Sri Lanka Institute of Information Technology

Year 2 semester 2

IT23360600
G. P. I. Perera

SLIIT KANDY UNI

BUG BOUNTY REPORT 6

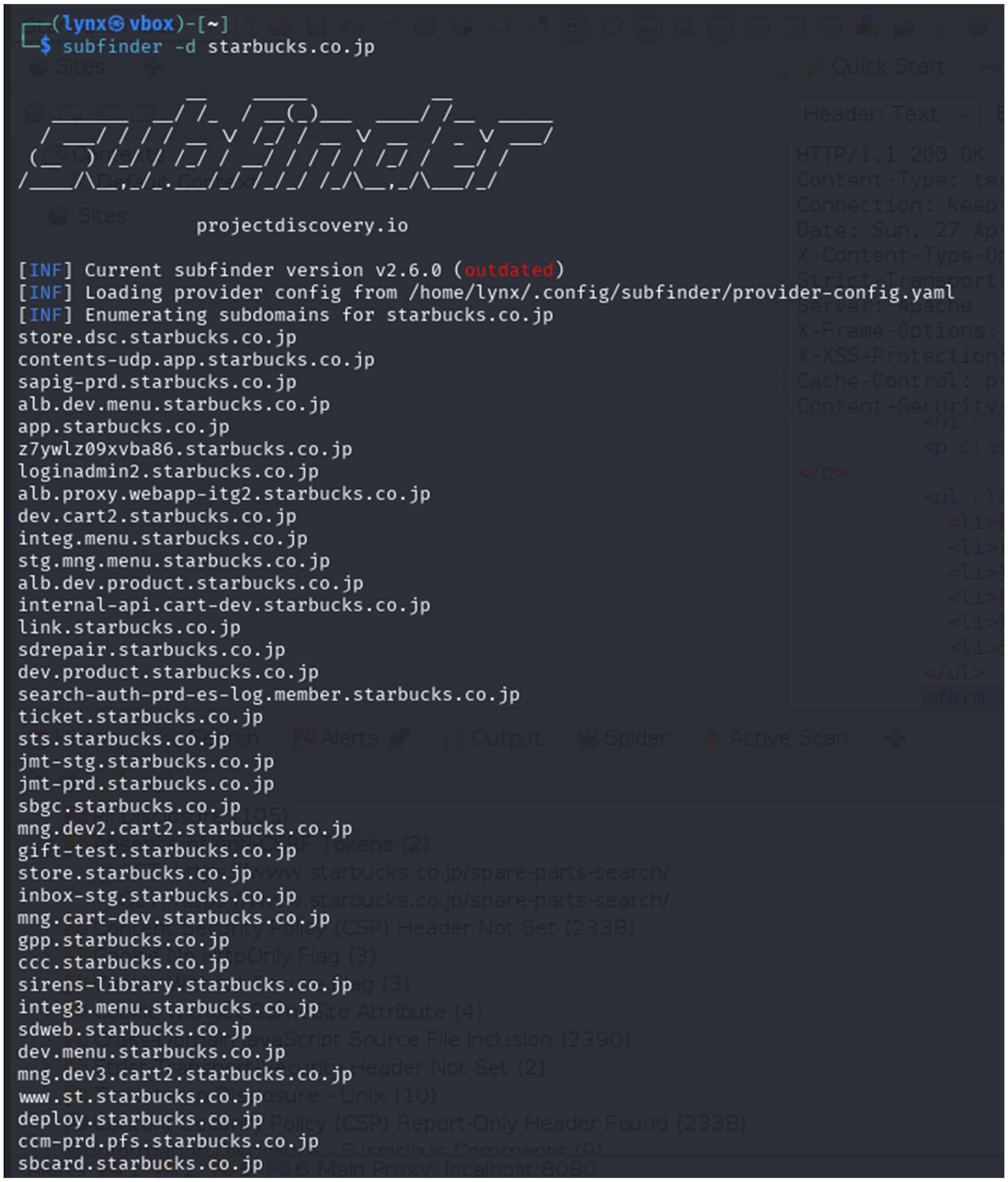
Web Security – IE2062

B.Sc. (Hons) in information Technology Specializing in Cyber Security

1. Requirement gathering and analysis

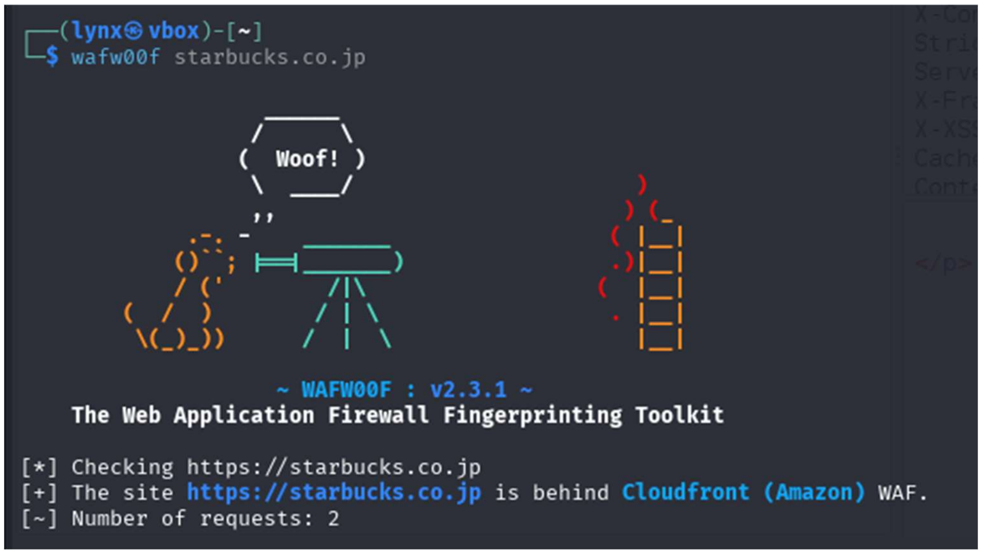
Selected sub domain	**www.starbucks.co.jp**
Hakerone URL	https://hackerone.com/starbucks_japan
IP address	**15.197.135.250**

Subdomain list



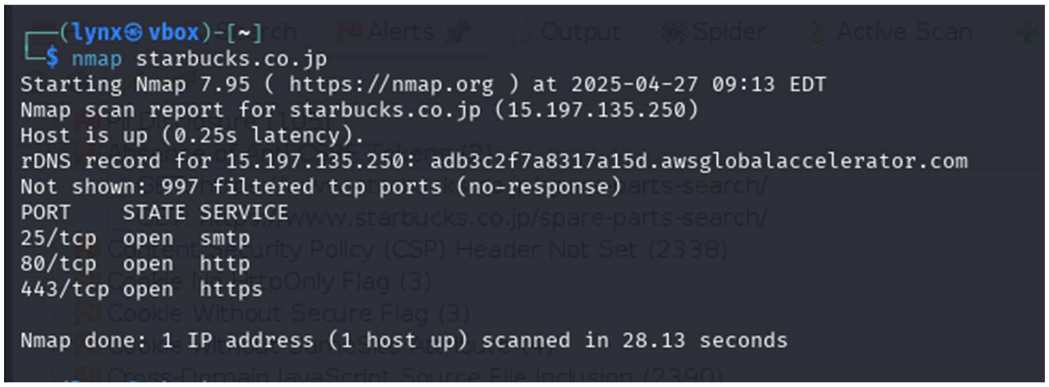
```
┌──(lynx㉿vbox)-[~]
└─$ subfinder -d starbucks.co.jp

               __    _____           __
   _______  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/

                projectdiscovery.io

[INF] Current subfinder version v2.6.0 (outdated)
[INF] Loading provider config from /home/lynx/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for starbucks.co.jp
store.dsc.starbucks.co.jp
contents-udp.app.starbucks.co.jp
sapig-prd.starbucks.co.jp
alb.dev.menu.starbucks.co.jp
app.starbucks.co.jp
z7ywlz09xvba86.starbucks.co.jp
loginadmin2.starbucks.co.jp
alb.proxy.webapp-itg2.starbucks.co.jp
dev.cart2.starbucks.co.jp
integ.menu.starbucks.co.jp
stg.mng.menu.starbucks.co.jp
alb.dev.product.starbucks.co.jp
internal-api.cart-dev.starbucks.co.jp
link.starbucks.co.jp
sdrepair.starbucks.co.jp
dev.product.starbucks.co.jp
search-auth-prd-es-log.member.starbucks.co.jp
ticket.starbucks.co.jp
sts.starbucks.co.jp
jmt-stg.starbucks.co.jp
jmt-prd.starbucks.co.jp
sbgc.starbucks.co.jp
mng.dev2.cart2.starbucks.co.jp
gift-test.starbucks.co.jp
store.starbucks.co.jp
inbox-stg.starbucks.co.jp
mng.cart-dev.starbucks.co.jp
gpp.starbucks.co.jp
ccc.starbucks.co.jp
sirens-library.starbucks.co.jp
integ3.menu.starbucks.co.jp
sdweb.starbucks.co.jp
dev.menu.starbucks.co.jp
mng.dev3.cart2.starbucks.co.jp
www.st.starbucks.co.jp
deploy.starbucks.co.jp
ccm-prd.pfs.starbucks.co.jp
sbcard.starbucks.co.jp
```

Firewall detection:



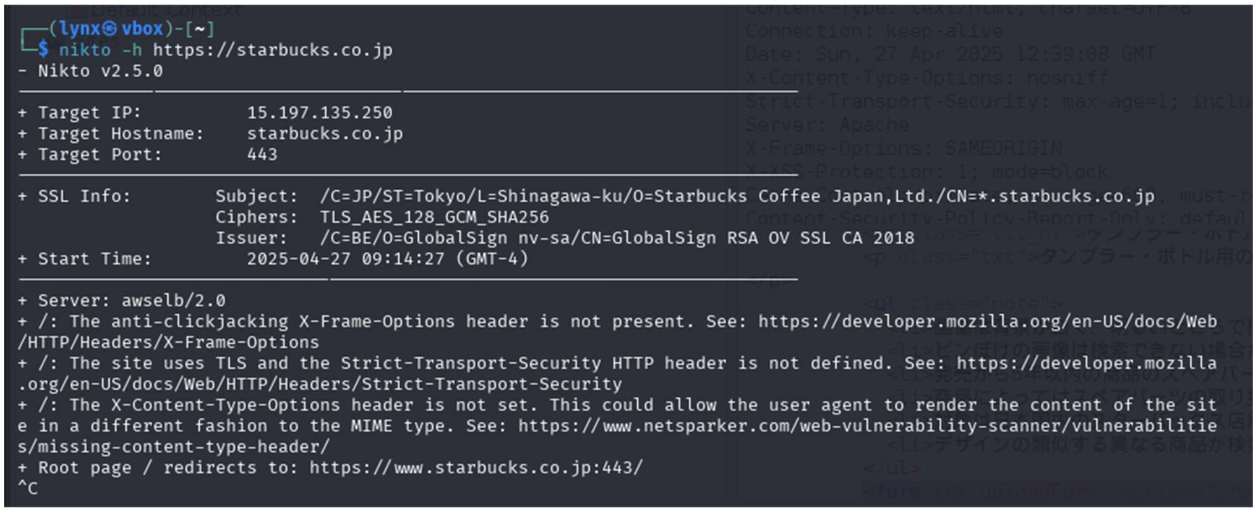
```
┌──(lynx㉿vbox)-[~]
└─$ wafw00f starbucks.co.jp

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

[*] Checking https://starbucks.co.jp
[+] The site https://starbucks.co.jp is behind Cloudfront (Amazon) WAF.
[~] Number of requests: 2
```

Nmap scan:



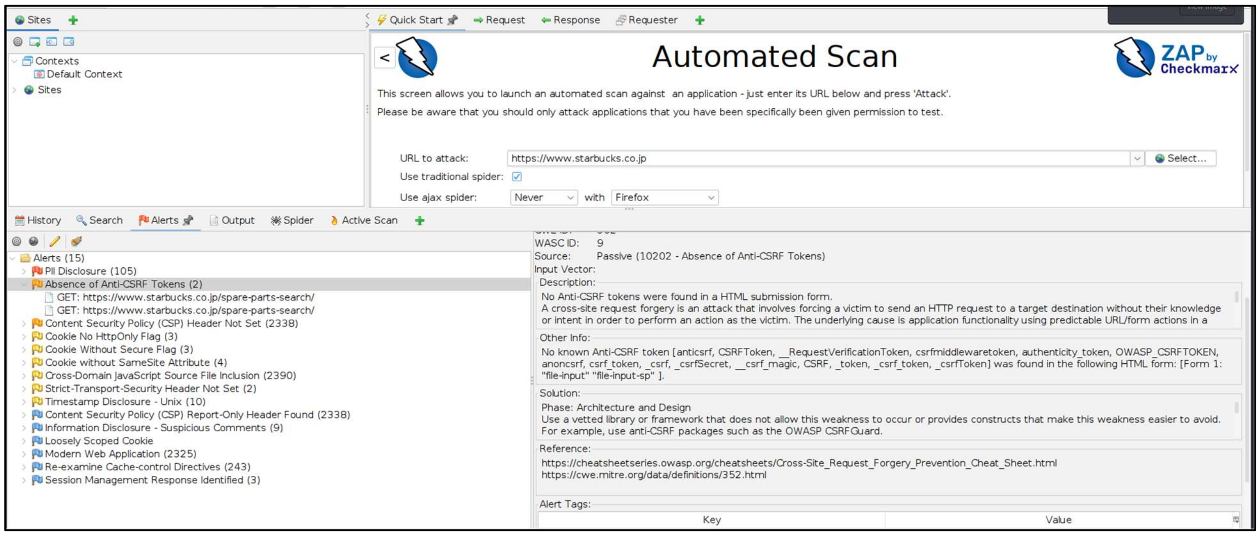
```
┌──(lynx㉿vbox)-[~]
└─$ nmap starbucks.co.jp
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 09:13 EDT
Nmap scan report for starbucks.co.jp (15.197.135.250)
Host is up (0.25s latency).
rDNS record for 15.197.135.250: adb3c2f7a8317a15d.awsglobalaccelerator.com
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 28.13 seconds
```

Nikto scan result



```
┌──(lynx㉿vbox)-[~]
└─$ nikto -h https://starbucks.co.jp
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          15.197.135.250
+ Target Hostname:    starbucks.co.jp
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=JP/ST=Tokyo/L=Shinagawa-ku/O=Starbucks Coffee Japan,Ltd./CN=*.starbucks.co.jp
                   Ciphers:  TLS_AES_128_GCM_SHA256
                   Issuer:   /C=BE/O=GlobalSign nv-sa/CN=GlobalSign RSA OV SSL CA 2018
+ Start Time:         2025-04-27 09:14:27 (GMT-4)
---------------------------------------------------------------------------
+ Server: awselb/2.0
+ /: 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 site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla
.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
e in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilitie
s/missing-content-type-header/
+ Root page / redirects to: https://www.starbucks.co.jp:443/
^C
```

Active scan result from OWASP ZAP:



This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: https://www.starbucks.co.jp
Use traditional spider: ✓
Use ajax spider: Never with Firefox

```
Alerts (15)
  PII Disclosure (105)
  Absence of Anti-CSRF Tokens (2)
      GET: https://www.starbucks.co.jp/spare-parts-search/
      GET: https://www.starbucks.co.jp/spare-parts-search/
  Content Security Policy (CSP) Header Not Set (2338)
  Cookie No HttpOnly Flag (3)
  Cookie Without Secure Flag (3)
  Cookie without SameSite Attribute (4)
  Cross-Domain JavaScript Source File Inclusion (2390)
  Strict-Transport-Security Header Not Set (2)
  Timestamp Disclosure - Unix (10)
  Content Security Policy (CSP) Report-Only Header Found (2338)
  Information Disclosure - Suspicious Comments (9)
  Loosely Scoped Cookie
  Modern Web Application (2325)
  Re-examine Cache-control Directives (243)
  Session Management Response Identified (3)
```

WASC ID: 9
Source: Passive (10202 - Absence of Anti-CSRF Tokens)
Input Vector:

Description:
No Anti-CSRF tokens were found in a HTML submission form.
A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a

Other Info:
No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "file-input" "file-input-sp"].

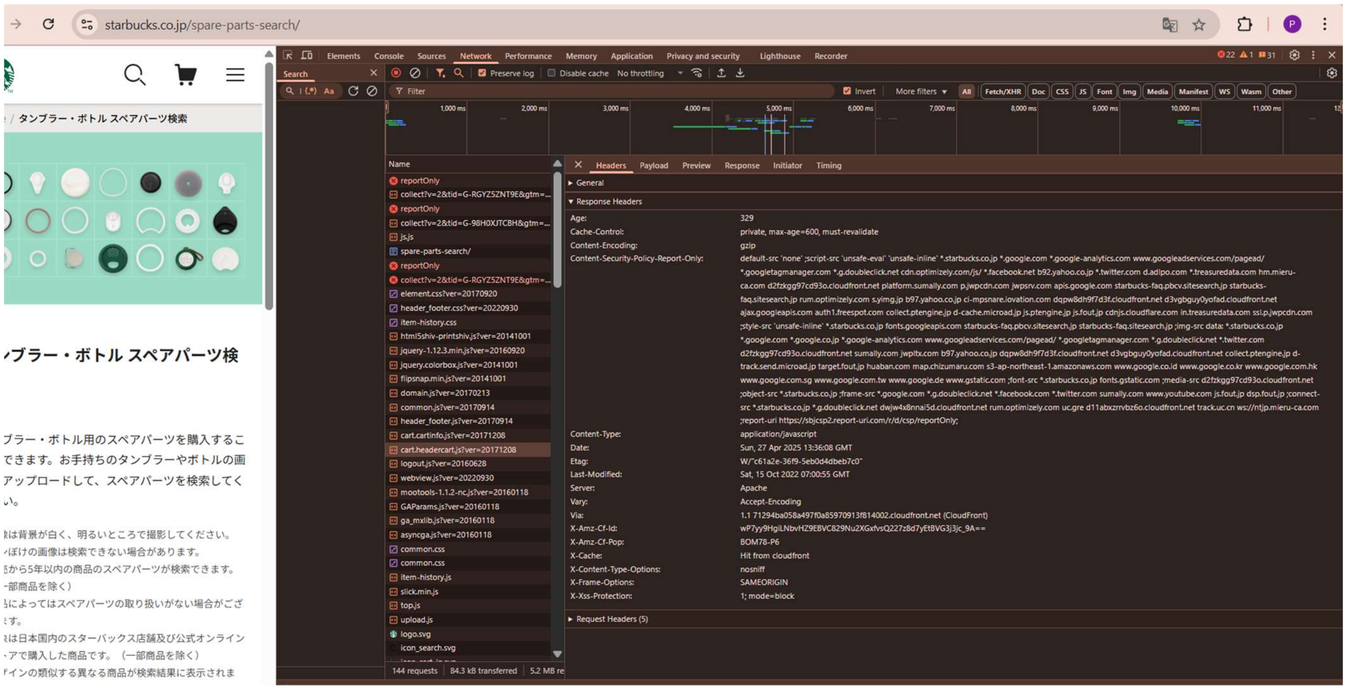
Solution:
Phase: Architecture and Design
Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.
For example, use anti-CSRF packages such as the OWASP CSRFGuard.

Reference:
https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html
https://cwe.mitre.org/data/definitions/352.html

Alert Tags:

Key	Value

Developer Tools:



ブラー・ボトル スペアパーツ検

ブラー・ボトル用のスペアパーツを購入するこ
できます。お手持ちのタンブラーやボトルの画
アップロードして、スペアパーツを検索してく
い。

象は背景が白く、明るいところで撮影してください。
ぼけの画像は検索できない場合があります。
から5年以内の商品のスペアパーツが検索できます。
-部商品を除く）
によってはスペアパーツの取り扱いがない場合がござ
す。
は日本国内のスターバックス店舗及び公式オンライン
アで購入した商品です。（一部商品を除く）
インの類似する異なる商品が検索結果に表示されま

```
Name
reportOnly
collect?v=2&tid=G-RGYZ5ZNT9E&gtm=...
reportOnly
collect?v=2&tid=G-98H0XJTCBH&gtm=...
js.js
spare-parts-search/
reportOnly
collect?v=2&tid=G-RGYZ5ZNT9E&gtm=...
element.css?ver=20170920
header_footer.css?ver=20220930
item-history.css
html5shiv-printshiv.js?ver=20141001
jquery-1.12.3.min.js?ver=20160920
jquery.colorbox.js?ver=20141001
flipsnap.min.js?ver=20141001
domain.js?ver=20170213
common.js?ver=20170914
header_footer.js?ver=20170914
cart.cartinfo.js?ver=20171208
cart.headercart.js?ver=20171208
logout.js?ver=20160628
webview.js?ver=20220930
mootools-1.1.2-nc.js?ver=20160118
GAParams.js?ver=20160118
ga_mxlib.js?ver=20160118
asyncga.js?ver=20160118
common.css
common.css
item-history.js
slick.min.js
top.js
upload.js
logo.svg
icon_search.svg

144 requests | 84.3 kB transferred | 5.2 MB re
```

```
▸ General
▾ Response Headers
Age:                                 329
Cache-Control:                       private, max-age=600, must-revalidate
Content-Encoding:                    gzip
Content-Security-Policy-Report-Only: default-src 'none' ;script-src 'unsafe-eval' 'unsafe-inline' *.starbucks.co.jp *.google.com *.google-analytics.com www.googleadservices.com/pagead/
                                     *.googletagmanager.com *.g.doubleclick.net cdn.optimizely.com/js/ *.facebook.net b92.yahoo.co.jp *.twitter.com d.adlpo.com *.treasuredata.com hm.mieru-
                                     ca.com d2fzkgg97cd93o.cloudfront.net platform.sumally.com p.jwpcdn.com jwpsrv.com apis.google.com starbucks-faq.pbcv.sitesearch.jp starbucks-
                                     faq.sitesearch.jp rum.optimizely.com s.yimg.jp b97.yahoo.co.jp ci-mpsnare.iovation.com dqpw8dh9f7d3f.cloudfront.net d3vgbguy0yofad.cloudfront.net
                                     ajax.googleapis.com auth1.freespot.com collect.ptengine.jp d-cache.microad.jp js.ptengine.jp js.fout.jp cdnjs.cloudflare.com in.treasuredata.com ssl.p.jwpcdn.com
                                     ;style-src 'unsafe-inline' *.starbucks.co.jp fonts.googleapis.com starbucks-faq.pbcv.sitesearch.jp starbucks-faq.sitesearch.jp ;img-src data: *.starbucks.co.jp
                                     *.google.com *.google.co.jp *.google-analytics.com www.googleadservices.com/pagead/ *.googletagmanager.com *.g.doubleclick.net *.twitter.com
                                     d2fzkgg97cd93o.cloudfront.net sumally.com jwpltx.com b97.yahoo.co.jp dqpw8dh9f7d3f.cloudfront.net d3vgbguy0yofad.cloudfront.net collect.ptengine.jp d-
                                     track.send.microad.jp target.fout.jp huaban.com map.chizumaru.com s3-ap-northeast-1.amazonaws.com www.google.co.id www.google.co.kr www.google.com.hk
                                     www.google.com.sg www.google.com.tw www.google.de www.gstatic.com ;font-src *.starbucks.co.jp fonts.gstatic.com ;media-src d2fzkgg97cd93o.cloudfront.net
                                     ;object-src *.starbucks.co.jp ;frame-src *.google.com *.g.doubleclick.net *.facebook.com *.twitter.com sumally.com www.youtube.com js.fout.jp dsp.fout.jp ;connect-
                                     src *.starbucks.co.jp *.g.doubleclick.net dwjw4x8nnai5d.cloudfront.net rum.optimizely.com uc.gre d11abxzrrvbz6o.cloudfront.net track.uc.cn ws://ntjp.mieru-ca.com
                                     ;report-uri https://sbjcsp2.report-uri.com/r/d/csp/reportOnly;
Content-Type:                        application/javascript
Date:                                Sun, 27 Apr 2025 13:36:08 GMT
Etag:                                W/"c61a2e-36f9-5eb0d4dbeb7c0"
Last-Modified:                       Sat, 15 Oct 2022 07:00:55 GMT
Server:                              Apache
Vary:                                Accept-Encoding
Via:                                 1.1 71294ba058a497f0a85970913f814002.cloudfront.net (CloudFront)
X-Amz-Cf-Id:                         wP7yy9HgiLNbvHZ9EBVC829Nu2XGxfvsQ227z8d7yEtBVG3j3jc_9A==
X-Amz-Cf-Pop:                        BOM78-P6
X-Cache:                             Hit from cloudfront
X-Content-Type-Options:              nosniff
X-Frame-Options:                     SAMEORIGIN
X-Xss-Protection:                    1; mode=block
▸ Request Headers (5)
```

2. Report Details

1. Vulnerability Title: Absence of Anti-CSRF Tokens

2. Vulnerability Description:

During OWASP ZAP scan it is discovered that the application does not implement anti-CSRF (Cross-Site Request Forgery) protection mechanisms, such as including and validating CSRF tokens in state-changing requests (e.g., POST, PUT, DELETE). Without these tokens, an attacker can trick an authenticated user into unknowingly submitting malicious requests to the application on their behalf. This can lead to unauthorized actions being performed, such as changing account settings, performing financial transactions, or even deleting data.

Impact:

- Unauthorized actions performed on behalf of authenticated users.
- Compromise of user accounts and sensitive data.
- Potential escalation to full account or system takeover depending on available actions.

3. Affected Components:

1. https://www.starbucks.co.jp/spare-parts-search/

4. Impact Assessment:

OWASP analysis:

Risk level	**Medium**
Confidence	High

Nikto –

Nikto finding	Meaning	Risk
Missing X-Frame-Options Header	The server does not send an X-Frame-Options HTTP header. This header protects against **clickjacking** attacks by preventing the site from being embedded inside an iframe on another site.	Medium

Missing Strict-Transport-Security (HSTS) Header	The server does not send a Strict-Transport-Security (HSTS) header. Without HSTS, users may initially connect over insecure HTTP, exposing them to **Man-in-the-Middle (MitM)** attacks.	High
Missing X-Content-Type-Options Header	The server does not send an X-Content-Type-Options: nosniff header. Without this, browsers may **MIME-sniff** content types incorrectly, possibly leading to **XSS (Cross-Site Scripting)** or other attacks.	Medium

5. Steps to reproduce –

- **On owasp zap –**
  Start the application, input target URL and run an automated scan.
  Observe alerts.
- **nikto-**
  perform a manual nikto scan by,
  ```
  nikto -h https://www.starbucks.co.jp
  ```
- **Network developer tools** -
  Use the browser's **developer tools** (press F12 in most browsers) to inspect network requests. Look for hidden form fields with names like csrf_token, anti_csrf, or auth_token in POST requests

6. Proposed mitigation or fix

1. **Implement CSRF Tokens**

- Introduce CSRF tokens for all state-changing requests (e.g., POST, PUT, PATCH, DELETE).
- Generate a unique, unpredictable CSRF token per user session.
- Embed the CSRF token into all forms and AJAX requests (e.g., as a hidden input field or custom HTTP header).
- Validate the token server-side for each request that modifies server state.

2. **Use Secure Framework Features**

- Leverage built-in CSRF protection offered by modern frameworks (e.g., Django's @csrf_protect, Laravel's CSRF middleware, Express.js CSURF middleware).
- Keep the security libraries and frameworks updated.

3. **Enforce SameSite Cookies**

- Set the SameSite attribute of session cookies to Strict or Lax where appropriate to prevent cookies from being sent in cross-site requests.

4. **Verify Request Origin (Optional but Recommended)**

- Validate the Origin and Referer headers to ensure that the request is coming from the expected domain, especially for high-risk operations (e.g., money transfers, password resets).