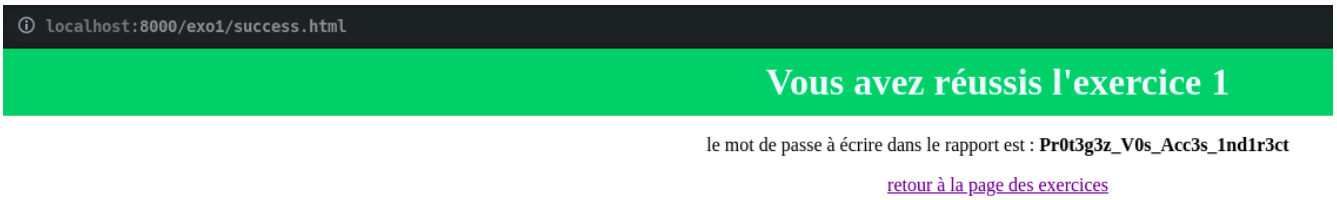
Quentin KACZMAREK

Exercice 1 :

password : Pr0t3g3z_V0s_Acc3s_1nd1r3ct
faille : accès indirect --> on peut accèder directement à la page success.html en modifiant l'url directement.
reproduction :
- allez sur la page de l'exercice 1
- changer l'url après "exo1/" de "index.html" à "success.html"

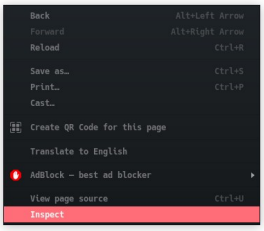


- vous atteignez la page success.html

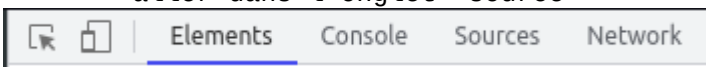
Quentin KACZMAREK

Exercice 2 :

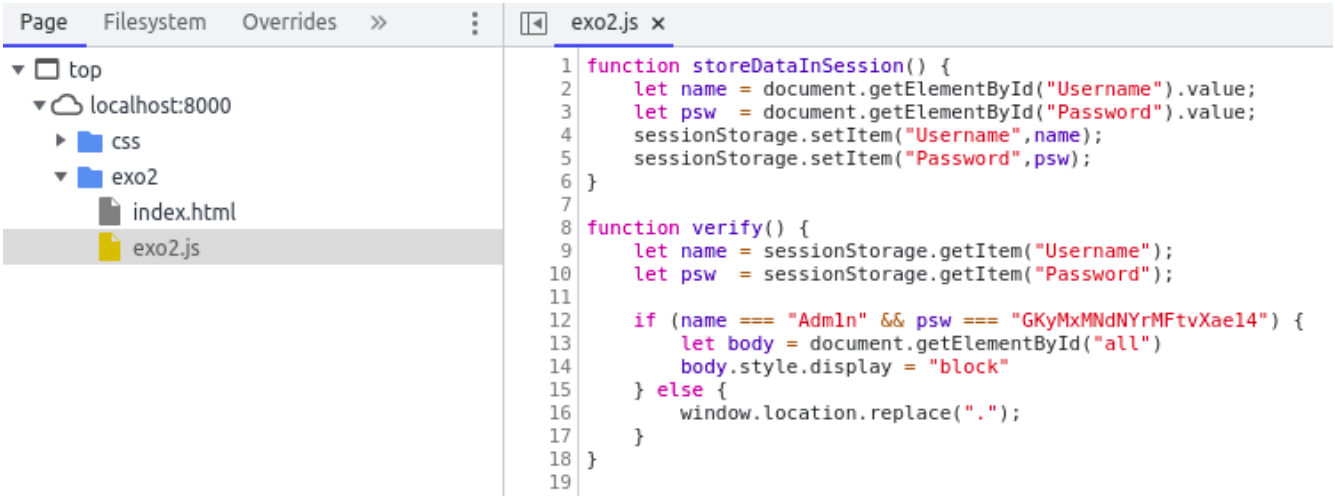
password : N3_p@s_St0ck3r_L3s_M0ts_D3_P@ss3_D@ns_L3_Fr0nt
faille : mot de passe et username stocker directement dans le script js en front.
reproduction :
- aller sur la page de l'exercice 2
- utiliser l'inspecteur de chrome



- aller dans l'onglet "source"



- cliquer sur exo2.js



- recupérer ligne 12 le username et le password
- remplir le formulaire
- vous accèder à la page voulu

Quentin KACZMAREK

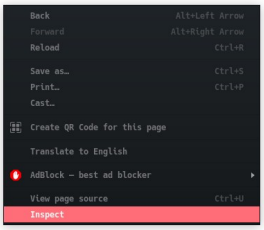
Exercice 3 :

faille : XSS , injection de script dans la page
reproduction :
- aller sur la page de l’exercice 3
- entrer :
- une alerte va se déclencher

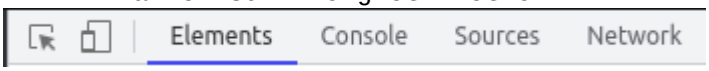
Quentin KACZMAREK

Exercice 4 :

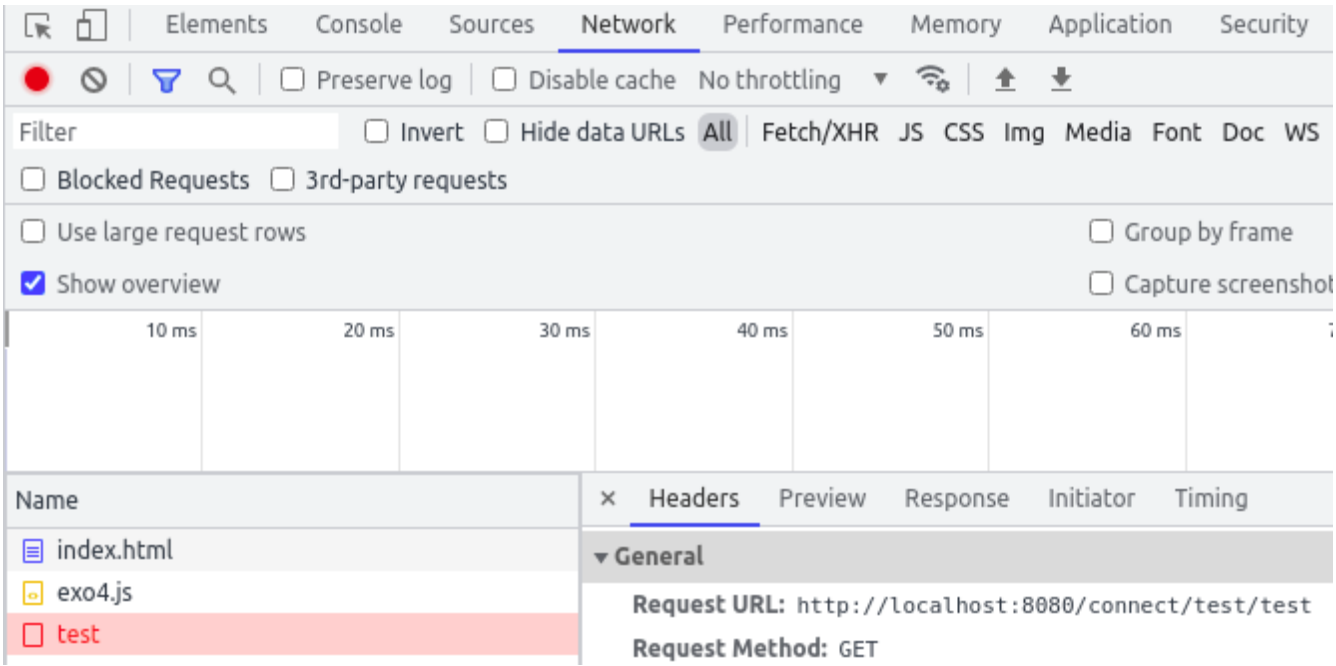
password : Jc8b&RM52AL
faille : mot de passe est identifiant attendus retourner dans le response header
reproduction :
- aller sur la page de l'exercice 4
- rentrer des identifiants au hasard
- cliquer sur se connecter
- inspecter la page



- aller sur l'onglet "Network"



- cliquer sur la requete afficher en rouge



Quentin KACZMAREK

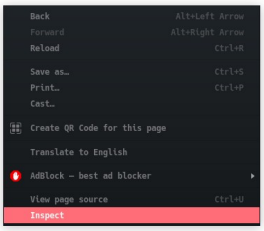
- regarder dans le "response header"

- les lignes X-User et X-Psw contiennet respectivement le username et le password
- utiliser ces deux identifiants pour vous connecter

Quentin KACZMAREK

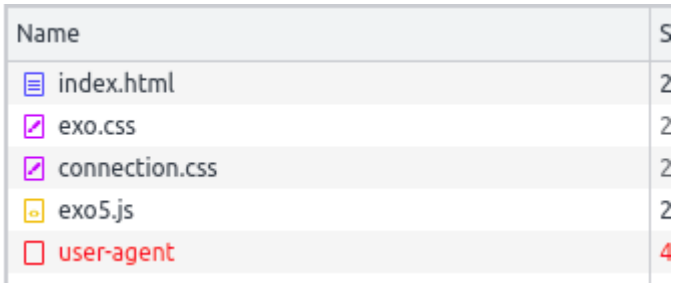
Exercice 5 :

user-agent : toto
faille : user-agent qui est voulu est renvoyer dans le response header
reproduction:
- aller sur la page de l'exercice 5
- clicker sur "se connecter"
- inspecter la page

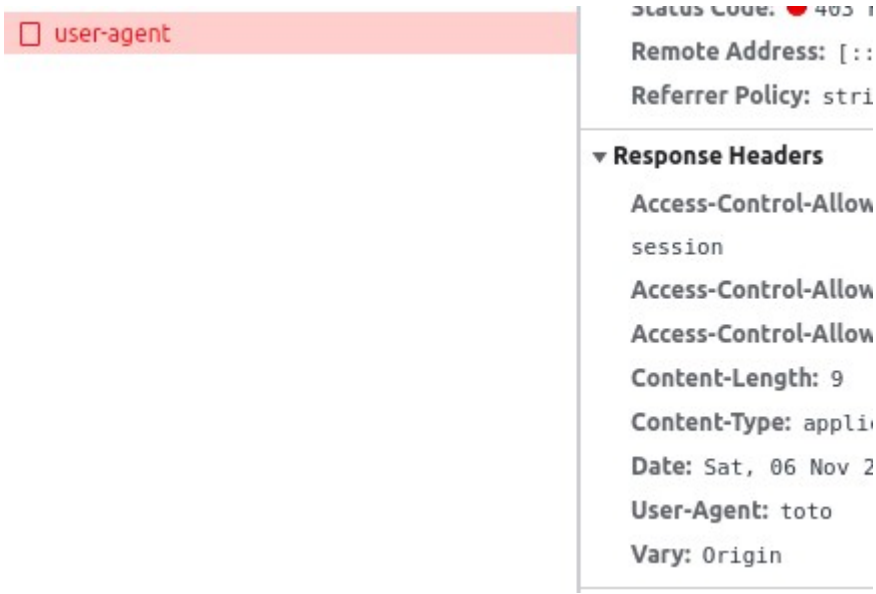


- regarder dans l'onglet "Network"

- cliquer sur la requete "user-agent"



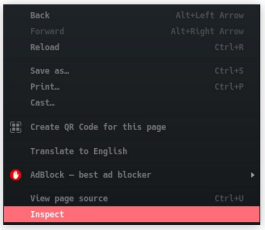
- regarder le "response header"



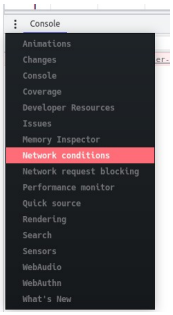
- regarder la ligne "user-agent" ==> "toto"

Quentin KACZMAREK

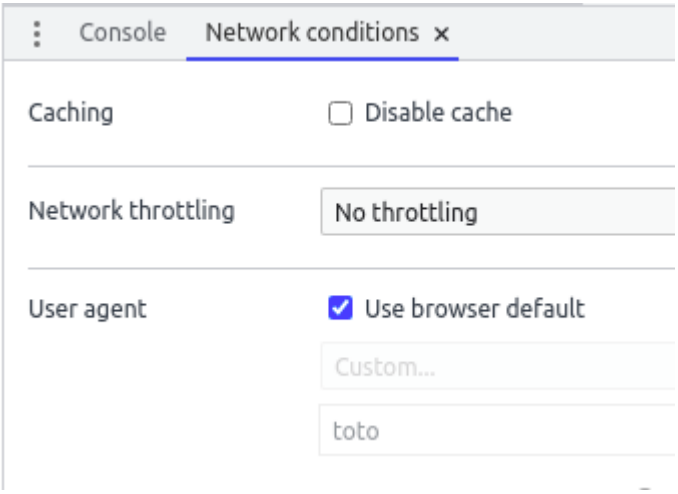
- faire inspecter la page



- sur la zone de la console, trouver les 3 points verticaux, cliquer dessus, et selectionner Network Conditions



- décocher la case "browser default" dans la zone user-agent

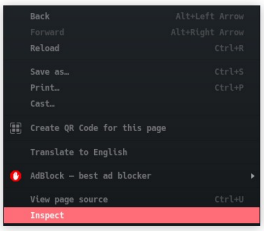


- remplir dans le champ de texte avec toto
- cliquer sur se connecter
- le alert voulu s'affiche;

Quentin KACZMAREK

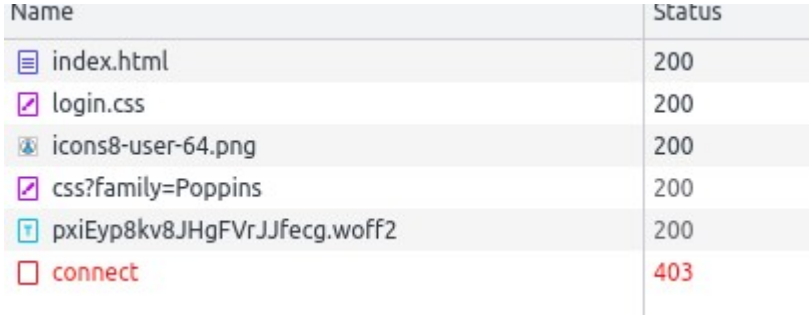
Exercice 6 :

:
faille : injection sql, la requête sql n'est pas prepared, donc on peut modifier la requête
reproduction :
- aller sur la page de l'exercice 6
- essayer de se connecter avec des identifiants aléatoire
- inspecter la page

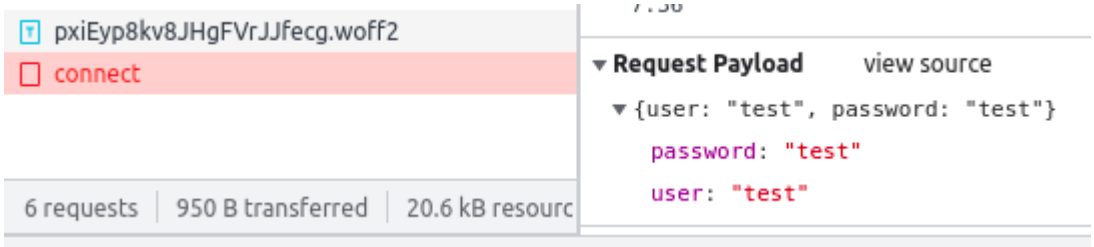


- regarder dans l'onglet "Network"

- cliquer sur la requête "connect"



- regarder le "request payload"



- nous allons essayer d'injecter du sql dans la requête
- entrer dans le champ login la chaine : " ' or '1' = '1
- entrer dans le champ password la chaine : " ' or '1' = '1
- cliquer sur "se connecter"
- vous êtes connecter

Quentin KACZMAREK

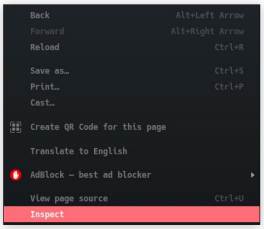
`Exercice 7:`

`password :` toto123lol

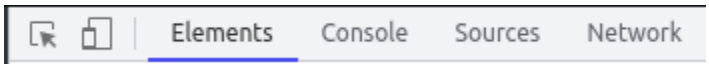
faille : Code source js avec mot de passe en dur, facile à récupérer même s'il est encoder en javascript

reproduction :

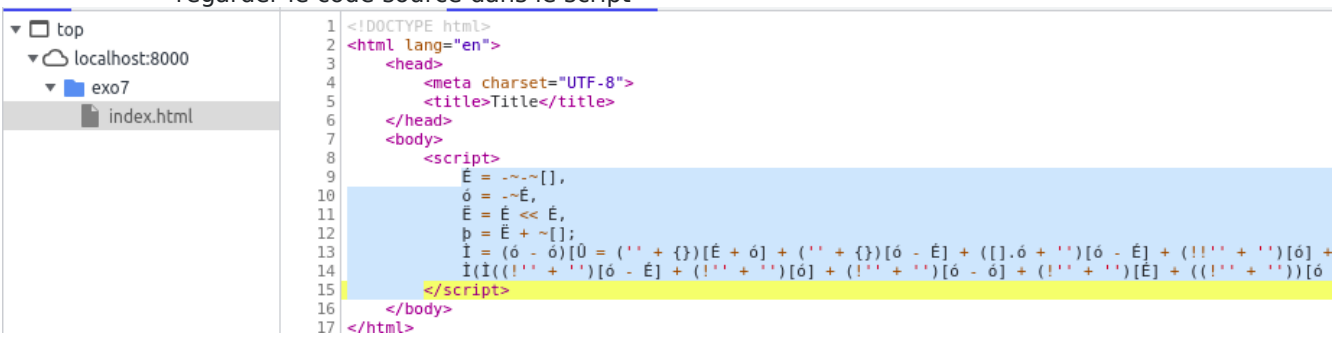
- allez sur la page de l'exercice 7
- inspecter la page



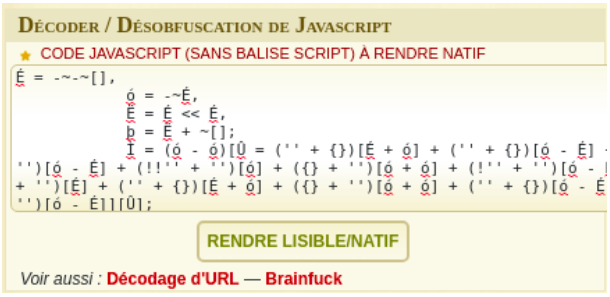
- regarder dans l'onglet "source"



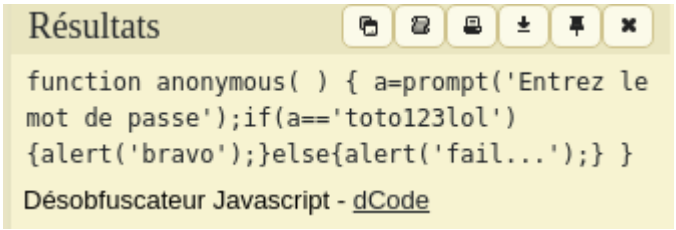
- regarder le code source dans le script



- le copier sur le site suivant : https://www.dcode.fr/desobfuscateur-javascript



- récupérer le mot de passe "toto123lol"



- vous avez trouver le mot de passe