XSS – lab 2 – Juice Shop

Locatie: http://juiceshop.mblomme.be

Oefeningen 1 - XSS - niveau 1

- Welk voor de hand liggend zoekveld zou je kunnen gebruiken op de hoofdpagina?
- Werkt onze basis xss test? (<script>alert(1)</script>)
- Probeer de volgende **incomplete** xss:
  < iframe src="alert(xss)">
- Tips oefening 1:
  - Via welk element kunnen we items in de shop opzoeken.
- **Hint vda2:** <iframe src="**javascript**:alert('xss')">

Oefening 2 - XSS – niveau 2

- Log in met een willekeurige account of maak een nieuw account aan.
- Koop iets op de website.
- Probeer bij de order overview pagina een xss uit te voeren.
- Tips oefening 2:
  - Zoek naar een track id
  - XSS hoeft niet altijd via formulier elementen uitgevoerd worden.

Oefening 2 – Bonus – niveau 1

- Het hoeft niet altijd een alert boodschap te zijn zoals in de vorige oefening.
- Probeer volgende XSS (gebruik oortjes of stille speakers voor deze XSS)
  - <iframe width="100%" height="166" scrolling="no" frameborder="no" allow="autoplay" src="https://w.soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/771984076&color=%23ff5500&auto_play=true&hide_related=false&show_comments=true&show_user=true&show_reposts=false&show_teaser=true"></iframe>