

/ XSS - stored (Blog) /

Add: ☒Show all: ☐Delete: ☐

All your entries were deleted!

#	Owner	Date	Entry
---	-------	------	-------

Giao diện trang web cho gửi một đoạn code vào database

Vì có vẻ input nhận vào là string nên ta sẽ thêm ">" để đóng tag hiện tại, sau đó thêm đoạn xss inject vào.

Thử với payload "><script>alert(1)</script>"

98nm-80.vlab.uit.edu.vn/bWAPP/xss_stored_1.php

...d043f68c909fa877f521f2-0-js6k98nm-80.vlab.uit.edu.vn says

1

OK

Kết quả inject thành công như hình trên.