🛡 **Rapport de Bug – Fuite de domaines internes via l'API publique des Feature Flags**

Titre : L'API publique expose des domaines internes et environnements sitetesté

Endpoint :

POST https://api.sitetesté.com/flags/api/v2/frontend/experimentValues

Description :
L'API des feature flags retourne des **domaines internes sitetesté, des URLs de staging et des adresses locales** dans sa réponse dynamic_configs. Ces informations sont accessibles **sans authentification**, via une clé API publique.

Étapes pour reproduire :

1. Envoyer une requête POST :

```
POST /flags/api/v2/frontend/experimentValues
Content-Type: application/json
X-Api-Key: <clé API publique>
```

2. Avec les identifiants et attributs personnalisés :

```
{
  "identifiers": { "analyticsAnonymousId": "test" },
  "customAttributes": { "atlCohort": 999, "browserUrl": "https://evil.com" },
  "targetApp": "atl-global-static_web"
}
```

3. Observer les domaines internes retournés :

```
"dynamic_configs": {
  "256845715": {
    "value": {
      "value": [
        "qa-wac.internal.sitetesté.com",
        "author.marketing.internal.sitetesté.com",
        "proof.marketing.internal.sitetesté.com",
        "truth.marketing.internal.sitetesté.com",
        "127.0.0.1:9000",
        "localhost:9000",
        ...
      ]
    }
  }
}
```

Résultat observé :

- Exposition de domaines internes et d'adresses locales.
- Les valeurs envoyées (browserUrl, atlCohort) sont ignorées ; l'API retourne des données statiques internes.

Résultat attendu :

- Aucune donnée interne ne devrait être exposée publiquement.
- L'API devrait exiger une authentification et filtrer les informations sensibles.

Impact :

- **Divulgation d'informations internes** : permet à un attaquant de connaître l'infrastructure interne.
- Facilite le reconnaissance, le phishing ou de futures attaques ciblées.

Recommandations :

- Restreindre l'accès aux utilisateurs authentifiés uniquement.
- Supprimer les domaines internes et localhost des réponses publiques.
- Valider le targetApp pour éviter l'accès non autorisé.

Gravité : Moyenne (Information Disclosure, aide à la reconnaissance)