

Quentin KACZMAREK

Exercice 1 :

password : Pr0t3g3z_V0s_Acc3s_1nd1r3ct

faille : accès indirect --> on peut accéder 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"

localhost:8000/exo1/index.html

Bienvenue sur l'exercice 1

Votre but est de trouver le moyen d'accéder à la page *success.html*

SUCCESS.HTML

© Université de Lorraine

localhost:8000/exo1/success.html

Vous avez réussi l'exercice 1

le mot de passe à écrire dans le rapport est : **Pr0t3g3z_V0s_Acc3s_1nd1r3ct**

[retour à la page des exercices](#)

- vous atteignez la page success.html

Quentin KACZMAREK

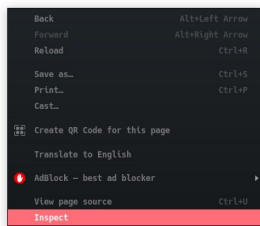
Exercice 2 :

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 :

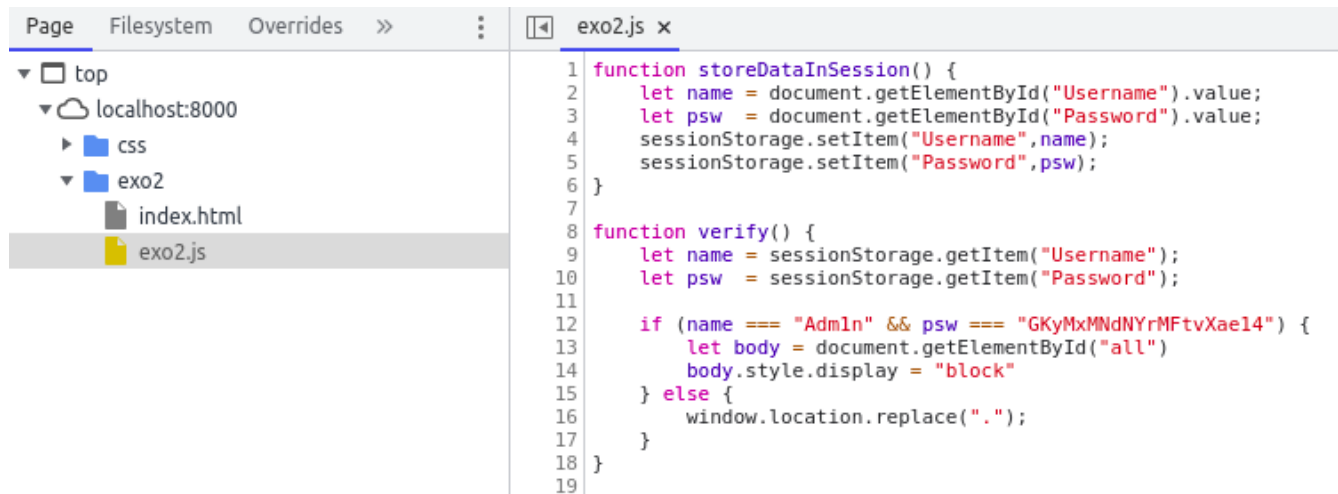
- aller sur la page de l'exercice 2
- utiliser l'inspecteur de chrome



- aller dans l'onglet "source"



- cliquer sur exo2.js



- récupérer ligne 12 le username et le password
- remplir le formulaire
- vous accéder 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

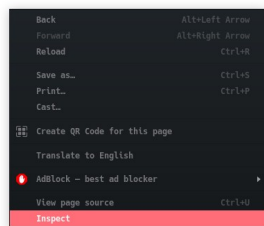
Exercice 4 :

password : Jc8b&RM52AL

faible : mot de passe est identifiant attendu retourner dans le response header

reproduction :

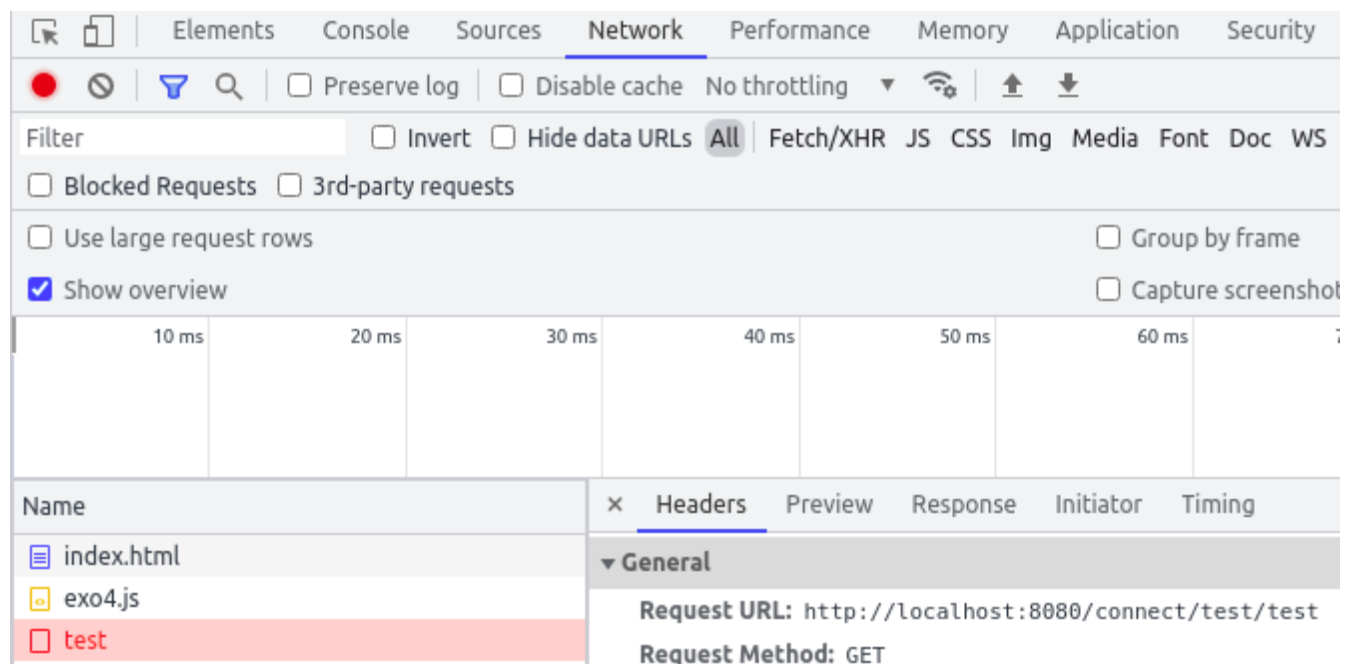
- aller sur la page de l'exercice 4
- rentrer des identifiants au hasard
- cliquer sur se connecter
- inspecter la page



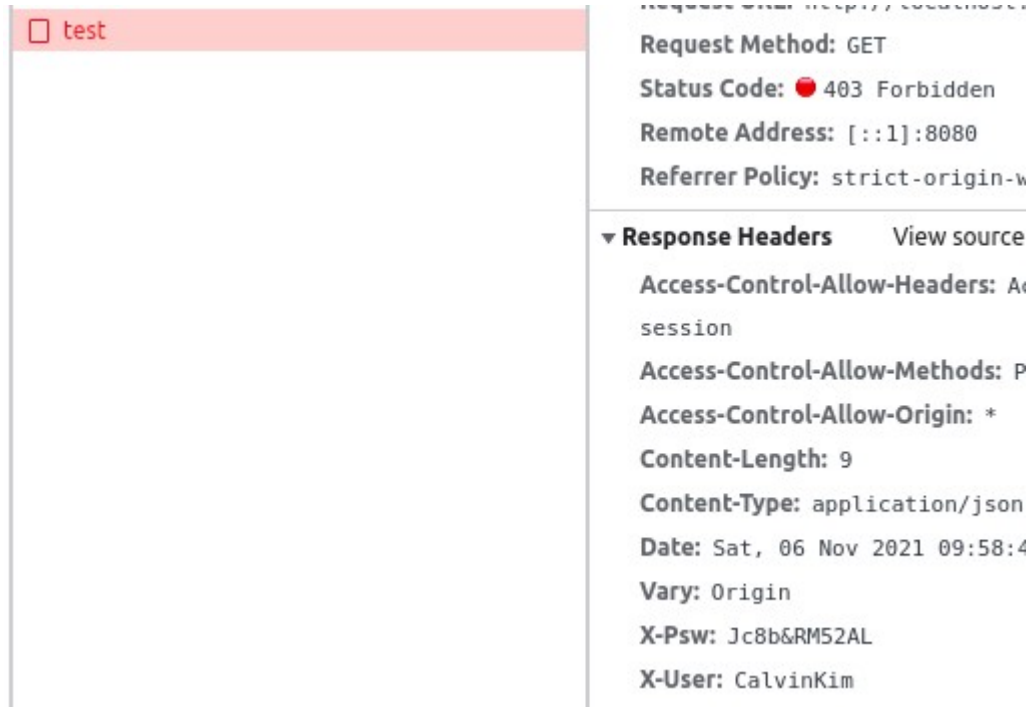
- aller sur l'onglet "Network"



- cliquer sur la requete afficher en rouge



- regarder dans le "response header"



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

Quentin KACZMAREK

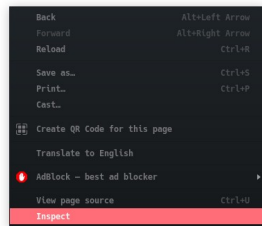
Exercice 5 :

user-agent : toto

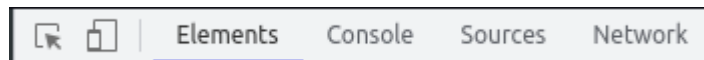
faible : user-agent qui est voulu est renvoyer dans le response header

reproduction:

- aller sur la page de l'exercice 5
- cliquer sur "se connecter"
- inspecter la page



- regarder dans l'onglet "Network"



- cliquer sur la requete "user-agent"

Name	Size
index.html	2
exo.css	2
connection.css	2
exo5.js	2
user-agent	4

- regarder le "response header"

user-agent

Status Code: 403

Remote Address: [::]

Referrer Policy: stri

▼ Response Headers

Access-Control-Allow session

Access-Control-Allow

Access-Control-Allow

Content-Length: 9

Content-Type: appli

Date: Sat, 06 Nov 2

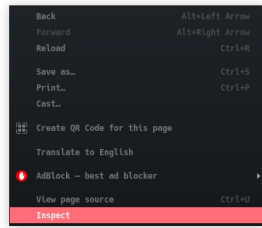
User-Agent: toto

Vary: Origin

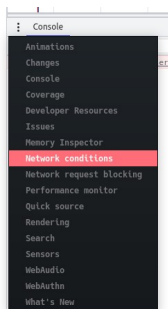
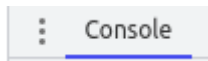
- regarder la ligne "user-agent" ==> "toto"

Quentin KACZMAREK

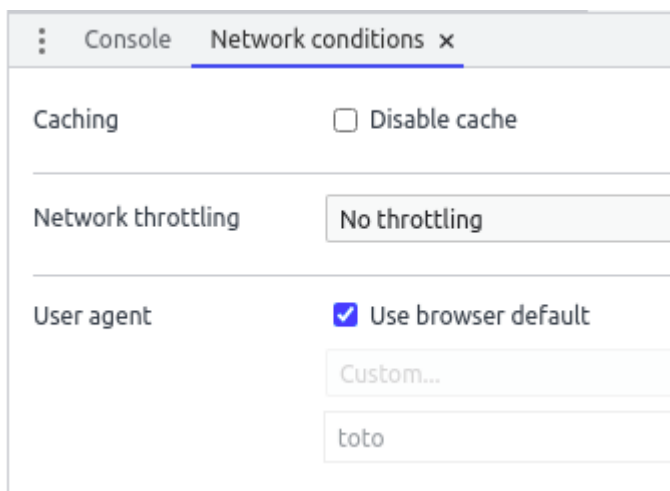
- faire inspecter la page



- sur la zone de la console, trouver les 3 points verticaux, cliquer dessus, et sélectionner 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;

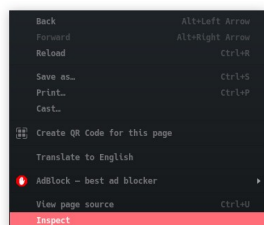
Quentin KACZMAREK

Exercice 6 :

:
faible : 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



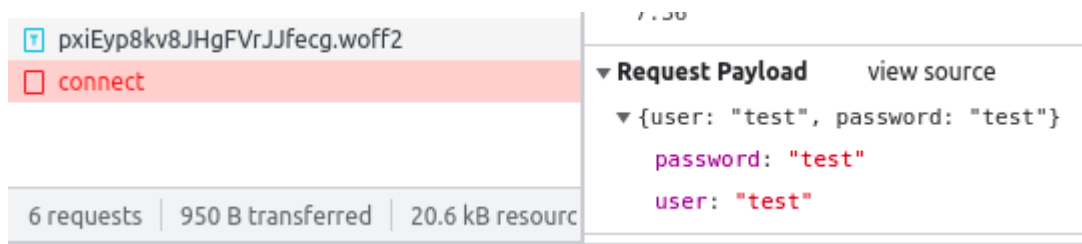
- regarder dans l'onglet "Network"



- cliquer sur la requête "connect"

Name	Status
index.html	200
login.css	200
icons8-user-64.png	200
css?family=Poppins	200
pxiEyp8kv8JHgFVrJJfecg.woff2	200
connect	403

- regarder le "request payload"



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

Quentin KACZMAREK

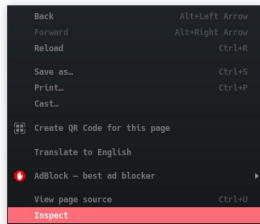
Exercice 7:

password : toto123lol

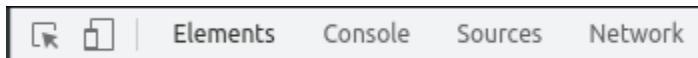
faillie : Code source js avec mot de passe en dur, facile à récupérer même s'il est encodé en javascript

reproduction :

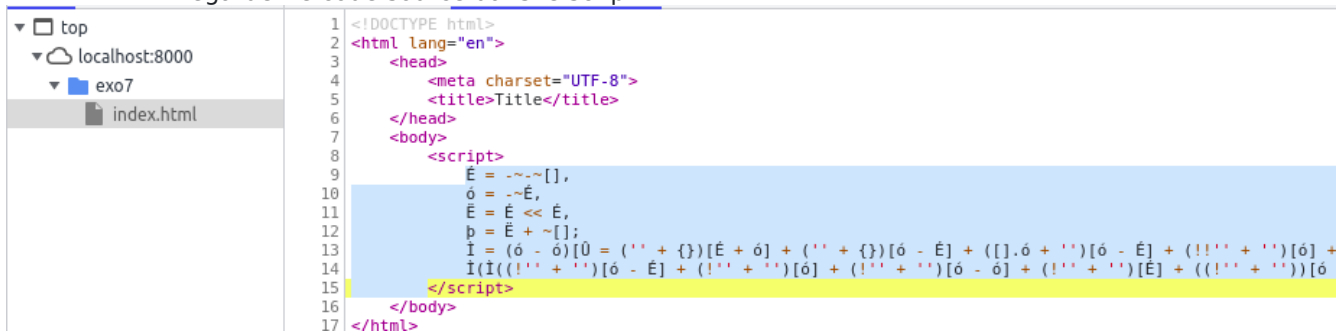
- allez sur la page de l'exercice 7
- inspecter la page



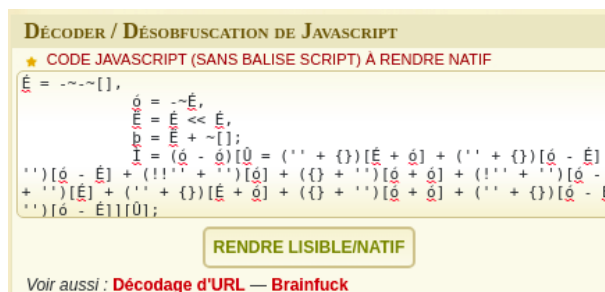
- regarder dans l'onglet "source"



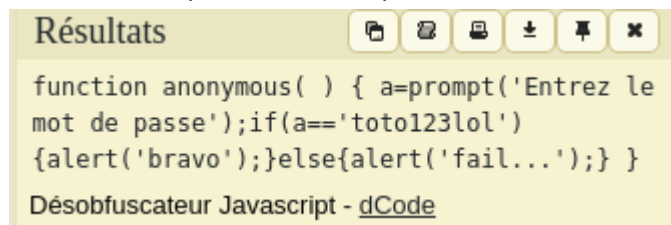
- regarder le code source dans le script



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



- récupérer le mot de passe "toto123lol"



- vous avez trouvé le mot de passe