(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :08/05/2023
(21) Application No.202311032528 A
(43) Publication Date : 09/06/2023

(54) Title of the invention : SYSTEM AND METHOD FOR DETECTING AND MITIGATING EXECUTE AFTER REDIRECT VULNERABILITIES

(51) International classification	:F42D 050450, G06F 215500, G06F 215700, H04L 675630, H04R 012400
(86) International Application No Filing Date	:PCT// :01/01/1900
(87) International Publication No	: NA
(61) Patent of Addition to Application Number Filing Date	:NA :NA
(62) Divisional to Application Number Filing Date	:NA :NA

(71)**Name of Applicant :**
1)Chitkara University
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ----------- -----------
2)Bluest Mettle Solutions Private Limited
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)MISHRA, Rahul
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ----------- -----------
2)SINGH, Dhiraj
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ----------- -----------
3)SHARMA, Bhanu
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ----------- -----------

(57) Abstract :

The present disclosure relates to a system (100) to detect and mitigate Execute After Redirect (EAR) vulnerabilities in web applications. The system (100) includes a processor and memory that store executable instructions for receiving requests from unauthenticated users to access content, redirecting them to a login page to obtain an authenticated session, and intercepting the redirected requests before the login page is loaded. The intercepted requests are then analyzed to identify if they contain sensitive content intended for authenticated users. Based on this analysis, the system determines if the requests are susceptible to an EAR exploit and transmit notifications to a computing device regarding the presence of an EAR vulnerability. The system also prevents execution of the remaining part of the login page after redirection, mitigating the EAR vulnerability to protect against potential exploitation and compromise of the web applications.

No. of Pages : 29 No. of Claims : 8