

Sri Lanka Institute of Information Technology



Bug Bounty Report 08

WS Assignment
IE2062 – Web Security

IT23159730

W.H.M.S.R.Bandara

Vulnerability Title

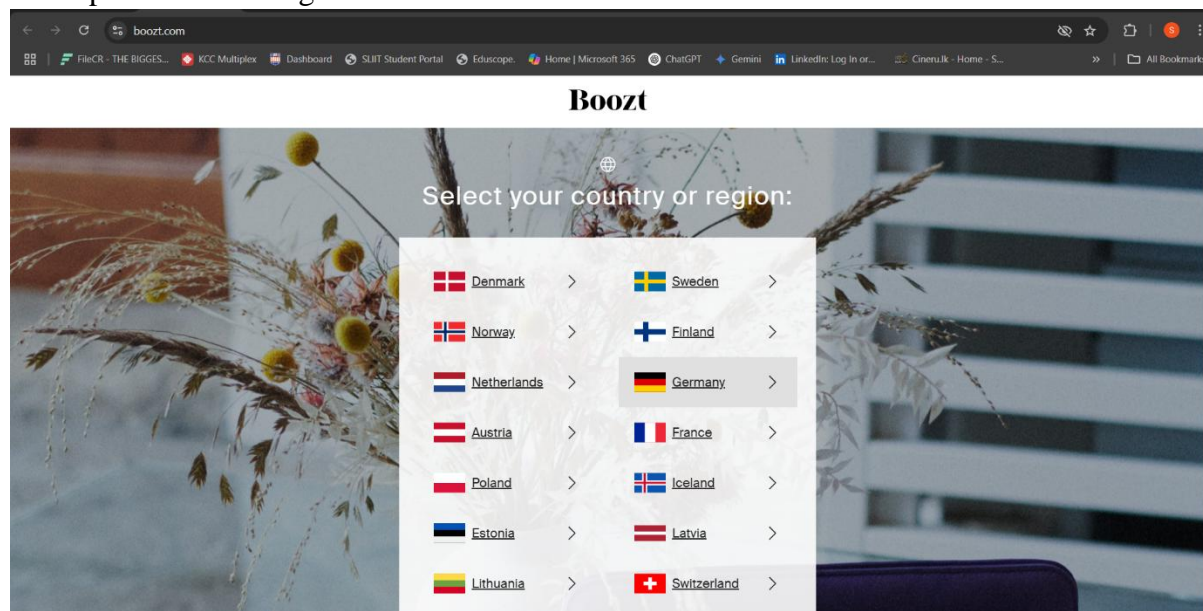
Absence of Anti-CSRF Tokens on www.boozt.com

Vulnerability Description

Cross-Site Request Forgery (CSRF) attack is an attack that leads an authenticated user into executing unwanted operations on a web application for which he/she is already authenticated. Anti-CSRF tokens are a security practice employed to protect against the same by ensuring that a request is made by the legitimate user and not an attacker. These tokens are typically unique, random values included in forms or requests that are verified by the server before the action is processed.

During a security scan of www.boozt.com, an automated scan using OWASP ZAP (version 2.16.1) identified the absence of anti-CSRF tokens in a form submission on the URL https://www.boozt.com/*/search?result (CWE-352). The form, a global search form with method="POST", lacks an anti-CSRF token and hence is vulnerable to CSRF attacks. This bug was detected with full confidence and ranks as a high-severity issue (P1) because it has the potential to make the attackers carry out actions on behalf of normal users with unvalidated actions, for example, edit account information, place orders, or set up user preferences for this internet marketplace.

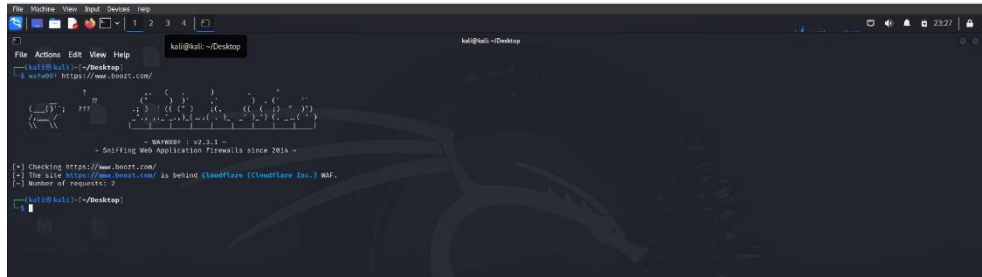
The ZAP scan also picked up other issues, including missing anti-clickjacking headers and missing a Content Security Policy (CSP) header, that add to the overall risk but are not what this report is addressing.



Other scans

Firewall Detection.

Before the automated scan with OWASP ZAP (2.16.0), Identify the Firewall by using Wafw00f Tool.



```
File Machine View Input Devices Help
kali@kali: ~/Desktop
$ wafw00f https://www.boozt.com/
[+] Checking https://www.boozt.com/
[+] The site https://www-boozt.com/ is behind cloudflare (Cloudflare Sec.) WAF.
[+] Number of requests: 2
[+] Status: 200
[+] Server: cloudflare
[+] Retrieved via header: 1.1 google.
[+] IP address found in the 'set-cookie' header. The IP is '0.e.1.1'. See: https://portswigger.net/kb/issues/0000300_private-ip-addresses-disclosed
[+] Uncommon header 'x-cookie-context' found, with contents: .
[+] Uncommon header 'x-type' found, with contents: home-index.
[+] Uncommon header 'x-release-version' found, with contents: 20250425185126.
[+] Uncommon header 'x-lbno' found, with contents: 8-395.
[+] An alt-svc header was found which is advertising HTTP/3. The endpoint is: '443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
[+] IP address found in the 'Cloud' cookie. The IP is: '0.e.1.1'.
[+] /NzMX03JL: Uncommon header 'cf-mitigated' found, with contents: challenge.
[+] /NzMX03JL: Uncommon header 'accept-ch' found, with contents: Sec-CH-UA-Bitness, Sec-CH-UA-Arch, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-Model, Sec-CH-UA-Platform-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Platf
[+] /NzMX03JL: Uncommon header 'server-timing' found, with contents: challenge.
[+] /NzMX03JL: Uncommon header 'cross-origin-embedder-policy' found, with contents: require-corp.
[+] /NzMX03JL: Uncommon header 'critical-ch' found, with contents: Sec-CH-UA-Bitness, Sec-CH-UA-Arch, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-Model, Sec-CH-UA-Platform-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Platf
[+] /NzMX03JL: Uncommon header 'x-internal-notice' found, with contents: script-ipc 'notice=851781a604979d6d4126f3d67a6d6'.
[+] /NzMX03JL: The 'Content-Type' options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerab
[+] /NzMX03JL: The 'Content-Type' options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerab
[+] No CCL directories found (use '-C all' to force check all possible dirs)
[+] Hostname 'www.boozt.com' does not match certificate's names: boozt.com. See: https://cve.mitre.org/data/definitions/297.html
[+] Suspended nikto -h https://www-boozt.com/
kali@kali: ~/Desktop
```

Open Ports Detection

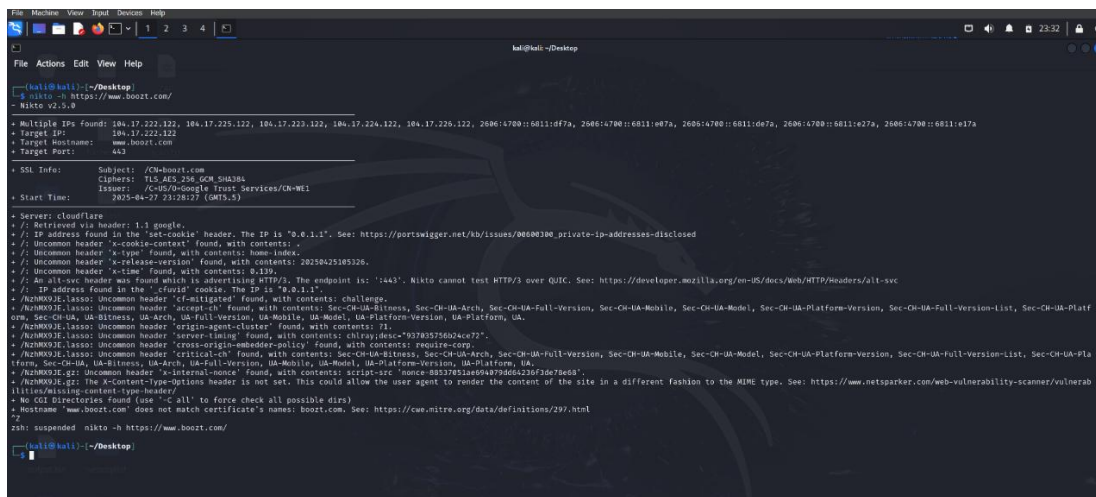
Done the nmap scan for detect open ports.



```
File Machine View Input Devices Help
kali@kali: ~/Desktop
$ nmap boozt.com
Starting Nmap (Nmap.org) at 2025-04-27 23:33:48530
Nmap scan report for boozt.com (184.17.222.122)
Host is up (0.159 latency).
Other addresses for boozt.com (not scanned): 184.17.225.122 184.17.223.122 184.17.224.122 184.17.226.122 2686:4700::6811:e07a 2686:4700::6811:e07a 2686:4700::6811:e07a 2686:4700::6811:e07a 2686:4700::6811:e07a 2686:4700::6811:e07a
Not shown: 966 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt
Nmap done: 1 IP address (1 host up) scanned in 20.15 seconds
kali@kali: ~/Desktop
```

Scanning for common Issues

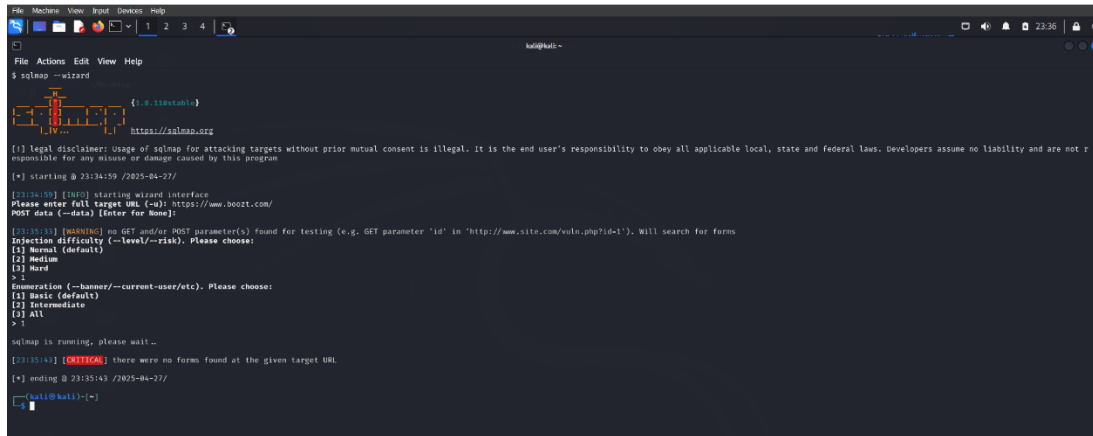
These scans done by with Nikto.



```
File Machine View Input Devices Help
kali@kali: ~/Desktop
$ nikto -h https://www-boozt.com/
- Nikto v2.5.0
+ Multiple IPs found: 184.17.222.122, 184.17.225.122, 184.17.223.122, 184.17.224.122, 184.17.226.122, 2686:4700::6811:e07a, 2686:4700::6811:e07a, 2686:4700::6811:e07a, 2686:4700::6811:e07a, 2686:4700::6811:e07a, 2686:4700::6811:e07a
+ Target IP: 184.17.222.122
+ Target hostname: www-boozt.com
+ Target port: 443
+ SSL Info: Subject: /CN=boozt.com
+ Start Time: 2025-04-27 23:32:17 (GMT+5)
+ Server: cloudflare
+ /: Retrieved via header: 1.1 google.
+ /: IP address found in the 'set-cookie' header. The IP is '0.e.1.1'. See: https://portswigger.net/kb/issues/0000300_private-ip-addresses-disclosed
+ /: Uncommon header 'x-cookie-context' found, with contents: .
+ /: Uncommon header 'x-type' found, with contents: home-index.
+ /: Uncommon header 'x-release-version' found, with contents: 20250425185126.
+ /: Uncommon header 'x-lbno' found, with contents: 8-395.
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: '443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /: IP address found in the 'Cloud' cookie. The IP is: '0.e.1.1'.
+ /NzMX03JL: Uncommon header 'cf-mitigated' found, with contents: challenge.
+ /NzMX03JL: Uncommon header 'accept-ch' found, with contents: Sec-CH-UA-Bitness, Sec-CH-UA-Arch, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-Model, Sec-CH-UA-Platform-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Platf
+ /NzMX03JL: Uncommon header 'server-timing' found, with contents: challenge.
+ /NzMX03JL: Uncommon header 'cross-origin-embedder-policy' found, with contents: require-corp.
+ /NzMX03JL: Uncommon header 'critical-ch' found, with contents: Sec-CH-UA-Bitness, Sec-CH-UA-Arch, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-Model, Sec-CH-UA-Platform-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Platf
+ /NzMX03JL: Uncommon header 'x-internal-notice' found, with contents: script-ipc 'notice=851781a604979d6d4126f3d67a6d6'.
+ /NzMX03JL: The 'Content-Type' options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerab
+ /NzMX03JL: The 'Content-Type' options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerab
+ No CCL directories found (use '-C all' to force check all possible dirs)
+ Hostname 'www.boozt.com' does not match certificate's names: boozt.com. See: https://cve.mitre.org/data/definitions/297.html
+ Suspended nikto -h https://www-boozt.com/
kali@kali: ~/Desktop
```

Detect and exploit SQL injection flaws

Detect and exploit SQL injection flaws



```
File Machine View Window Devices Help
sqlmap --wizard
[!] legal disclaimer: usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 23:34:59 /2025-04-27/
[23:34:59] [INFO] starting wizard interface
Please enter full target URL (-u): https://www.boozt.com/
POST data (--data) [Enter for None]:
[23:35:13] [WARNING] no GET and/or POST parameter(s) found for testing (e.g. GET parameter 'id' in 'http://www.site.com/vuln.php?id=1'). Will search for forms
Injection difficulty (--level/--risk), please choose:
(1) Normal (default)
(2) Medium
(3) Hard
P >
Enumeration (--banner/--current-user/etc), Please choose:
(1) Basic (default)
(2) Intermediate
(3) All
P >
sqlmap is running, please wait...
[23:35:43] [CRITICAL] there were no forms found at the given target URL
[*] ending @ 23:35:43 /2025-04-27/
kali@kali:~$
```

Affected Components

- **Domain:** www.boozt.com
- **Endpoint:** /search/result
- **Form:** form global-search-form__form
- **Risk Level:** Medium
- **Confidence:** Low (based on automated passive scan without active exploitation)
- **Detection Method:** Passive Scan

Impact Assessment

The absence of an anti-CSRF tokens could lead to the following risks:

- **Cross-Site Request Forgery (CSRF):** Malicious requests may be crafted by attackers to make authenticated users execute unwarranted actions, such as sending search queries, updating account options, adding products into the shopping cart, or placing orders without their knowledge.
- **Illegal Actions:** In an e-commerce website such as Boozt, CSRF attacks could lead to unauthorized purchasing, changing user preference, or modifying account details, which may lead to a monetary loss or taking control of an account.
- **Data Exposure:** If form submission leads to other sensitive activities (e.g., updating profiles), the attackers can utilize this to disclose or modify individual user data.
- **Business Impact:** A CSRF attack could cause monetary loss, legal problems, and customer trust erosion, which are critical to an e-commerce platform.
- **Reputation Risk:** Misuse could lead to negative publicity and user confidence loss, damaging the platform's reputation in the competitive e-commerce market.
- **Exacerbated Risk:** The absence of other security controls, such as a CSP header and anti-clickjacking headers (also picked up by ZAP), increases the overall attack

surface, which makes CSRF attacks more successful if used in combination with XSS or clickjacking.

Steps to Reproduce

1. Configure OWASP ZAP

- Launch OWASP ZAP and set the target <https://www.boozt.com/>.
- Add the site to the context and ensure it's in scope.

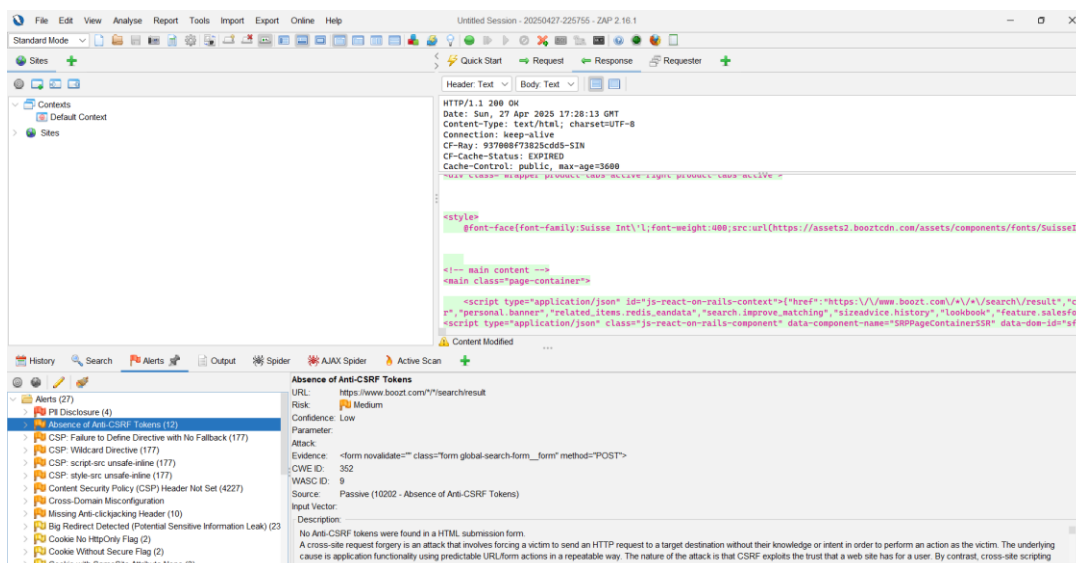
2. Perform an Automated Scan

- Spider the site with the AJAX Spider and detect dynamic content.
- Start an automated scan by clicking the "Attack" button in the Automated Scan window.
- Wait until the scan finishes.

3. Analyze Alerts

- Alert: "Absence of Anti-CSRF Tokens" (CWE-352).
- URL: https://www.boozt.com/*/search?result.
- Parameter: form (class="form_global-search_form", method="POST").
- Risk: Medium (P1), Confidence: Low (due to potential false positives in passive scans, but the issue warrants investigation).
- Source: Passive scan (10202 - Absence of Anti-CSRF Tokens).

Proof of Concept Screenshot



Proposed Mitigation or Fix

For to prevent clickjacking attack options due to absence of the anti-CSRF tokens header, do these steps below:

- **Use Anti-CSRF Tokens:** Include secure, random, session-based CSRF tokens in all forms that modify server-side data, including search functionality.
- **Use HTTP Headers:** Consider using custom headers for AJAX requests to secure API endpoints (e.g., X-CSRF-Token).
- **Token Validation on Server Side:** Validate submitted CSRF tokens on the server for all sensitive requests.
- **Framework Security Features:** Take advantage of in-built CSRF protection features offered by web frameworks like Ruby on Rails, Django, Spring, or Express.js.
- **Form Revalidation:** Ensure that all form submissions executing POST, PUT, DELETE, or PATCH requests require a valid CSRF token.

Conclusion.

OWASP ZAP vulnerability scan of www.boozt.com/ uncovered a deficiency of anti-CSRF tokens in a search form on the entire site, which makes the site vulnerable to Cross-Site Request Forgery (CSRF) attacks. The high-severity (P1) issue is seriously troublesome for an e-commerce site where sensitive actions like orders or modifications to account details are carried out by users, and therefore could be taken advantage of using CSRF to cause financial loss or account compromise. The absence of other security mechanisms, such as a CSP header and anti-clickjacking headers (also found by ZAP), increases the overall risk by facilitating corresponding attacks like XSS or clickjacking more readily. Utilizing anti-CSRF tokens, leveraging framework defenses, and employing complementary security mechanisms will significantly reduce CSRF attack risk and enhance the security posture of the platform. This report provides step-by-step instructions to reproduce the vulnerability and practical mitigations. Regular monitoring, secure coding, and periodic audits are essential in ensuring that the platform is immune from future attacks, especially in the competitive e-business industry.