RSTCon CTF

Author: <Mihai Cujba / 0x435446> - <mihai.cujba @yahoo.com / 0x435446 @gmail.com>

Summary

RSTCon CTF	1
Summary	1
<motorul cautare="" de="" pentru="" vulnerabilitati=""> (<428>): <web></web></motorul>	2
Proof of Flag	2
Summary	2
Proof of Solving	2
<interviul> (<428>): <misc></misc></interviul>	5
Proof of Flag	5
Summary	5
Proof of Solving	5
<mesajul -="" de="" i="" pe="" retea=""> (<50>): <crypto></crypto></mesajul>	6
Proof of Flag	6
RST{15ef7619e4db40f47be08e2e8c263ec2f688464b62598c713c1b68e0240fedce}	6
Summary	6
Proof of Solving	6
< Mesajul de pe retea - II> (<482>): <crypto></crypto>	7
Proof of Flag	7
Summary	7
Proof of Solving	7

<Motorul de cautare pentru vulnerabilitati> (<428>): <Web>

Proof of Flag

RST{74343420409df9ada2608b0d8f070c1b7932f53a0c317cede3097e0c36a04352}

Summary

Folosirea unui token jwt vulnerabil din cauza secretului.

Proof of Solving

Prima data am incercat pe acel search-bar de pe prima pagina cateva tipuri de atac, pentru a verifica daca site-ul este vulnerabil. De aici am cautat sa verific daca este ceva in cookie-uri sau robots.txt, dar tot nimc, insa am gasit un token pus pe hidden in sursa paginii. L-am luat, l-am decodificat base64 ca sa pot vedea continutul si am vazut asta:

eyJhbGciOiJIUzI1NiJ9.eyJzdWliOiJ1c2VyliwiY2FuU2VhcmNoljoibm8iLCJpYXQiOjE2MDYwNjU1NTYsImV4cCl6MTYwNjA2OTE1
Nn0.D8lGxTJAV5LLkbcXpGKaajNUajzYkmNil7sOWbRQJ2Y

for encoded binaries (like images, documents, etc.) use the file upload form a bit further down on this page.

UTF-8

Source character set.

Decode each line separately (useful for multiple entries).

Live mode OFF

Decodes your data into the textarea below.

Source character set.

Decodes your data into the textarea below.

Source character: "no", "iat":1606065556, "exp":1606069156} Company (Company Company Compa

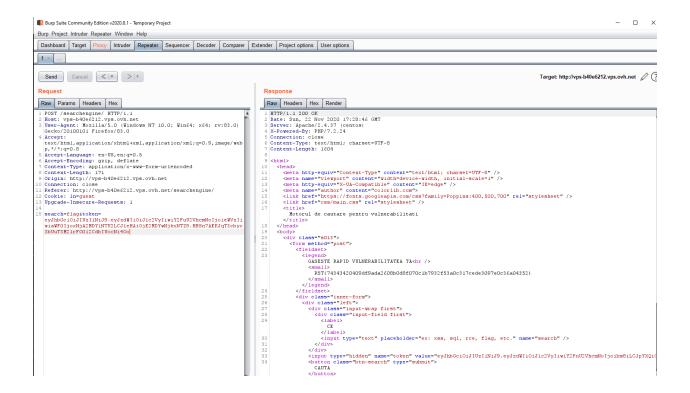
De aici am luat token-ul, i-am scos hash-ul cu jwt2john si i-am facut bruteforce la secret cu john.

Acum am mai avut doar de craftat un token care sa aiba setat "canSearch" pe "yes". M-am folosit de jwt.io pentru asta.

```
HEADER: ALGORITHM & TOKEN TYPE
eyJhbGci0iJIUzI1NiJ9.eyJzdWIi0iJ1c2VyIi
wiY2FuU2VhcmNoIjoieWVzIiwiaWF0IjoxNjA2M
                                                                "alg": "HS256"
DY1NTU2LCJleHAiOjE2MDYwNjkxNTZ9.HBSn7AE
KJqT3cbyc3bUuT3M21rF0012CdbIUocNi40o
                                                             PAYLOAD: DATA
                                                                "sub": "user",
                                                                "canSearch": "yes",
                                                                "iat": 1606065556,
                                                                "exp": 1606069156
                                                             VERIFY SIGNATURE
                                                             HMACSHA256(
                                                               base64UrlEncode(header) + "." +
                                                               base64UrlEncode(payload),
                                                               livestrong
```

Dupa ce l-am craftat am interceptat un request catre site in care am pus "flag" in searchbar, am inlocuit token-ul cu cel generat si am scos flag-ul.

) ☐ secret base64 encoded



<Interviul> (<428>): <Misc>

Proof of Flag

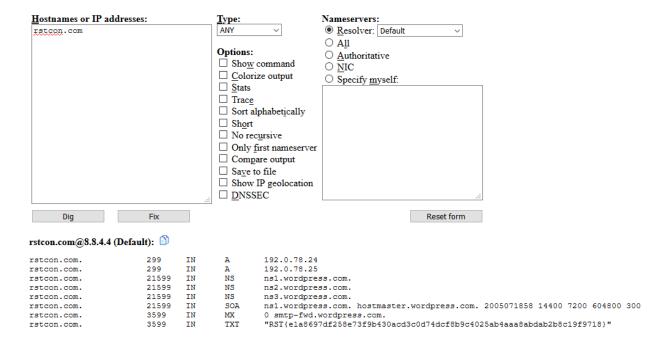
RST{e1a8697df258e73f9b430acd3c0d74dcf8b9c4025ab4aaa8abdab2b8c19f9718}

Summary

DNS Records

Proof of Solving

Cand am citit prima data descrierea challenge-ului, am crezut ca trebuie sa caut recursiv prin toate paginile de pe rstcon.com si flag-ul se va gasi pe undeva printr-un comentariu, dar aparent nu era asa. Dupa ce m-am gandit putin am incercat sa verific DNS Records. Am intrat pe https://www.digwebinterface.com, am pus site-ul in textbox, am dat pe ANY Records si am gasit flag-ul in cele TXT.



<Mesajul de pe retea - I> (<50>): <Crypto>

Proof of Flag

RST{15ef7619e4db40f47be08e2e8c263ec2f688464b62598c713c1b68e0240fedce}

Summary

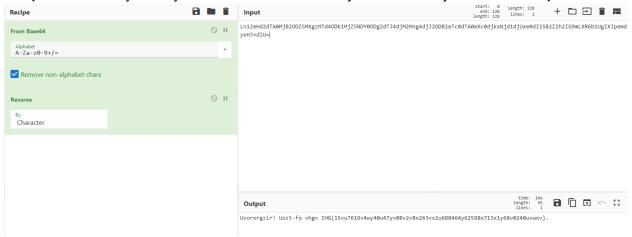
Am primit un mesaj codificat.

Proof of Solving

De cand am vazut padding-ul de la base64 am incercat sa vad daca as putea decodifica mesajul cu aceasta metoda. Dupa decodificare am primit in mesaj ce parea scris de la dreapta la stanga, asa ca am facut un rev() pe el si a iesit cam asa:

Uvorxrgzir! Uozt-fo vhgv

IHG{15vu7619v4wy40u47yv08v2v8x263vx2u688464y62598x713x1y68v0240uvwxv}.



De aici am incercat diferite metode de criptare pe care se paote face usor bruteforce si am gasit ca este criptat folosind affine.



< Mesajul de pe retea - II> (<482>): < Crypto>

Proof of Flag

RST{84aa7743e2633f55a8a9d9322cd30d664e8440a4341f08b00f72ceb5e411133a}

Summary

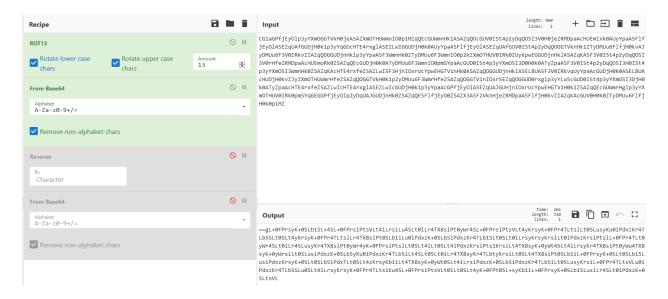
Asemanator cu Mesajul de pe retea – I, am primit un mesaj encodat.

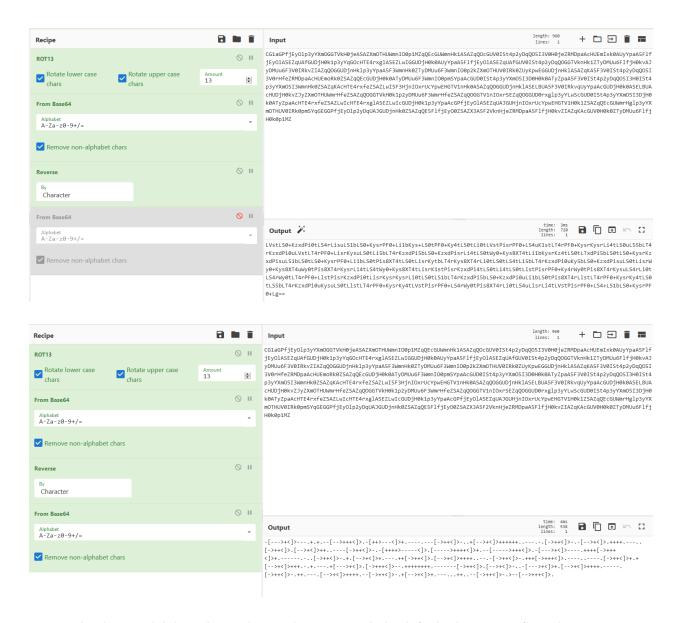
Proof of Solving

Pentru inceput am incercat sa trec mesajul prin base32, base58, base62 si base64, dar fara succes. De aici m-am gandit sa fac acelasi lucru, dar facut un rev() peste textul initial; tot nimic.

Am mai stat putin sa ma gandesc si am incercat caesar peste text, iar la ROT 13 am reusit sa scot un text in clar, folosind base32 peste.

Textul avea un padding la inceput, deci am dedus ca este scris de la dreapta la stanga. Am facut un rev() pe el si arata a text encodat cu base64. L-am decodificat si mi-a dat de brainfuck (literalmente (a)).





Am luat codul, I-am bagat intr-un interpretor de brainfuck si am scos flag-ul.

