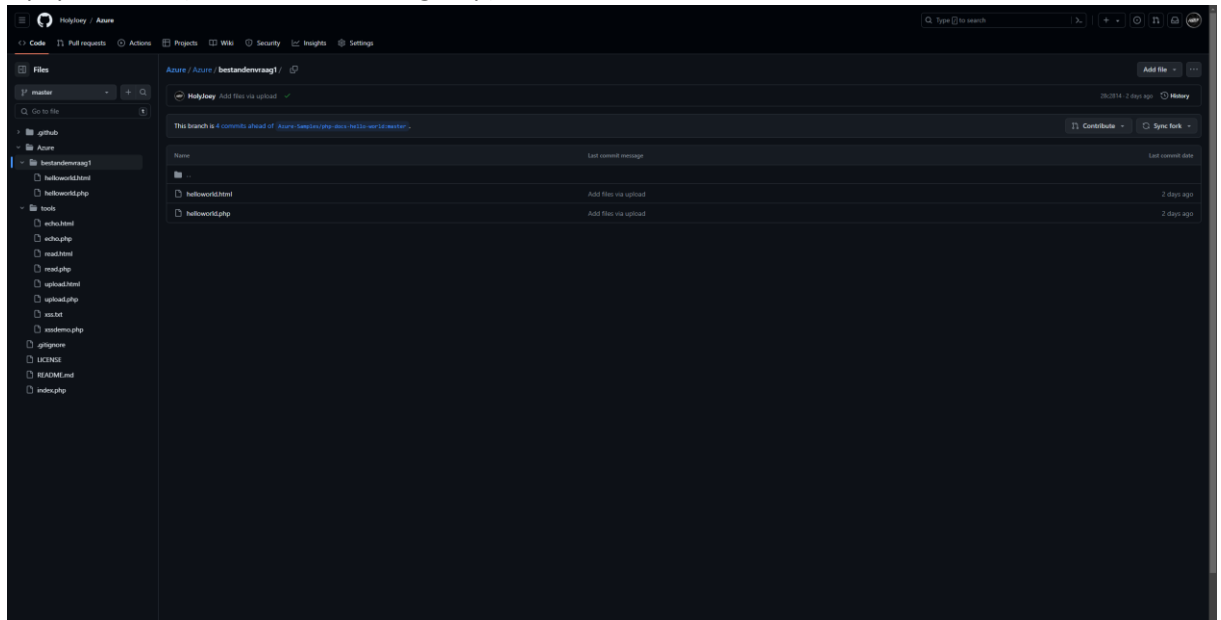


CST2 Practicum Azure Webapp 1

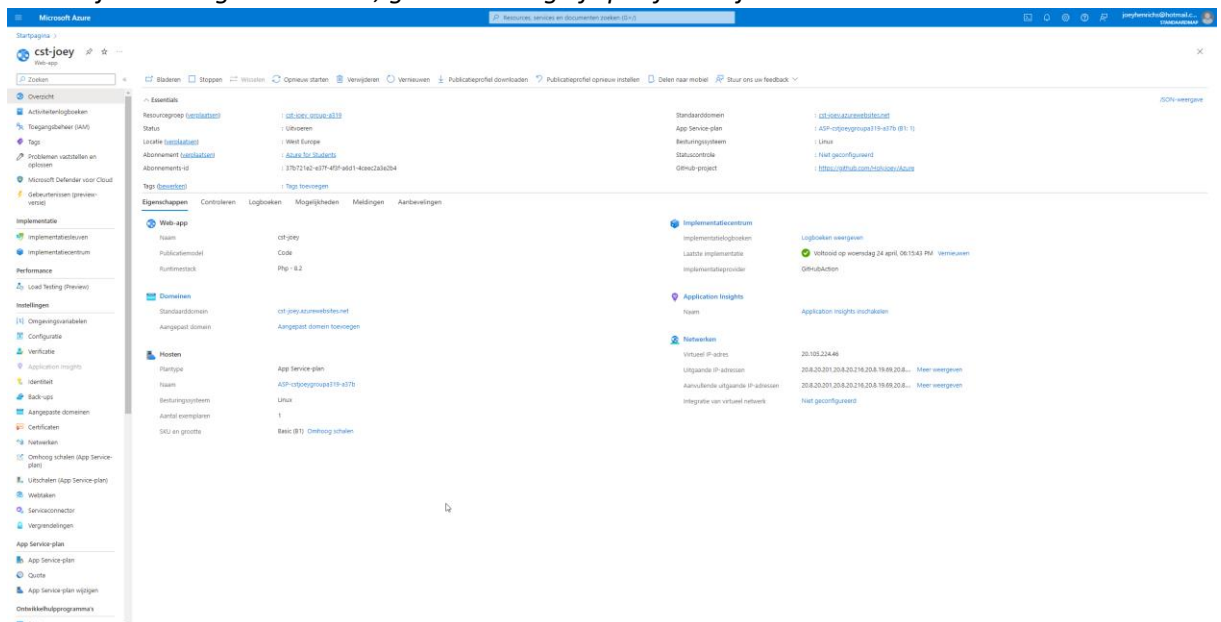
Practicum opdrachten

Maak de volgende opdrachten en beantwoordt de vragen:

1. *Maak een directory met daarin de bestanden van BrightSpace. Hierin staat 1 html bestand en 1 php bestand (webbestandenvraag1.zip)*










2. *Deploy volgens stap 2 uit de quickstart handleiding. Geef optioneel de website een eigen naam en geef een locatie op. NB: er kan maar 1 website in de Free Tier aangemaakt worden. Dus als je deze al gebruikt hebt, gooi deze weg of specificeer bijvoorbeeld –sku=B1*



3. *Test de website. NB: doet de website wat je verwacht?*

De website start de “index.php” pagina. Dit was inderdaad te verwachten aangezien deze in de root van de directory website directory staat. Deze wordt aangeroepen zodra je de website opent.

4. *Controleer de lokale directory of hier nog bestanden zijn aangemaakt. Zoja beschrijf deze*
Ik zie de Azure map die ik heb gemaakt met de bestanden van brightspace erin. Verder is er naast de index.php ook een gitnore, license en readme aangemaakt.

 HolyJoey Add files via upload ✓	28c2814 · 2 days ago	🕒 14 Commits
 .github/workflows	Add or update the Azure App Service build and deployment ...	2 days ago
 Azure	Add files via upload	2 days ago
 .gitignore	Initial commit	7 years ago
 LICENSE	Initial commit	7 years ago
 README.md	Update README.md	5 years ago
 index.php	Yippie	2 days ago

5. *Check op de Azure portal welke resources er aangemaakt en beschrijf deze*
Er is een web applicatie, een resourcegroep en een identiteit aangemaakt.

Microsoft Azure

Startpagina > **cst-joeyp_group-a319** Resourcegroep

Essentials

Abonnement [\(verplaatsen\)](#) : Azure for Students

Abonnement-id : 37b72162-437f-4b3f-a6d1-4ccc2a3e2b4

Implementaties : 1 [Geflaagd](#)

Locatie : West Europe

Tags [\(beveelken\)](#) : [Tags toevoegen](#)

Resources Aanbevelingen

Filteren op elk veld... Type is gelijk aan **alles** X Locatie is gelijk aan **alles** X Filter toevoegen

1 t/m 3 van 3 records weergeven. ☐ Verborgen typen weergeven

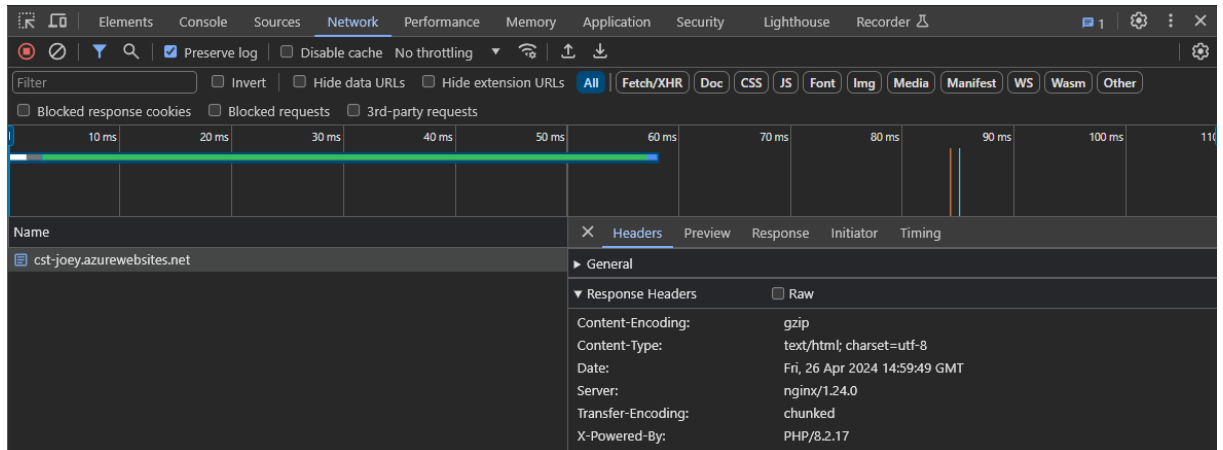
Naam ↑↓	Type ↑↓	Locatie ↑↓
<input type="checkbox"/> AGP-cstjoeypgroupa319-a37b	App Service-plan	West Europe
<input type="checkbox"/> cst-joeyp	App Service	West Europe
<input type="checkbox"/> cst-joeyp-id-8d28	Beheerde identiteit	West Europe

< Vorige Pagina 1 van 1 Volgende >

Feedback geven

6. Als gebruiker/hacker welke informatie kan ik achterhalen over deze website? (In het kader van reconnaissance)

Vanuit de DNS kan je al zien dat de website draait op azure. Via de netwerk tab in de browser is te zien waarop de webserver draait, in dit geval nginx versie 1.24.0 en dat er PHP versie 8.2.17 draait.



Je kan de website pingen om achter het IP adres te komen. Hiermee kan je informatie verkrijgen over de provider.

```
C:\Users\joeyh>ping cst-joeey.azurewebsites.net

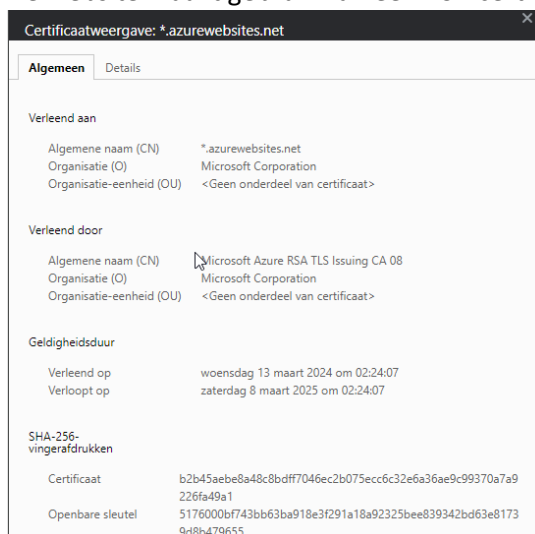
Pinging waws-prod-am2-751-e167.westeurope.cloudapp.azure.com [20.105.224.46] with 32 bytes of data:
Reply from 20.105.224.46: bytes=32 time=26ms TTL=117
Reply from 20.105.224.46: bytes=32 time=25ms TTL=117
Reply from 20.105.224.46: bytes=32 time=26ms TTL=117
Reply from 20.105.224.46: bytes=32 time=25ms TTL=117

Ping statistics for 20.105.224.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 25ms, Maximum = 26ms, Average = 25ms

C:\Users\joeyh>
```

7. Welke TLS certificaat gebruikt de website?

De website maakt gebruik van een RSA certificaat van Microsoft Azure.



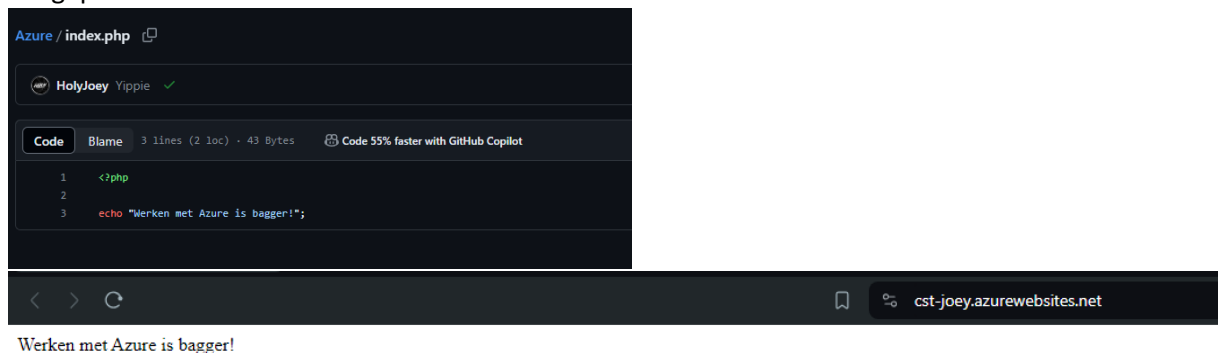
8. Kan je de website ook openen via http? (gebruik de netwerk tab van de browser om te checken wat er gebeurt)

De website kan alleen bezocht worden via HTTPS. Zodra je gebruik probeert te maken van HTTP, wordt je automatisch doorverwezen naar de HTTPS pagina.

Name	Status	Type	Initiator	Size	Time
cst-joeey.azurewebsites.net	200	document	cst-joeey.azurewebsites.net/	254 B	281 ms
cst-joeey.azurewebsites.net	200	document / Redirect	Other	0 B	Pending

9. Pas 1 bestand lokaal aan en voeg 1 bestand lokaal toe en redeploy volgens de handleiding. Test het resultaat

Ik heb de index.php aangepast in mijn github omgeving. Azure ziet deze verandering en redeployt dan automatisch. Zodra ik mijn website bezoek zie ik dat de index inderdaad is aangepast.



10. Kan een medestudent (of iemand anders) ook code deployen als hij de beschikking heeft over de informatie uit vraag 4? Zoja hoe? Zonee waarom niet?

Een ander persoon kan niet bij mijn azure omgeving waardoor deze hier geen aanpassingen kan doen. Aangezien ik gebruik maak van een github repo die gelinked staat aan mijn azure, kan hier wel gebruik van gemaakt worden. Dan moet diegene wel toegang hebben tot deze repo. Zodra iemand geen rechten heeft, kan diegene er niet bij. Zodra diegene wel rechten heeft, kan deze aanpassingen doen.

11. Deploy de bestanden van BrightSpace die in tools.zip staan. Deze zip bevat meer php code.

Wie is verantwoordelijk om deze code te testen op security

Deze bestanden heb ik bij vraag 1 al gelijk in 1 keer toegevoegd en gedeployed. Azure is een PaaS. Bij een PaaS moet je dan zelf de Applications managen. Deze code valt dan onder het stukje Applications. Je bent zelf verantwoordelijk om deze code te testen

12. Demonstreer zowel een reflected XSS mbv van de code uit de vorige vraag

In de php code is te zien dat er een naam opgevraagd wordt, "Hello World!" wordt geprint en de variabele naam wordt geprint. Zodra je in de URL de naam meegeeft, wordt deze vertoond. Door

"?naam=<img%20src=https://www.alimentarium.org/sites/default/files/media/image/2017-02/AL027-01_pomme_de_terre_0_0.jpg">" als url parameter mee te geven, krijgt naam de inhoud van een afbeelding van een aardappel en wordt deze later vertoond.


Azure / Azure / bestandenvraag1 / helloworld.php

HolyJoey Add files via upload ✓

Code Blame 14 lines (13 loc) · 164 Bytes Code 55% faster with GitHub Copilot

```
1 <!DOCTYPE html>
2 <html>
3 <body>
4
5 <h1>My first PHP page</h1>
6 <div>
7 <?php
8 $naam= $_GET["naam"];
9 echo "Hello World!";
10 echo $naam;
11 ?>
12 </div>
13 </body>
14 </html>
```

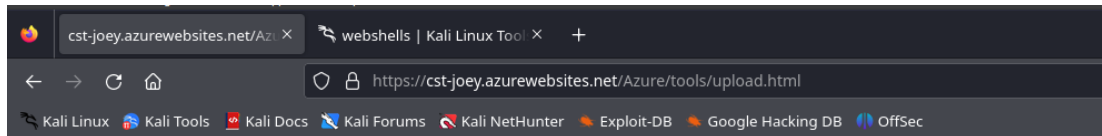
My first PHP page



Hello World

13. Idem voor een stored XSS

Bij de upload.html pagina heb ik een shell ingevoegd. Deze heb ik de naam "shell.php" gegeven als destination file name.

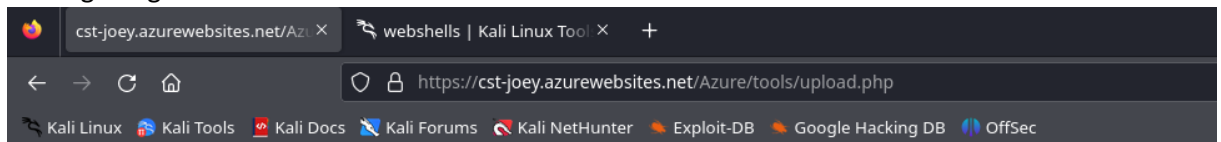


Upload image

Select image to upload: shell.php

Destination File Name:

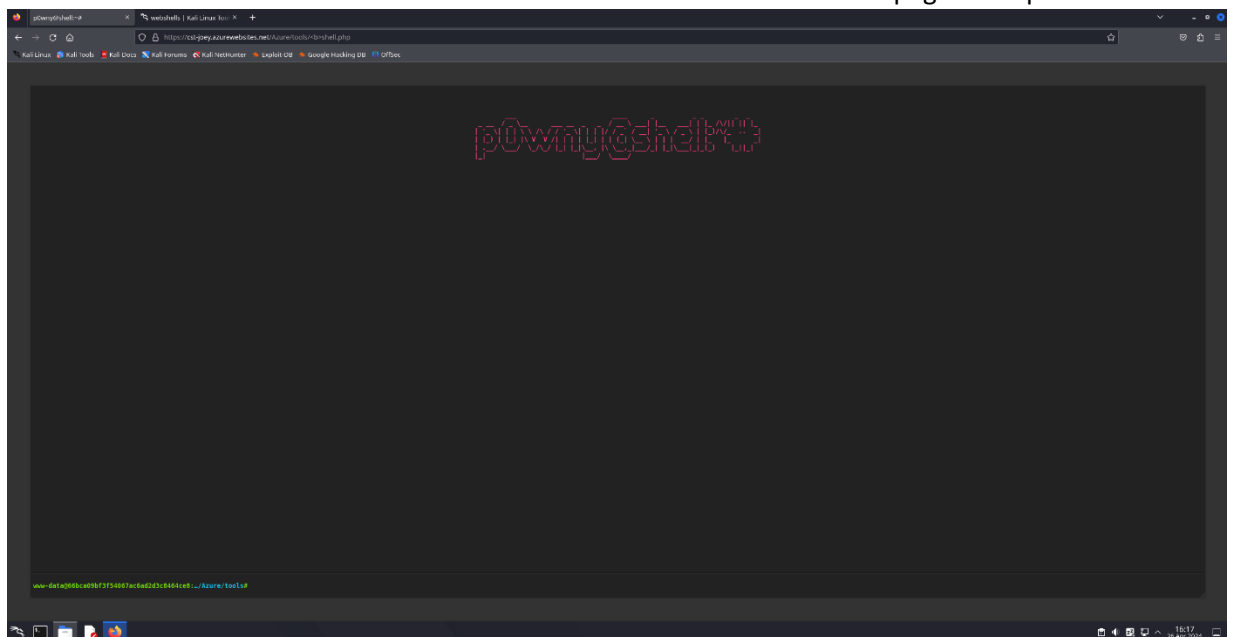
Na op upload te drukken is te zien dat "shell.php" is geüpload. Deze heeft een dikgedrukte naam gekregen door "".



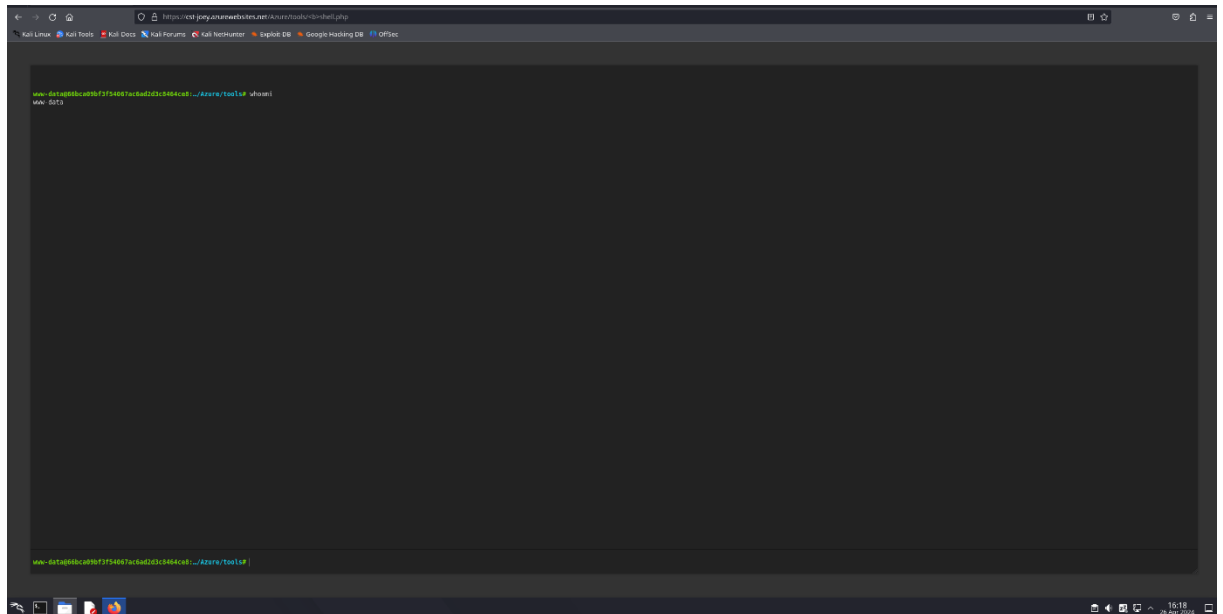
Upload file

The file shell.php has been uploaded as: **shell.php** ;

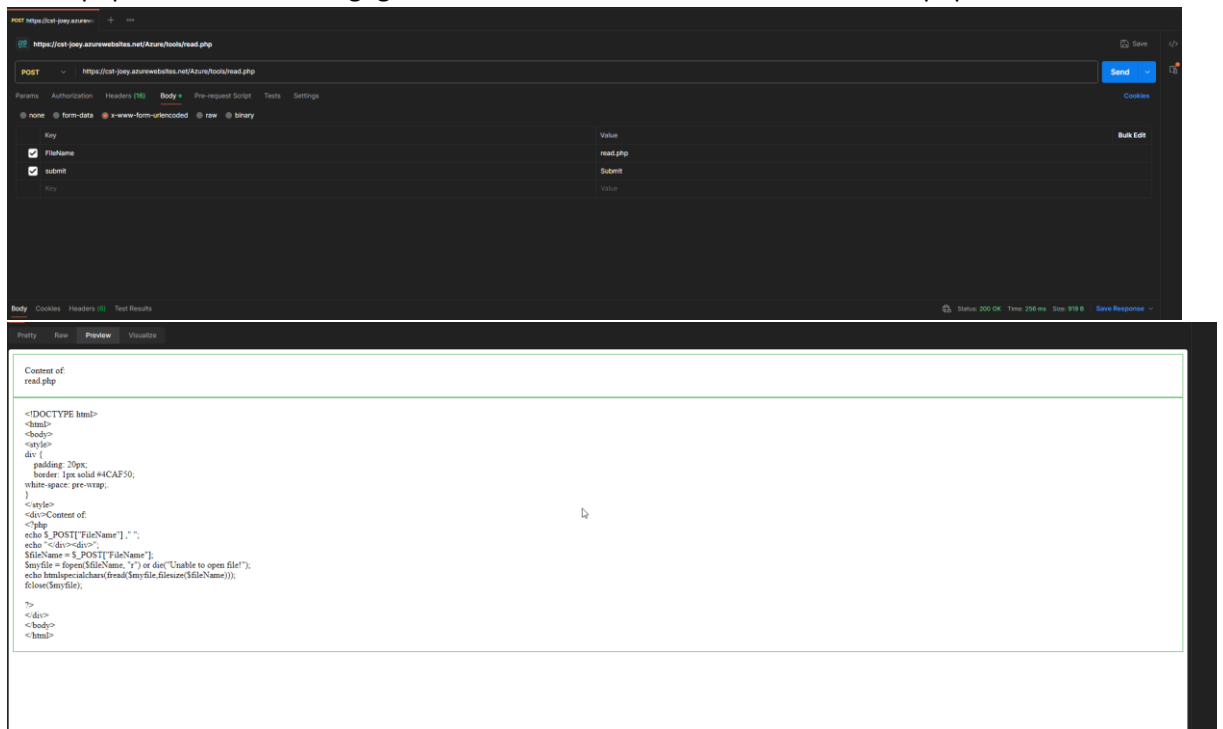
Deze shell kan gebruikt worden via de url: <https://cst-joeey.azurewebsites.net/Azure/tools/%3Cb%3Eshell.php>. De shell is opgeslagen in de server waardoor het stored XSS is. Iedereen kan hierdoor deze shell zien door de pagina te openen.



14. Laat zien dat je een commando naar keuze op de webserver kan laten uitvoeren? Onder welke account wordt dit commando uitgevoerd? (Hint hiervoor is een Linux commando)
- Ik heb het linux commando "whoami" uitgevoerd in de shell. De output geeft weer dat ik op het account "www-data" zit.

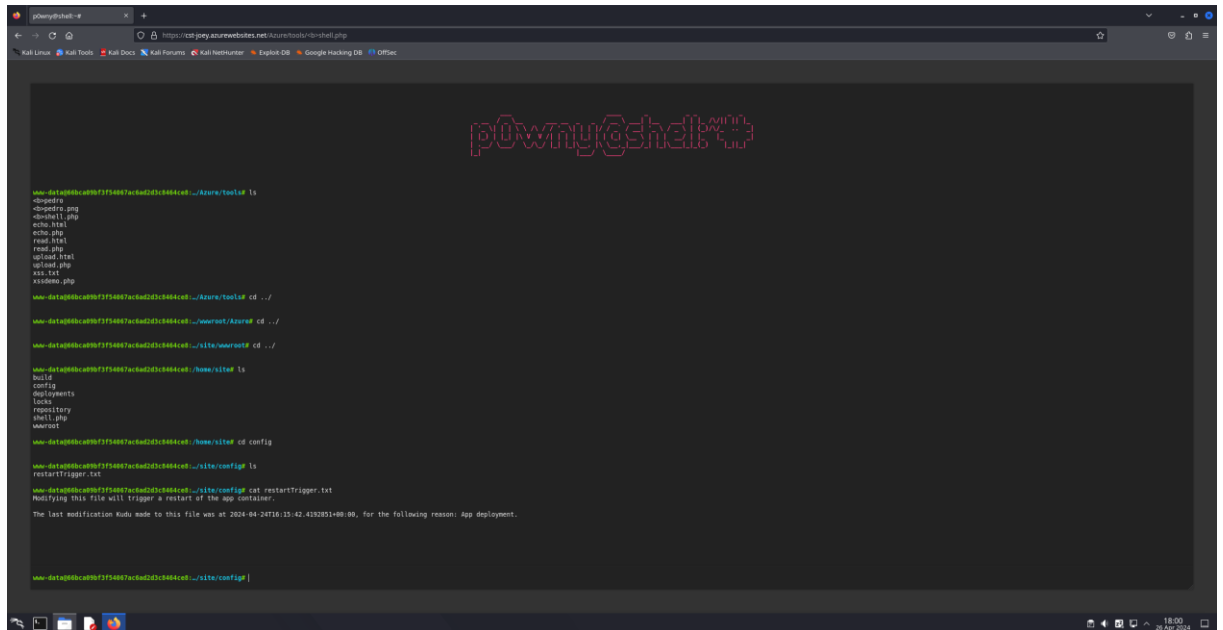


15. Laat zien dat je de broncode van een php kan tonen (als normale gebruiker met de browser)
- Je kunt het read.html en read.php bestand gebruiken om de broncode van bestanden te tonen. De read.html voert een post request uit read.php. Deze post request heb ik "read.php" als filename meegegeven. Hierdoor wordt de broncode van read.php vertoond.



16. Laat zien dat je de inhoud van een bestand buiten de webroot kan tonen (als normale gebruiker met de browser)

Ik heb de shell pagina opnieuw geopend om te vinden in welke directory upload.php staat en waar de webroot zich bevindt.



```
p0wny@shell:~$ cd /opt/joey.azurewebsites.net/AzureTools/bin/shell.php
www-data@80bc0907f5407ac6d2d3b04ced:/AzureTools$ ls
bindeploy.php
binshell.php
binhttp
binread.php
binupload.php
binwrite.php
binwrite.php

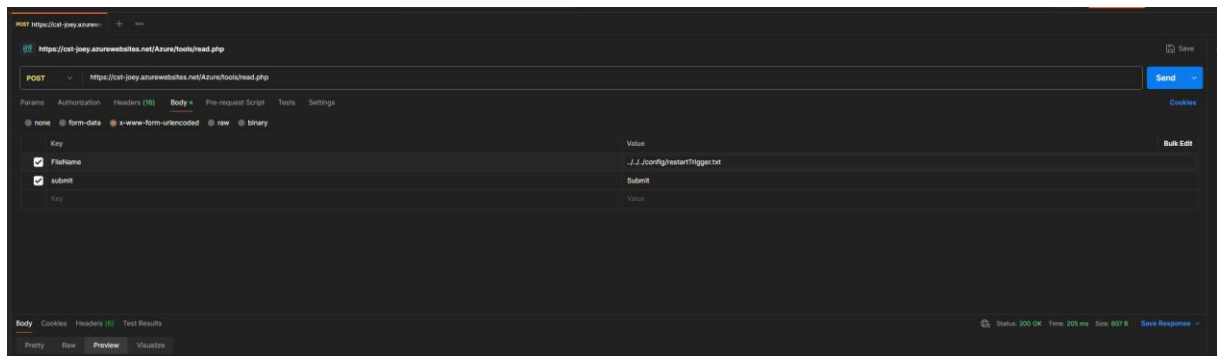
www-data@80bc0907f5407ac6d2d3b04ced:/AzureTools$ cd ../
www-data@80bc0907f5407ac6d2d3b04ced:/wwwroot/AzureTools$ cd ../
www-data@80bc0907f5407ac6d2d3b04ced:/site/wwwroot$ cd ../
www-data@80bc0907f5407ac6d2d3b04ced:/home/site$ ls
config
deployments
logs
repository
shell.php
wwwroot

www-data@80bc0907f5407ac6d2d3b04ced:/home/site$ cd config
www-data@80bc0907f5407ac6d2d3b04ced:/site/config$ ls
restartTrigger.txt

www-data@80bc0907f5407ac6d2d3b04ced:/site/config$ cat restartTrigger.txt
Modifying this file will trigger a restart of the app container.
The last modification kudu made to this file was at 2024-04-24T16:15:42.4192851+00:00, for the following reason: App deployment.

www-data@80bc0907f5407ac6d2d3b04ced:/site/config$
```

Hierdoor weet ik dat ik 3 directories terug moet om uit de webroot te komen. Vervolgens heb ik de directory config gevonden met het bestand “restartTrigger.txt” erin. Ik heb de filename aangepast naar “../../././config/restartTrigger.txt”. Hierdoor wordt het txt bestand in de config map aangegeven. Deze was uit te lezen.



POST https://cat-j0ey.azurewebsites.net/AzureTools/head.php

Key	Value
Filename	../../././config/restartTrigger.txt
submit	Submit

Content of: ../../././config/restartTrigger.txt

Modifying this file will trigger a restart of the app container.

The last modification Kudu made to this file was at 2024-04-24T16:15:42.4192851+00:00, for the following reason: App deployment.

17. Laat zien dat je een bestand kan uploaden naar de website (als normale gebruiker met de browser)

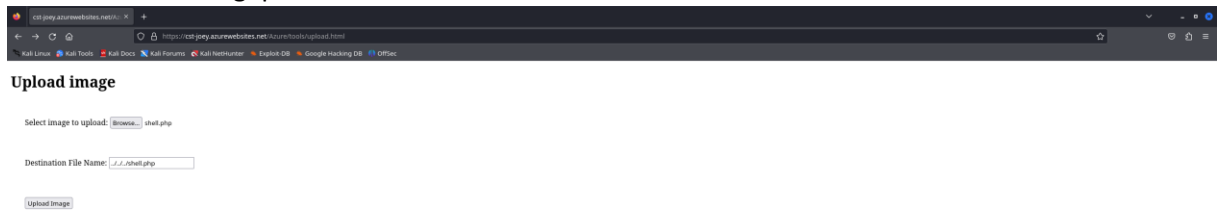
Bij vraag 13 heb ik al een bestand geupload.

18. Kan je ook een php bestand uploaden?

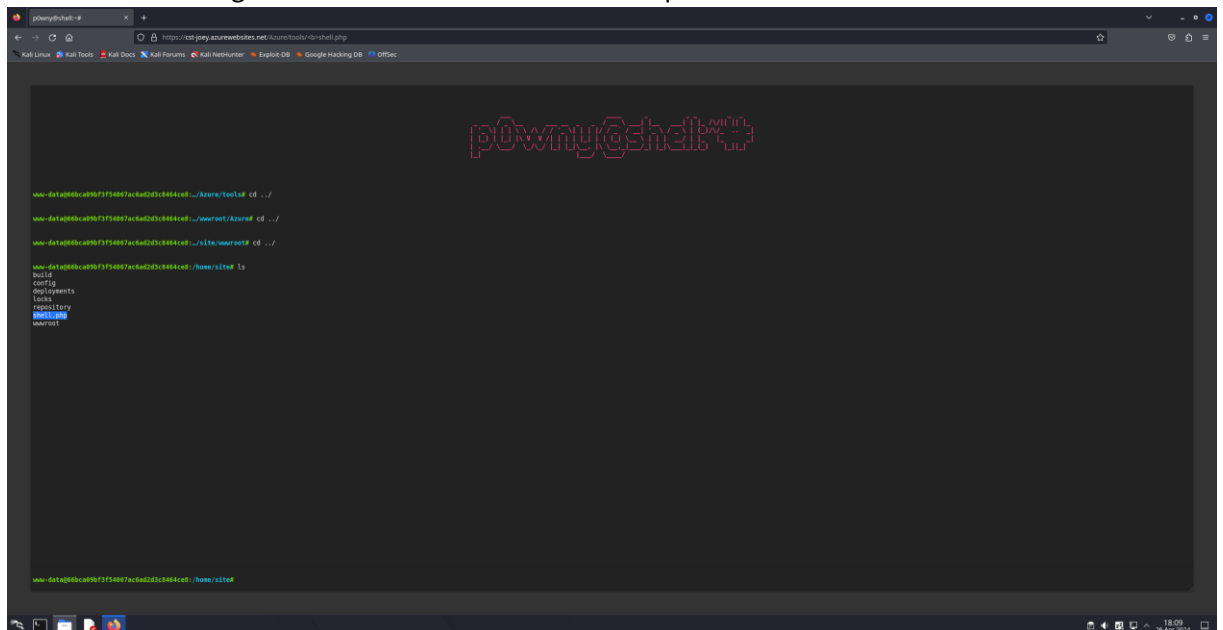
Ja dit kan. Dit heb ik namelijk bij vraag 13 gedaan.

19. Kan je ook een bestand buiten de webroot uploaden? Hint: directory traversal

Door de destination file name aan te passen met ".././../" ervoor, wordt deze in de map boven de webroot geplaatst.



Dit heb ik bevestigd door mijn shell te openen, naar deze directory te browsen en de bestanden te weergeven. De shell is te vinden in de map boven de webroot.



20. *Wat gebeurt er met bestanden die je in de website hebt toegevoegd bij vraag 17 en 18, als je redeployed. Idem voor een bestand dat wel lokaal staat maar via de manier van vraag 17 of 18 hebt aangepast?*

De bestanden die zijn toegevoegd blijven staan. Hetzelfde geldt voor een bestand dat lokaal staat maar is aangepast.

21. *Gooi de website nog niet weg, maar stop deze. Test of de website inderdaad gestopt is. Dit kost ook minder credits als je een betaalde versie gebruikt.*

Gedaan.