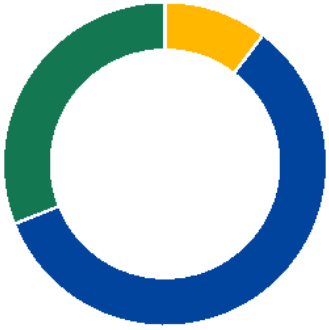
Target: **https://bafs.da.gov.ph/**

Date: **Fri Apr 12 2024**

Found Issues: **29**

scan **finished** within **2' 26"** after **786** requests.

Risk



Issue Severity

Executive Summary

SmartScanner conducted a scan on bafs.da.gov.ph to find security weaknesses and vulnerabilities. The scan took 2 minutes and 26 seconds. After performing 786 requests, SmartScanner found 29 issues in which 3 of them have medium severity. The overall security risk of bafs.da.gov.ph is 3.2 out of 5. To reduce the security risk, please fix the found issues as soon as possible. Technical details, as well as remediation of results, can be found in the following. *

* DISCLAIMER: This report is only limited to the results of SmartScanner findings.

List of Issues

1– Internal Server Error

1.1– http://bafs.da.gov.ph/
1.2– https://bafs.da.gov.ph/page/read_more_news_article?news=a%7Cid&article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODA%3D

2– No Redirection from HTTP to HTTPS

2.1– https://bafs.da.gov.ph/

3– WordPress Login Page Found

3.1– https://www.da.gov.ph/wp-login.php

4– Insecure Inline Frame

4.1– https://bafs.da.gov.ph/page/contact
4.2– https://bafs.da.gov.ph/page/ListPGSCertifiedOrganicFarmer-MembersinthePhilippines
4.3– https://bafs.da.gov.ph/page/OrganicAgricultureResources
4.4– https://bafs.da.gov.ph/page/OrganicAgricultureResources
4.5– https://bafs.da.gov.ph/page/OrganicAgricultureResources
4.6– https://bafs.da.gov.ph/page/OrganicAgricultureResources
4.7– https://bafs.da.gov.ph/page/OrganicAgricultureResources
4.8– https://bafs.da.gov.ph/page/OrganicAgricultureResources
4.9– https://bafs.da.gov.ph/page/OrganicAgricultureResources
4.10– https://bafs.da.gov.ph/page/OrganicAgricultureResources
4.11– https://bafs.da.gov.ph/page/OrganicAgricultureResources

5– Subresource Integrity is Missing

5.1– https://bafs.da.gov.ph/
5.2– https://bafs.da.gov.ph/page/NewsRelease

6– Strict-Transport-Security Header is Missing

6.1– https://bafs.da.gov.ph/

7– Content-Security-Policy Header is Missing

7.1– https://bafs.da.gov.ph/

8– X-Frame-Options Header is Missing

8.1– https://bafs.da.gov.ph/

9– Email Address Disclosure

9.1– https://bafs.da.gov.ph/

9.2– https://bafs.da.gov.ph/page/OBCAManual

9.3– https://bafs.da.gov.ph/page/OrganicAgricultureResources

9.4– https://bafs.da.gov.ph/page/read_more_news_article?news=MTA3Mg%3D%3D or 1%3DExtractValue(1,CoNCaT(0x3a,(md5(122459))))&article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODA%3D

10– Target Information

10.1– https://bafs.da.gov.ph

10.2– https://www.da.gov.ph

11– X-Content-Type-Options Header is Missing

11.1– https://bafs.da.gov.ph/

12– Missing or Insecure Cache-Control Header

12.1– https://bafs.da.gov.ph/page/InfoGraphics

13– Referrer-Policy Header is Missing

13.1– https://bafs.da.gov.ph/

1.1 Internal Server Error

SEVERITY	Low
URL	http://bafs.da.gov.ph/
HTTP ERROR	502

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 502 Connection refused
Date: Thu, 11 Apr 2024 23:33:13 GMT
Cache-Control: no-cache
Pragma: no-cache
Content-Type: text/html; charset="UTF-8"
Content-Length: 74230
Via: HTTP/1.1 forward.http.proxy:3128
Connection: close


                    <!doctype html>
                    <html>
                        <head>
                            <meta charset='utf-8'>

...[truncated]...
```

DESCRIPTION

Unhandled exceptions have two primary risks.

- **Denial of service:** When an unhandled exception occurs, it might cause memory leakage or consume server resources by performing more process than usual.
- **Leaking information:** Unhandled exceptions can generate error messages with sensitive information. When these error messages are shown to users, attackers can take advantage of them to develop their attack on the target.

RECOMMENDATION

Properly handle all types of exceptions and display a generic error message.

1.2 Internal Server Error

SEVERITY	Medium
URL	https://bafs.da.gov.ph/page/read_more_news_article?news=a%7Cid&article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODA%3D
REFERER	https://bafs.da.gov.ph/
PARAMETER (QUERY)	news
AFFECTED URLS	bafs.da.gov.ph/page/read_more_news_article?article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODA%3D&news=a%7Cid bafs.da.gov.ph/page/read_more_news_article?article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODA%3D&news=(SELECT(1)FROM(SELECT(if(now()%3Dsysdate(),sleep(9),0)))A)
HTTP ERROR	500
INJECTION	a|id

DETAILS

When the `a|id` was set as the parameter `news` value, the server replied with the `500` error code.

REQUEST / RESPONSE

#1

```
GET /page/read_more_news_article?news=a%7Cid&article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODA%3D HTTP/1.1
Referer: https://bafs.da.gov.ph/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 500 Internal Server Error
Date: Fri, 12 Apr 2024 00:05:33 GMT
Server: Apache
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8


<!DOCTYPE html>
<html lang="en">

<head>
<script async src="https://www.googletagmanager.com/gtag/js?id=G-DQ2XPCY040"></script>
<script>
  window.dataL
...[truncated]...
```

DESCRIPTION

Unhandled exceptions have two primary risks.

- **Denial of service:** When an unhandled exception occurs, it might cause memory leakage or consume server resources by performing more process than usual.

- **Leaking information:** Unhandled exceptions can generate error messages with sensitive information. When these error messages are shown to users, attackers can take advantage of them to develop their attack on the target.

RECOMMENDATION

Properly handle all types of exceptions and display a generic error message.

2.1 No Redirection from HTTP to HTTPS

SEVERITY	Medium
URL	https://bafs.da.gov.ph/

DESCRIPTION

When HTTPS is enabled but, HTTP requests are not redirected to HTTPS automatically, users have to open the HTTPS URL explicitly. Otherwise, communication is not encrypted and can be captured by an attacker who has access to a network interface.

RECOMMENDATION

Enforce using HTTPS. You can do it by redirecting any HTTP request to HTTPS using your application or web server configuration. You can also use the **Strict-Transport-Security** HTTP response header as an extra security defense.

3.1 WordPress Login Page Found

SEVERITY	Medium
URL	https://www.da.gov.ph/wp-login.php

REQUEST / RESPONSE

#1

```
GET /wp-login.php HTTP/1.1
Referer: https://www.da.gov.ph/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:04:12 GMT
Server:
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
Set-Cookie: wordpress_test_cookie=WP%20Cookie%20check; path=/; secure
Upgrade: h2,h2c
Connection: Upgrade, Keep-Alive
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=100
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
        <html lang="en-US">
        <head>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
        <title>Log In &lsaquo; Official Portal of t
...[truncated]...
```

DESCRIPTION

WordPress `wp-login.php` is a well-known login page for both users and administrators. *Password guessing* and *Brute Force* attacks are the main methods attackers use to break into WordPress using this page. Another common attack is sending too many requests to this page and causing *Denial Of Service*.

RECOMMENDATION

You can take the following actions:

- Restrict access to `wp-login.php`
- Do not use the `admin` username
- Use strong passwords

- Limit number of failed login attempts
- Use two-factor authentication

See references for more.

4.1 Insecure Inline Frame

SEVERITY	Low
URL	https://bafs.da.gov.ph/page/contact
IFRAME URL	https://maps.google.com/maps?q=BAFS Building , Visayas Avenue, Diliman Quezon City 1101 Philippines&t=k&z=15&ie=UTF8&iwloc=&output=embed

DETAILS

An `iframe` tag is loading an external URL without `sandbox` attribute.

REQUEST / RESPONSE

#1

```
GET /page/contact HTTP/1.1
Referer: https://bafs.da.gov.ph/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:04:46 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
   </div>
          </aside>
        </div>
        <div class="span8">
          <iframe id="gmap_canvas" src="https://maps.google.com/maps?q=BAFS%20Building%2
...[truncated]...
```

DESCRIPTION

An inline frame tag (`iframe`) on the page refers to an external resource, and no `sandbox` is set. This allows the external URL to trick users into doing unwanted actions like submitting passwords.

RECOMMENDATION

Set `sandbox` attribute for iframes with external URL.

4.2 Insecure Inline Frame

SEVERITY	Low
URL	https://bafs.da.gov.ph/page/ListPGSCertifiedOrganicFarmer-MembersinthePhilippines
IFRAME URL	https://www.google.com/maps/d/u/3/embed?mid=1adwj1i3pXhUtn44nY55ajUxAigCixhM&ehbc=2E312F

DETAILS

An `iframe` tag is loading an external URL without `sandbox` attribute.

REQUEST / RESPONSE

#1

```
GET /page/ListPGSCertifiedOrganicFarmer-MembersinthePhilippines HTTP/1.1
Referer: https://bafs.da.gov.ph/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:04:46 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=97
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...


                        </div>
             <div class="tab-pane fade" id="map">
             <iframe src="https://www.google.com/maps/d/u/3/embed?mid=1adwj1i3pXhUtn44nY55a
...[truncated]...
```

DESCRIPTION

An inline frame tag (`iframe`) on the page refers to an external resource, and no `sandbox` is set. This allows the external URL to trick users into doing unwanted actions like submitting passwords.

RECOMMENDATION

Set `sandbox` attribute for iframes with external URL.

4.3 Insecure Inline Frame

SEVERITY	Low
URL	https://bafs.da.gov.ph/page/OrganicAgricultureResources
IFRAME URL	https://docs.google.com/spreadsheets/d/e/2PACX-1vRnYflkTrDE6F3pqaWENHcOryik9s0SU_rnjmbviZZk6z-chCZUx_9v2QlFBGMcFg/pubhtml?gid=1809074667&single=true&widget=true&headers=false

DETAILS

An `iframe` tag is loading an external URL without `sandbox` attribute.

REQUEST / RESPONSE

#1

```
GET /page/OrganicAgricultureResources HTTP/1.1
Referer: https://bafs.da.gov.ph/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:04:45 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

...[truncated]...
          <div class="tab-pane fade in active" id="osaproducts">
               <iframe   src="https://docs.google.com/spreadsheets/d/e/2PACX-1vRnYflkTrDE6F3p
...[truncated]...
```

DESCRIPTION

An inline frame tag (`iframe`) on the page refers to an external resource, and no `sandbox` is set. This allows the external URL to trick users into doing unwanted actions like submitting passwords.

RECOMMENDATION

Set `sandbox` attribute for iframes with external URL.

4.4 Insecure Inline Frame

SEVERITY	Low
URL	https://bafs.da.gov.ph/page/OrganicAgricultureResources
IFRAME URL	https://docs.google.com/spreadsheets/d/e/2PACX-1vTp5kBCtXP6ijq2srGrKLvD-2eEb_kv20uTYpDMZePa7BP8oaTbE4uD1-h8-7qReg/pubhtml?gid=1809074667&single=true&widget=true&headers=false

DETAILS

An `iframe` tag is loading an external URL without `sandbox` attribute.

REQUEST / RESPONSE

#1

```
GET /page/OrganicAgricultureResources HTTP/1.1
Referer: https://bafs.da.gov.ph/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:04:45 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

...[truncated]...
iv>
              <div class="tab-pane fade" id="osaproducers">
                <iframe src="https://docs.google.com/spreadsheets/d/e/2PACX-1vTp5kBCtXP6ijq2sr
...[truncated]...
```

DESCRIPTION

An inline frame tag (`iframe`) on the page refers to an external resource, and no `sandbox` is set. This allows the external URL to trick users into doing unwanted actions like submitting passwords.

RECOMMENDATION

Set `sandbox` attribute for iframes with external URL.

4.5 Insecure Inline Frame

SEVERITY	Low
URL	https://bafs.da.gov.ph/page/OrganicAgricultureResources
IFRAME URL	https://docs.google.com/spreadsheets/d/e/2PACX-1vQgFBQwH0nhIaeQUKw92283JnZ8kBI7CPI-69VpI7XfVbsCDp91Qs8UKjMsjwCsBQ/pubhtml?gid=1056614392&single=true&widget=true&headers=false

DETAILS

An `iframe` tag is loading an external URL without `sandbox` attribute.

REQUEST / RESPONSE

#1

```
GET /page/OrganicAgricultureResources HTTP/1.1
Referer: https://bafs.da.gov.ph/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:04:45 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

...[truncated]...
      </div>
                        <div class="tab-pane fade" id="obcaproducts">
                <iframe src="https://docs.google.com/spreadsheets/d/e/2PACX-1vQgFBQwH0nhIaeQUK
...[truncated]...
```

DESCRIPTION

An inline frame tag (`iframe`) on the page refers to an external resource, and no `sandbox` is set. This allows the external URL to trick users into doing unwanted actions like submitting passwords.

RECOMMENDATION

Set `sandbox` attribute for iframes with external URL.

4.6 Insecure Inline Frame

SEVERITY	Low
URL	https://bafs.da.gov.ph/page/OrganicAgricultureResources
IFRAME URL	https://docs.google.com/spreadsheets/d/e/2PACX-1vTC0KkfKR57A5kgcbGKwW80gDEiJh0B5vWwFNV3O5Z3TxAq0yzGejjdIKOGw6wUTg/pubhtml?gid=1056614392&single=true&widget=true&headers=false

DETAILS

An `iframe` tag is loading an external URL without `sandbox` attribute.

REQUEST / RESPONSE

#1

```
GET /page/OrganicAgricultureResources HTTP/1.1
Referer: https://bafs.da.gov.ph/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:04:45 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

...[truncated]...
                        </div>
                        <div class="tab-pane fade" id="obcaproducers">
                <iframe src="https://docs.google.com/spreadsheets/d/e/2PACX-1vTC0KkfKR57A5kgcb
...[truncated]...
```

DESCRIPTION

An inline frame tag (`iframe`) on the page refers to an external resource, and no `sandbox` is set. This allows the external URL to trick users into doing unwanted actions like submitting passwords.

RECOMMENDATION

Set `sandbox` attribute for iframes with external URL.

4.7 Insecure Inline Frame

SEVERITY	Low
URL	https://bafs.da.gov.ph/page/OrganicAgricultureResources
IFRAME URL	https://docs.google.com/spreadsheets/d/e/2PACX-1vQiuZltAZvV7kkcLbqyMGSipFdgf6Nl5HFLaa36W7H6Etu3HQ6c3hbdOv2ED0tmfA/pubhtml?gid=1913912109&single=true&widget=true&headers=false

DETAILS

An `iframe` tag is loading an external URL without `sandbox` attribute.

REQUEST / RESPONSE

#1

```
GET /page/OrganicAgricultureResources HTTP/1.1
Referer: https://bafs.da.gov.ph/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:04:45 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

...[truncated]...

              </div>
                          <div class="tab-pane fade" id="organicfarm">
                          <iframe src="https://docs.google.com/spreadsheets/d/e/2PACX-1vQiuZltAZvV7kkcLb
...[truncated]...
```

DESCRIPTION

An inline frame tag (`iframe`) on the page refers to an external resource, and no `sandbox` is set. This allows the external URL to trick users into doing unwanted actions like submitting passwords.

RECOMMENDATION

Set `sandbox` attribute for iframes with external URL.

4.8 Insecure Inline Frame

SEVERITY	Low
URL	https://bafs.da.gov.ph/page/OrganicAgricultureResources
IFRAME URL	https://docs.google.com/spreadsheets/d/e/2PACX-1vR2vEAN28R-7eCTZh8J-Yp28uGgQ6KCGp5BdXN1TNaSLhvqj-kpcK9pUTlfl__Apy4EX6YTIHj9PVD8/pubhtml?gid=243602999&single=true&widget=true&headers=false

DETAILS

An `iframe` tag is loading an external URL without `sandbox` attribute.

REQUEST / RESPONSE

#1

```
GET /page/OrganicAgricultureResources HTTP/1.1
Referer: https://bafs.da.gov.ph/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:04:45 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

...[truncated]...
iv>

                        <div class="tab-pane fade" id="obcaresearcher">
              <iframe src="https://docs.google.com/spreadsheets/d/e/2PACX-1vR2vEAN28R-7eCTZh
...[truncated]...
```

DESCRIPTION

An inline frame tag (`iframe`) on the page refers to an external resource, and no `sandbox` is set. This allows the external URL to trick users into doing unwanted actions like submitting passwords.

RECOMMENDATION

Set `sandbox` attribute for iframes with external URL.

4.9 Insecure Inline Frame

SEVERITY	Low
URL	https://bafs.da.gov.ph/page/OrganicAgricultureResources
IFRAME URL	https://docs.google.com/spreadsheets/d/e/2PACX-1vSUq8_VKuViZhakLZ0LZ3epSkNQkgwbk15AapHg-IDCRtDh5SOHvpArdhsp6LFtsfyydMvwJL0yvf8q/pubhtml?gid=1028191100&single=true&widget=true&headers=false

DETAILS

An `iframe` tag is loading an external URL without `sandbox` attribute.

REQUEST / RESPONSE

#1

```
GET /page/OrganicAgricultureResources HTTP/1.1
Referer: https://bafs.da.gov.ph/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:04:45 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

...[truncated]...
              </div>
                          <div class="tab-pane fade" id="pgs">
                <iframe src="https://docs.google.com/spreadsheets/d/e/2PACX-1vSUq8_VKuViZhakLZ
...[truncated]...
```

DESCRIPTION

An inline frame tag (`iframe`) on the page refers to an external resource, and no `sandbox` is set. This allows the external URL to trick users into doing unwanted actions like submitting passwords.

RECOMMENDATION

Set `sandbox` attribute for iframes with external URL.

4.10 Insecure Inline Frame

SEVERITY	Low
URL	https://bafs.da.gov.ph/page/OrganicAgricultureResources
IFRAME URL	https://docs.google.com/spreadsheets/d/1JQ-dUHHAb9p3yUpvjGfItTN65FqlnKcFr7jKpIlKkDo/pubhtml?gid=676660840&single=true&widget=true&headers=false

DETAILS

An `iframe` tag is loading an external URL without `sandbox` attribute.

REQUEST / RESPONSE

#1

```
GET /page/OrganicAgricultureResources HTTP/1.1
Referer: https://bafs.da.gov.ph/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:04:45 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

...[truncated]...
            </div>
                        <div class="tab-pane fade" id="operators">
            <iframe src="https://docs.google.com/spreadsheets/d/1JQ-dUHHAb9p3yUpvjGfItTN65
...[truncated]...
```

DESCRIPTION

An inline frame tag (`iframe`) on the page refers to an external resource, and no `sandbox` is set. This allows the external URL to trick users into doing unwanted actions like submitting passwords.

RECOMMENDATION

Set `sandbox` attribute for iframes with external URL.

4.11 Insecure Inline Frame

SEVERITY	Low
URL	https://bafs.da.gov.ph/page/OrganicAgricultureResources
AFFECTED URLS	bafs.da.gov.ph/page/ListPGSCertifiedOrganicFarmer-MembersinthePhilippines bafs.da.gov.ph/page/OrganicAgricultureResources
IFRAME URL	https://docs.google.com/spreadsheets/d/e/2PACX-1vQHuSgY8qAvlxuI3Tq0BG5B9_16XqCZT2zlMGialEXwV0D6RFD9T9p-SqzOd8kpthMcbSF0j5BZWhCn/pubhtml?gid=676660840&single=true&widget=true&headers=false

DETAILS

An `iframe` tag is loading an external URL without `sandbox` attribute.

REQUEST / RESPONSE

#1

```
GET /page/OrganicAgricultureResources HTTP/1.1
Referer: https://bafs.da.gov.ph/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:04:45 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

...[truncated]...
         </div>
                        <div class="tab-pane fade" id="pgsfarmer">
              <iframe src="https://docs.google.com/spreadsheets/d/e/2PACX-1vQHuSgY8qAvlxuI3T
...[truncated]...
```

DESCRIPTION

An inline frame tag (`iframe`) on the page refers to an external resource, and no `sandbox` is set. This allows the external URL to trick users into doing unwanted actions like submitting passwords.

RECOMMENDATION

Set `sandbox` attribute for iframes with external URL.

5.1 Subresource Integrity is Missing

SEVERITY	Low
URL	https://bafs.da.gov.ph/
AFFECTED URLS (66)	bafs.da.gov.ph/page/read_more_news_article?article[]=NTIyYTlhZTlhOTk4ODBkMzllNWRhZWMzNTM3NWU5OTk%3D&news=MTA3OA%3D%3D bafs.da.gov.ph/page/read_more_news_article?news=MTA3Mg%3D%3D bafs.da.gov.ph/page/read_more_news_article?article=J1hPUigoU0VMRUNUKDEpRlJPTShTRUxFQ1QoaWYobm93KCk9c3lzZGF0ZSgpLHNsZWVwKDEwKSwwKSkpQSkpT1In&news=MTA3OA%3D%3D bafs.da.gov.ph/page/InfoGraphics bafs.da.gov.ph/page/read_more_news_article?article=OGExZTgwOGI1NWZkZTk0NTVjYjNkODg1N2VkODgzODk%3D&news=MTA3Ng%3D%3D bafs.da.gov.ph/page/read_more_news_article?article=OGExZTgwOGI1NWZkZTk0NTVjYjNkODg1N2VkODgzODk7IGlmICgxPTEpIHdhaXRmb3IgZGVsYXkgJzAwOjAwOjEwJy0t&news=MTA3Ng%3D%3D bafs.da.gov.ph/page/read_more_news_article?article=KFNFTEVDVCgxKUZST00oU0VMRUNUKGlmKG5vdygpPXN5c2RhdGUoKSxzbGVlcCg5KSwwKSkpQSk%3D&news=MTA3Ng%3D%3D bafs.da.gov.ph/page/read_more_news_article?article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODA%3D&news=MTA3Mg%3D%3D and 1%3E1-- a bafs.da.gov.ph/page/ListPGSCertifiedOrganicFarmer-MembersinthePhilippines bafs.da.gov.ph/page/OBCAManual bafs.da.gov.ph/page/read_more_news_article?article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODA%3D&news=a%7Cver bafs.da.gov.ph/page/read_more_news_article?article=OGExZTgwOGI1NWZkZTk0NTVjYjNkODg1N2VkODgzODknIGFuZCAxPjEtLSBh&news=MTA3Ng%3D%3D bafs.da.gov.ph/page/read_more_news_article?article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODA%3D&news=MTA3Mg%3D%3D or 1%3DExtractValue(1,CoNCaT(0x3a,(md5(122459)))) bafs.da.gov.ph/page/JointCirculars bafs.da.gov.ph/page/read_more_news_article?article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODA%3D&news=MTA3Mg%3D%3D'; if (1%3D1) waitfor delay '00:00:10'-- bafs.da.gov.ph/page/read_more_news_article?article=NTIyYTlhZTlhOTk4ODBkMzllNWRhZWMzNTM3NWU5OTknOyBpZiAoMT0xKSB3YWl0Zm9yIGRlbGF5ICcwMDowMDoxMSctLQ%3D%3D&news=MTA3OA%3D%3D bafs.da.gov.ph/page/read_more_news_article?article=YWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWE%3D&news=MTA3Ng%3D%3D bafs.da.gov.ph/page/FOImanual

EXTERNAL RESOURCES (10)

https://fonts.googleapis.com/css?family=Open+Sans:400italic,400,600,700
https://cdnjs.cloudflare.com/ajax/libs/d3/5.9.1/d3.min.js
https://cdn.datatables.net/1.10.21/css/jquery.dataTables.css
https://connect.facebook.net/en_US/sdk.js#xfbml=1&version=v18.0
https://cdn.rawgit.com/juijs/vue-graph/2216ae2f/dist/vue-graph.js
https://www.googletagmanager.com/gtag/js?id=G-DQ2XPCY040
https://cdnjs.cloudflare.com/ajax/libs/gsap/1.19.0/TweenMax.min.js
https://cdnjs.cloudflare.com/ajax/libs/vue/2.5.16/vue.js

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:03:58 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8


<!DOCTYPE html>
<html lang="en">

<head>
<script async src="https://www.googletagmanager.com/gtag/js?id=G-DQ2XPCY040"></script>
<script>
  window.dataLayer = window.dataLayer || [];
  function gtag(){dataLayer.push(arguments);}
  gtag('js', new Date());

  gtag('config', 'G-DQ2XPCY040');
</script>
  <meta charset="utf-8">
  <!--meta http-equiv="Content-Security-Policy" content="default-src https:" /-->
  <title>BAFS | Bureau Of Agriculture And Fisheries Standards </title>
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta name="description" content="">
  <meta name="author" content="">
   <meta name="viewport" content="width=device-width, initial-scale=1"><link rel="stylesheet" href="chart/style.css">
  <!-- styles -->
  <link href="https://fonts.googleapis.com/css?family=Open+Sans:400italic,400,600,700" rel="stylesheet">
  <link href="assets/css/bootstrap.css" rel="stylesheet">
  <link href="assets/css/bootstrap-responsive.css" rel
...[truncated]...
```

DESCRIPTION

Subresource Integrity (SRI) is a security feature that enables browsers to verify that resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing you to provide a cryptographic hash that a fetched resource must match. Moilla

RECOMMENDATION

Add a base64-encoded hash of the resource in the value of the `integrity` attribute of the `<script>` or `<link>` element. You can ask the resource provider for the hash of the file or calculate it on your own. Please references for details.

5.2 Subresource Integrity is Missing

SEVERITY	Low
URL	https://bafs.da.gov.ph/page/NewsRelease
AFFECTED URLS	bafs.da.gov.ph/page/read_more_news_article?article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODA%3D&news=a%7Cid bafs.da.gov.ph/page/read_more_news_article?article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODA%3D&news=(SELECT(1)FROM(SELECT(if(now()%3Dsysdate(),sleep(9),0)))A) bafs.da.gov.ph/page/NewsRelease
EXTERNAL RESOURCES	https://cdn.plot.ly/plotly-latest.min.js https://fonts.googleapis.com/css?family=Open+Sans:400italic,400,600,700 https://cdn.datatables.net/1.10.21/css/jquery.dataTables.css https://connect.facebook.net/en_US/sdk.js#xfbml=1&version=v18.0 https://www.googletagmanager.com/gtag/js?id=G-DQ2XPCY040

REQUEST / RESPONSE

#1

```
GET /page/NewsRelease HTTP/1.1
Referer: https://bafs.da.gov.ph/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:04:45 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8


<!DOCTYPE html>
<html lang="en">

<head>
<script async src="https://www.googletagmanager.com/gtag/js?id=G-DQ2XPCY040"></script>
<script>
  window.dataLayer = window.dataLayer || [];
  function gtag(){dataLayer.push(arguments);}
  gtag('js', new Date());

  gtag('config', 'G-DQ2XPCY040');
</script>
  <meta charset="utf-8">
  <!--meta http-equiv="Content-Security-Policy" content="default-src https:" /-->
  <title>BAFS | Bureau Of Agriculture And Fisheries Standards </title>
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
```

```
  <meta name="description" content="">
  <meta name="author" content="">
   <meta name="viewport" content="width=device-width, initial-scale=1"><link rel="stylesheet" href="chart/style.css">
  <!-- styles -->
  <link href="https://fonts.googleapis.com/css?family=Open+Sans:400italic,400,600,700" rel="stylesheet">
  <link href="assets/css/bootstrap.css" rel="stylesheet">
  <link href="assets/css/bootstrap-responsive.css" rel
...[truncated]...
```

DESCRIPTION

Subresource Integrity (SRI) is a security feature that enables browsers to verify that resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing you to provide a cryptographic hash that a fetched resource must match. Moilla

RECOMMENDATION

Add a base64-encoded hash of the resource in the value of the `integrity` attribute of the `<script>` or `<link>` element. You can ask the resource provider for the hash of the file or calculate it on your own. Please references for details.

6.1 Strict-Transport-Security Header is Missing

SEVERITY	Low
URL	https://bafs.da.gov.ph/
AFFECTED URLS (17)	bafs.da.gov.ph bafs.da.gov.ph/page/Comics bafs.da.gov.ph/page/ListPGSCertifiedOrganicFarmer-MembersinthePhilippines bafs.da.gov.ph/page/contact bafs.da.gov.ph/page/read_more_news_article bafs.da.gov.ph/index bafs.da.gov.ph/page/OrganicAgricultureResources bafs.da.gov.ph/page/OrganicAgriculture bafs.da.gov.ph/page/GeneralMemorandumsOrders bafs.da.gov.ph/page/DraftPhilippinesNationalStandards bafs.da.gov.ph/page/FOImanual bafs.da.gov.ph/page/OBCAManual bafs.da.gov.ph/page/OperationsManual bafs.da.gov.ph/page/JointCirculars bafs.da.gov.ph/page/InfoGraphics bafs.da.gov.ph/page/Third-PartyAccreditedOrganicCertifyingBodies bafs.da.gov.ph/page/NewsRelease

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:03:58 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8


<!DOCTYPE html>
<html lang="en">

<head>
<script async src="https://www.googletagmanager.com/gtag/js?id=G-DQ2XPCY040"></script>
<script>
  window.dataLa
...[truncated]...
```

DESCRIPTION

The HTTP Strict-Transport-Security response header (often abbreviated as HSTS) lets a web site tell browsers that it should only be accessed using HTTPS, instead of using HTTP. Mozilla

RECOMMENDATION

Configure your server to send this header for all pages. You can see references for possible values.

7.1 Content-Security-Policy Header is Missing

SEVERITY	Low
URL	https://bafs.da.gov.ph/
AFFECTED URLS (17)	bafs.da.gov.ph bafs.da.gov.ph/page/Comics bafs.da.gov.ph/page/ListPGSCertifiedOrganicFarmer-MembersinthePhilippines bafs.da.gov.ph/page/contact bafs.da.gov.ph/page/read_more_news_article bafs.da.gov.ph/index bafs.da.gov.ph/page/OrganicAgricultureResources bafs.da.gov.ph/page/OrganicAgriculture bafs.da.gov.ph/page/GeneralMemorandumsOrders bafs.da.gov.ph/page/DraftPhilippinesNationalStandards bafs.da.gov.ph/page/FOImanual bafs.da.gov.ph/page/OBCAManual bafs.da.gov.ph/page/OperationsManual bafs.da.gov.ph/page/JointCirculars bafs.da.gov.ph/page/InfoGraphics bafs.da.gov.ph/page/Third-PartyAccreditedOrganicCertifyingBodies bafs.da.gov.ph/page/NewsRelease

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:03:58 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8


<!DOCTYPE html>
<html lang="en">

<head>
<script async src="https://www.googletagmanager.com/gtag/js?id=G-DQ2XPCY040"></script>
<script>
  window.dataLa
...[truncated]...
```

DESCRIPTION

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement to distribution of malware. Mozilla

RECOMMENDATION

Configure your server to send this header for all pages. You can see references for possible values.

8.1 X-Frame-Options Header is Missing

SEVERITY	Low
URL	https://bafs.da.gov.ph/
AFFECTED URLS (17)	bafs.da.gov.ph bafs.da.gov.ph/page/Comics bafs.da.gov.ph/page/ListPGSCertifiedOrganicFarmer-MembersinthePhilippines bafs.da.gov.ph/page/contact bafs.da.gov.ph/page/read_more_news_article bafs.da.gov.ph/index bafs.da.gov.ph/page/OrganicAgricultureResources bafs.da.gov.ph/page/OrganicAgriculture bafs.da.gov.ph/page/GeneralMemorandumsOrders bafs.da.gov.ph/page/DraftPhilippinesNationalStandards bafs.da.gov.ph/page/FOImanual bafs.da.gov.ph/page/OBCAManual bafs.da.gov.ph/page/OperationsManual bafs.da.gov.ph/page/JointCirculars bafs.da.gov.ph/page/InfoGraphics bafs.da.gov.ph/page/Third-PartyAccreditedOrganicCertifyingBodies bafs.da.gov.ph/page/NewsRelease

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:03:58 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8


<!DOCTYPE html>
<html lang="en">

<head>
<script async src="https://www.googletagmanager.com/gtag/js?id=G-DQ2XPCY040"></script>
<script>
  window.dataLa
...[truncated]...
```

DESCRIPTION

The `X-Frame-Options` HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a `<frame>`, `<iframe>`, `<embed>` or `<object>`. Sites can use this to avoid click-jacking attacks, by ensuring that their content is not embedded into other sites. Mozilla

RECOMMENDATION

Configure your server to send this header for all pages. You can see references for possible values.

9.1 Email Address Disclosure

SEVERITY: Informational

URL: https://bafs.da.gov.ph/

FOUND EMAILS: bafs@da.gov.ph

FOUND IN (46):

bafs.da.gov.ph/page/read_more_news_article?article[]=NTIyYTlhZTlhOTk4ODBkMzllNWRhZWMzNTM3NWU5OTk%3D&news=MTA3OA%3D%3D
bafs.da.gov.ph/page/read_more_news_article?article=J1hPUigoU0VMRUNUKDEpRlJPTShTRUxFQ1QoaWYobm93KCk9c3lzZGF0ZSgpLHNsZWVwKDEwKSwwKSkpQSkpT1In&news=MTA3OA%3D%3D
bafs.da.gov.ph/page/InfoGraphics
bafs.da.gov.ph/page/read_more_news_article?article=OGExZTgwOGI1NWZkZTk0NTVjYjNkODg1N2VkODgzODk7IGlmICgxPTEpIHdhaXRmb3IgZGVsYXkgJzAwOjAwOjEwJy0t&news=MTA3Ng%3D%3D
bafs.da.gov.ph/page/read_more_news_article?article=OGExZTgwOGI1NWZkZTk0NTVjYjNkODg1N2VkODgzODk%3D&news=MTA3Ng%3D%3D
bafs.da.gov.ph/page/read_more_news_article?article=KFNFTEVDVCgxKUZST00oU0VMRUNUKGlmKG5vdygpPXN5c2RhdGUoKSxzbGVlcCg5KSwwKSkpQSk%3D&news=MTA3Ng%3D%3D
bafs.da.gov.ph/page/ListPGSCertifiedOrganicFarmer-MembersinthePhilippines
bafs.da.gov.ph/page/read_more_news_article?article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODA%3D&news=a%7Cver
bafs.da.gov.ph/page/read_more_news_article?article=OGExZTgwOGI1NWZkZTk0NTVjYjNkODg1N2VkODgzODknIGFuZCAxPjEtLSBh&news=MTA3Ng%3D%3D
bafs.da.gov.ph/page/JointCirculars
bafs.da.gov.ph/page/read_more_news_article?article=NTIyYTlhZTlhOTk4ODBkMzllNWRhZWMzNTM3NWU5OTknOyBpZiAoMT0xKSB3YWl0Zm9yIGRlbGF5ICcwMDowMDoxMSctLQ%3D%3D&news=MTA3OA%3D%3D
bafs.da.gov.ph/page/read_more_news_article?article=YWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWE%3D&news=MTA3Ng%3D%3D
bafs.da.gov.ph/page/FOImanual
bafs.da.gov.ph/page/read_more_news_article?article=OTk5OTkgb3IgMT4wLS0gYQ%3D%3D&news=MTA3OA%3D%3D
bafs.da.gov.ph/page/DraftPhilippinesNationalStandards
bafs.da.gov.ph/page/read_more_news_article?article=NTIyYTlhZTlhOTk4ODBkMzllNWRhZWMzNTM3NWU5OTkgb3IgMT1FeHRyYWN0VmFsdWUoMSxDb05DYVQoMHgzYSwobWQ1KDEyMjQ1OSkpKSk%3D&news=MTA3OA%3D%3D
bafs.da.gov.ph/page/GeneralMemorandumsOrders

REQUEST / RESPONSE

bafs.da.gov.ph/page/read_more_news_article?article=[illegible]
[illegible]
(9),0)))A))OR'

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:03:58 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

...[truncated]...
"></i> bafs@da.gov.ph
                                                </address-->
                         <ul
...[truncated]...
```

DESCRIPTION

Spambots can harvest email addresses from webpages and use them for sending spam emails.

RECOMMENDATION

Do not show personal email addresses. Use submission forms with CAPTCHA for receiving messages.

9.2 Email Address Disclosure

SEVERITY	Informational
URL	https://bafs.da.gov.ph/page/OBCAManual
FOUND EMAILS	bafs@da.gov.ph oars.bafs@gmail.com

REQUEST / RESPONSE

#1

```
GET /page/OBCAManual HTTP/1.1
Referer: https://bafs.da.gov.ph/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:05:31 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...[truncated]...
> oars.bafs@gmail.com</li>
              </ul>
            </div>
          </aside>
        </div>
                        <div class="span8">
                         <ul id="myTab" class="nav nav-tabs">
             <li class="active"><a href="#manual" data-to
...[truncated]...
```

DESCRIPTION

Spambots can harvest email addresses from webpages and use them for sending spam emails.

RECOMMENDATION

Do not show personal email addresses. Use submission forms with CAPTCHA for receiving messages.

9.3 Email Address Disclosure

SEVERITY	Informational
URL	https://bafs.da.gov.ph/page/OrganicAgricultureResources
FOUND EMAILS (8)	bafs@da.gov.ph info@occpphils.org occp.min@gmail.com occp.vis@gmail.com swickramaarachchi@controlunion.com vgcanedo@controlunion.com nicertservices@gmail.com nicertservices08@yahoo.com
FOUND IN	bafs.da.gov.ph/page/OrganicAgricultureResources bafs.da.gov.ph/page/Third-PartyAccreditedOrganicCertifyingBodies

REQUEST / RESPONSE

#1

```
GET /page/OrganicAgricultureResources HTTP/1.1
Referer: https://bafs.da.gov.ph/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:04:45 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

...[truncated]...
: swickramaarachchi@controlunion.com, vgcanedo@controlunion.com</p>
                                                <p>Taguig City Telephone no.: (+63) 5310 2542 </p>
                            <p>Davao City Telephone no.: 082 222 0668 </p>
                                                <p>Website: https://certificatio
...[truncated]...
```

DESCRIPTION

Spambots can harvest email addresses from webpages and use them for sending spam emails.

RECOMMENDATION

Do not show personal email addresses. Use submission forms with CAPTCHA for receiving messages.

9.4 Email Address Disclosure

SEVERITY	Informational
URL	https://bafs.da.gov.ph/page/read_more_news_article?news=MTA3Mg%3D%3D or 1%3DExtractValue(1,CoNCaT(0x3a,(md5(122459))))&article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODA%3D
FOUND EMAILS	bafs@da.gov.ph register.bafs@gmail.com
FOUND IN (17)	bafs.da.gov.ph/page/read_more_news_article?article=OTk5OTkgb3IgMT4wLS0gYQ%3D%3D&news=MTA3Mg%3D%3D bafs.da.gov.ph/page/read_more_news_article?article=OTk5OTknIG9yIDE%2BMC0tIGE%3D&news=MTA3Mg%3D%3D bafs.da.gov.ph/page/read_more_news_article?article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODA%3D&news=MTA3Mg%3D%3D; if (1%3D1) waitfor delay '00:00:10'-- bafs.da.gov.ph/page/read_more_news_article?article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODA%3D&news=MTA3Mg%3D%3D bafs.da.gov.ph/page/read_more_news_article?news=MTA3Mg%3D%3D bafs.da.gov.ph/page/read_more_news_article?article=JyIhPy0lcw%3D%3D&news=MTA3Mg%3D%3D bafs.da.gov.ph/page/read_more_news_article?article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODA7IGlmICgxPTEpIHdhaXRmb3IgZGVsYXkgJzAwOjAwOjEwJy0t&news=MTA3Mg%3D%3D bafs.da.gov.ph/page/read_more_news_article?article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODA%3D&news=MTA3Mg%3D%3D' and 1%3E1-- a bafs.da.gov.ph/page/read_more_news_article?article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODA%3D&news=MTA3Mg%3D%3D and 1%3E1-- a bafs.da.gov.ph/page/read_more_news_article?article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODAgYW5kIDE%2BMS0tIGE%3D&news=MTA3Mg%3D%3D bafs.da.gov.ph/page/read_more_news_article?article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODAnIGFuZCAxPjEtLSBh&news=MTA3Mg%3D%3D bafs.da.gov.ph/page/read_more_news_article?article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODA%3D&news=MTA3Mg%3D%3D' or 1%3DExtractValue(1,CoNCaT(0x3a,(md5(122459)))) or 1%3D'2 bafs.da.gov.ph/page/read_more_news_article?article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODA%3D&news=MTA3Mg%3D%3D'; if (1%3D1) waitfor delay '00:00:10'-- bafs.da.gov.ph/page/read_more_news_article?article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODAgb3IgMT1FeHRyYWN0VmFsdWUoMSxDb05DYVQoMHgzYSwobWQ1KDEyMjQ1OSkpKSk%3D&news=MTA3Mg%3D%3D bafs.da.gov.ph/page/read_more_news_article?article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODA%3D&news=MTA3Mg%3D%3D or 1%3DExtractValue(1,CoNCaT(0x3a,(md5(122459)))) bafs.da.gov.ph/page/read_more_news_article?article=YXxpZA%3D%3D&news=MTA3Mg%3

REQUEST / RESPONSE

#1 bafs.da.gov.ph/page/read_more_news_article?article=KFNFTEVDVCgxKUZST00oU0VMRUNUKGlmKG5vdygpPXN5c2RhdGUoKSxzbGVlcCg5KSwwKSkpQSk%3D&news=MTA3Mg%3D%3D

```
GET /page/read_more_news_article?news=MTA3Mg%3D%3D%20or%201%3DExtractValue(1,CoNCaT(0x3a,(md5(122459))))&article=YTE1MTlkZTViNWQ0NGIzMWEwMWRlMDEzYjliNTFhODA%3D HTTP/1.1
Referer: https://bafs.da.gov.ph/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:05:33 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

...[truncated]...
t register.bafs@gmail.com</p>

<p>To register your organic input products, you may check our list of requirements: <a href="https://drive.google.com/file/d/11ltmbAuV4cCNqcKxT2k48VkRUAB5rzhM/view?fbclid=IwAR1KXzobBatH81FIAXsaT0MtuwxlYsUrprk6l9AKcz4b
...[truncated]...
```

DESCRIPTION

Spambots can harvest email addresses from webpages and use them for sending spam emails.

RECOMMENDATION

Do not show personal email addresses. Use submission forms with CAPTCHA for receiving messages.

10.1 Target Information

SEVERITY	Informational
URL	https://bafs.da.gov.ph
EMAILS (10)	bafs@da.gov.ph info@occpphils.org occp.min@gmail.com occp.vis@gmail.com swickramaarachchi@controlunion.com vgcanedo@controlunion.com nicertservices@gmail.com nicertservices08@yahoo.com register.bafs@gmail.com oars.bafs@gmail.com
HTTPS	TLS 1.2
SERVER BANNER	apache
SERVICES	HTTPS
WEB SERVER	apache

10.2 Target Information

SEVERITY	Informational
URL	https://www.da.gov.ph
WORDPRESS	https://www.da.gov.ph/

11.1 X-Content-Type-Options Header is Missing

SEVERITY	Informational
URL	https://bafs.da.gov.ph/
AFFECTED URLS (17)	bafs.da.gov.ph bafs.da.gov.ph/page/Comics bafs.da.gov.ph/page/ListPGSCertifiedOrganicFarmer-MembersinthePhilippines bafs.da.gov.ph/page/contact bafs.da.gov.ph/page/read_more_news_article bafs.da.gov.ph/index bafs.da.gov.ph/page/OrganicAgricultureResources bafs.da.gov.ph/page/OrganicAgriculture bafs.da.gov.ph/page/GeneralMemorandumsOrders bafs.da.gov.ph/page/DraftPhilippinesNationalStandards bafs.da.gov.ph/page/FOImanual bafs.da.gov.ph/page/OBCAManual bafs.da.gov.ph/page/OperationsManual bafs.da.gov.ph/page/JointCirculars bafs.da.gov.ph/page/InfoGraphics bafs.da.gov.ph/page/Third-PartyAccreditedOrganicCertifyingBodies bafs.da.gov.ph/page/NewsRelease

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:03:58 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8


<!DOCTYPE html>
<html lang="en">

<head>
<script async src="https://www.googletagmanager.com/gtag/js?id=G-DQ2XPCY040"></script>
<script>
  window.dataLa
...[truncated]...
```

DESCRIPTION

The `X-Content-Type-Options` response HTTP header is used by the server to prevent browsers from guessing the media type (MIME type).

This is known as **MIME sniffing** in which the browser guesses the correct MIME type by looking at the contents of the resource.
The absence of this header might cause browsers to transform non-executable content into executable content.

RECOMMENDATION

Configure your server to send this header with the value set to `nosniff`.

12.1 Missing or Insecure Cache-Control Header

SEVERITY	Informational
URL	https://bafs.da.gov.ph/page/InfoGraphics
AFFECTED URLS (16)	bafs.da.gov.ph/page/Comics bafs.da.gov.ph/page/ListPGSCertifiedOrganicFarmer-MembersinthePhilippines bafs.da.gov.ph/page/contact bafs.da.gov.ph/page/read_more_news_article bafs.da.gov.ph/index bafs.da.gov.ph/page/OrganicAgricultureResources bafs.da.gov.ph/page/OrganicAgriculture bafs.da.gov.ph/page/GeneralMemorandumsOrders bafs.da.gov.ph/page/DraftPhilippinesNationalStandards bafs.da.gov.ph/page/FOImanual bafs.da.gov.ph/page/OBCAManual bafs.da.gov.ph/page/OperationsManual bafs.da.gov.ph/page/JointCirculars bafs.da.gov.ph/page/InfoGraphics bafs.da.gov.ph/page/Third-PartyAccreditedOrganicCertifyingBodies bafs.da.gov.ph/page/NewsRelease

DETAILS

The `Cache-Control` header is not set

REQUEST / RESPONSE

#1

```
GET /page/InfoGraphics HTTP/1.1
Referer: https://bafs.da.gov.ph/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:04:45 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8


<!DOCTYPE html>
<html lang="en">
```

```
<head>
<script async src="https://www.googletagmanager.com/gtag/js?id=G-DQ2XPCY040"></script>
<script>
  window.dataLa
...[truncated]...
```

DESCRIPTION

Web cache or HTTP cache is a system for optimizing the web. Browsers cache contents of a resource once and reuse it on consequent requests. Caching images on the web can boost page load time. But clients should not be allowed to cache pages that display sensitive, dynamic, or user specific contents.

RECOMMENDATION

Set any of following headers to prevent clients from caching the page.

```
Cache-Control: no-cache, no-store
```

```
Cache-Control: max-age=0, must-revalidate
```

```
Cache-Control: private
```

13.1 Referrer-Policy Header is Missing

SEVERITY	Informational
URL	https://bafs.da.gov.ph/
AFFECTED URLS (17)	bafs.da.gov.ph bafs.da.gov.ph/page/Comics bafs.da.gov.ph/page/ListPGSCertifiedOrganicFarmer-MembersinthePhilippines bafs.da.gov.ph/page/contact bafs.da.gov.ph/page/read_more_news_article bafs.da.gov.ph/index bafs.da.gov.ph/page/OrganicAgricultureResources bafs.da.gov.ph/page/OrganicAgriculture bafs.da.gov.ph/page/GeneralMemorandumsOrders bafs.da.gov.ph/page/DraftPhilippinesNationalStandards bafs.da.gov.ph/page/FOImanual bafs.da.gov.ph/page/OBCAManual bafs.da.gov.ph/page/OperationsManual bafs.da.gov.ph/page/JointCirculars bafs.da.gov.ph/page/InfoGraphics bafs.da.gov.ph/page/Third-PartyAccreditedOrganicCertifyingBodies bafs.da.gov.ph/page/NewsRelease

REQUEST / RESPONSE

#1

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 12 Apr 2024 00:03:58 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8


<!DOCTYPE html>
<html lang="en">

<head>
<script async src="https://www.googletagmanager.com/gtag/js?id=G-DQ2XPCY040"></script>
<script>
  window.dataLa
...[truncated]...
```

DESCRIPTION

The `Referrer-Policy` HTTP header controls how much referrer information (sent via the `Referer` header) should be included with requests. Mozilla

The `Referer` (sic) header contains the address of the previous web page from which a link to the currently requested page was followed, which has lots of fairly innocent uses including analytics, logging, or optimized caching. However, there are more problematic uses such as tracking or stealing information, or even just side effects such as inadvertently leaking sensitive information. Mozilla

RECOMMENDATION

Configure your server to send the `Referrer-Policy` header for all pages with the value set to `strict-origin-when-cross-origin`. You can see references for other possible values.