**EJERCICIOS XSS**

**Prerrequisitos**

**Kali Linux**

**OWASP BWE**

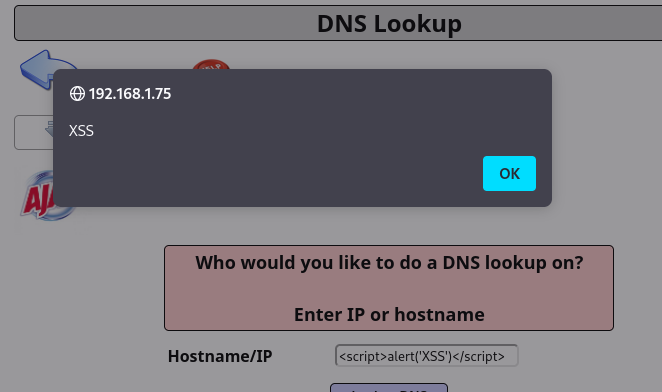
**Ejercicio 1 - Mutillidae**

**Realizar los ejercicios de XSS de la máquina Mutillidae:**

**OWASP 2013 -> A3 - Cross-Site Scripting (XSS) -> Reflected (First Order):**

**DNS Lookup**

Hay que introducir el siguiente payload en el campo de entrada: <script>alert('XSS')</script>.

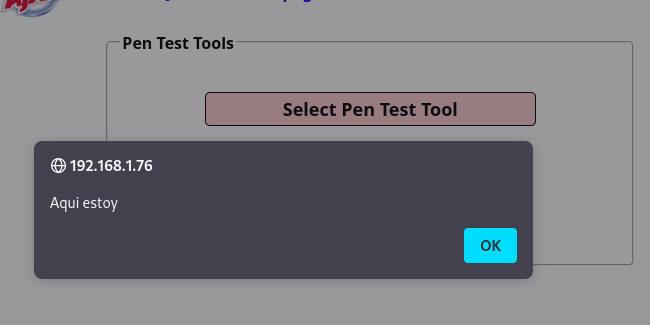


**Pen Test Tool Lookup**

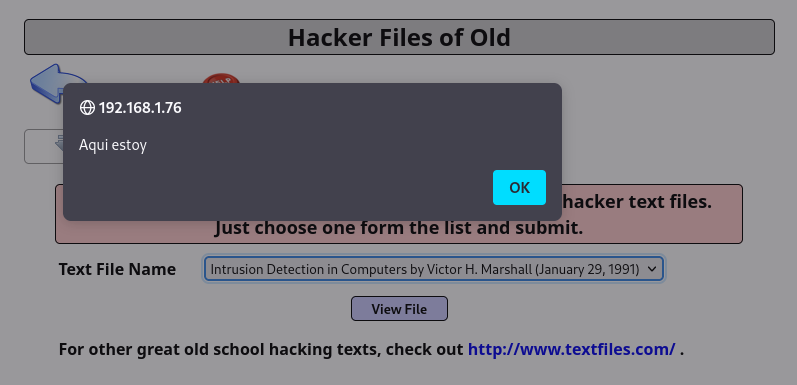
Introducir al final de cada URL el payload: %22%3E%3Cscript%3Ealert(%22Aqui%20estoy%22)%3C/script%3E

Por ejemplo en este ejercicio quedaría algo así:

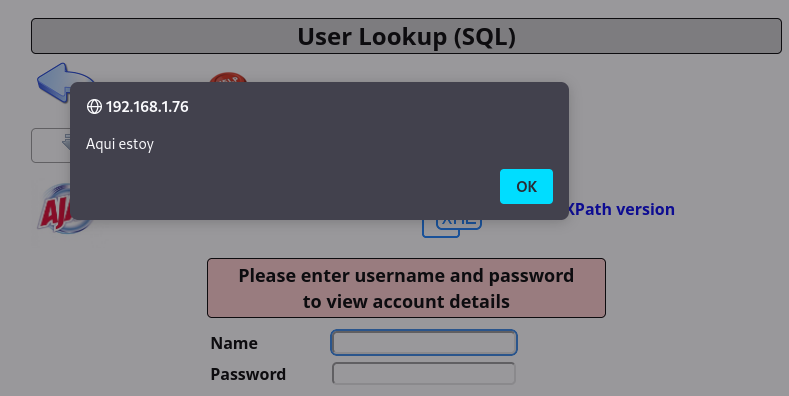
http://192.168.1.76/mutillidae/index.php?page=pen-test-tool-lookup.php%22%3E%3Cscript%3Ealert(%22Aqui%20estoy%22)%3C/script%3E



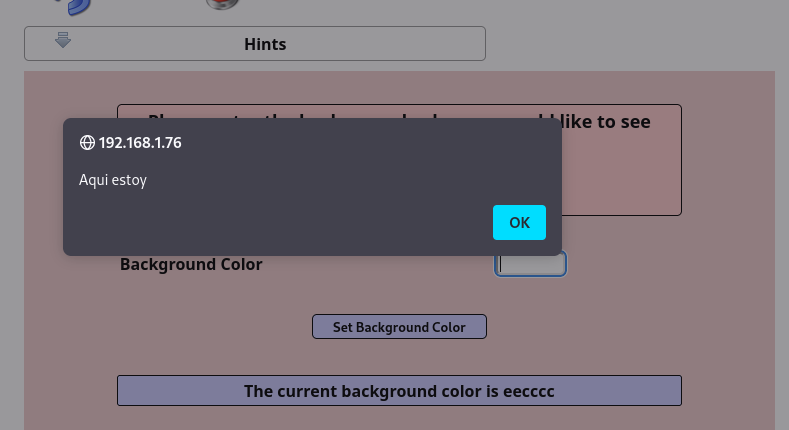
**Text File Viewer**

****

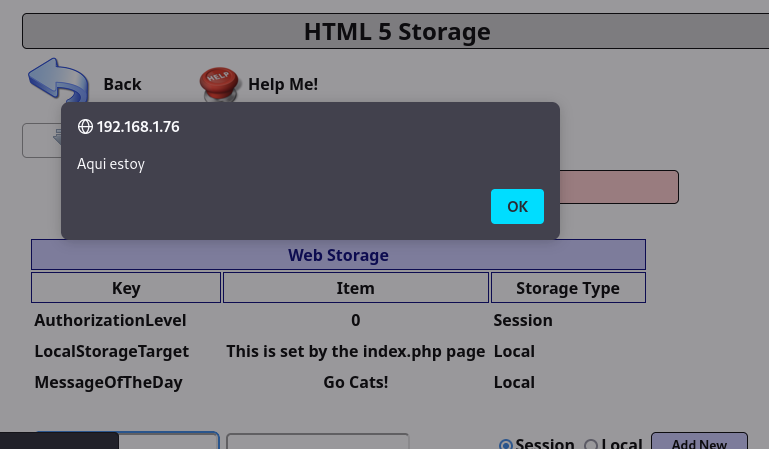
**User Info (SQL)**

****

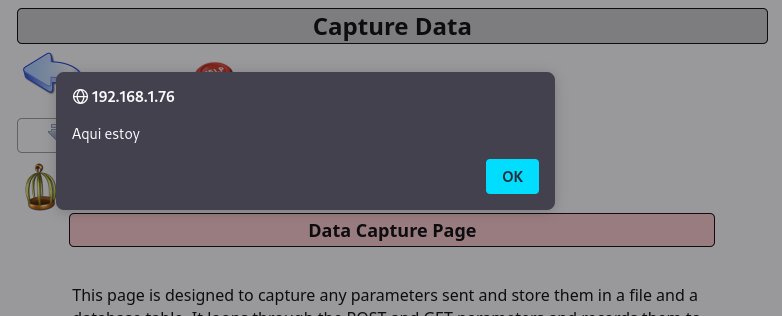
**Set Background Color**

****

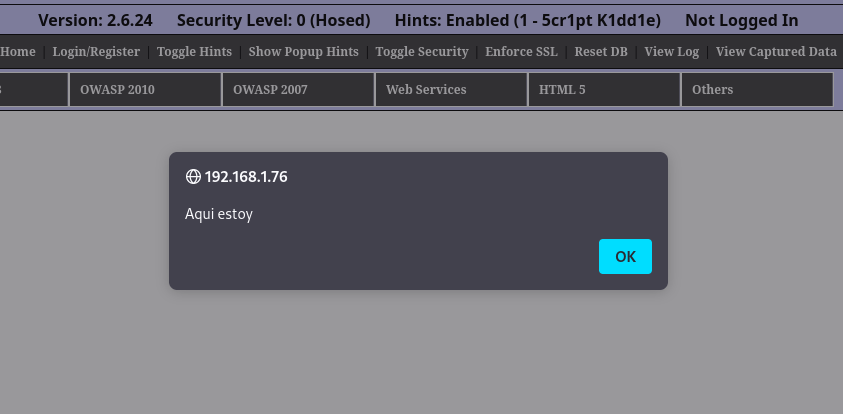
**HTML5 Storage**

****

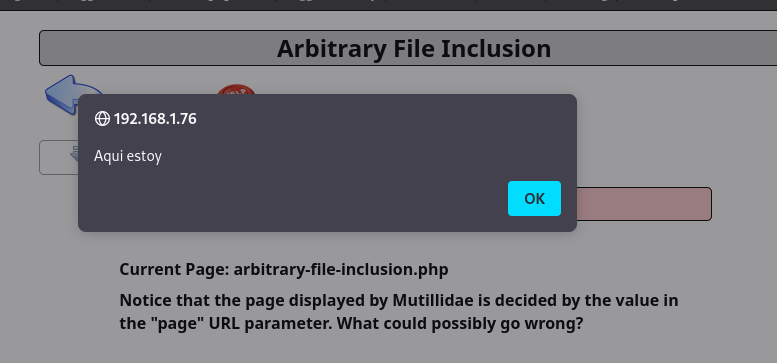
**Capture Data Page**

****

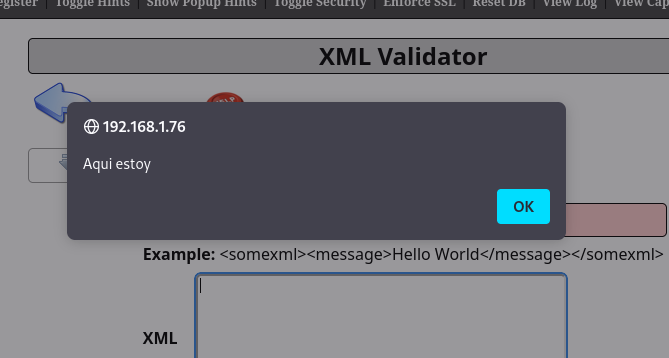
**Document Viewer**

****

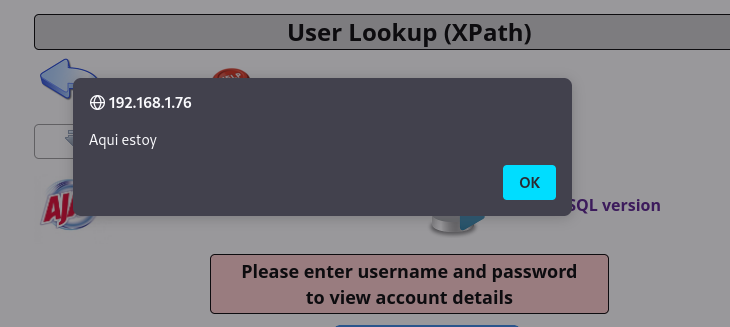
**Arbitrary File Inclusion**

****

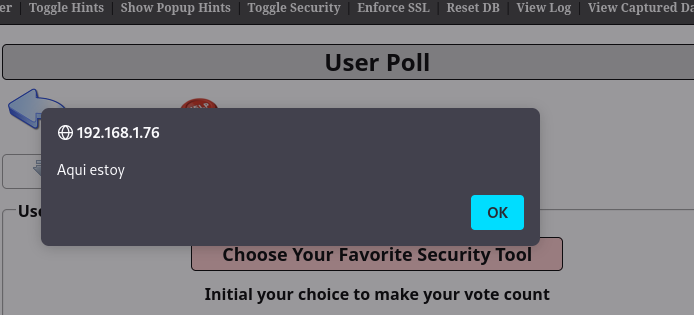
**XML Validator**

****

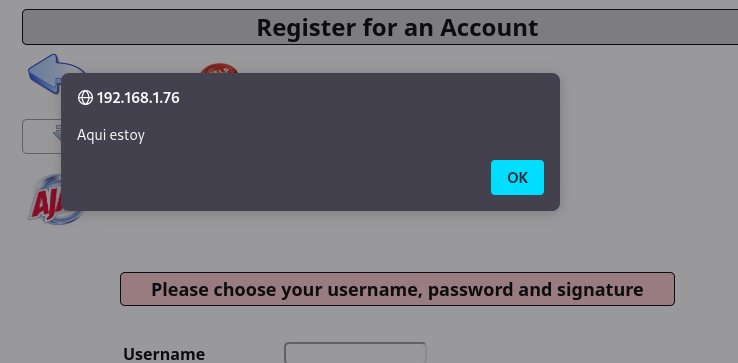
**User Info (XPath)**

****

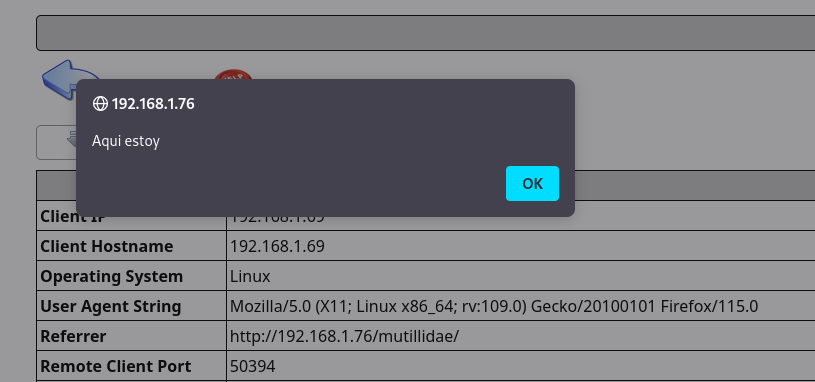
**Poll Question**

****

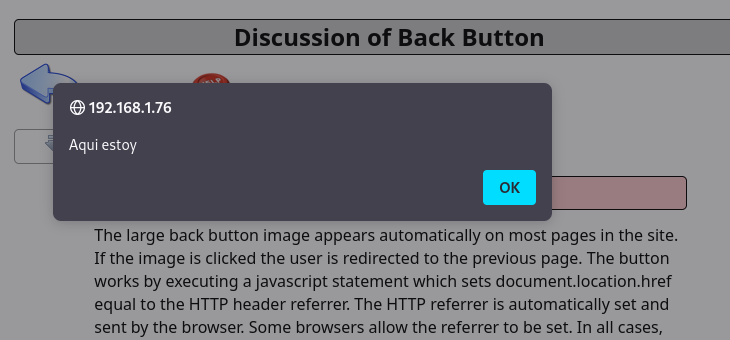
**Register User**

****

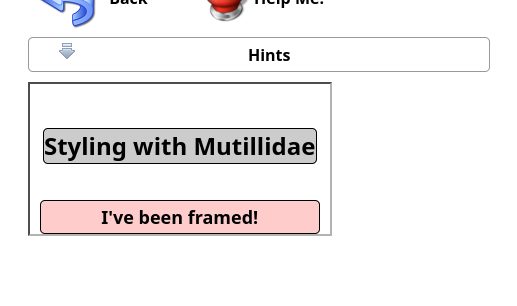
**Browser Info**

****

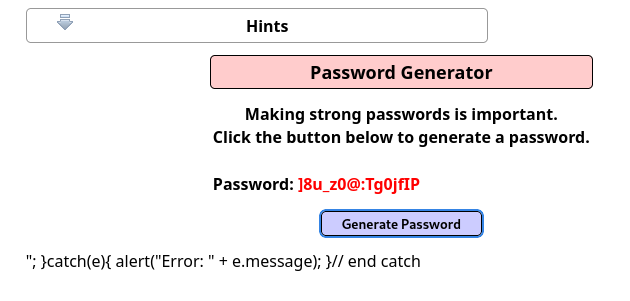
**Those "Back" Buttons**

****

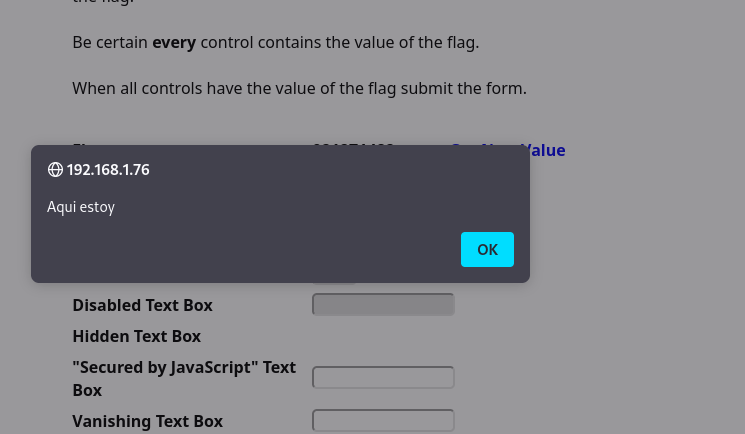
**Styling with Mutilidae**

****

**Password Generator**

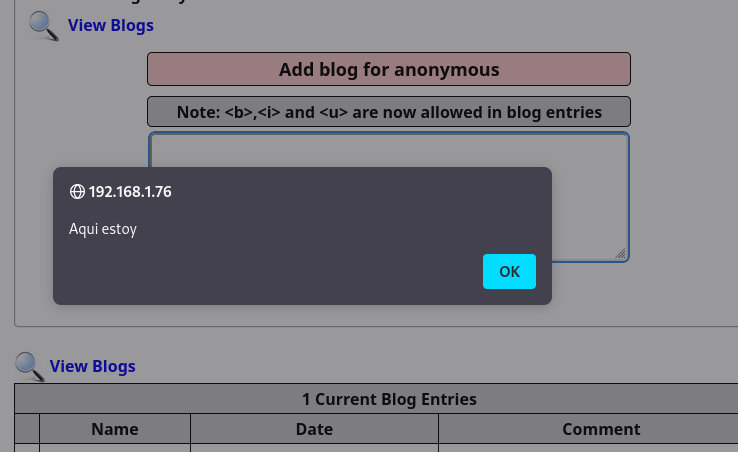
****

**Client-side Control Challenge**

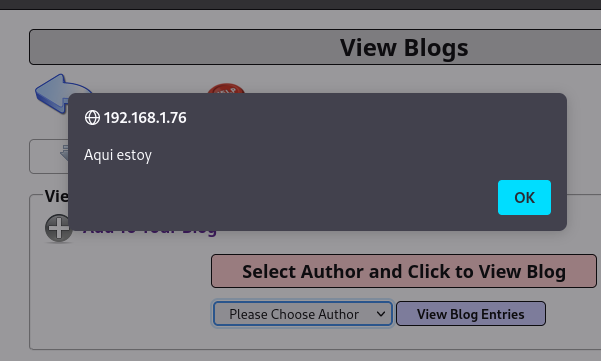
****

**OWASP 2013 -> A3 - Cross-Site Scripting (XSS) -> Persisted (Second Order):**

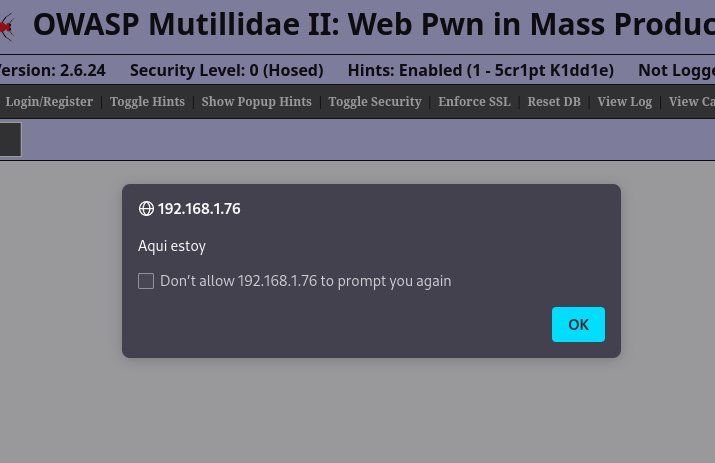
**Add to your blog**

****

**View someone's blog**

****

**Show log**

****