code16

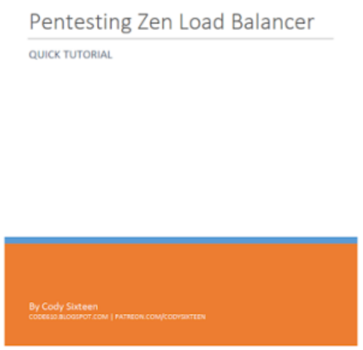
Strona główna | Mini arts | Notes Magazine | Found bugs | CTFs | Contact

NIEDZIELA, 29 MARCA 2020

Pentesting Zen Load Balancer - quick tutorial

Last time we talked about Zen Load Balancer few weeks ago. Yesterday I decided to check it again to find something similar and maybe create a little tutorial. Below you will find the details. Here we go...

Today we will start here:

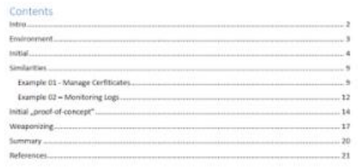


Pentesting Zen Load Balancer

QUICK TUTORIAL

By Cody Sixteen
CODE610.BLOGSPOT.COM | PATREON.COM/CODYSIXTEEN

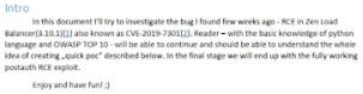
In the PDF file you'll find (~20 pages about) RCE found in Zen Load Balancer as well as few other details:



Contents

Intro 2
Environment 3
Initial 4
Similarities 5
  Example 01 - Manage Certificates 5
  Example 02 – Monitoring Logs 12
Initial „proof-of-concept" 14
Weaponizing 17
Summary 20
References 21

Small intro:



Intro

In this document I'll try to investigate the bug I found few weeks ago - RCE in Zen Load Balancer(3.10.1)[1] also known as CVE-2019-7301[2]. Reader – with the basic knowledge of python language and OWASP TOP 10 - will be able to continue and should be able to understand the whole idea of creating „quick poc" described below. In the final stage we will end up with the fully working postauth RCE exploit.

Enjoy and have fun! ;)

I decided that this one will be available for free. Maybe you'll find it useful.

Special thanks goes to my **new Patrons**:
- Daniel
- julianvolodia

If you like the content I'm creating here - feel free to support me. ;)

See you next time!

Cheers

Posted by code16 at 08:14

Labels: debug, infrastructure, notes, poc, pwn, web, writeup

Brak komentarzy:

Prześlij komentarz

Wpisz komentarz

O MNIE

code16

Cody Sixteen

Wyświetl mój pełny profil

ARCHIWUM BLOGA

► 2022 (16)
► 2021 (37)
▼ 2020 (62)
  ► 12 (1)
  ► 11 (2)
  ► 10 (1)
  ► 09 (2)
  ► 08 (5)
  ► 07 (5)
  ► 06 (7)
  ► 05 (5)
  ► 04 (11)
  ▼ 03 (10)
    Pentesting Zen Load Balancer - quick tutorial
    Creating poc for preauth Symantec Web Gateway RCE
    Postauth RCE in Symantec Web Gateway
    Creating poc for NagiosXI 0day
    Postauth RCE in ManageEngine 14
    Postauth RCE bugs in NagiosXI 5.6.11
    Postauth SQLi in latest NagiosXI 5.6.11
    Nagios 5.6.11 XSS'd
    RCE in Artica 4.26
    Playing games with Games
  ► 02 (6)
  ► 01 (7)
► 2019 (97)
► 2018 (67)
► 2017 (58)
► 2016 (63)

ETYKIETY

.net
android
binary
crackme
ctf
debug
docker
drones
enlil
FortiGate
fuzz
infrastructure
malware
notes
pentest
poc

Nowszy post Strona główna Starszy post

Subskrybuj: Komentarze do posta (Atom)

pwn
RE
web
writeup