./ Vitthal S.github.io

View on GitHub

Hello Guys,

This is a short post to illustrate how I discovered my first CVE and how the process is much simpler than I first imagined.

My target was to get CVE assigned on my name no matter what product is, So I started crawling CVE website and gathered couple of products which was having CVEs patched in recent months which includes products like CMS, etc. After downloading couple of products I installed first product Hoteldruid 3.0.2 which is hotel management application. After analyzing the application I started to check if I can intercept the request in burp proxy and I configured a system proxy and I was able to intercept the traffic in my Burp proxy. Later I crawled the application and and intercepted the request and added special characters to check the handling mechanism and I found my input was getting reflected in response. I have then inserted a XSS payload and observed javascript got executed, and yeah I have a CVE-2021-38559 on my name.

Details of the Vulnerability

>> Product Name : Hoteldruid developed by DigitalDruid.Net
>> Product Version : 3.0.2
>> Fixed product version : [hoteldruid version 3.0.3 (August 20, 2021)]

>> Vulnerability Name : Reflected Cross Site Scripting

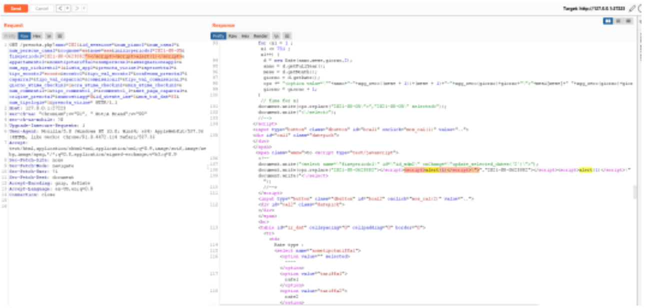
>> Description: Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

>> Vulnerable URL : `http://localhost:<PORT>/prenota.php?anno=2021&id_sessione=&num_piano1=&num_casa1=&num_persone_casa1=&cognome=ss&nome=sss&inizioperiodo1=2021-08-05&fineperiodo1=2021-08-0623882%22%3E%3C/script%3E%3Cscript%3Ealert(1)%3C/script%3E&appartamento1=&nometipotariffa1=&numpersone1=&assegnazioneapp1=&num_app_richiesti1=1&lista_app1=&prenota`

>> Vulnerable Parameter : `fineperiodo1`

>> Steps to Reproduce :

>> Change the Port & Open the above URL in browser
>> Observe the javascript execution



>> Impact :

>> steal credentials
>> steal secrets that are stored in JS variables.
>> display text that seems to come from the site owners. Think phishing.
>> display a password input, log keystrokes, and send the result to a site of your choosing

Thank you for reading, Happy Hacking!