**Rapport de Test d'Intrusion – Site Web myauthenticstore.com**

1. **Informations Générales et Exécutives**
2. **Résumé Exécutif (Executive Summary)**

### Évaluation Globale de la Posture de Sécurité

### 2.2. Recommandations Managériales Stratégiques

## 3. Méthodologie et Périmètre du Test

### 3.1. Périmètre Exact

### 3.2. Approche Suivie

## 4. Constatations Techniques et Recommandations (Détails)

4.1. Vulnérabilité V-01

1. Tests effectués

**1. Informations Générales et Exécutives**

**Titre du Document -** Rapport de Test d'Intrusion – myauthenticstore.com

**Entreprise d'Audit - Anguima Sécurité**

**Client -** myauthenticstore.com

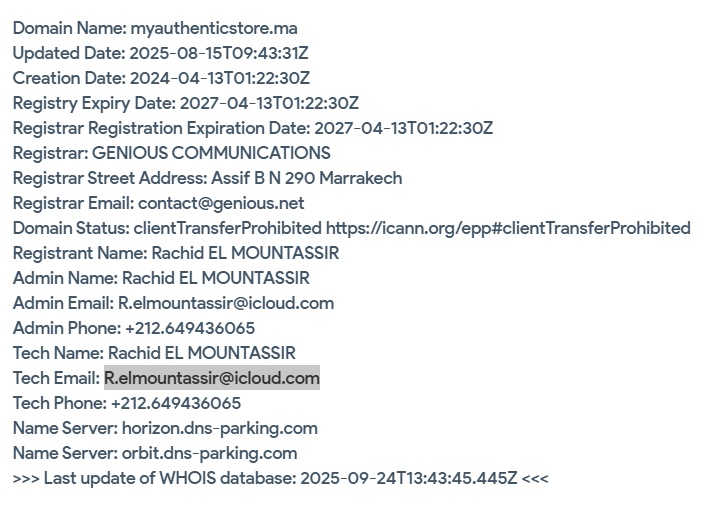
**Périmètre du Test -** Application Web et infrastructure externe accessible par Internet

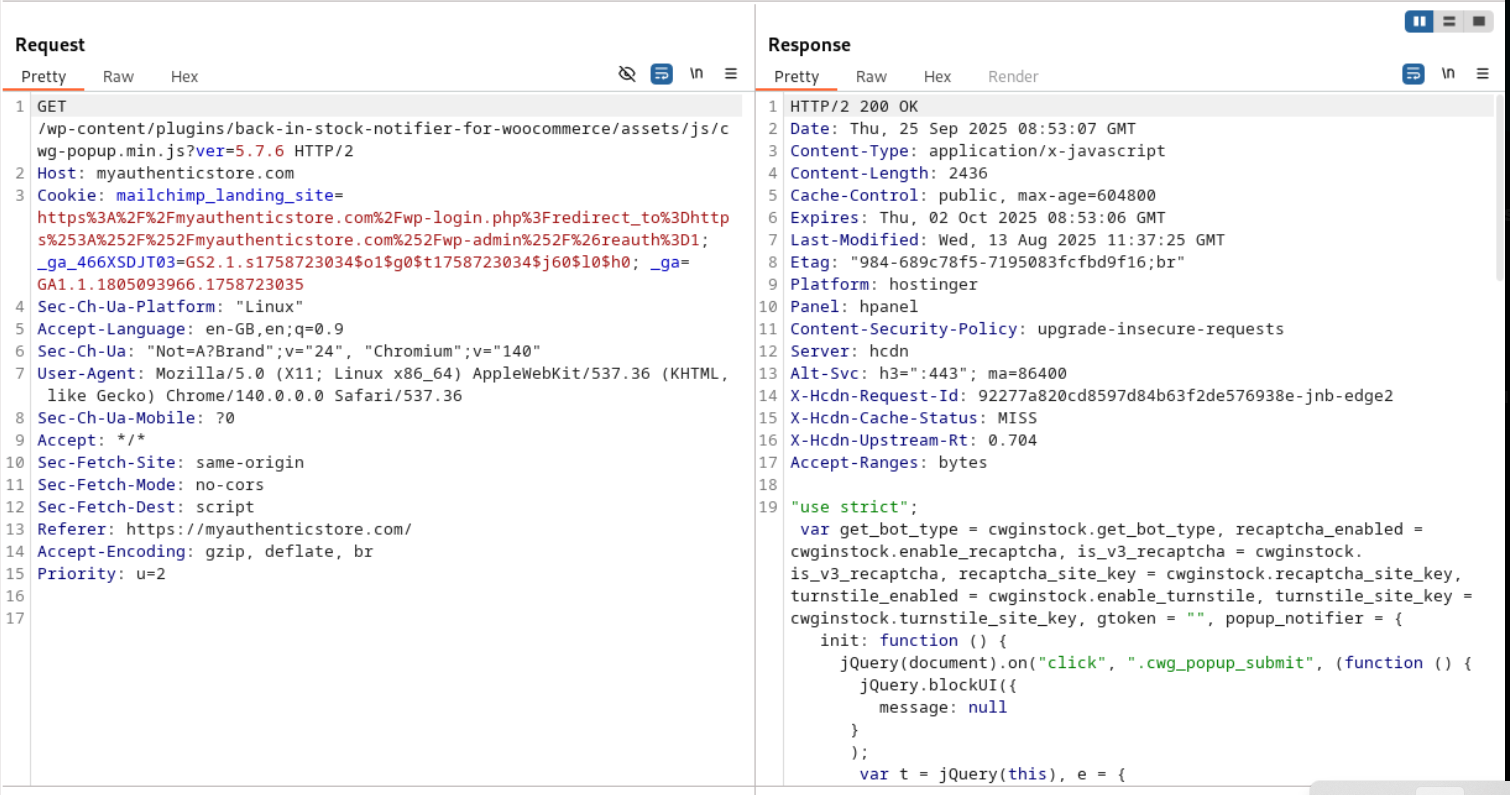
**Dates du Test** - 24.09.2025 au 26.09.2025

**Auteur(s) du Rapport - VERGIER Guillaume, Antoine Moreaux, Mathys Domergue**

**Version du Rapport -** V1.0

**Niveau de Confidentialité - STRICTEMENT CONFIDENTIEL**







## 2. Résumé Exécutif (Executive Summary)

*Cette section est destinée aux dirigeants. Elle doit être non technique et axée sur le risque métier.*

### 2.1. Évaluation Globale de la Posture de Sécurité

Le Test d'Intrusion mené par Anguima Sécurité sur le site web myauthenticstore.com a permis d'identifier 0 **vulnérabilités**, dont **0 critiques** et 0 **de niveau élevé**.

Bien que l'équipe de myauthenticstore.com ait mis en place certaines défenses de base, des faiblesses critiques persistent dans [mentionner la zone principale, ex: le mécanisme d'authentification ou la gestion des entrées utilisateur]. L'exploitation de ces failles pourrait conduire à une **compromission totale des données** stockées, incluant potentiellement des informations sensibles sur la société et ses utilisateurs.

### 2.2. Recommandations Managériales Stratégiques

1. **Priorité Absolue (Urgent) :** Affecter immédiatement des ressources pour corriger les **[Nombre] failles CRITIQUES (ID V-XX)** détaillées dans ce rapport.
2. **Renforcement des Processus :** Mettre en œuvre une politique de **mise à jour régulière** des composants et systèmes d'exploitation pour éviter l'exposition à des vulnérabilités publiques.
3. **Audit de Code :** Lancer un audit approfondi des **bonnes pratiques de développement sécurisé** pour éliminer la racine des failles d'injection et de contrôle d'accès.

## 3. Méthodologie et Périmètre du Test

### 3.1. Périmètre Exact

* **Cible Principale :** https://www.myauthenticstore.com/
* **Adresses IP Testées :** [Liste des IPs/plages testées]
* **Technologies Identifiées :** [Ex: PHP, Apache, MySQL, CMS WordPress, etc.]
* **Type de Test :** Boîte Noire (simulant un attaquant sans aucune connaissance préalable de l'infrastructure interne).

### 3.2. Approche Suivie

Le test a suivi la méthodologie standard de l'industrie, en s'appuyant sur l'**OWASP Testing Guide (Web)** et le cadre **PTES (Penetration Testing Execution Standard)**. Les phases suivantes ont été complétées :

1. **Reconnaissance :** Collecte d'informations publiques (OSINT) sur les sous-domaines, les adresses IP et les technologies.
2. **Analyse de Vulnérabilités :** Balayage de ports et services, identification des points faibles et erreurs de configuration.
3. **Exploitation (Simulée) :** Tentatives d'exploitation **éthiques et non destructives** pour valider la réalité des vulnérabilités.
4. **Rapport et Documentation (Phase Actuelle) :** Détail des résultats et des recommandations.

## 4. Constatations Techniques et Recommandations (Détails)

*Cette section est destinée aux équipes techniques de myauthenticstore.com. Elle fournit toutes les preuves nécessaires à la correction.*

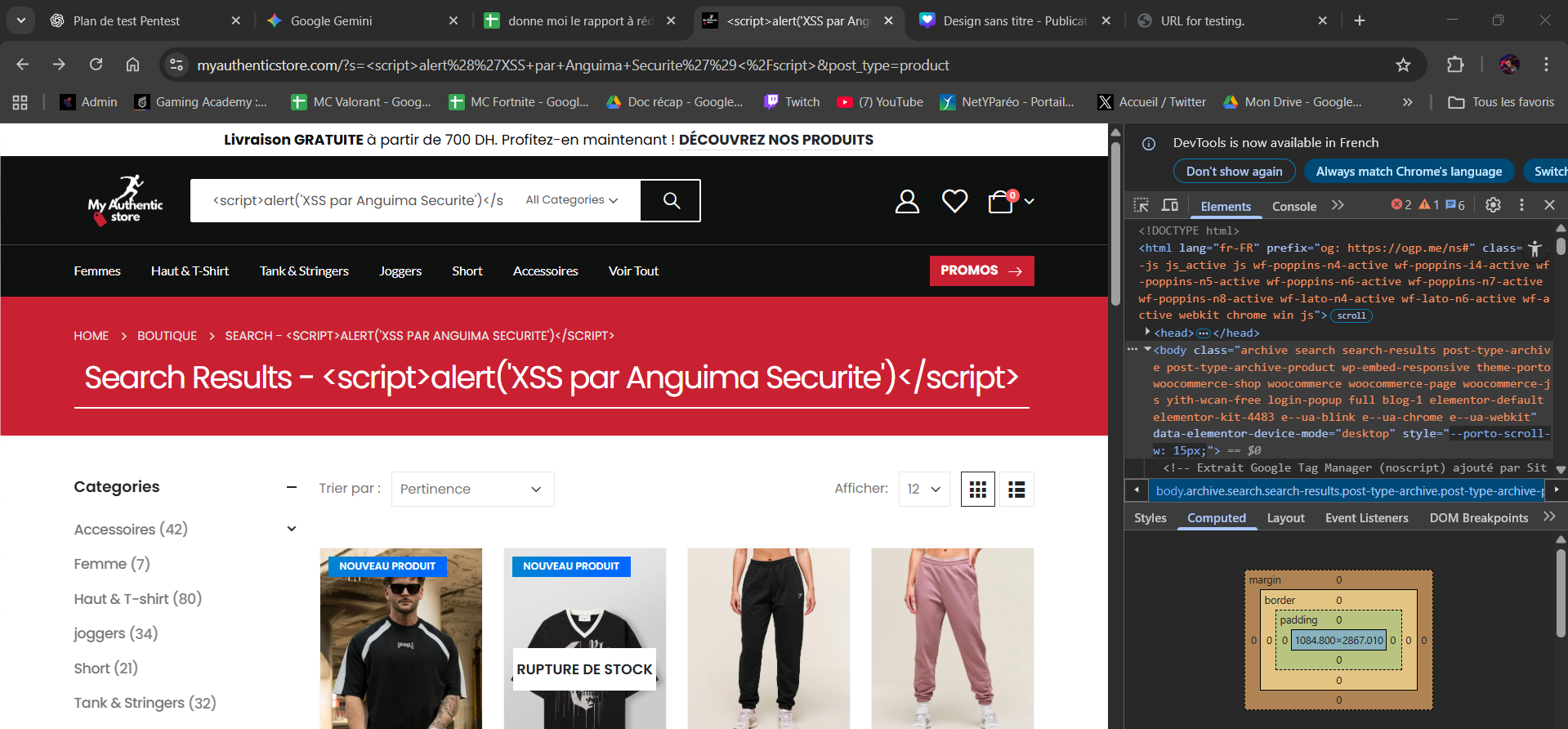
Pour chaque vulnérabilité identifiée, fournissez une fiche comme celle-ci :

### 4.1. Vulnérabilité V-01 : Injection SQL (Critique)

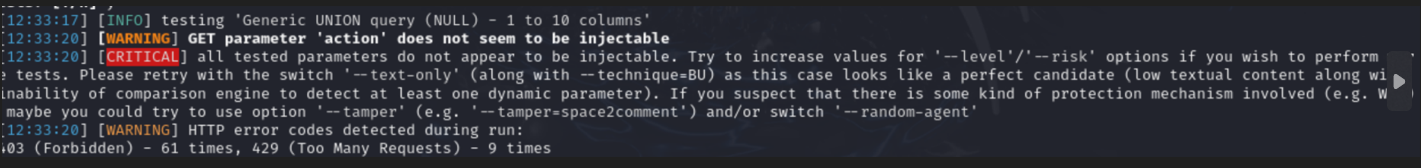
| Détails de la Faille | Informations |
| --- | --- |
| **Niveau de Risque** | **CRITIQUE** |
| **Score CVSS v3.1** | [Insérer score (ex: 9.8)] |
| **Localisation** | https://openclassrooms.com/forum/sujet/includerequire-et-chemin-relatifabsolu-83668 |
| **Type de Test** | Validation des entrées utilisateur. |

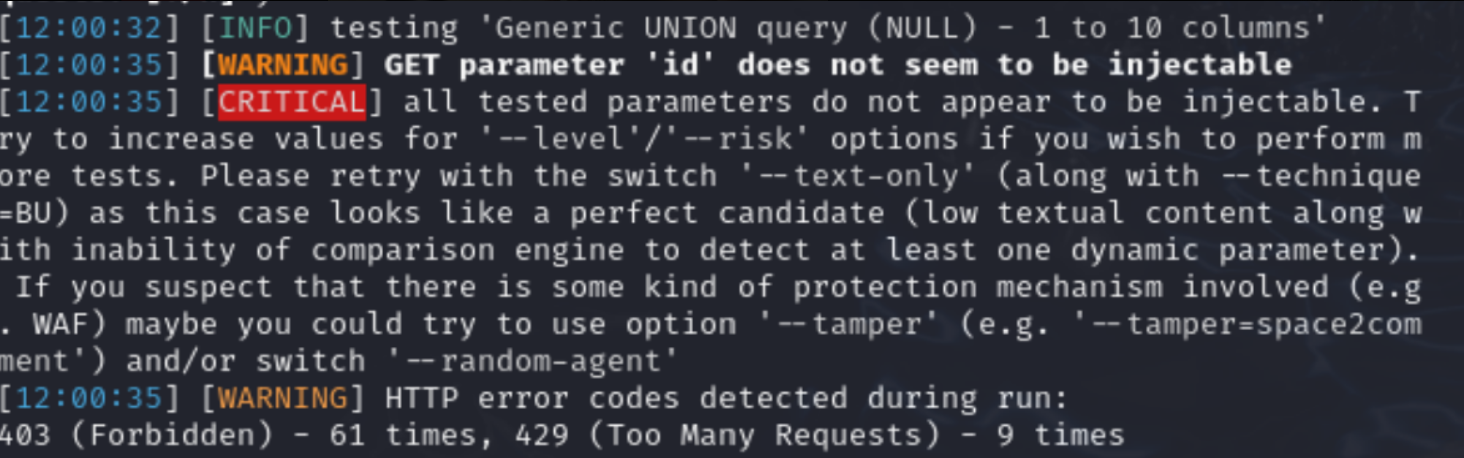
1. **Tests effectués**

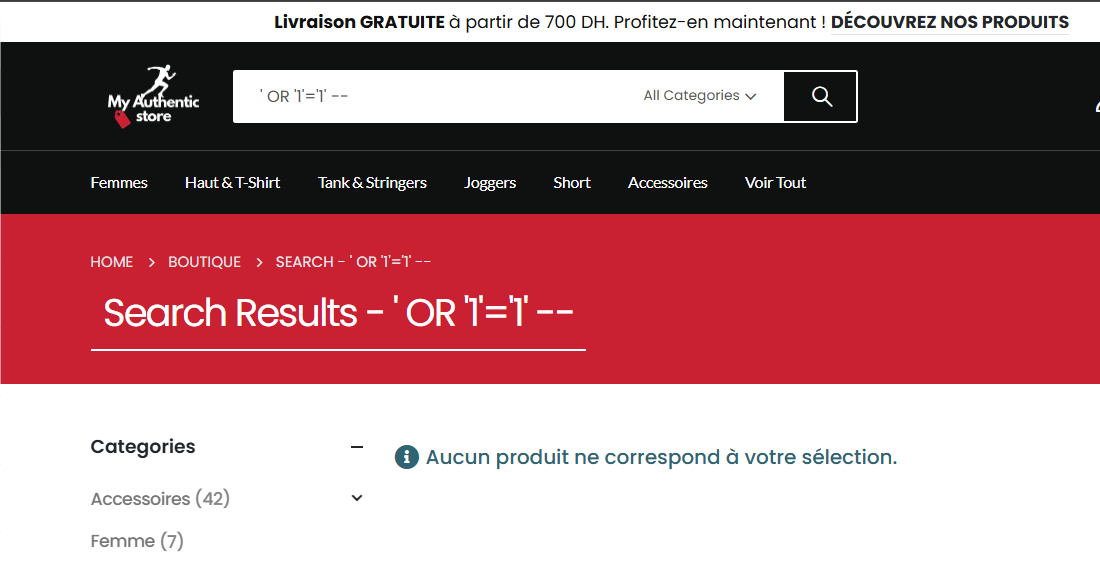
Faille XSS -> protégé

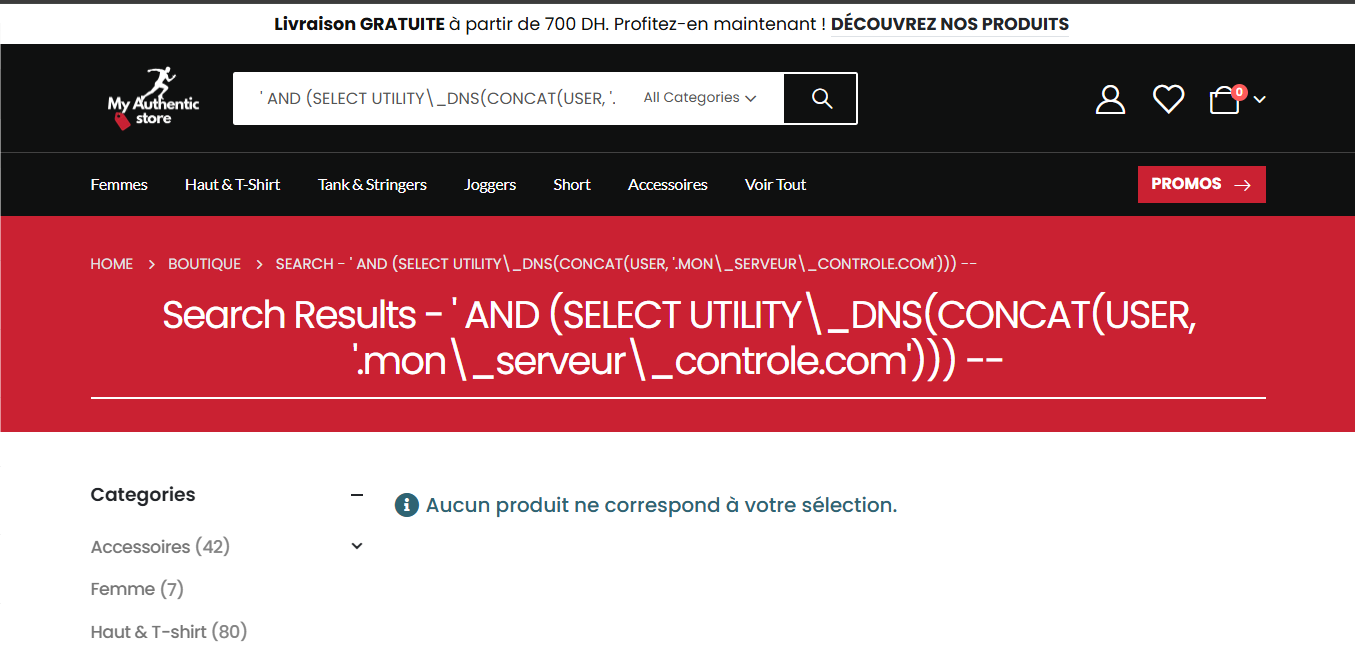


Injection SQL -> protégé

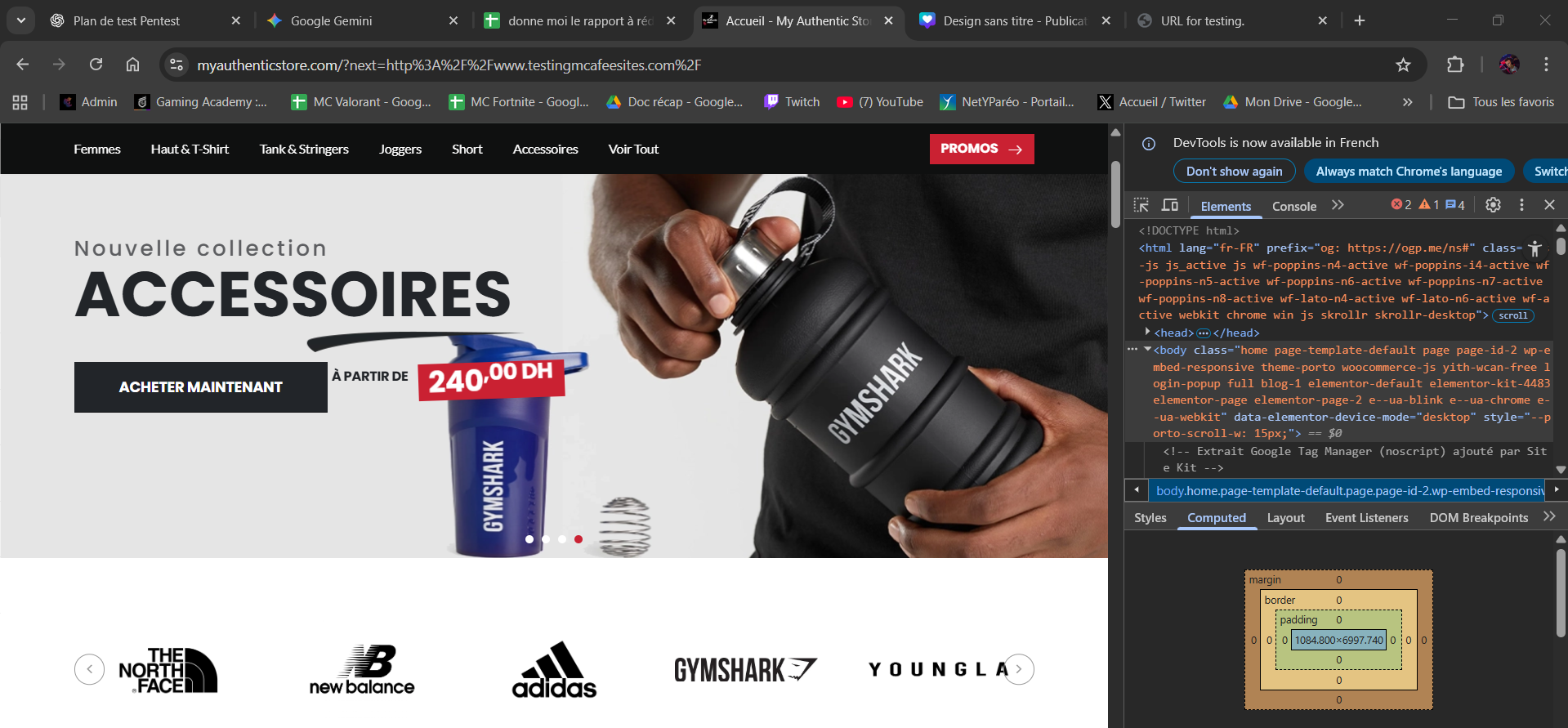




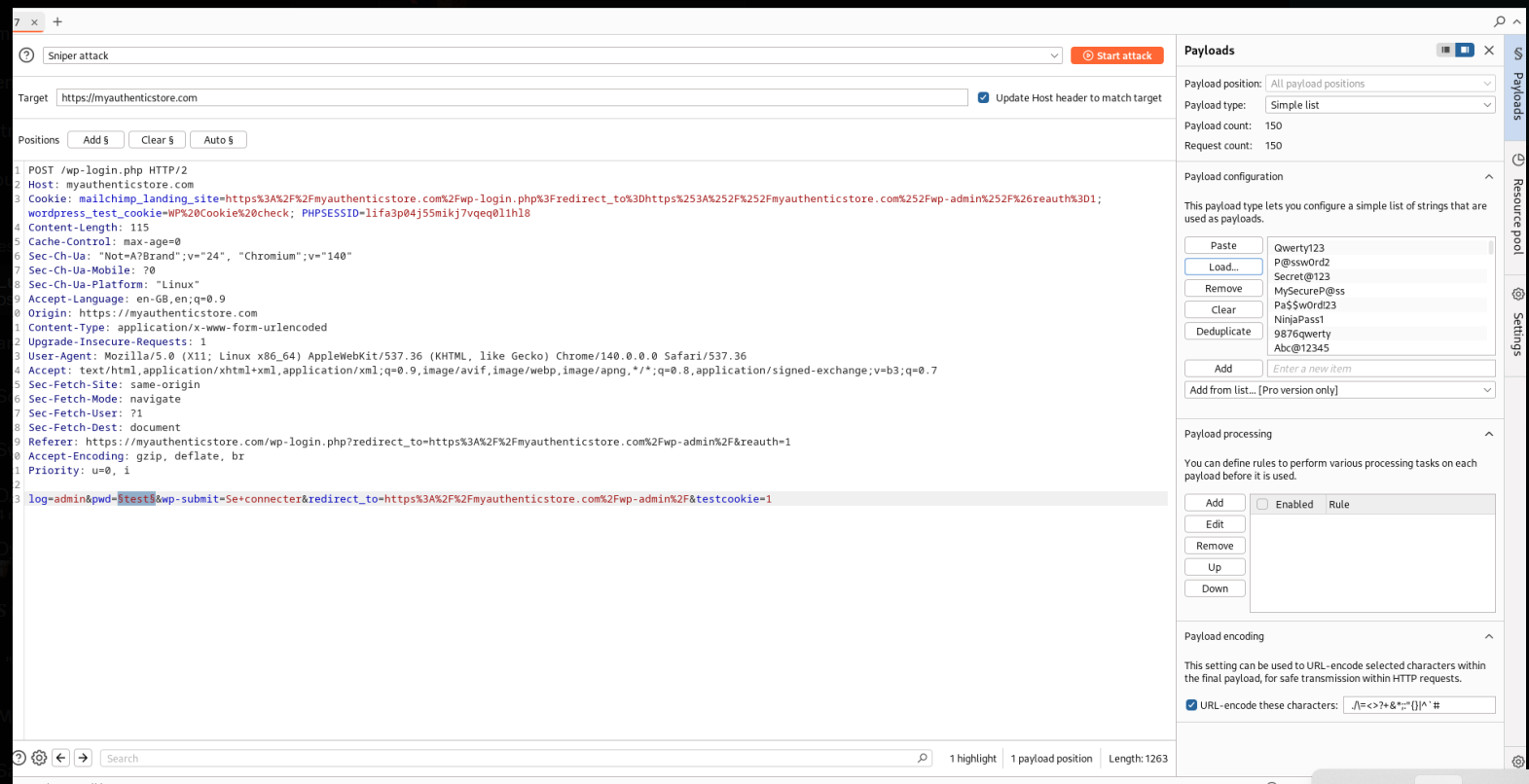


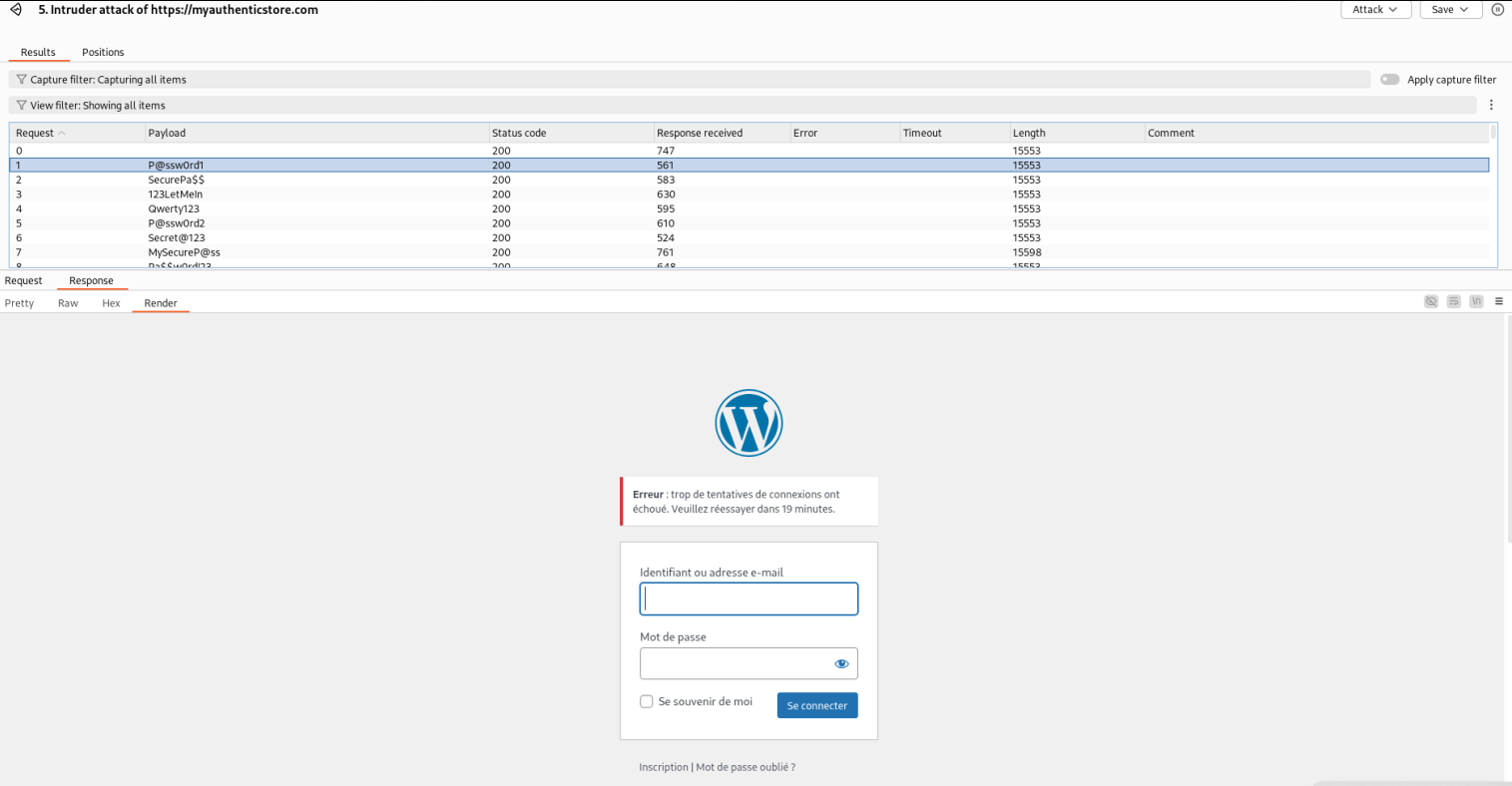


Faille redirection -> protégé



Bruteforce -> protégé





**Gestion de Session et Authentification :**

* Tester les formulaires de connexion WordPress et WooCommerce (Brute Force léger, Énumération d'utilisateurs). & idem reset MDP - Protégé

Fonctionnalités E-commerce (WooCommerce) – prix & commande - protégé