שלבים בניצול stored XSS

[bWAPP - XSS](http://localhost/xss_stored_1.php)

reset

1. מכניסים ערך כלשהו ל FORM
2. בודקים מה קורה עם submit:
   1. GET (REFLECTED)
   2. POST
3. האם ה INPUT שלנו חוזר בלי שום ולידציה:
   1. הכנסנו > חוזר >
   2. מכניסים script שגונב cookie
4. מגדירים עוד יוזר עבור התוקף
5. מקימים שרת לוקלי של התוקף:

Python –m http.server 8000

1. נכנסים לבלוג עם היוזר של הקורבן
2. אם יש שם את ה XSS שהכנסנו קודם, אז נקבל את ה cookie בשרת של התוקף