Su-zen Geurts

PXL | Elfde-linie, Hasselt

**Red Team**

DOCUMENTATIE

Inhoudsopgave

[Rooms 2](#_Toc131191318)

[PXL Platformer 3](#_Toc131191319)

[Tijd 3](#_Toc131191320)

[Antwoorden 3](#_Toc131191321)

[Taak 1: Introductie 3](#_Toc131191322)

[Taak 2: Cetus 3](#_Toc131191323)

[Taak 1: Introduction 4](#_Toc131191324)

[I have got my docker container running 4](#_Toc131191325)

[I have tried the platform game 4](#_Toc131191326)

[Taak 2: Cetus 5](#_Toc131191327)

[Look up information on Cetus and how to use it 5](#_Toc131191328)

[Empathetic Flag 6](#_Toc131191329)

[Multi-disciplinary Flag 10](#_Toc131191330)

[Internation Flag 11](#_Toc131191331)

[Room: 13](#_Toc131191332)

[Taak 1: 13](#_Toc131191333)

[Koptekst 3 13](#_Toc131191334)

# Rooms

|  |  |  |
| --- | --- | --- |
| Done | Room | Tijd |
| X | PXL Platformer | 01h 00min 00sec |
| X | The Docker Rodeo | 01h 57min 00sec |
| X | Microsoft Windows Hardening | 01h 36min 00sec |
| X | PrintNightMare | 01h 07min 00sec |
|  | AV Evasion: Shellcode |  |

# PXL Platformer

## Tijd

|  |  |
| --- | --- |
| Taak | Duur |
| Taak 1 | 00h 06min |
| Taak 2 | 00h 54min |
| TOTAAL | 01h 00min |

## Antwoorden

### Taak 1: Introductie

|  |
| --- |
| I have got my docker container running |
| Geen antwoord nodig |

|  |
| --- |
| I have tried the platform game |
| Geen antwoord nodig |

### Taak 2: Cetus

|  |
| --- |
| Look up information on Cetus and how to use it |
| Geen antwoord nodig |

|  |
| --- |
| Empathetic Flag |
| PXL{empPAssie\_voor\_SEC} |

|  |
| --- |
| Multi-disciplinary Flag |
| PXL{MULTIMULTIMULTI} |

|  |
| --- |
| Internation Flag |
| PXL{OP\_rEIS\_voorXFactor} |

## Taak 1: Introduction

### I have got my docker container running

1. Repo [pxl-platformer-Su-zenGeurtsPXL](https://github.com/PXL-SecurityAdvanced2223/pxl-platformer-Su-zenGeurtsPXL) gekloond.  
   A screenshot of a computer

   Description automatically generated with medium confidence
2. Commando ***docker-compose up*** ingevoerd in de terminal.  
   Graphical user interface, website

   Description automatically generated
3. Alle bestanden globaal overlopen.

### I have tried the platform game

1. Dimanten verzameld.
2. Zevende, de laatste, diamant is nergens te vinden.

## Taak 2: Cetus

### Look up information on Cetus and how to use it

Ik deed een Google search “Cetus” 🡪 nutteloos  
A screenshot of a computer

Description automatically generated with medium confidence

Google search: cetus browser extension 🡪 Eerste link lijkt nuttig want gaat over hacken  
A screenshot of a computer

Description automatically generated

Repo [Qwokka/Cetus](https://github.com/Qwokka/Cetus) README bekeken. De extensie volgens de instructies van de README gevolgd 🡪 Repo gekloond.

Google chrome: extensie toegevoegd zoals volgende instructies [link]

1. Extensies in Chrome geopend(Menu > Meer hulpprogramma’s > Extensies).
2. Ontwikkelaarmodus ingeschakeld (rechtsboven).
3. Geklikt op “Uitgepakte extensies laden”.
4. Map van de repo uitgekozen

A screenshot of a computer

Description automatically generated with medium confidence

Bij het inspecteren staat nu ook de optie “Cetus”.  
Graphical user interface, application, Teams

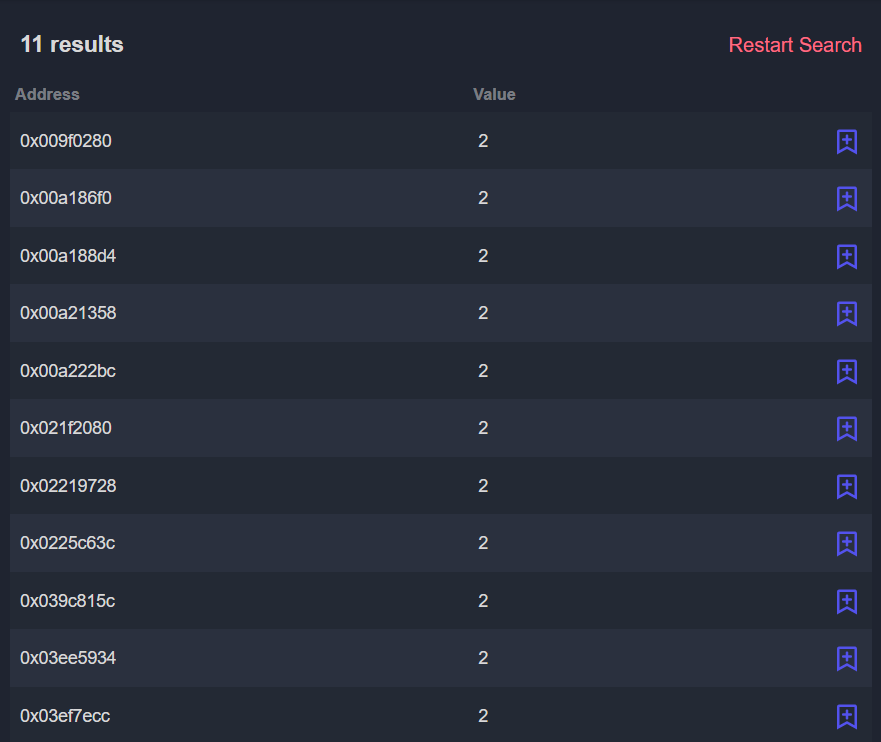
Description automatically generated

### Empathetic Flag

Ik las de [Guide](https://media.defcon.org/DEF%20CON%2027/DEF%20CON%2027%20presentations/DEFCON-27-Jack-Baker-Hacking-Web-Assembly-Games.pdf) in de README maar de informatie was te globaal. De [Tutorial](https://www.youtube.com/watch?v=V8UkCsPzbhQ) en [documentatie](https://github.com/Qwokka/Cetus/wiki/Cetus-101---Invincibility) in de README was wel zeer handig om mij op weg te helpen. Zoals getoond in de video ging ik mijn gewenste variabele zoeken: de diamanten. Eerst heb ik voor “6” gezocht omdat ik al 6 diamenten verzameld had maar dan krijg je 28552 resultaten.  
A screenshot of a computer

Description automatically generated with medium confidence

Refresh pagina. Nieuwe pogingen, na het verzamelen van x diamanten:

1. 0 🡪 15495229 resultaten, na de uitleg 0 🡪 15474916 resultaten
2. 1 🡪 1975 resultaten
3. 2 🡪 11 resultaten  
   
4. 3 🡪 3 resultaten  
   Graphical user interface, application, Teams

   Description automatically generated
5. 4 🡪 3 resultaten  
   Graphical user interface, application

   Description automatically generated
6. 5 🡪 3 resultaten  
   Graphical user interface, application, Teams

   Description automatically generated
7. Ik dacht ook even 7 te zoeken 🡪 3602 resultaten 🡪 teveel

Resultaten: 0x039c815c, 0x03ee5934, 0x03ef7ecc

Ik hoopte op minder dan 3 resultaten, maar ze blijken bij elke waarde wel dezelfde resultaten te zijn. Ik bookmark de 3 variabelen zodat ik deze kan proberen wijzigen. De methode zoeken zoals in de video is moeilijk. Ik begrijp niks van de honderden lijnen code en ik heb geen zin om het te zoeken dus ik besluit om de writups te lezen. Enkel die van [Zense](https://ctftime.org/writeup/20756) is nog beschikbaar. Hij gebruikt f32 ipv i32 dus ik doe hem na. Ofja, ik wilde hem nadoen maar ik kan de optie niet eens aanduiden...

Ik refresh weer de pagina en krijg nieuwe resultaten! Bij 5 diamanten heb ik nu 4 resultaten.

Graphical user interface, application, Teams

Description automatically generated

Ik besluit om nog eens te proberene en ik zie dat ik de value gewoon kan veranderen en niet zo ingewikkeld moet doen als in de tutorial!

1. 0x039c815c: Aantal diamanten wijzigen niet
2. 0x03ee5934: Aantal diamanten wijzigen!
3. 0x03ef7ecc: Aantal diamanten wijzigen niet

Ik krijg zelfs een melding dat ik vals speel en dat ik goed bezig ben.

A screenshot of a computer

Description automatically generated with medium confidence

Graphical user interface

Description automatically generated with medium confidence

Eerste flag gevonden!

Graphical user interface

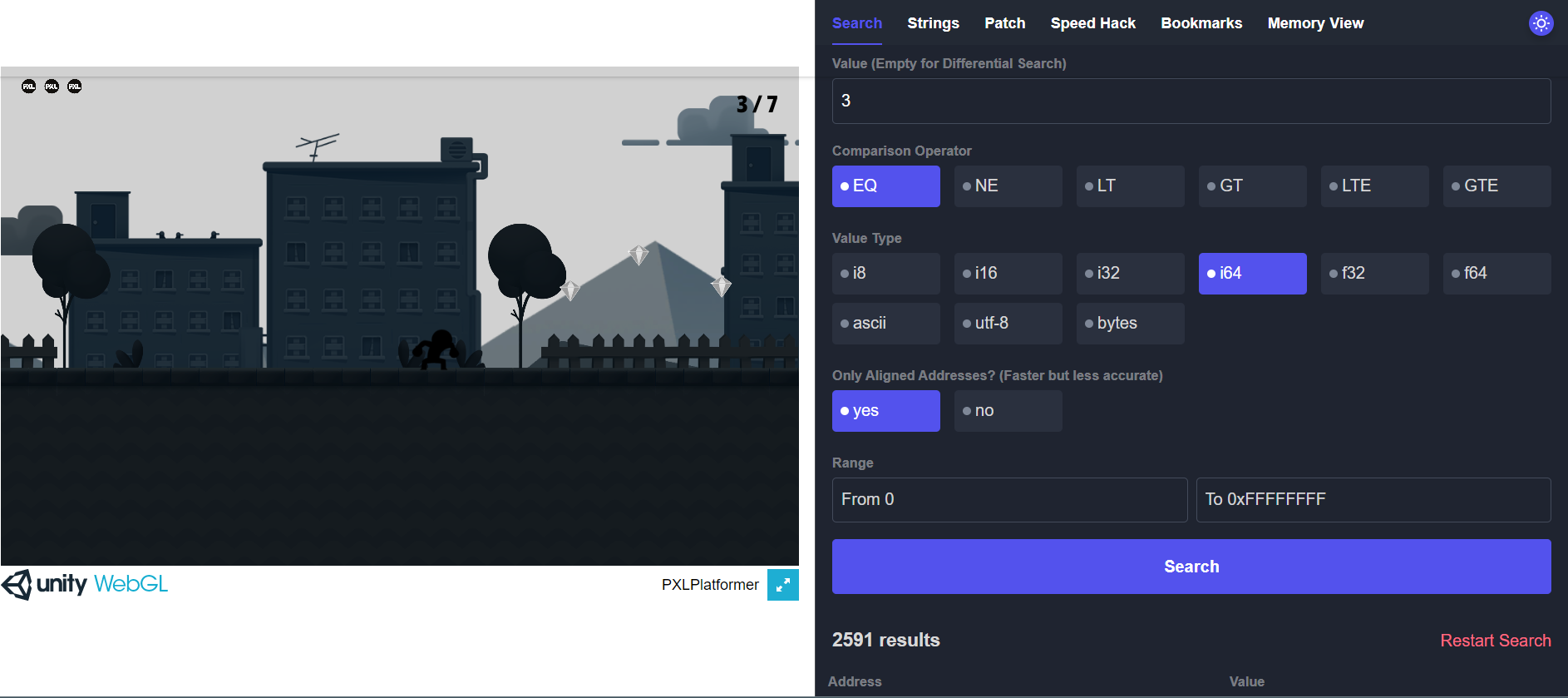
Description automatically generated

### Multi-disciplinary Flag

Ik kom obstakels tegen en verlies al meteen een leven dus ga ik op zoek naar de variabelen van mijn leven.

Blijkbaar kan ik wel f32 kiezen wanneer ik de search refresh...

3 diamanten en 3 levens zorgt voor 2591 zoekresultaten bij de waarde 3.



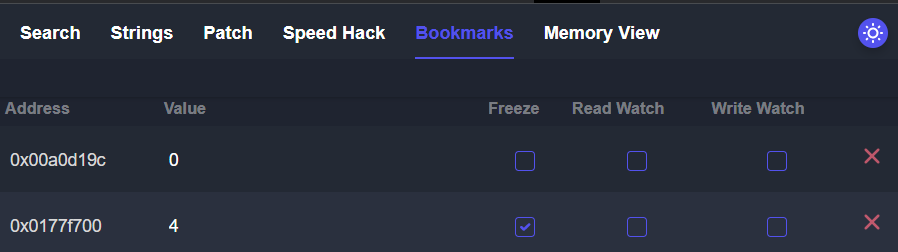
Ik zorg dat ik sterf en zoek heel snel de waarde 0 op. Dat geeft mij 5 resultaten.

A screenshot of a computer

Description automatically generated with medium confidence

Ik bookmark ze allemaal en probeer uit te zoeken welke variabele mijn levens zijn door ze aan te passen.

Bij het herboren worden veranderen er maar 2 variabelen naar “3”, het aantal levens dat ik dan weer heb. Enkel 0x0177f700 verandert mee, dus levens gevonden! Ik bevries de variabelen zodat ik zonder schade doorheen het spel kan gaan.



Dit lukt en ik heb mijn vlag gevonden!

A screenshot of a video game

Description automatically generated with medium confidence

### Internation Flag

Ik stierf per ongeluk en kwam de vlag tegen.

Graphical user interface, application

Description automatically generated

# Room:

## Tijd 1h58min

|  |  |
| --- | --- |
| Taak | Duur |
| Taak 1 | 00h 01min 30sec |
| Taak 2 | 00h 00min |
| TOTAAL | 00h 00min |

## Antwoorden

### Taak 1: Introductie

|  |
| --- |
| Click and continue learning! |
| Geen antwoord nodig |

### Taak 2: Challenge

|  |
| --- |
| Which Antivirus software is running on the VM? |
|  |

|  |
| --- |
| What is the name of the user account to which you have access? |
|  |

|  |
| --- |
| Establish a working shell on the victim machine and read the file on the user's desktop. What is the flag? |
|  |

## Taak 2: Challenge

### Which Antivirus software is running on the VM?

### What is the name of the user account to which you have access?

### Establish a working shell on the victim machine and read the file on the user's desktop. What is the flag?