

Assingment 2

The screenshot shows the ZAP (Zed Attack Proxy) interface. The 'Alerts' tab is selected, displaying 15 alerts. The first alert is expanded, showing details about a 'Vulnerable JS Library'. The URL is https://ginandjuice.shop/resources/js/angular_1-7-7.js. The risk is High, confidence is Medium, and the parameter is unspecified. The attack is identified as a CSRF token absence. The evidence points to AngularJS v1.7.7 and CWE ID 1395. The WASC ID is also listed. The source is Passive (10003 - Vulnerable JS Library (Powered by Retire.js)). The input vector is described as 'The identified library appears to be vulnerable.' Other info notes that the identified library angularjs, version 1.7.7 is vulnerable. A tooltip window titled 'Kuvakaappaustyökalu' provides additional context: 'Näytökuva kopioitu leikepöydälle' (Screenshot copied to clipboard), 'Tallennettu automaattisesti Näytökuvat-kansioon.' (Automatically saved to the Screenshots folder), and a 'Merkitse ja jaa' (Mark and Share) button.

Haavoittuvuus löytyi.

Kyllä, korjaisin tämän. ZAP luokittelee riskin korkeaksi, ja vanhentuneiden komponenttien käyttö on yksi yleisimmistä reiteistä, joita hyökkääjät käyttävät sivuston murtamiseen, joten sen jättäminen korjaamatta olisi huolimatonta.