**DATE: 13TH January 2023**

**NAME: DHAVALKUMAR VIJAYKYMAR PATEL**

**CLASS: M.Sc. CS SEM-1**

**ENROLLMENT NO: 032200300002034**

**QUESTION / PROBLEM: TO PERFORM CROSS-SITE SCRIPTING IN DVWA IN HIGH , LOW MEDIUM**

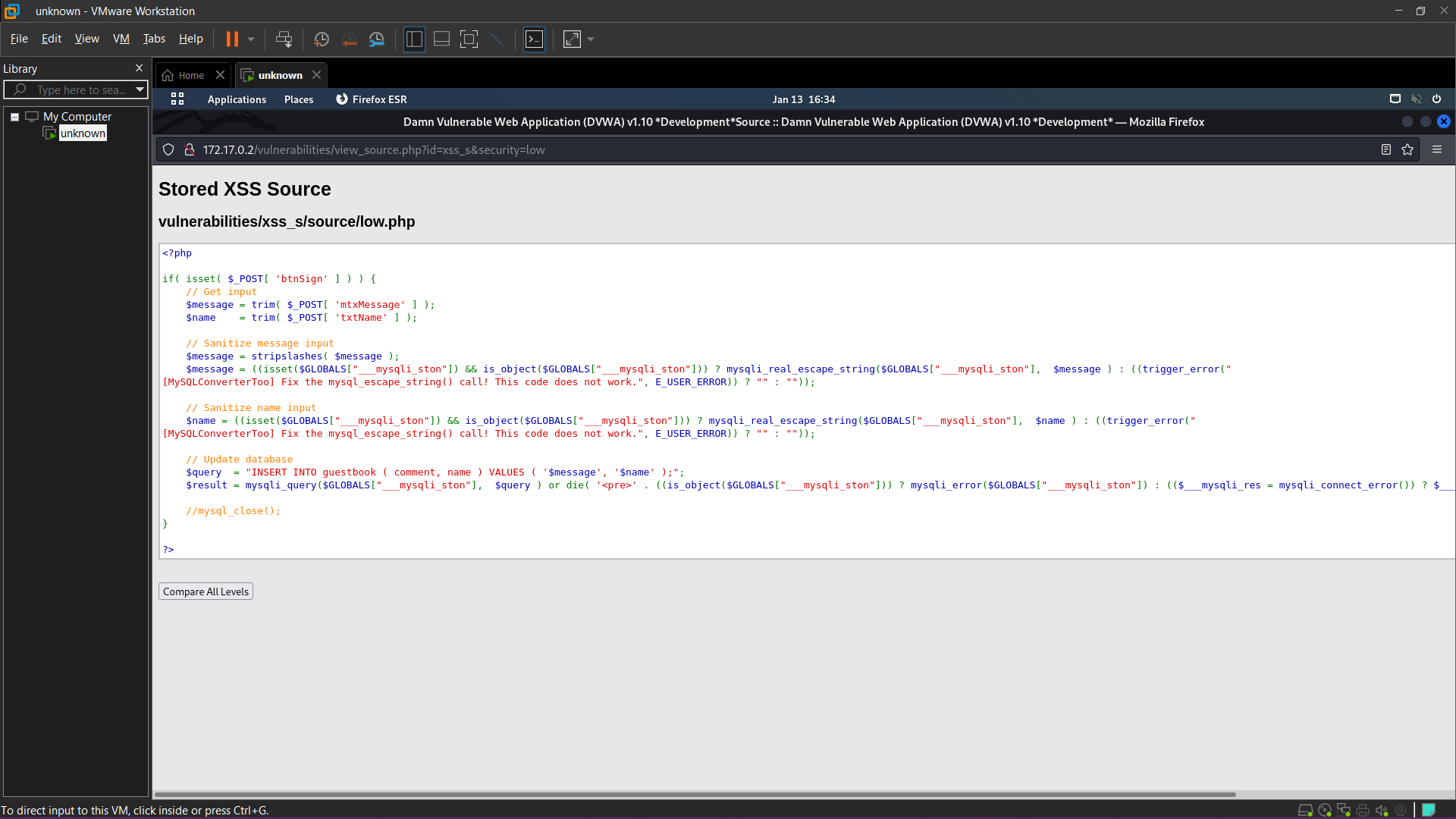
**SECURITY CONTROLL.**

Cross site scripting is a type of injection in which attacker inject a malicious script into the benign and trusted website. It accrues when attacker uses a web application to send malicious code in the form of a browser side script to a different user. Cross site scripting is a common vulnerability found in a web application.

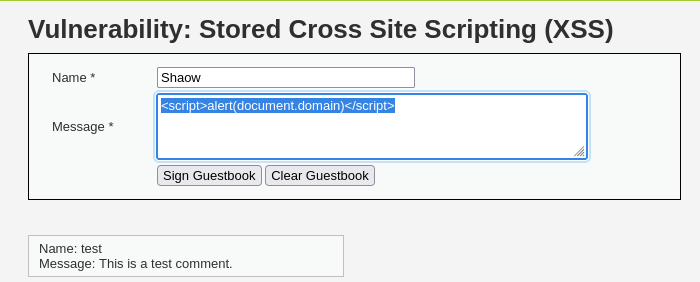
Stored XSS is the most dangerous cross-site scripting vulnerability. This type of vulnerability arises whenever a web application stores user-supplied data for later use in the backend without performing any filter or input sanitization. Since the web application does not apply any filter therefore an attacker can inject some malicious code into this input field. This malicious code can also be a valid XSS payload. So whenever any person visits the vulnerable page where malicious code is injected he will get a popup on his browser window. This will prove that the given webpage is vulnerable to Stored XSS vulnerability.

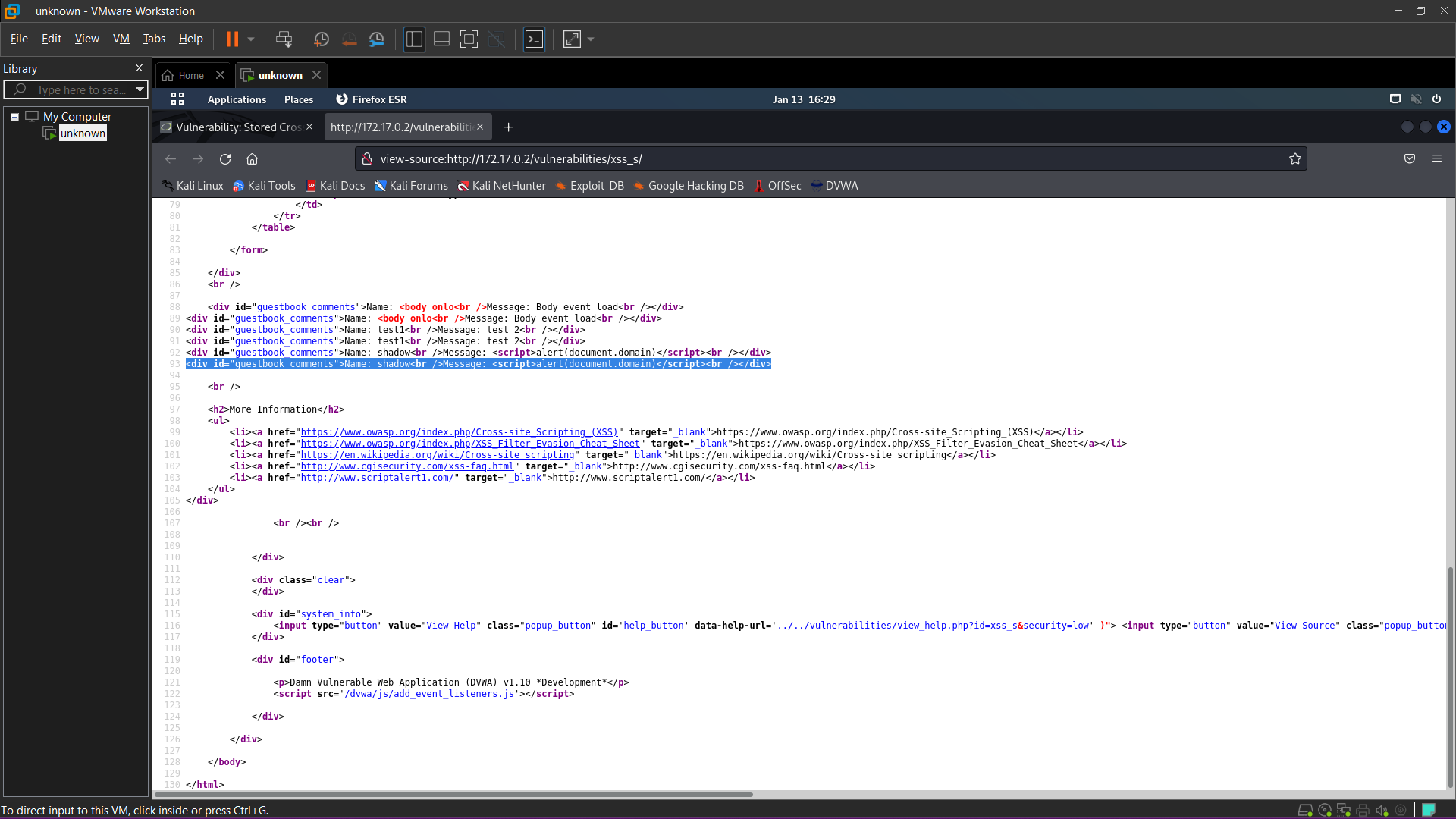
**SECURITY LEVEL: LOW**

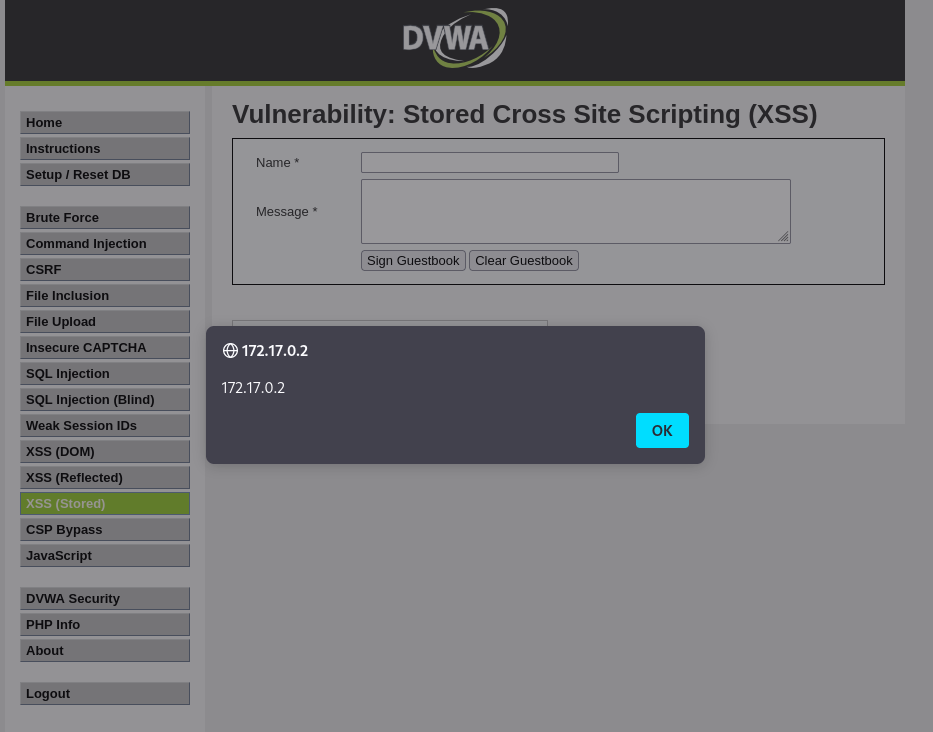
**Low level will not check the requested input before including it to be used in the output text.**

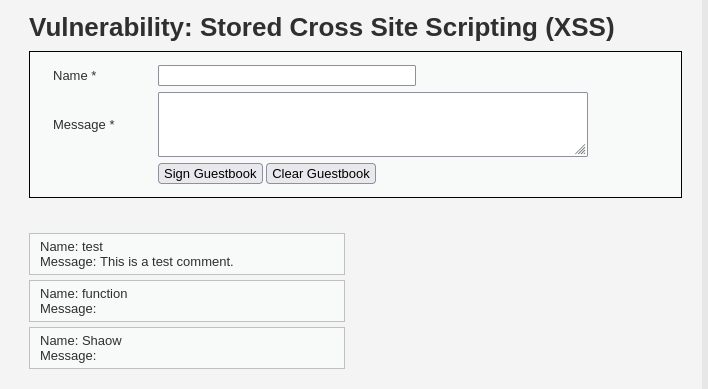


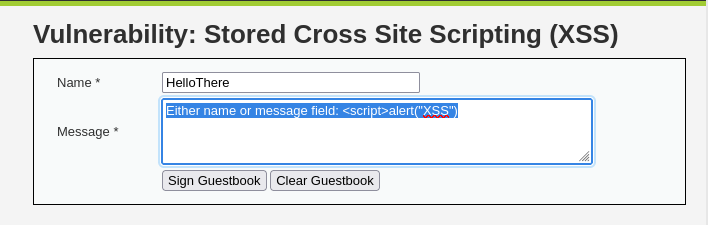
**<script>alert(document.domain)</script> (return a domain)**

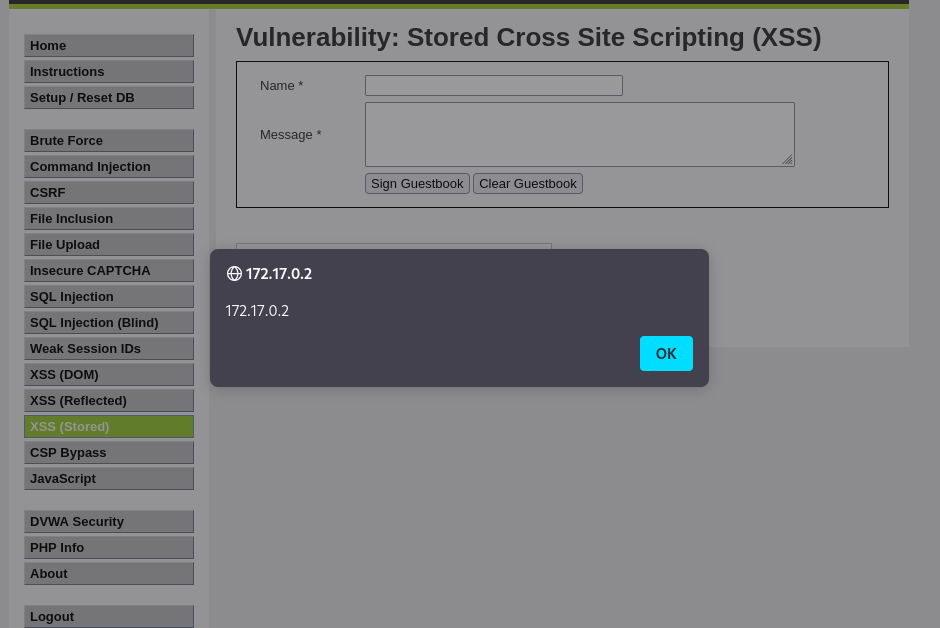
****

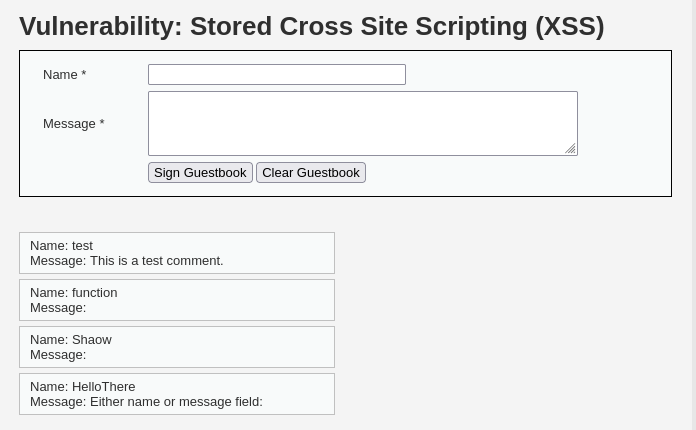


****

****

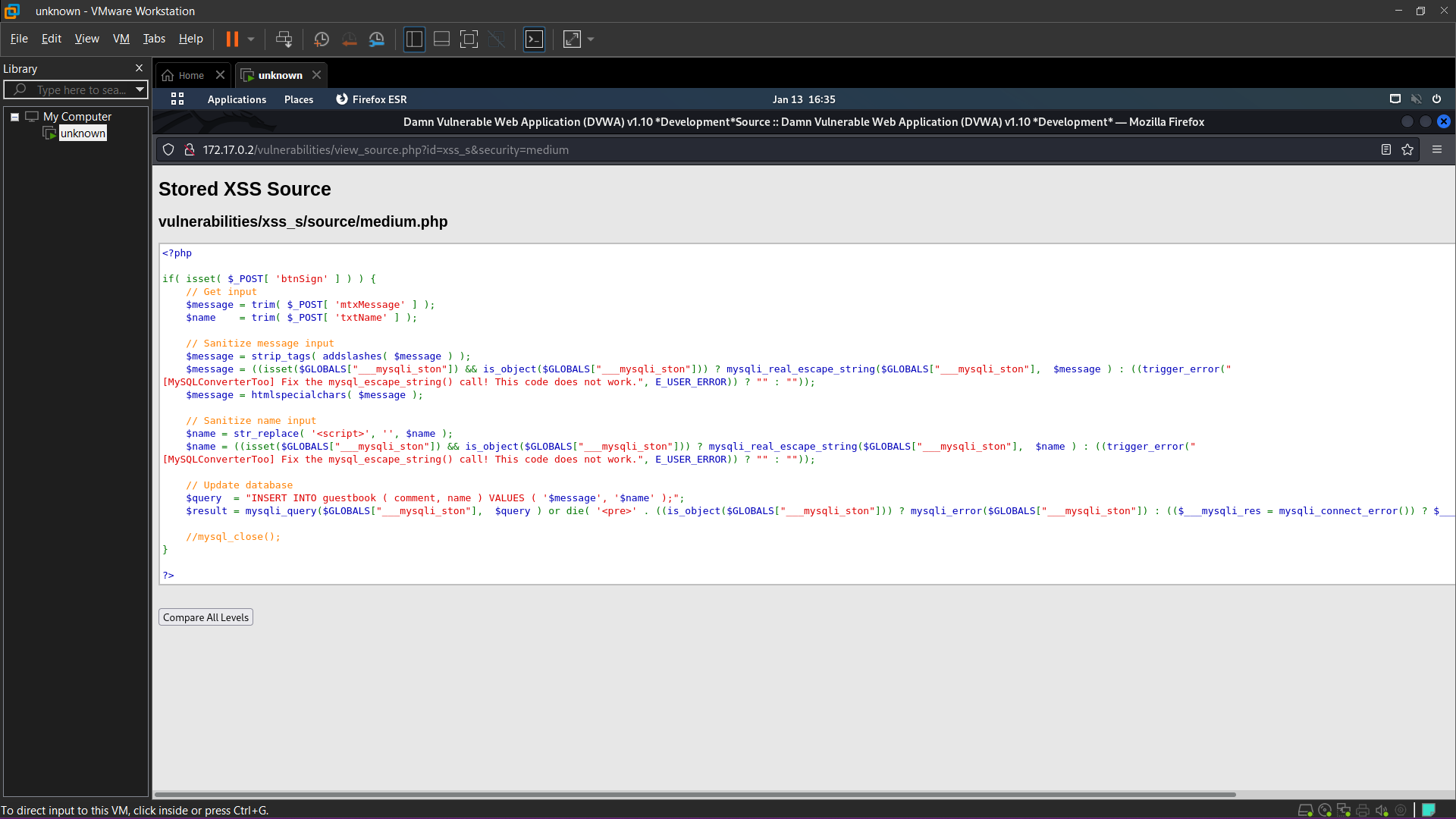
****

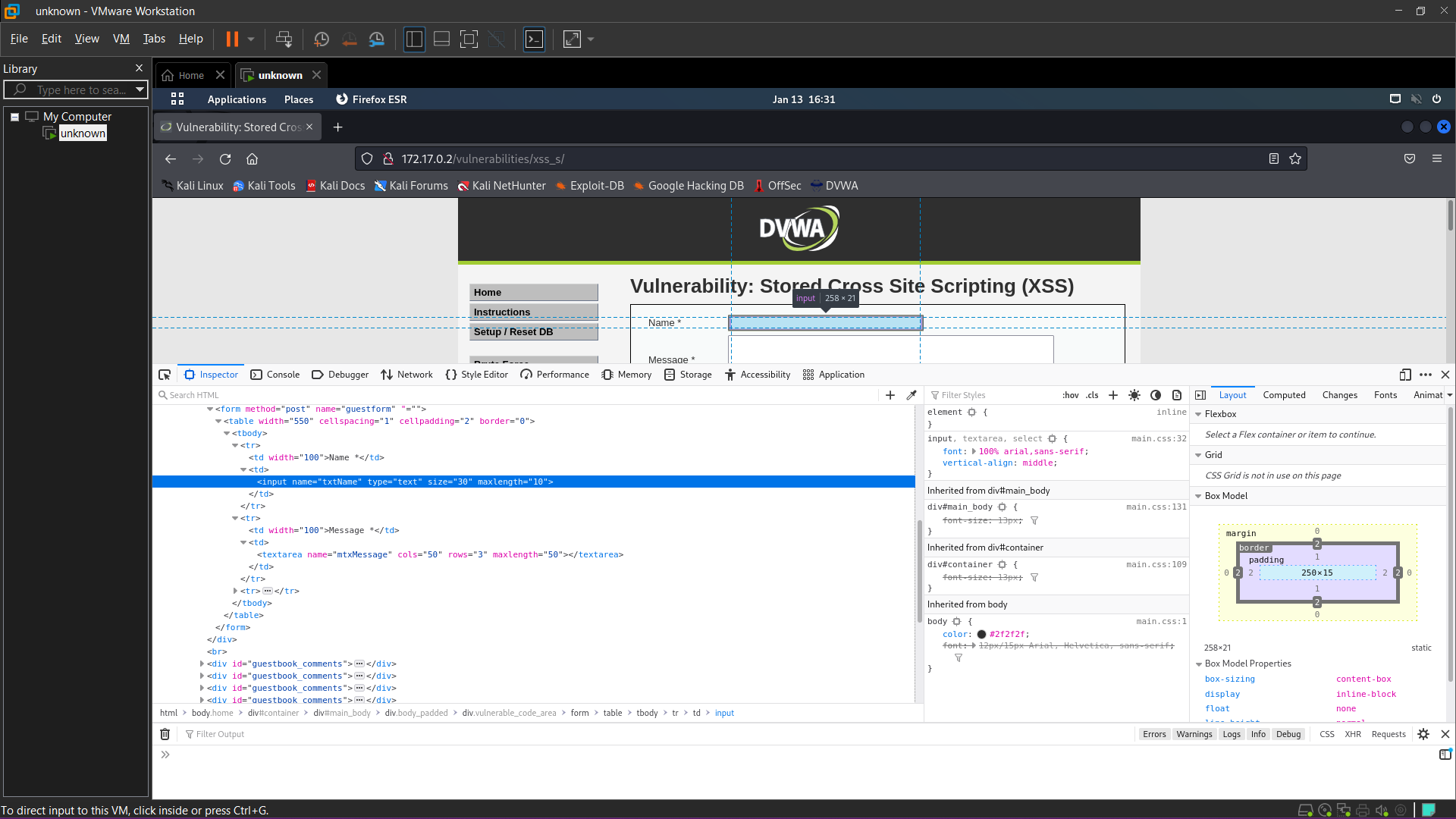
****

****

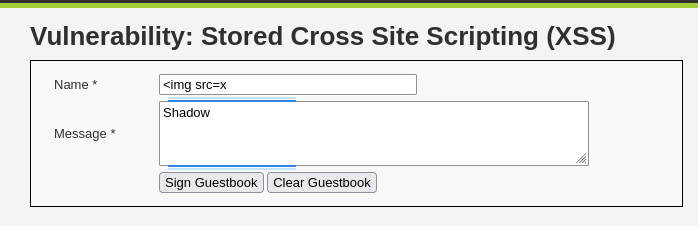
**SECURITY LEVEL: Medium**

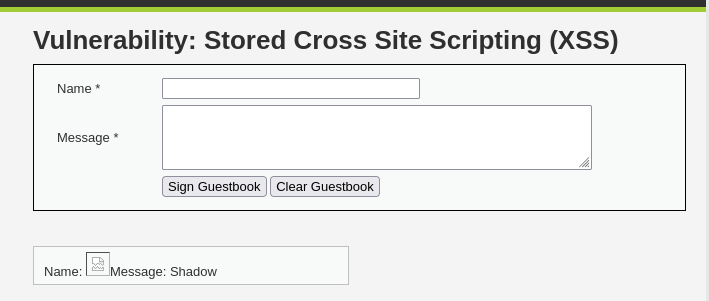
**The developer had added some protection, however hasn't done every field the same way.**





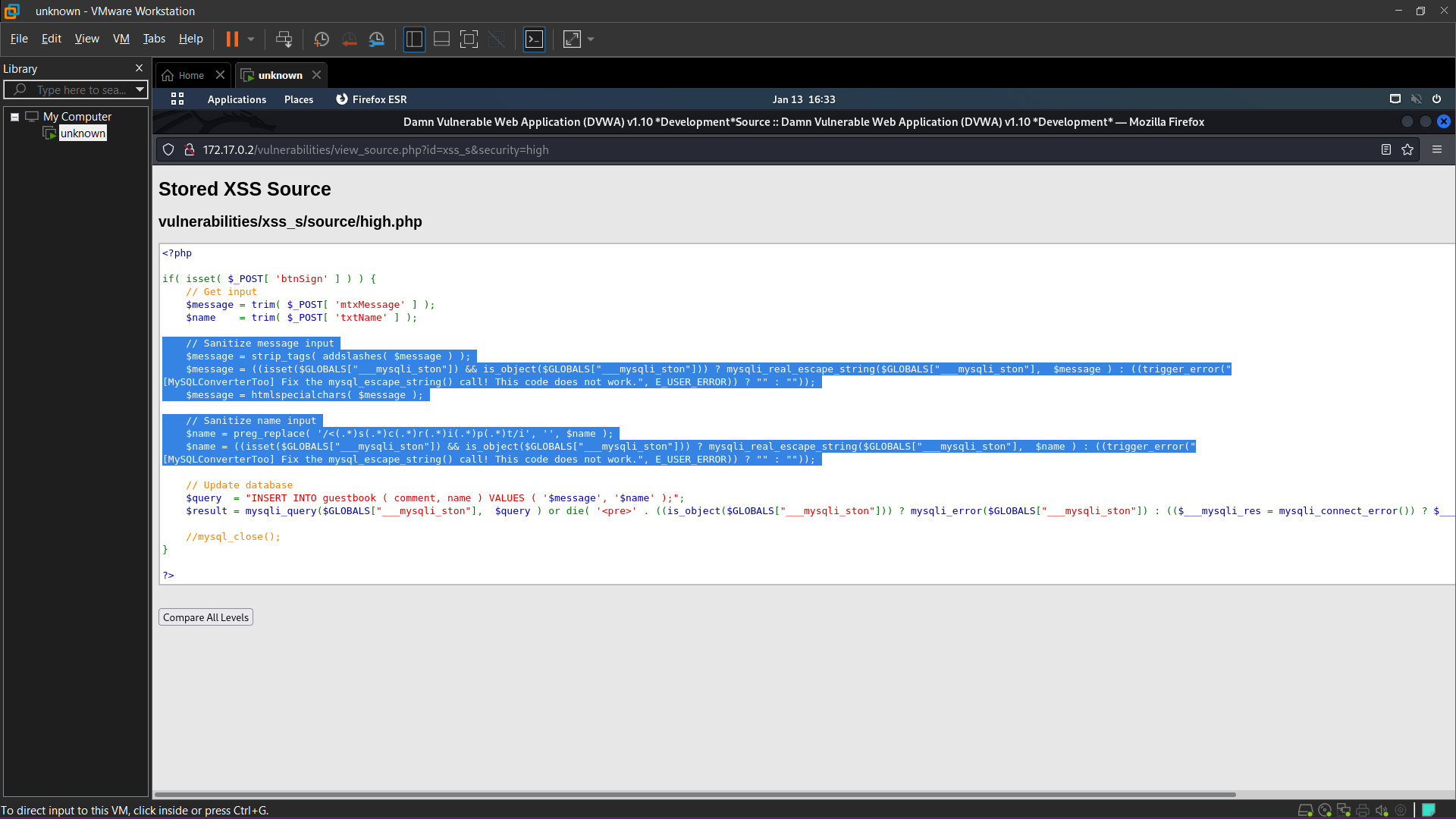
**<img src=x onerror=alert(document.domain)>**

****

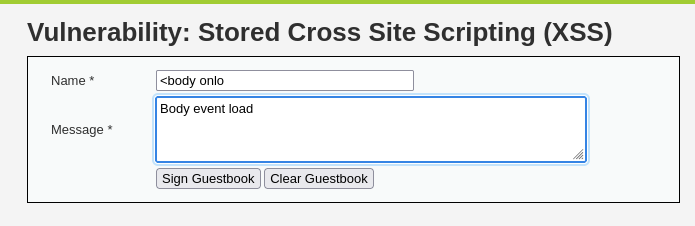
****

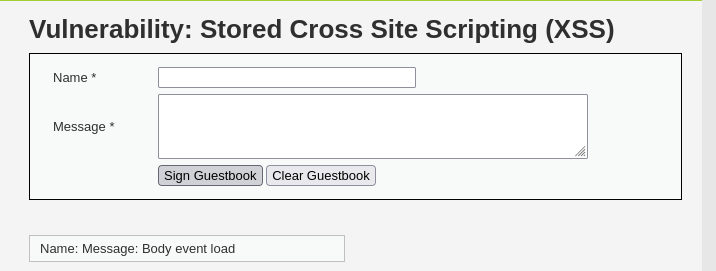
**SECURITY LEVEL: High**

**Allow HTML events**



**<body onload=alert(“bingo”)>**

****

****