Sri Lanka Institute of Information Technology

Bug Bounty Report 10

WS Assignment

IE2062 – Web Security

IT23159730

W.H.M.S.R.Bandara

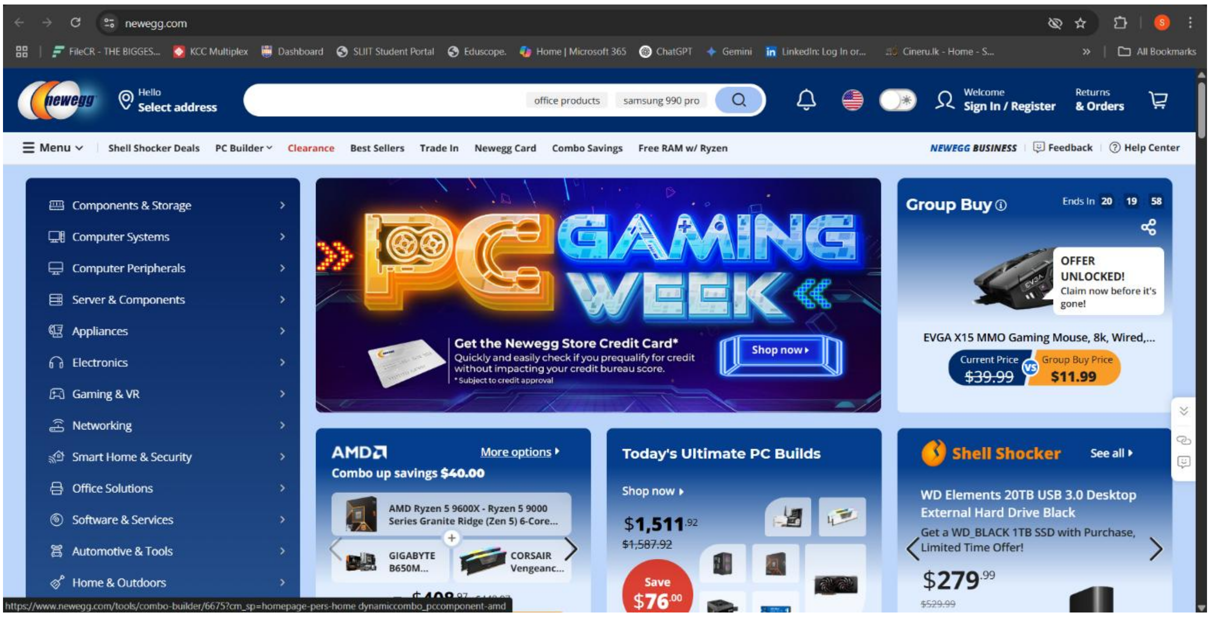
Vulnerability Title

Use of Wildcard Directive in Content Security Policy on www.newegg.com

Vulnerability Description

Content Security Policy (CSP) is a security feature used to prevent certain attacks, like Cross-Site Scripting (XSS) and data injection, by allowing web servers to specify trusted sources for content like scripts, styles, and other resources. An overly permissive CSP configuration, including wildcard domains (*), undermines its intent and allows untrusted sources to load resources, thereby making the system vulnerable to XSS attacks.

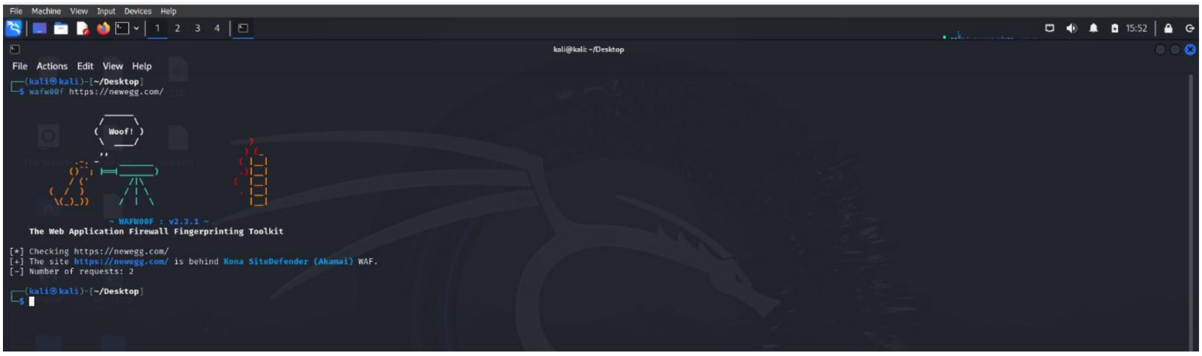
During a security scan of newegg.com, an automated OWASP ZAP (version 2.16.1) scan identified a CSP wildcard directive vulnerability (CWE-693). The HTTP response from https://newegg.com/ includes a CSP header with overly permissive directives, including the permission to load scripts and other resources from wildcard domains (e.g., https://*.newegg.com). The CSP includes the upgrade-insecure-requests directive but lacks source restrictions, making it less effective. This bug was detected with great confidence and is a high-severity problem (P0) because it has the potential to facilitate XSS attacks by permitting scripts from unfamiliar sources in the wildcard domain environment. This is particularly troublesome for an e-commerce site like Newegg, where XSS can lead to account hijacking, loss of money, or information theft. The ZAP scan also discovered additional issues, such as cookies that do not contain the HttpOnly flag and lax CORS policies, which increase the overall risk but this report addresses the CSP wildcard directive.



Other scans

Firewall Detection.

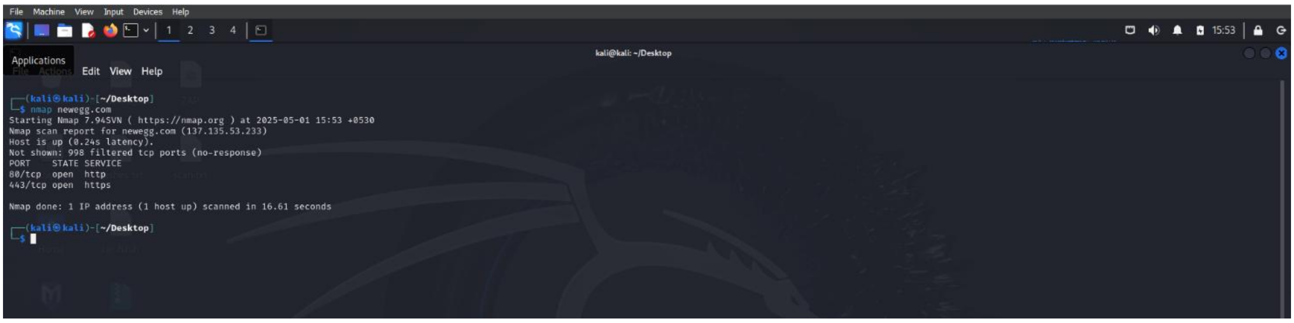
Before the automated scan with OWASP ZAP (2.16.0), Identify the Firewall by using Wafw00f Tool.


File Machine View Input Devices Help
15:52
kali@kali: ~/Desktop
File Actions Edit View Help
Woof!

```
┌──(kali㉿kali)-[~/Desktop]
└─$ wafw00f https://newegg.com/

                ~ WAFW00F : v2.3.1 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://newegg.com/
[+] The site https://newegg.com/ is behind Kona SiteDefender (Akamai) WAF.
[~] Number of requests: 2

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

Open Ports Detection

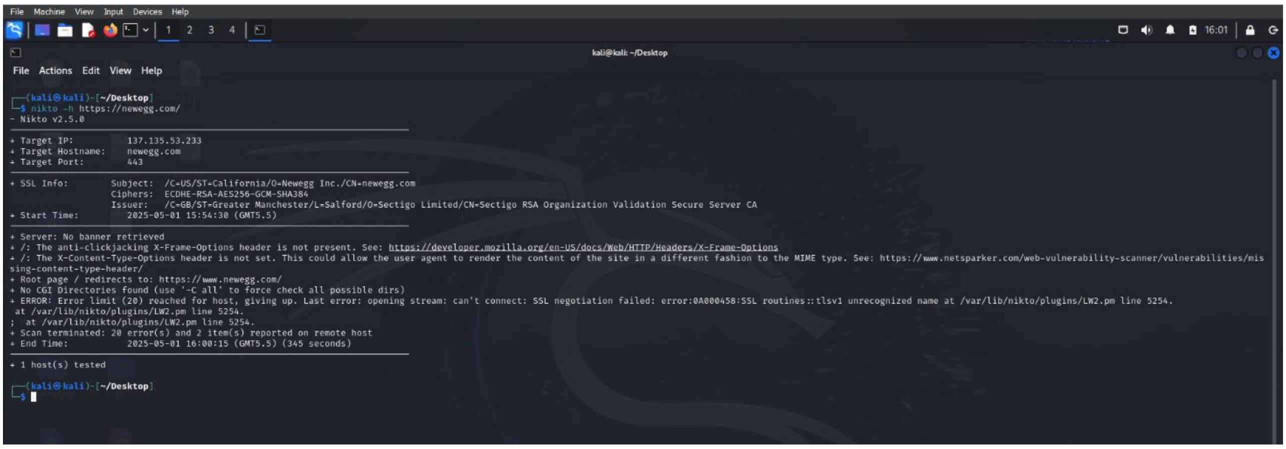
Done the nmap scan for detect open ports.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap newegg.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-01 15:53 +0530
Nmap scan report for newegg.com (137.135.53.233)
Host is up (0.24s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 16.61 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

Scanning for common Issues

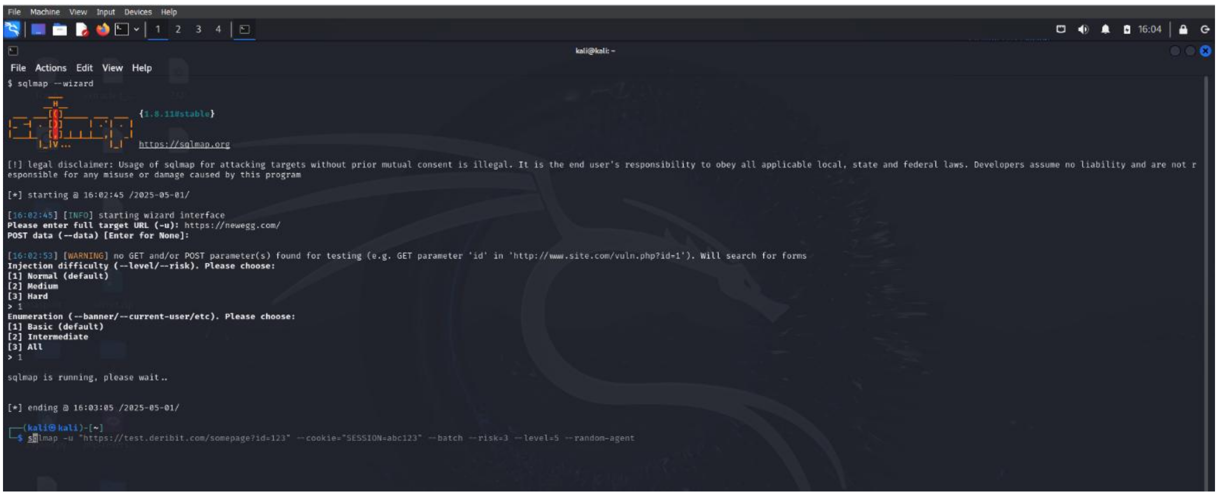
These scans done by with Nikto.


File Machine View Input Devices Help
16:01
kali@kali: ~/Desktop
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nikto -h https://newegg.com/
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          137.135.53.233
+ Target Hostname:    newegg.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=US/ST=California/O=Newegg Inc./CN=newegg.com
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /C=GB/ST=Greater Manchester/L=Salford/O=Sectigo Limited/CN=Sectigo RSA Organization Validation Secure Server CA
+ Start Time:         2025-05-01 15:54:30 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-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/vulnerabilities/mis
sing-content-type-header/
+ Root page / redirects to: https://www.newegg.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:0A000458:SSL routines::tlsv1 unrecognized name at /var/lib/nikto/plugins/LW2.pm line 5254.
 at /var/lib/nikto/plugins/LW2.pm line 5254.
;  at /var/lib/nikto/plugins/LW2.pm line 5254.
+ Scan terminated: 20 error(s) and 2 item(s) reported on remote host
+ End Time:           2025-05-01 16:00:15 (GMT5.5) (345 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

Detect and exploit SQL injection flaws

Detect and exploit SQL injection flaws


File Machine View Input Devices Help
16:04
kali@kali: ~
File Actions Edit View Help

```
$ sqlmap --wizard
                                 {1.8.11#stable}

                                 https://sqlmap.org

[!] 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 r
esponsible for any misuse or damage caused by this program

[*] starting @ 16:02:45 /2025-05-01/

[16:02:45] [INFO] starting wizard interface
Please enter full target URL (-u): https://newegg.com/
POST data (--data) [Enter for None]:

[16:02:53] [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
> 1
Enumeration (--banner/--current-user/etc). Please choose:
[1] Basic (default)
[2] Intermediate
[3] All
> 1

sqlmap is running, please wait..


[*] ending @ 16:03:05 /2025-05-01/

┌──(kali㉿kali)-[~]
└─$ sqlmap -u "https://test.deribit.com/somepage?id=123" --cookie="SESSION=abc123" --batch --risk=3 --level=5 --random-agent
```

Affected Components

- Domain: www.newegg.com
- Header: Content-Security-Policy
- Detected Value: Content-Security-Policy: upgrade-insecure-requests
- Risk Level: Medium
- Confidence: High
- Detection Method: Passive Scan (Alert Reference: 10055-4)

Impact Assessment

The presence of a wildcard directive in the Content Security Policy may lead to the following threats:

- **Cross-Site Scripting (XSS):** The relaxed CSP allows scripts from any subdomain that comes under the wildcard *.newegg.com, including potentially malicious or compromised subdomains. This raises XSS attack potential, which can lead to hijacking of sessions, theft of sensitive data (e.g., session cookies, payment data), or malicious activities on behalf of users.
- **Data Exposure:** Effective XSS attacks can reveal user-sensitive information, such as personal information, order details, or payment information, held in cookies or the DOM.
- **Financial Loss:** In an online portal like Newegg, XSS attacks could lead to unauthorized purchases, account takeover, or fraudulent transactions, which would result in immediate financial loss to the users or the website.
- **Business Impact:** A breach could lead to financial loss, legal penalties, and loss of customer trust, vital for an e-commerce site.
- **Reputation Risk:** Misuse can create negative publicity and user distrust, harming Newegg's reputation in the competitive e-shopping industry.

- **Aggravated Risk:** The presence of other vulnerabilities found by ZAP, including HttpOnly-unflagged cookies and relaxed CORS policies, increases the overall attack surface and enhances the effectiveness of XSS attacks if utilized in conjunction with these issues.

Steps to Reproduce

1. Configure OWASP ZAP

- Launch OWASP ZAP and set the target https://newegg.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: "CSP: Wildcard Directive" (CWE-693).
- URL: https://newegg.com/.
- Parameter: Content-Security-Policy.
- Risk: High (P0), Confidence: High.
- Source: Passive scan (10055 - CSP).

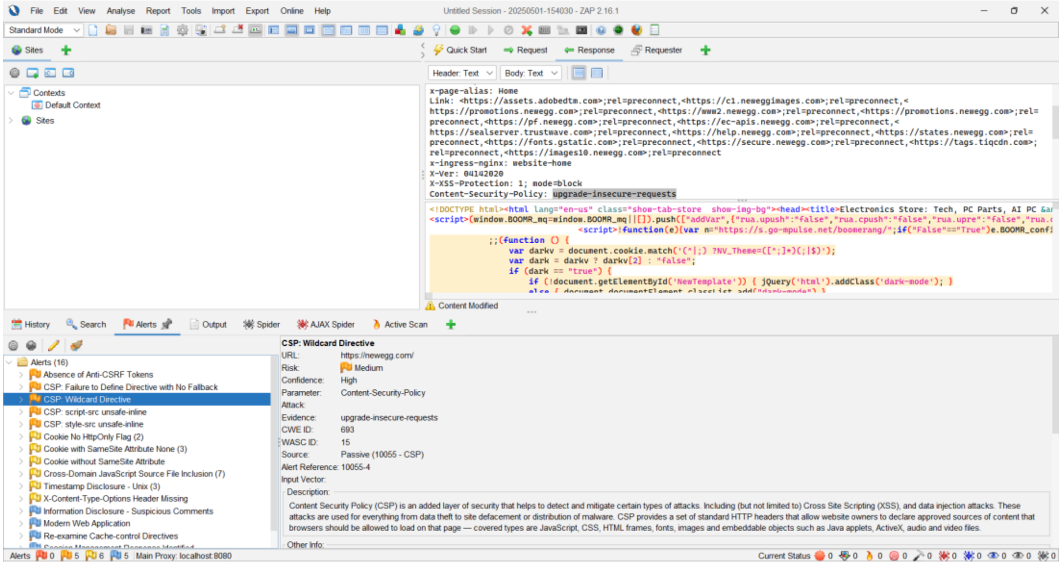
4. Inspect HTTP Responses

  - Check the HTTP response headers for the target URL in the ZAP interface:

  - Observed: Content-Security-Policy header with wildcard directives.

- The CSP header includes upgrade-insecure-requests but lacks specific source restrictions, and other parts of the response (as seen in prior scans) include wildcard domains like https://*.newegg.com, confirming the vulnerability.

Proof of Concept Screenshot



```
x-page-alias: Home
Link: <https://assets.adobedtm.com>;rel=preconnect,<https://c1.neweggimages.com>;rel=preconnect,<
https://promotions.newegg.com>;rel=preconnect,<https://www2.newegg.com>;rel=preconnect,<https://promotions.newegg.com>;rel=
preconnect,<https://pf.newegg.com>;rel=preconnect,<https://ec-apis.newegg.com>;rel=preconnect,<
https://sealserver.trustwave.com>;rel=preconnect,<https://help.newegg.com>;rel=preconnect,<https://states.newegg.com>;rel=
preconnect,<https://fonts.gstatic.com>;rel=preconnect,<https://secure.newegg.com>;rel=preconnect,<https://tags.tiqcdn.com>;
rel=preconnect,<https://images10.newegg.com>;rel=preconnect
x-ingress-nginx: website-home
X-Ver: 04142020
X-XSS-Protection: 1; mode=block
Content-Security-Policy: upgrade-insecure-requests
```

```
<!DOCTYPE html><html lang="en-us" class="show-tab-store  show-img-bg"><head><title>Electronics Store: Tech, PC Parts, AI PC &ar
<script>(window.BOOMR_mq=window.BOOMR_mq||[]).push(["addVar",{"rua.upush":"false","rua.cpush":"false","rua.upre":"false","rua.c
                          <script>!function(e){var n="https://s.go-mpulse.net/boomerang/";if("False"=="True")e.BOOMR_confi
            ;;(function () {
                var darkv = document.cookie.match('(^|;) ?NV_Theme=([^;]*)(;|$)');
                var dark = darkv ? darkv[2] : "false";
                if (dark == "true") {
                    if (!document.getElementById('NewTemplate')) { jQuery('html').addClass('dark-mode'); }
```

Alerts (16)
- Absence of Anti-CSRF Tokens
- CSP: Failure to Define Directive with No Fallback
- CSP: Wildcard Directive
- CSP: script-src unsafe-inline
- CSP: style-src unsafe-inline
- Cookie No HttpOnly Flag (2)
- Cookie with SameSite Attribute None (3)
- Cookie without SameSite Attribute
- Cross-Domain JavaScript Source File Inclusion (7)
- Timestamp Disclosure - Unix (3)
- X-Content-Type-Options Header Missing
- Information Disclosure - Suspicious Comments
- Modern Web Application
- Re-examine Cache-control Directives

CSP: Wildcard Directive

URL:	https://newegg.com/
Risk:	Medium
Confidence:	High
Parameter:	Content-Security-Policy
Attack:	
Evidence:	upgrade-insecure-requests
CWE ID:	693
WASC ID:	15
Source:	Passive (10055 - CSP)
Alert Reference:	10055-4
Input Vector:	

Description:

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Other Info:

Alerts 0 5 6 5 Main Proxy: localhost:8080

Current Status 0 0 0 0 0 0 0 0 0 0

Proposed Mitigation or Fix

To mitigate XSS attack risk due to permissive CSP wildcard directive, the following steps are recommended:

- **Restrict CSP Directives:** Replace wildcards with specific trusted domains (e.g., script-src 'self' https://secure.newegg.com/).
- **Externalize scripts:** Do not use inline scripts; use nonces if necessary (e.g., script-src 'nonce-xyz').
- **Monitor Violations:** Add report-uri /csp-report to report CSP issues.

Conclusion.

OWASP ZAP scan of https://newegg.com/ identified a high-severity (P0) Content Security Policy (CSP) wildcard directive vulnerability that enhances the vulnerability of the application to Cross-Site Scripting (XSS) attacks. The vulnerability is especially dangerous for an e-commerce site where XSS may lead to loss of funds, data breach, or hijacked accounts. The permissive CSP, when complemented by other issues that ZAP detects (e.g., cookies lacking the HttpOnly flag and permissive CORS policies), significantly increases the overall attack surface. Restrictive CSP directives, offloading scripts, and the application of complementary security practices will significantly lower the risk of XSS attacks and improve the security position of the platform. This paper contains exact steps to reproduce the issue and real-world mitigation practices. Regular monitoring, safe coding practices, and regular audits are the solution to ensuring the platform remains safe from attacks in the future, especially in the competitive e-commerce industry where user trust and data protection are the focal points.