Summary:
This study gives a general overview of Cross-Site Scripting (XSS) vulnerabilities, investigates frequently used testing tools, describes the testing scope, displays the findings of XSS testing, and offers suggestions for reducing XSS risks.

Introduction:

A common web security flaw called cross-site scripting (XSS) enables attackers to insert malicious scripts into web sites that other users are viewing. These scripts have the ability to compromise the integrity of web applications, hijack user sessions, and steal confidential data.

Tools Used:

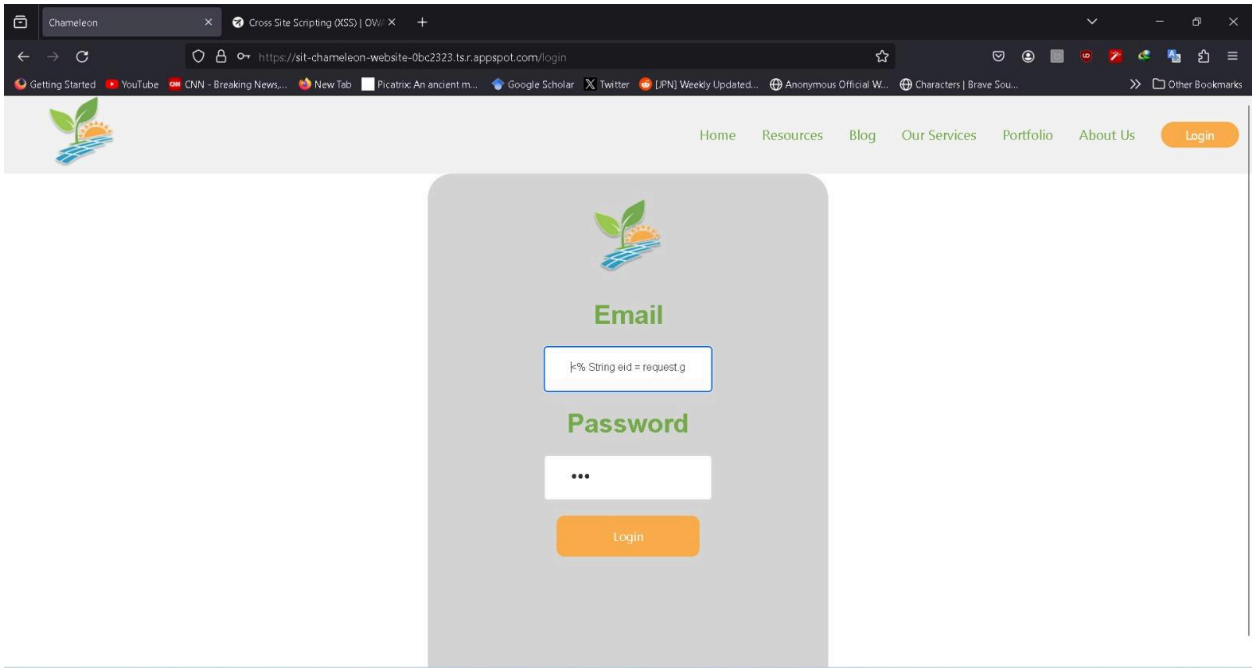
- **Burp Suite:** An all-inclusive web vulnerability scanner with tools especially made to find cross-site scripting (XSS) vulnerabilities.
- **OWASP ZAP:** An open-source security tool called OWASP ZAP (Zed Attack Proxy) can be used to identify XSS vulnerabilities in online applications.

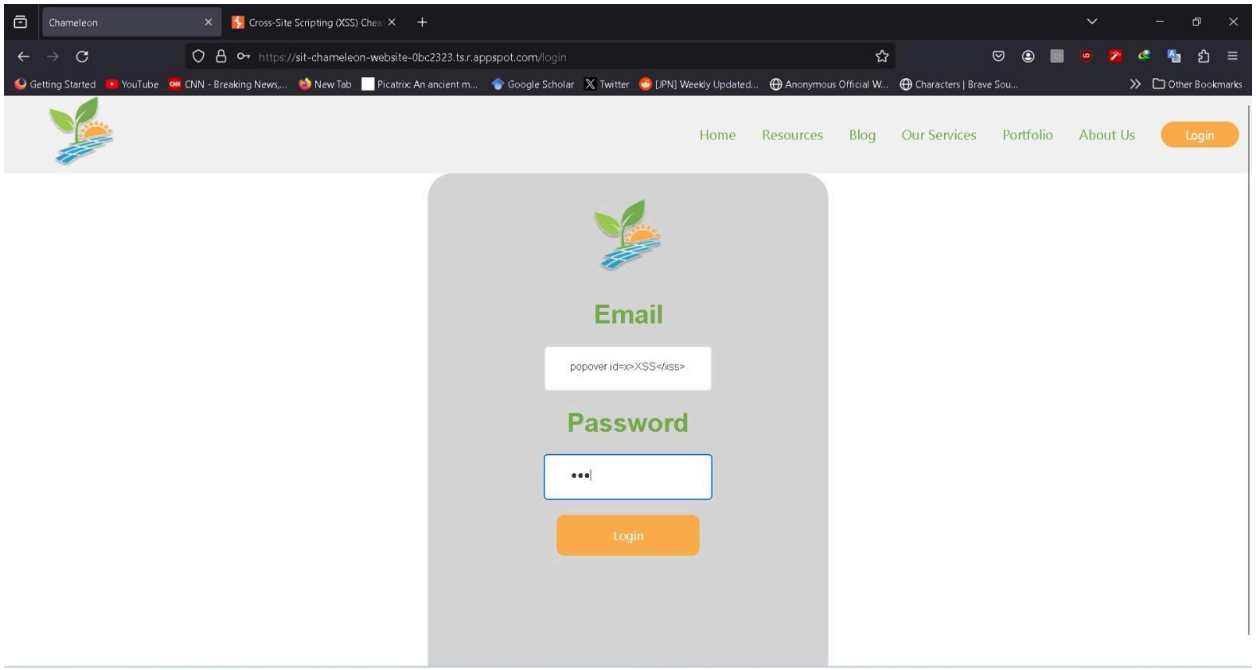
Scope of Testing:

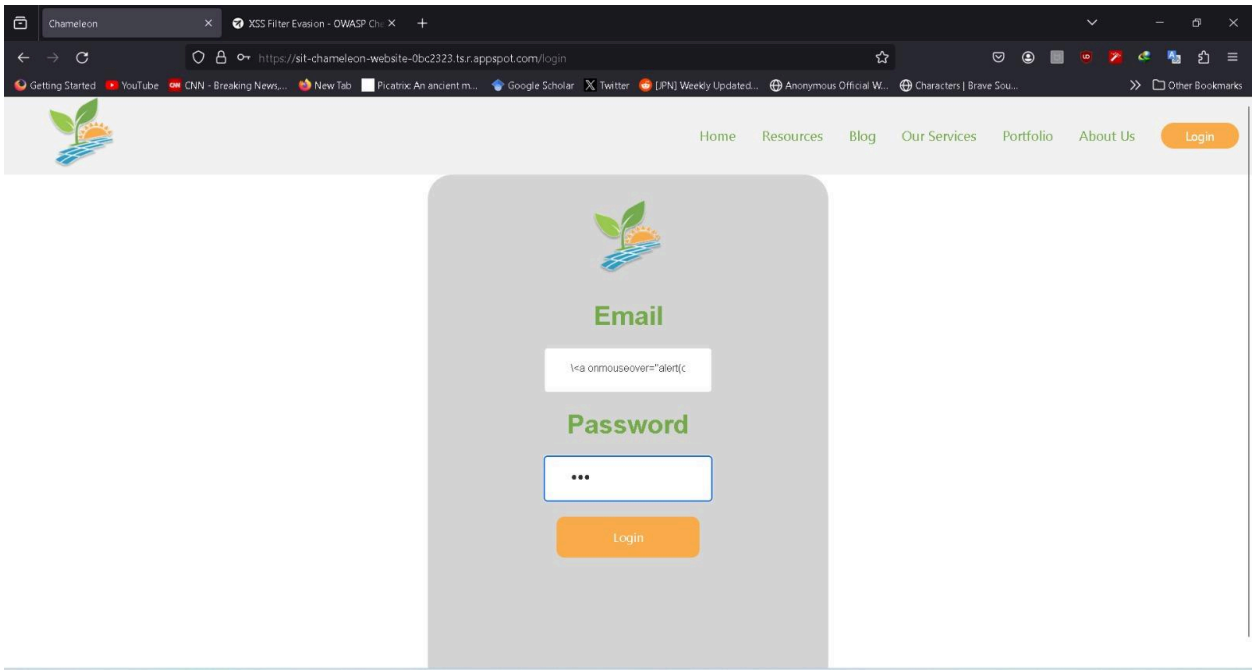
In order to find weaknesses in web applications, XSS testing involved inserting malicious scripts into URLs, input fields, and other user-controllable data. The scope included automated scanning with specific tools in addition to manual testing methods like input validation bypass.

Results:

In order to find weaknesses in web applications, XSS testing involved inserting malicious scripts into URLs, input fields, and other user-controllable data. The scope included both automatic and manual testing methods, such as input validation bypass. There were no vulnerabilities recorded during the testing. The following were the output we got after testing:







Conclusion:

Web applications still pose a serious security risk due to Cross-Site Scripting (XSS), which can have detrimental effects on users and companies alike. It is imperative that developers and website administrators establish strong input validation and output encoding techniques, perform frequent security audits, and make use of automated tools for vulnerability screening and testing in order to prevent the dangers associated with cross-site scripting attacks (XSS).

References:

1. OWASP XSS Prevention Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html
2. Burp Suite Documentation: https://portswigger.net/burp/documentation
3. OWASP ZAP Official Website: https://www.zaproxy.org/
4. Netsparker XSS Scanner: https://www.netsparker.com/web-vulnerability-scanner/xss-scanner/
5. Acunetix XSS Vulnerability Scanner: https://www.acunetix.com/vulnerability-scanner/