Tutorial No. 7

Title: XSS

Roll No.: 16010420075 **Tutorial No.: 7**

Aim:

1. XSS (3 Types) on DVWA
2. Document any one recent XSS vulnerability attack or disclosure

\

Resources: virtual box

Theory

Cross-Site Scripting (XSS) assaults are injection attacks in which malicious scripts are inserted into otherwise trustworthy and innocent websites. XSS attacks occur when an attacker utilizes a web application to transmit malicious code to a separate end user, usually in the form of a browser side script. The flaws that allow these attacks to succeed are common and can be found whenever a web application accepts user input in its output without verifying or encoding it.

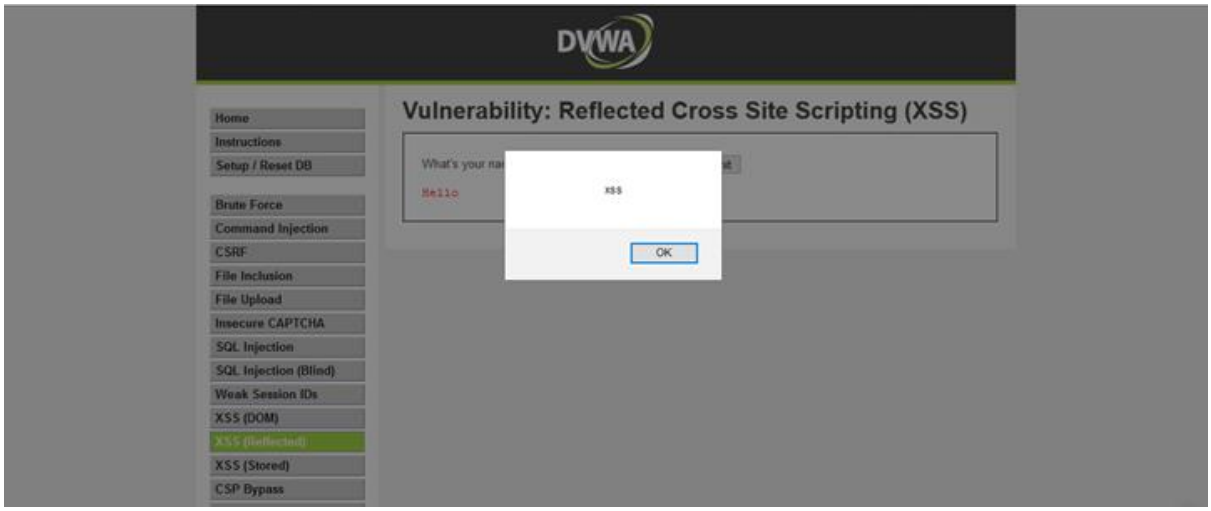
XSS can be used by an attacker to send a malicious script to an unwitting user. The browser of the end user has no means of knowing that the script should not be trusted and will run it nonetheless. The malicious script can access any cookies, session tokens, or other sensitive information stored by the browser and used with that site since it believes the script came from a trusted source. These programs can even rewrite the HTML page's content.

IMPLEMENTATION AND RESULTS:

XSS

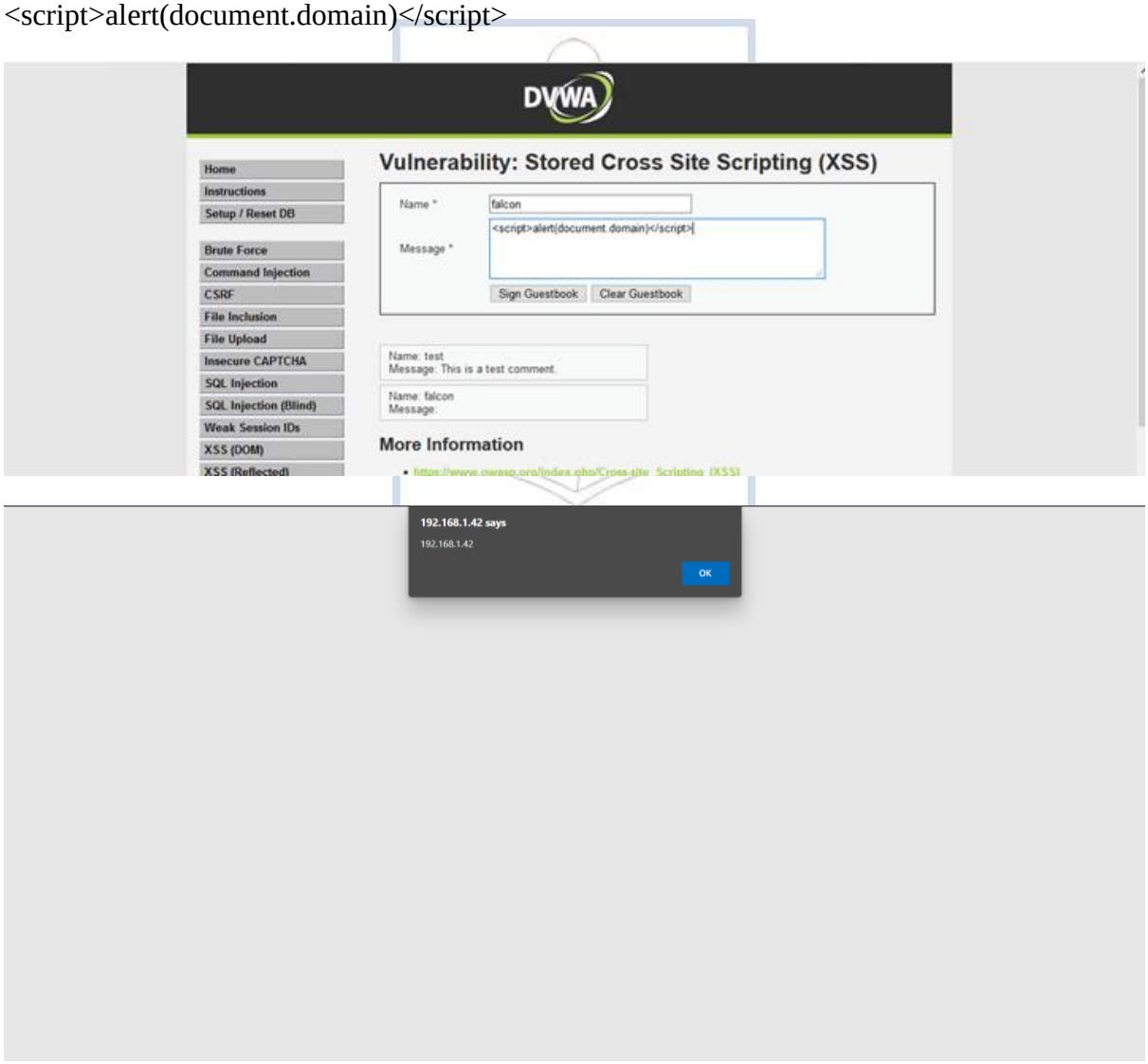
Type 1 (Reflected):

<script>alert(“XSS”)</script>

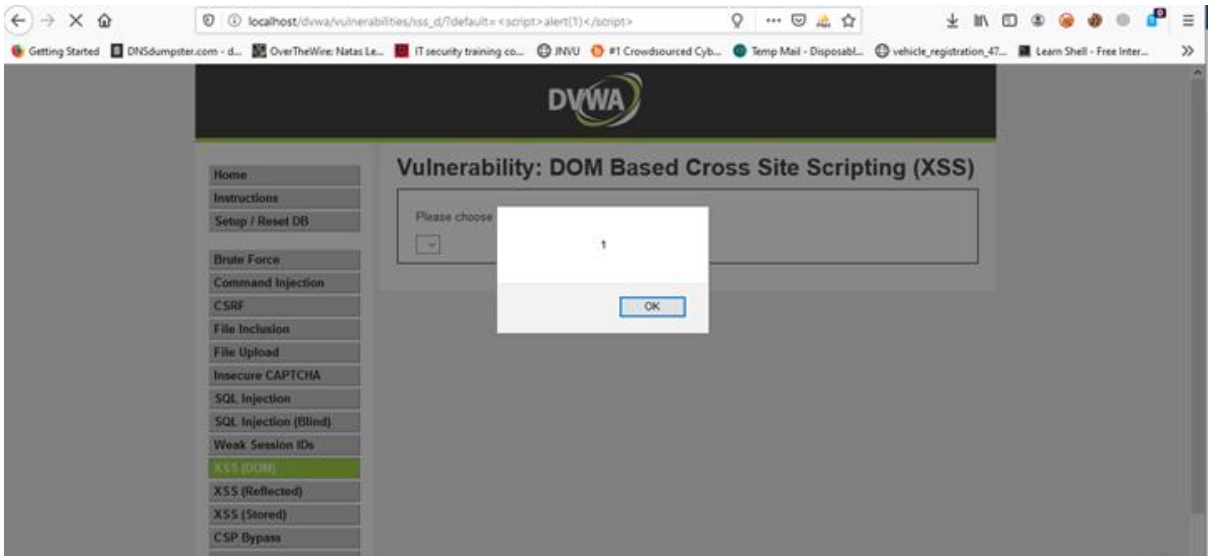


Type 2 (Stored):

<script>alert(document.domain)</script>



Type 3 (DOM):



Recent Vulnerability Attack:

Microweber, an open-source website builder and content management system, has a stored cross-site scripting (XSS) vulnerability, according to security researchers (CMS).

The security flaw, identified as CVE-2022-0930 by researchers James Yeung and Bozhidar Slaveykov, was fixed in Microweber version 1.2.12.

The issue developed as a result of flaws in older versions of Microweber's content filtering measures.

Because of these flaws, attackers could upload an XSS payload as long as it contained a file ending in 'html' — a category that encompasses far more than simply plain.html files.

Once this payload has been uploaded, a URL containing malicious HTML and malicious JavaScript can be visited and executed.

An attacker could grab cookies before impersonating a victim, potentially the administrator of a compromised system, by controlling a script that runs in the victim's browser.

Outcomes:

CO-3: Understand attack methodology

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

Cross side scripting was performed on DVWA and a report of recent XSS vulnerability was documented.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

REFERENCES:

- www.dvwa.com