Name: Akshat Gupta

Registration Number: 18BIT0330

Project Review: 3

Title: OWASP Attacks and Vulnerability Assessment - *XSS Attacks*

GitHub Repo: https://github.com/akshatvg/Vulnerability-Testing-Solutions

Project Explanation Video: https://bit.ly/NasscomReview3

Review 3 Implementation Video: https://bit.ly/StoredXSSakshatvg

Team C:

Individual performance analysis for OWASP attacks:

- ***Compare your system developed for a particular attack and its variants prevention with the existing research techniques. Which mechanism from which research paper has been taken for preventing attacks for your system.***

  1) The Stored XSS Attack in level 6 was taken from the first research paper from review 1 as both the system models were the same.
  2) They suggested to escape all HTML, CSS and JavaScript attributes before performing any new operation and hence in each level I either removed the script tags as a whole or used regular expressions or removed the starting of the tag and even replaced common attack queries and words with blank strings.
  3) Preventing attacks by using server specific functions like *htmlspecialchars()* in case of PHP to sanitise the strings was inspired by the paper 4 from my review 1 document.
  4) The 5th research paper from review 1 is a very good future scope for this project as it can help eliminate the Stored XSS threats even though it is very tough to implement.

- ***Analyse the various performance parameters like execution time for identifying an attack and prevention and also other parameters given in the research papers with your system for a specific attack.***

  1) The execution time as well as detection of these attacks takes not more than a few seconds.
  2) Whenever someone is trying to attack and steal info or do something, if it takes more than 4.5 seconds to load, the user gets suspicious and leaves the page.
  3) If an antivirus or preventive measure can't even find and prevent an attack within 3 seconds, it's considered to be incapable of being helpful to large MNCs and projects.

4) Only Stored XSS manipulates the browser contents even for later whereas DOM Based and Reflected XSS don't and hence Stored XSS is more dangerous and has longer lasting effects.

- ***Identify what could be the other efficient possible mechanisms to overcome the attacks for a specific variant. Give links from where these information is obtained.***

1) N- Stalker, Acunetix, Paros, Hackbar and XSS ME are some tools to be used for detection of XSS vulnerabilities.
2) Also, escape all HTML, CSS and JavaScript attributes before performing any new operation.
3) Replacing keywords used for attacks is another mechanism for preventing any kind of XSS attacks.
4) Using default server specific functions is another prevention mechanism to sanitise strings.
5) Using regular expressions to find and replace scripts and on error callbacks is the last suggested prevention mechanism.

Links:

- ***https://ieeexplore.ieee.org/document/7813770***
- ***https://www.researchgate.net/publication/315365856_XSS_vulnerability_assessment_and_prevention_in_web_application***
- ***https://owasp.org/www-community/attacks/xss/***