

## XSS – lab 1 – Bwapp

### Oefeningen 1 – Reflected XSS – Get

[http://bwapp.mblomme.be/xss\\_get.php](http://bwapp.mblomme.be/xss_get.php)

Voer een reflected XSS aanval uit.

Welk voor de hand liggend zoekveld zou je kunnen gebruiken?

Welke basis XSS test hebben we gezien?

**Hint vda2:** `<script>alert(1);</script>`

### Oefening 2 - Reflected XSS – Post

[http://bwapp.mblomme.be/xss\\_post.php](http://bwapp.mblomme.be/xss_post.php)

Voer een reflected XSS aanval uit.

Uitdaging wanneer de oefening werkt:

Stel dat de inputvelden in de browser gefilterd worden op vreemde XSS aanvallen.

Via welke tool zou je dit kunnen omzeilen? Hoe komt dit?

### Oefening 2 – Persisted XSS -

[http://bwapp.mblomme.be/xss\\_stored\\_1.php](http://bwapp.mblomme.be/xss_stored_1.php)

Voer een persisted (stored) XSS aanval uit.

Test via een incognito tabblad of de oefening werkt.