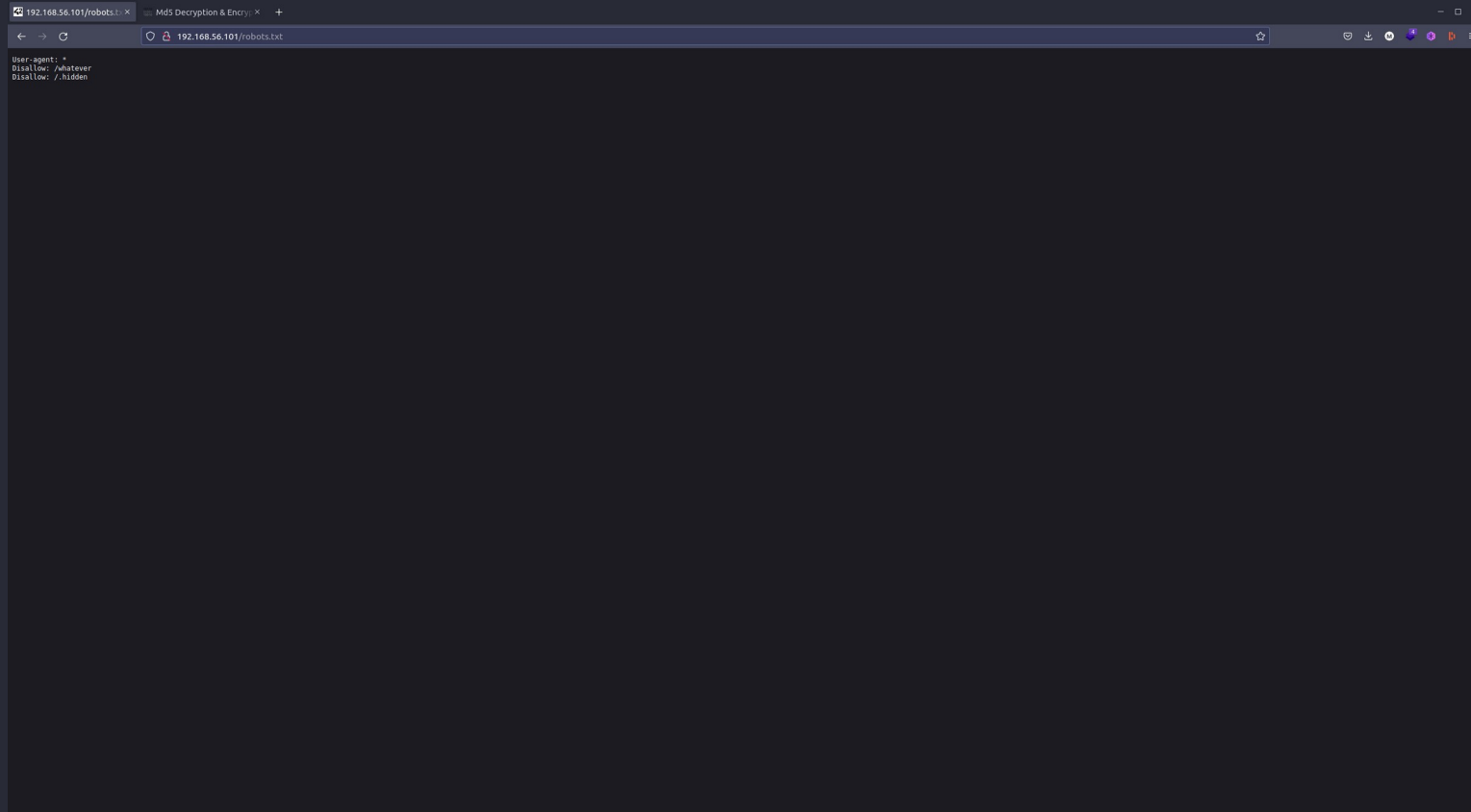
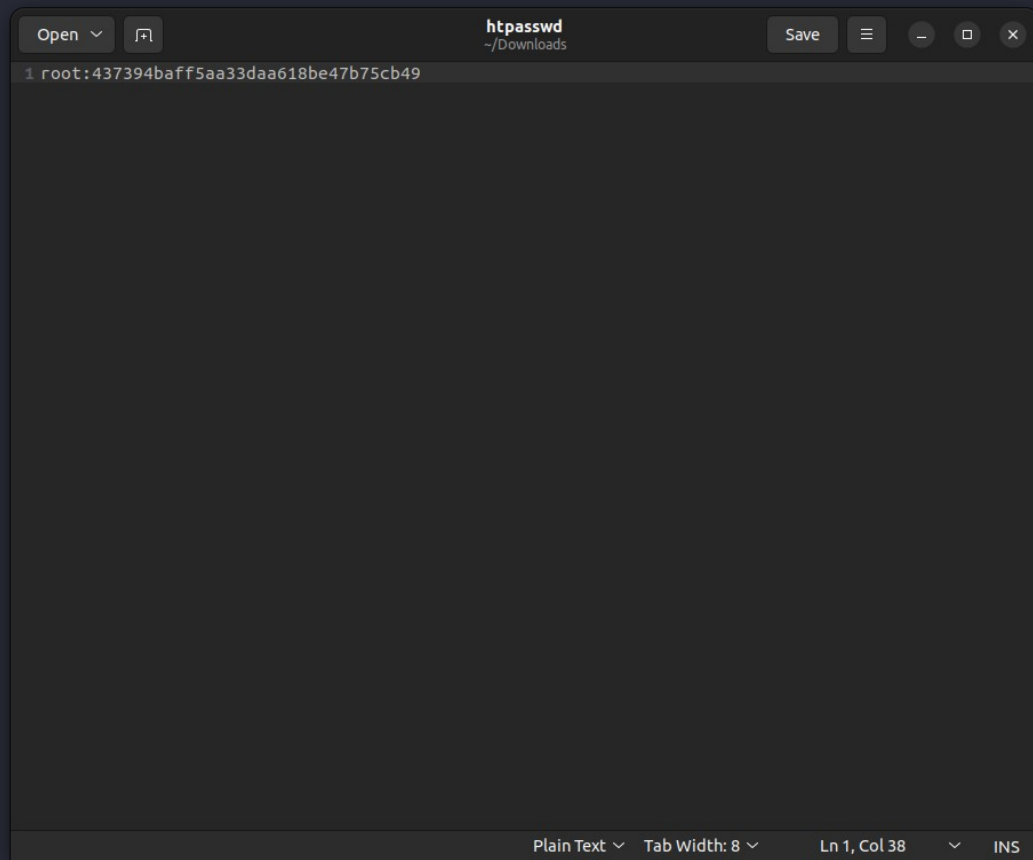


Walk through

Step 1 : Try access to robots.txt file we found a whatever directory !



Step 2 : Access to the /whatever directory we found a htpasswd file with a user:password but the password seem to be crypted :(



The image shows a text editor window titled "htpasswd" with a subtitle "~/Downloads". The editor contains a single line of text: "1 root:437394baff5aa33daa618be47b75cb49". The status bar at the bottom indicates "Plain Text", "Tab Width: 8", "Ln 1, Col 38", and "INS".

```
1 root:437394baff5aa33daa618be47b75cb49
```

Step 3 : Decrypt the password :

192.168.56.101/robots.txt

Md5 Decrypt & Encrypt

→

https://md5decrypt.net/#answer

Accueil

Encrypt / Decrypt

Outils de conversion

Chiffres

Outils divers


API

Contact

FR

I

EN




129€
103€

Equipez vous pour l'automne

BUT

Rosny Sous Bois




129€
103€

Equipez vous pour l'automne

BUT

Rosny Sous Bois




129€
103€

Equipez vous pour l'automne

BUT

Rosny Sous Bois

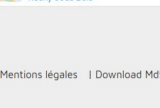


129€
103€

Jusqu'à -30% en Magasin

BUT

Rosny Sous Bois




129€
103€

Jusqu'à -30% en Magasin

BUT

Rosny Sous Bois



Bâissez des applications web

Démarrez avec notre offre gratuite

Md5 Decrypt & Encrypt


Collez un ou plusieurs hashes (maximum 100)

Crypter

Décrypter

437394baff5aa33daa618be47b75cb49 : qwerty123@

Trouvé en 0.139s



Déployez plus vite grâce au DevOps sur AWS

Démarrez avec notre offre gratuite

Decryption Md5 :

Le Md5 (Message Digest 5) est une fonction cryptographique qui permet de "hasher" (encoder) une séquence numérique en un hash md5 de 128 bits, soit 32 caractères, et ce peu importe la longueur de la séquence originale. Ce système cryptographique est irréversible, il n'est pas possible d'obtenir la séquence originale (de décrypter) en utilisant seulement le hash md5. La seule façon de décrypter le hash est donc de le comparer à une base contenant les hashes md5 en ligne et leur séquence correspondante. Ce site se sert d'une base de 15183605161 hashes md5 pour vous proposer une séquence correspondante à votre hash afin de le décrypter. Une fonction de hachage de séquence (encryption md5) est aussi disponible, nous ne stockons pas les mots que vous encodez. Le dictionnaire utilisé provient de tous les dictionnaires (wordlists) que j'ai pu trouver sur internet, compilés, triés, puis élargis grâce à un script de ma fabrication. Après plusieurs jours de calculs, j'en suis arrivé à une base de données unique et pertinente.

Le md5 n'est plus considéré comme sûr depuis un certain temps. En 2004 une collision complète a été découverte par des chercheurs chinois. Depuis cette date, les collisions sont de plus en plus facilitées notamment par l'amélioration de la puissance de traitement des ordinateurs. Il est maintenant possible de trouver une collision en md5 en moins de quelques minutes. Si vous voulez en apprendre plus sur les collisions md5, vous pouvez consulter [ce lien](#). Il est maintenant conseillé d'utiliser le sha256, 512, bcrypt, scrypt ou whirlpool pour stocker vos mots de passe.

Si toutefois vous souhaitez conserver le md5 comme fonction de hachage pour votre site, il est conseillé d'utiliser un "salt" pour le rendre plus difficile à cracker par brute-force (et par rainbow tables). Un salt est simplement une chaîne de caractère que l'on ajoute au mot de passe fourni par l'utilisateur pour le rendre plus compliqué à casser. Par exemple, si on utilise le mot de passe "password", qui est évidemment très facile à casser. Il suffit de lui concaténer une chaîne de caractère aléatoire créée via une fonction en php par exemple. Imaginons une chaîne de caractère utilisant tous les caractères alphanumériques et de 14 caractères de long, par exemple a-/c*12/"bn@(. Si on concatène ceci à "password", cela donne a-/c*12/"bn@(password. Il est évident que ce mot de passe sera difficilement trouvable dans une base de données en ligne. Vous pouvez aussi séparer le salt en deux mots de taille égale et les concaténer en début et en fin de mot de passe par exemple. Par ailleurs, si vous cherchez une astuce pour créer un mot de passe simple à se souvenir en tant qu'utilisateur, mais aussi résistant au bruteforce et aux rainbow tables, vous pouvez utiliser une phrase complète. Par exemple jemesouviensdecetmotdepassecestsur. Cela présente l'avantage d'être facile à se remémorer, et d'être très difficile à casser. Pour peu que vous ajoutiez une majuscule et un chiffre le mot de passe sera très difficile à cracker.

#LeChoixDeSe

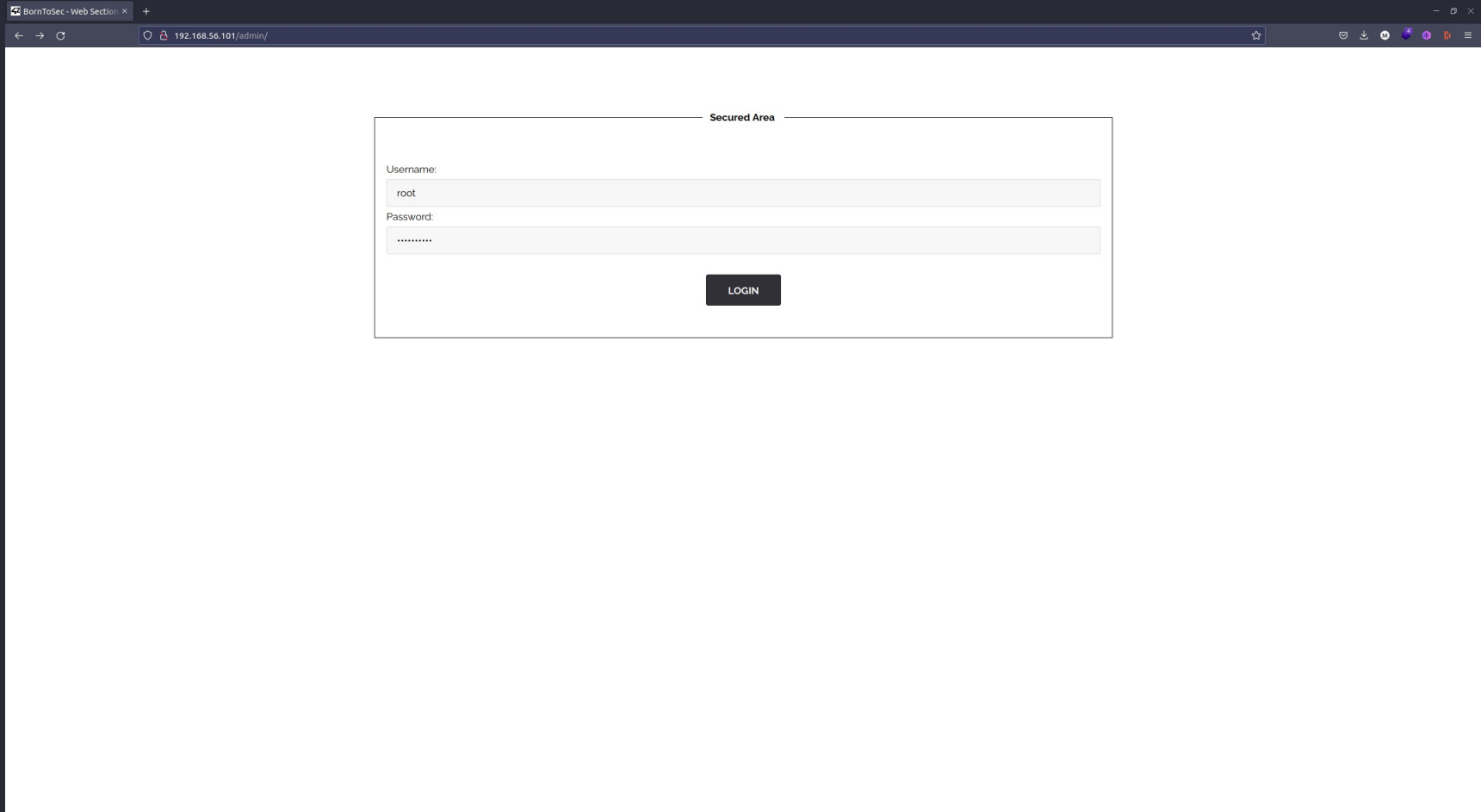
JE M'ENGAGE

e2oic

Annance Report 2019-2020

Mentions légales | Download Md5decrypt's Wordlist

Step 4 : Enter the credentials root:qwerty123@ on the admin page



The screenshot shows a web browser window with the title 'BornToSec - Web Section'. The address bar displays the URL '192.168.56.101/admin/'. The main content area features a 'Secured Area' login form. The form includes a 'Username:' label, a text input field containing 'root', a 'Password:' label, a password input field with masked characters '.....', and a 'LOGIN' button.

BornToSec - Web Section

192.168.56.101/admin/

Secured Area

Username:

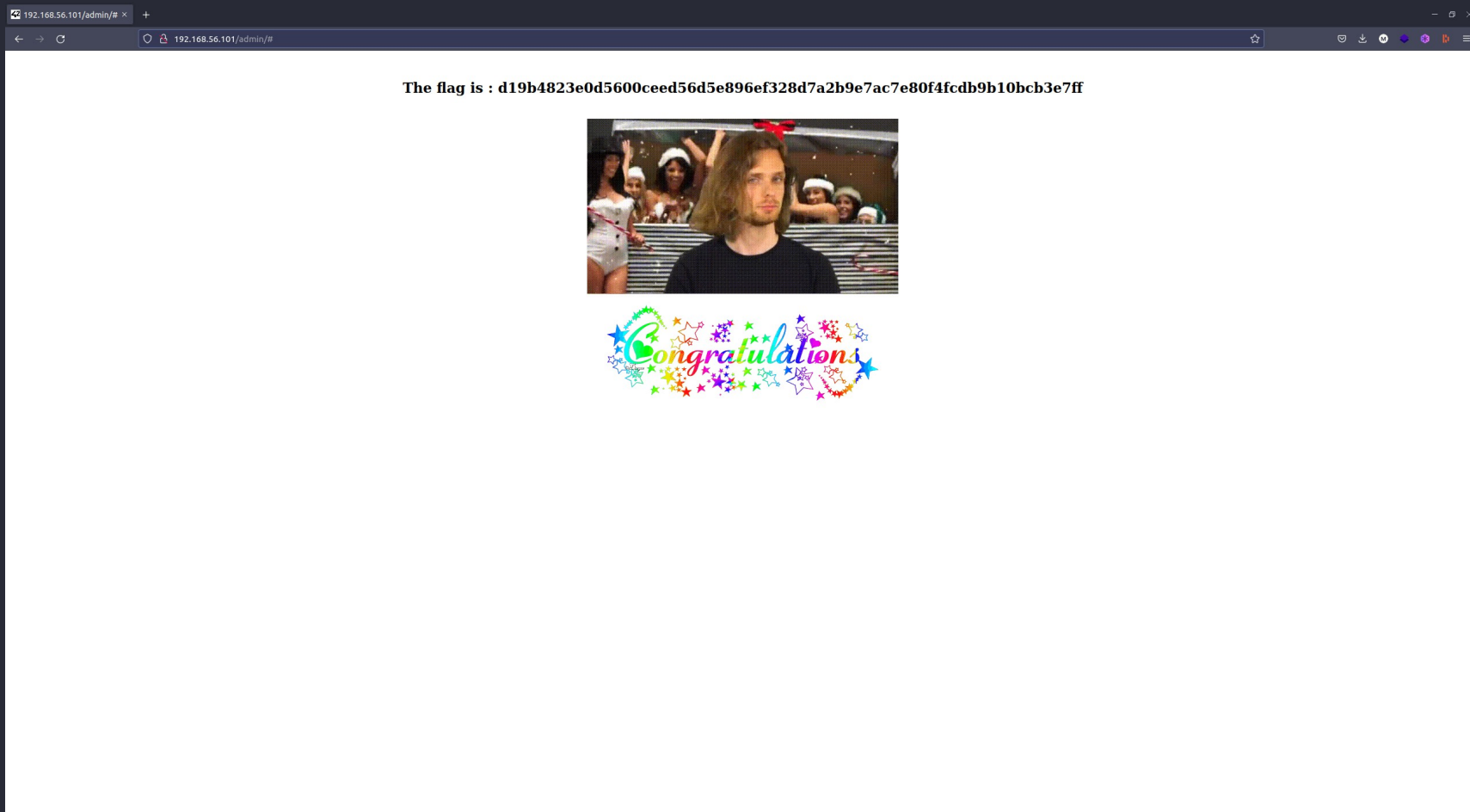
root

Password:

.....

LOGIN

Step 5 : Get the flag !



Tools

- <https://md5decrypt.net/> to decrypt the hash

How to fix

- Use a more secure hash algorithm
- Block the access of sensible directory/files for clients