DOM-Based XSS

- DOM-XX 跟前兩者最大的不同在於 DOM-Based 的攻擊要防護必須做在用戶端。
- 基於 JS 的利用
  - document.url, document.history, etc.
- 難出現、相當少見

怎麼測試

- 見縫插針；見框就插
- 修改隱藏欄位或者封包參數
- 修改 URL 參數
- 分析 JS