

Project 2: Detecting and Mitigating Cross-Site Scripting (XSS)

The image displays a web application interface on the left and the Burp Suite HTTP history and request details on the right.

Web Application Interface (bwAPP):

- Header: bwAPP an extremely buggy web app!
- Navigation: Bugs, Change Password, Create User, Set Security Level, Reset, Create...
- Section: / XSS - stored (Blog) /
- Form: A text input field containing "Hello world!". Below it are buttons for "Submit", "Add", "Show all", "Delete", and a status message "All your entries were deleted!".
- Table: A table with columns #, Owner, Date, and Entry. The first row shows an entry with #1, Owner "me", Date "2023-10-01", and Entry "Hello world!".

Burp Suite HTTP History:

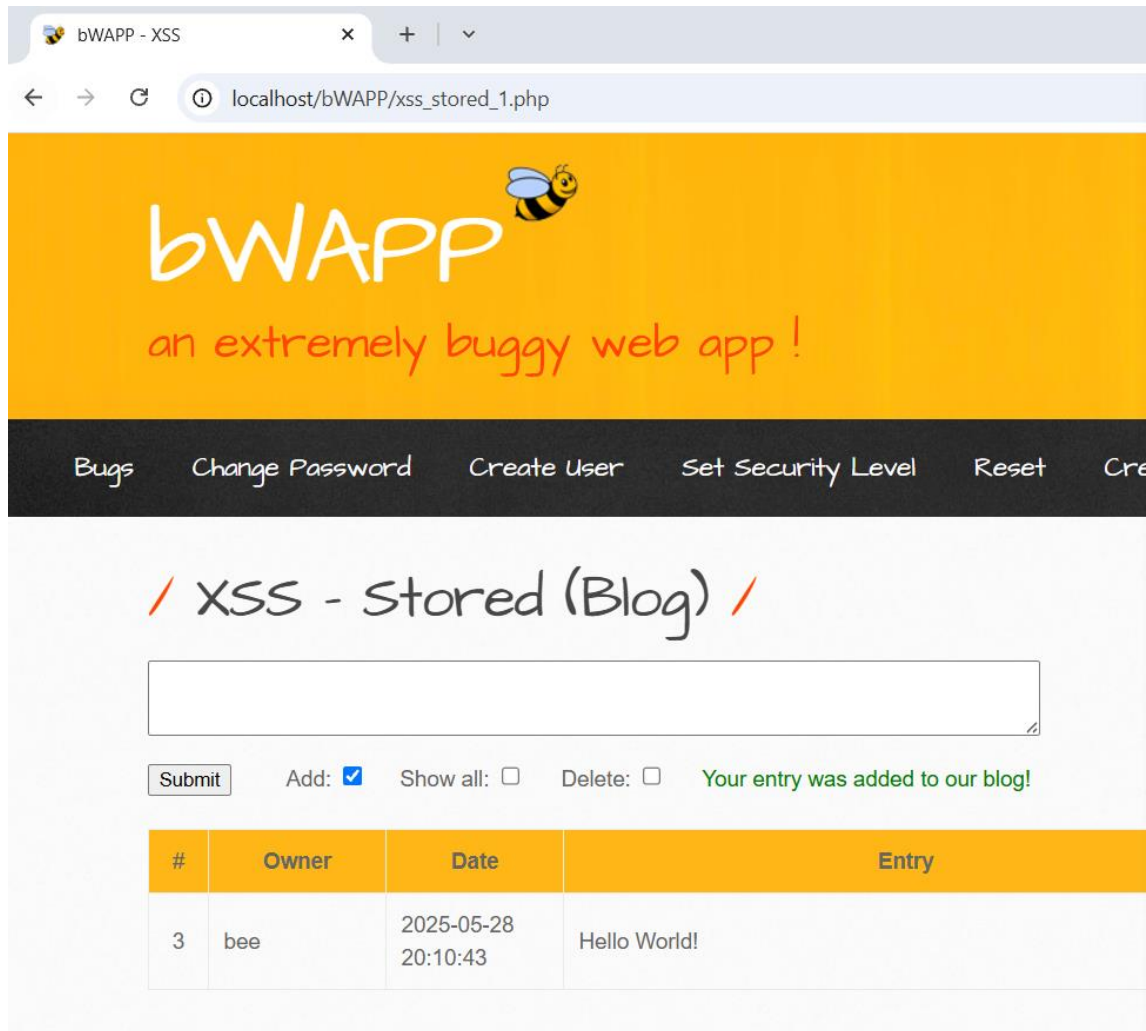
- Request to http://localhost:80 (127.0.0.1) /
- Method: POST
- URL: http://localhost/bwAPP/xss_stored_1.php

Request Details (Inspector):

```
POST /bwAPP/xss_stored_1.php HTTP/1.1
Host: localhost
Content-Length: 43
Cache-Control: max-age=0
sec-ch-ua: "Microsoft Edge", "Chromium", "v118"
sec-ch-ua-mobile: 0
sec-ch-ua-platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Referer: http://localhost/bwAPP/xss_stored_1.php
Cookie: security=low; PHPSESSID=mb5gip5bqce3yb335m0n; security_level=0
Connection: keep-alive
entry=Hello+World!&blog=submit&entry_add=
```

The request body parameters are visible in the Inspector:

Name	Value
entry	Hello World
blog	submit
entry_add	



Intercept request with Burp Suite and modify with XSS payload

