File Upload

NICOLAS DAYOT, SAMUEL ADONE & MARIE DUGOUA

Présentation

- Création d'une application de téléchargement d'un fichier avec Node.Js
  - 1er server non sécurisé (tout type de fichier)
  - 2nd server sécurisé (seulement les images)

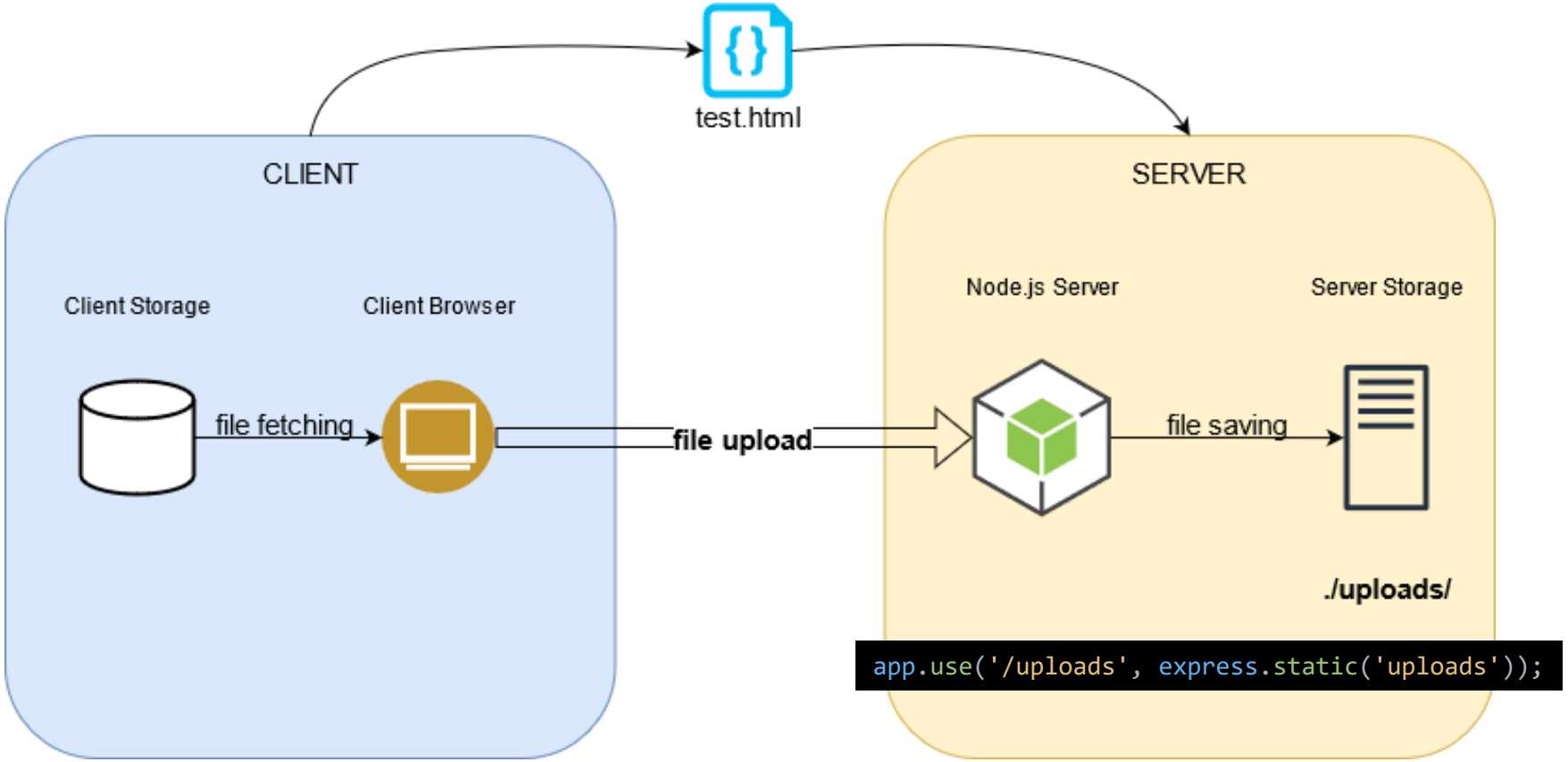
- Recherche de failles possible
  - Injection de scripte
  - Bypasse sécurité extension

Difficultées

- 1er server
  - Le script s'exécute, mais seulement coté client
  - Internet Explorer a sécurisé la faille d'injection de script
- 2nd server
  - Burp peut modifier l'extension mais la vérification = côté server

Démo

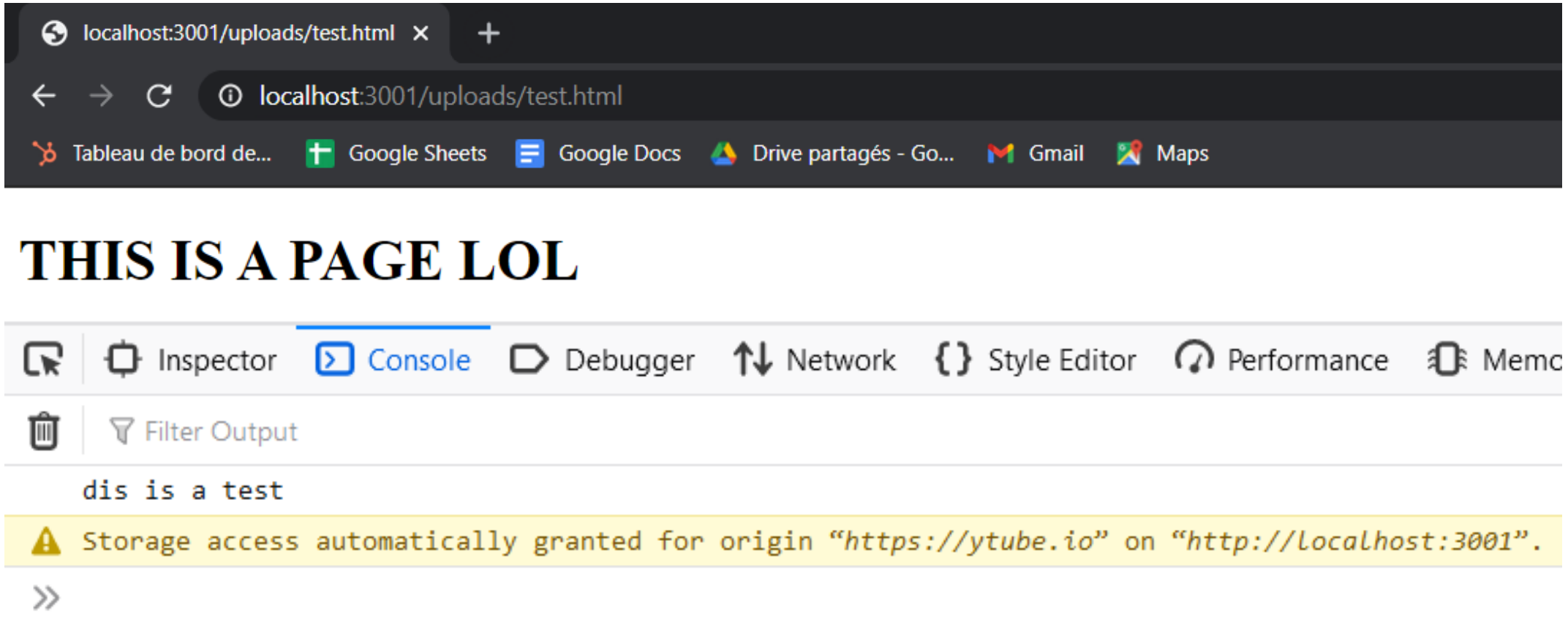
Explication



Explication

```
<!DOCTYPE html>
<head>
</head>
<body>
    <h1>
        THIS IS A PAGE LOL
        <script>
            console.log('dis is a test');
            window.open("https://ytube.io/3Ggn");
        </script>
    </h1>
</body>
```

Explication



Conclusion

- Réaliser plus de recherche pour un contrôle coté server
  - Comment faire tourner un script
  - Comment Bypass extension
  - Prendre la main cotes server