Acunetix by Invicti

Comprehensive Report

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

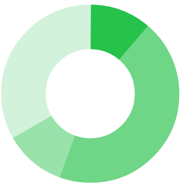
Scan Detail

Target	muslimbibah.ssbmultiservices.com
Scan Type	Full Scan
Start Time	Feb 8, 2024, 7:16:26 PM GMT+8
Scan Duration	24 minutes
Requests	8442
Average Response Time	1073ms
Maximum Response Time	29615ms
Application Build	v23.7.230728157

0	9	6	9
High	Medium	Low	Informational

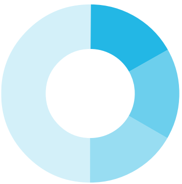
Severity	Vulnerabilities	Instances
High	0	0
Medium	4	9
Low	6	6
Informational	6	9
Total	16	24

Informational



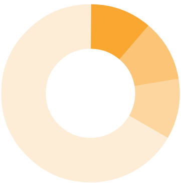
		Instances
🟩	Content Security Policy (CSP) not implement…	1
🟩	Outdated JavaScript libraries	4
🟩	Permissions-Policy header not implemented	1
🟩	Others	3

Low Severity



		Instances
🟦	Clickjacking: X-Frame-Options header	1
🟦	Cookies with missing, inconsistent or contra…	1
🟦	Cookies without Secure flag set	1
🟦	Others	3

Medium Severity



		Instances
🟧	Application error messages	1
🟧	Development configuration files	1
🟧	Directory listings	1
🟧	Others	6

Impacts

SEVERITY	IMPACT	
! Medium	1	Application error messages
! Medium	1	Development configuration files
! Medium	1	Directory listings
! Medium	6	Vulnerable JavaScript libraries
! Low	1	Clickjacking: X-Frame-Options header
! Low	1	Cookies with missing, inconsistent or contradictory properties
! Low	1	Cookies without Secure flag set
! Low	1	Documentation files
! Low	1	HTTP Strict Transport Security (HSTS) not implemented
! Low	1	Possible sensitive directories
ⓘ Informational	1	Content Security Policy (CSP) not implemented
ⓘ Informational	4	Outdated JavaScript libraries
ⓘ Informational	1	Permissions-Policy header not implemented
ⓘ Informational	1	Possible server path disclosure (Unix)
ⓘ Informational	1	Reverse proxy detected
ⓘ Informational	1	Subresource Integrity (SRI) not implemented

Application error messages

This alert requires manual confirmation

Acunetix found one or more error/warning messages. Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.
These messages may also contain the location of the file that produced an unhandled exception.
Consult the 'Attack details' section for more information about the affected page(s).

Impact

Error messages may disclose sensitive information which can be used to escalate attacks.

https://muslimbibah.ssbmultiservices.com/

Application error messages:

- https://muslimbibah.ssbmultiservices.com/search
  Unknown column 'Array' in 'where clause'

Request

```
POST /search HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: https://muslimbibah.ssbmultiservices.com/
Cookie: ci_session=c585cfa9268c1753244567e4295eccd08ea181da
Content-Length: 68
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: muslimbibah.ssbmultiservices.com
Connection: Keep-alive

age1[]=16&age2=19&gender=male&living=1&religion=Muslim&tounge=Arabic
```

Recommendation

Verify that these page(s) are disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.

References

PHP Runtime Configuration

https://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors
Improper Error Handling
https://www.owasp.org/index.php/Improper_Error_Handling

Development configuration files

One or more configuration files (e.g. Vagrantfile, Gemfile, Rakefile, ...) were found. These files may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of files from production systems.

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

https://muslimbibah.ssbmultiservices.com/

Development configuration files:

- https://muslimbibah.ssbmultiservices.com/**composer.json**

```
composer.json => Composer configuration file. Composer is a dependency manager
for PHP.
```

Request

```
GET /composer.json HTTP/1.1
Cookie: ci_session=c585cfa9268c1753244567e4295eccd08ea181da
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: muslimbibah.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Remove or restrict access to all configuration files acessible from internet.

Directory listings

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

https://muslimbibah.ssbmultiservices.com/ Verified

Folders with directory listing enabled:

- https://muslimbibah.ssbmultiservices.com/design/
- https://muslimbibah.ssbmultiservices.com/design/vendors/
- https://muslimbibah.ssbmultiservices.com/design/vendors/revolution/
- https://muslimbibah.ssbmultiservices.com/design/vendors/revolution/js/
- https://muslimbibah.ssbmultiservices.com/design/vendors/revolution/js/extensions/
- https://muslimbibah.ssbmultiservices.com/design/admin_panel/

Request

```
GET /design/ HTTP/1.1
Cookie: ci_session=c585cfa9268c1753244567e4295eccd08ea181da
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: muslimbibah.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

References

CWE-548: Exposure of Information Through Directory Listing
https://cwe.mitre.org/data/definitions/548.html

Vulnerable JavaScript libraries

You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

Impact

Consult References for more information.

https://muslimbibah.ssbmultiservices.com/ Confidence: 95%

- **jQuery 3.3.1**
  - URL: https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js
  - Detection method: The library's name and version were determined based on the file's CDN URI.
  - CVE-ID: CVE-2020-11022, CVE-2020-11023, CVE-2019-11358
  - Description: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / jQuery mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.
  - References:
    - https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
    - https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html
    - https://jquery.com/upgrade-guide/3.5/
    - https://api.jquery.com/jQuery.htmlPrefilter/
    - https://www.cvedetails.com/cve/CVE-2020-11022/
    - https://github.com/advisories/GHSA-gxr4-xjj5-5px2
    - https://www.cvedetails.com/cve/CVE-2020-11023/
    - https://github.com/advisories/GHSA-jpcq-cgw6-v4j6
    - https://github.com/jquery/jquery/pull/4333
    - https://nvd.nist.gov/vuln/detail/CVE-2019-11358
    - https://nvd.nist.gov/vuln/detail/CVE-2019-5428
    - https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/

Request

```
GET / HTTP/1.1
Referer: https://muslimbibah.ssbmultiservices.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: muslimbibah.ssbmultiservices.com
```

```
Connection: Keep-alive
```

https://muslimbibah.ssbmultiservices.com/ Confidence: 95%

- **jQuery 1.12.4**
  - URL: https://code.jquery.com/jquery-1.12.4.js
  - Detection method: The library's name and version were determined based on the file's CDN URI.
  - CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
  - Description: Possible Cross Site Scripting via third-party text/javascript responses (1.12.0-1.12.2 mitigation reverted) / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
  - References:
    - https://github.com/jquery/jquery/issues/2432
    - https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
    - https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html
    - https://jquery.com/upgrade-guide/3.5/
    - https://api.jquery.com/jQuery.htmlPrefilter/
    - https://www.cvedetails.com/cve/CVE-2020-11022/
    - https://github.com/advisories/GHSA-gxr4-xjj5-5px2
    - https://www.cvedetails.com/cve/CVE-2020-11023/
    - https://github.com/advisories/GHSA-jpcq-cgw6-v4j6

Request

```
GET / HTTP/1.1
Referer: https://muslimbibah.ssbmultiservices.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: muslimbibah.ssbmultiservices.com
Connection: Keep-alive
```

https://muslimbibah.ssbmultiservices.com/ Confidence: 95%

- **jQuery UI 1.12.1**
  - URL: https://code.jquery.com/ui/1.12.1/jquery-ui.js
  - Detection method: The library's name and version were determined based on the file's CDN URI.
  - CVE-ID: CVE-2021-41184

    - Description: XSS in the 'of' option of the '.position()' util
    - References:
        - https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/
        - https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327

Request

```
GET / HTTP/1.1
Referer: https://muslimbibah.ssbmultiservices.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: muslimbibah.ssbmultiservices.com
Connection: Keep-alive
```

https://muslimbibah.ssbmultiservices.com/ Confidence: 95%

- **jQuery 2.0.3**
    - URL: https://muslimbibah.ssbmultiservices.com/admin/
    - Detection method: The library's name and version were determined based on its dynamic behavior.
    - CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023, CVE-2019-11358
    - Description: Possible Cross Site Scripting via third-party text/javascript responses (1.12.0-1.12.2 mitigation reverted) / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / jQuery mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.
    - References:
        - https://github.com/jquery/jquery/issues/2432
        - https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
        - https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html
        - https://jquery.com/upgrade-guide/3.5/
        - https://api.jquery.com/jQuery.htmlPrefilter/
        - https://www.cvedetails.com/cve/CVE-2020-11022/
        - https://github.com/advisories/GHSA-gxr4-xjj5-5px2
        - https://www.cvedetails.com/cve/CVE-2020-11023/
        - https://github.com/advisories/GHSA-jpcq-cgw6-v4j6
        - https://github.com/jquery/jquery/pull/4333
        - https://nvd.nist.gov/vuln/detail/CVE-2019-11358
        - https://nvd.nist.gov/vuln/detail/CVE-2019-5428
        - https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/

Request

```
GET /admin/ HTTP/1.1
Referer: https://muslimbibah.ssbmultiservices.com/
Cookie: ci_session=c585cfa9268c1753244567e4295eccd08ea181da
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: muslimbibah.ssbmultiservices.com
Connection: Keep-alive
```

https://muslimbibah.ssbmultiservices.com/ Confidence: 95%

- **jQuery 2.1.4**
  - URL: https://muslimbibah.ssbmultiservices.com/search
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023, CVE-2019-11358
  - Description: Possible Cross Site Scripting via third-party text/javascript responses (1.12.0-1.12.2 mitigation reverted) / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / jQuery mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.
  - References:
    - https://github.com/jquery/jquery/issues/2432
    - https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
    - https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html
    - https://jquery.com/upgrade-guide/3.5/
    - https://api.jquery.com/jQuery.htmlPrefilter/
    - https://www.cvedetails.com/cve/CVE-2020-11022/
    - https://github.com/advisories/GHSA-gxr4-xjj5-5px2
    - https://www.cvedetails.com/cve/CVE-2020-11023/
    - https://github.com/advisories/GHSA-jpcq-cgw6-v4j6
    - https://github.com/jquery/jquery/pull/4333
    - https://nvd.nist.gov/vuln/detail/CVE-2019-11358
    - https://nvd.nist.gov/vuln/detail/CVE-2019-5428
    - https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/

Request

```
POST /search HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: https://muslimbibah.ssbmultiservices.com/
Cookie: ci_session=c585cfa9268c1753244567e4295eccd08ea181da
Content-Length: 66
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: muslimbibah.ssbmultiservices.com
Connection: Keep-alive

age1=16&age2=19&gender=male&living=1&religion=Muslim&tounge=Arabic
```

https://muslimbibah.ssbmultiservices.com/ Confidence: 95%

- **jQuery UI Datepicker 1.12.1**
  - URL: https://muslimbibah.ssbmultiservices.com/search
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: CVE-2021-41182, CVE-2021-41183
  - Description: XSS in the 'altField' option of the Datepicker widget / XSS in '*Text' options of the Datepicker widget
  - References:
    - https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/
    - https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwc
    - https://github.com/jquery/jquery-ui/security/advisories/GHSA-j7qv-pgf6-hvh4

Request

```
POST /search HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: https://muslimbibah.ssbmultiservices.com/
Cookie: ci_session=c585cfa9268c1753244567e4295eccd08ea181da
Content-Length: 66
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: muslimbibah.ssbmultiservices.com
Connection: Keep-alive

age1=16&age2=19&gender=male&living=1&religion=Muslim&tounge=Arabic
```

Recommendation

Upgrade to the latest version.

Clickjacking: X-Frame-Options header

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server did not return an **X-Frame-Options** header with the value DENY or SAMEORIGIN, which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into untrusted sites.

Impact

The impact depends on the affected web application.

https://muslimbibah.ssbmultiservices.com/

Paths without secure XFO header:

- https://muslimbibah.ssbmultiservices.com/
- https://muslimbibah.ssbmultiservices.com/admin/
- https://muslimbibah.ssbmultiservices.com/search
- https://muslimbibah.ssbmultiservices.com/access
- https://muslimbibah.ssbmultiservices.com/Welcome/searchByid/2
- https://muslimbibah.ssbmultiservices.com/resources/demos/style.css
- https://muslimbibah.ssbmultiservices.com/Welcome2/complaint
- https://muslimbibah.ssbmultiservices.com/memberDetails/26
- https://muslimbibah.ssbmultiservices.com/Welcome2/complaintSend

Request

```
GET / HTTP/1.1
Referer: https://muslimbibah.ssbmultiservices.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: muslimbibah.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

References

The X-Frame-Options response header
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Clickjacking
https://en.wikipedia.org/wiki/Clickjacking

OWASP Clickjacking
https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

Frame Buster Buster
https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed

Cookies with missing, inconsistent or contradictory properties

At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.

Impact

Cookies will not be stored, or submitted, by web browsers.

https://muslimbibah.ssbmultiservices.com/ Verified

List of cookies with missing, inconsistent or contradictory properties:

- https://muslimbibah.ssbmultiservices.com/

Cookie was set with:

```
Set-Cookie: ci_session=c585cfa9268c1753244567e4295eccd08ea181da; expires=Thu, 08-
Feb-2024 13:16:57 GMT; Max-Age=7200; path=/; HttpOnly
```

This cookie has the following issues:

```
- Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and
sometimes unexpected defaults. It is therefore recommended to add a SameSite
attribute with an appropriate value of either "Strict", "Lax", or "None".
```

Request

```
GET / HTTP/1.1
Referer: https://muslimbibah.ssbmultiservices.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: muslimbibah.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Ensure that the cookies configuration complies with the applicable standards.

References

MDN | Set-Cookie
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie

Securing cookies with cookie prefixes
https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/

Cookies: HTTP State Management Mechanism
https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05

SameSite Updates - The Chromium Projects
https://www.chromium.org/updates/same-site

draft-west-first-party-cookies-07: Same-site Cookies
https://tools.ietf.org/html/draft-west-first-party-cookies-07

Cookies without Secure flag set

One or more cookies does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL/TLS channels. This is an important security protection for session cookies.

Impact

Cookies could be sent over unencrypted channels.

https://muslimbibah.ssbmultiservices.com/ Verified

Cookies without Secure flag set:

- https://muslimbibah.ssbmultiservices.com/

```
Set-Cookie: ci_session=c585cfa9268c1753244567e4295eccd08ea181da; expires=Thu, 08-Feb-2024 13:16:57 GMT; Max-Age=7200; path=/; HttpOnly
```

Request

```
GET / HTTP/1.1
Referer: https://muslimbibah.ssbmultiservices.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: muslimbibah.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

If possible, you should set the Secure flag for these cookies.

Documentation files

One or more documentation files (e.g. readme.txt, changelog.txt, ...) were found. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

https://muslimbibah.ssbmultiservices.com/

Documentation files:

- https://muslimbibah.ssbmultiservices.com/**license.txt**
  File contents (first 100 characters):

```
The MIT License (MIT)

Copyright (c) 2014 - 2017, British Columbia Institute of Technology

Permissi ...
```

Request

```
GET /license.txt HTTP/1.1
Cookie: ci_session=c585cfa9268c1753244567e4295eccd08ea181da
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: muslimbibah.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Remove or restrict access to all documentation file acessible from internet.

HTTP Strict Transport Security (HSTS) not implemented

HTTP Strict Transport Security (HSTS) tells a browser that a web site is only accessable using HTTPS. It was detected that your web application doesn't implement HTTP Strict Transport Security (HSTS) as the Strict Transport Security header is missing from the response.

Impact

HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

https://muslimbibah.ssbmultiservices.com/

URLs where HSTS is not enabled:

- https://muslimbibah.ssbmultiservices.com/
- https://muslimbibah.ssbmultiservices.com/admin/
- https://muslimbibah.ssbmultiservices.com/search
- https://muslimbibah.ssbmultiservices.com/access
- https://muslimbibah.ssbmultiservices.com/Welcome/searchByid/2
- https://muslimbibah.ssbmultiservices.com/resources/demos/style.css
- https://muslimbibah.ssbmultiservices.com/Welcome2/complaint
- https://muslimbibah.ssbmultiservices.com/memberDetails/26
- https://muslimbibah.ssbmultiservices.com/Welcome2/complaintSend

Request

```
GET / HTTP/1.1
Referer: https://muslimbibah.ssbmultiservices.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: muslimbibah.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

It's recommended to implement HTTP Strict Transport Security (HSTS) into your web application. Consult web references for more information

References

hstspreload.org
https://hstspreload.org/

Strict-Transport-Security
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security

Possible sensitive directories

One or more possibly sensitive directories were found. These resources are not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

Impact

These directories may expose sensitive information that could help a malicious user to prepare more advanced attacks.

https://muslimbibah.ssbmultiservices.com/

Possible sensitive directories:

- https://muslimbibah.ssbmultiservices.com/**db**

Request

```
GET /db/ HTTP/1.1
Cookie: ci_session=c585cfa9268c1753244567e4295eccd08ea181da
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: muslimbibah.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Restrict access to these directories or remove them from the website.

References

Web Server Security and Database Server Security
https://www.acunetix.com/websitesecurity/webserver-security/

Content Security Policy (CSP) not implemented

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.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
default-src 'self';
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

https://muslimbibah.ssbmultiservices.com/

Paths without CSP header:

- https://muslimbibah.ssbmultiservices.com/
- https://muslimbibah.ssbmultiservices.com/admin/
- https://muslimbibah.ssbmultiservices.com/Welcome/searchByid/2
- https://muslimbibah.ssbmultiservices.com/resources/demos/style.css
- https://muslimbibah.ssbmultiservices.com/Welcome2/complaint
- https://muslimbibah.ssbmultiservices.com/memberDetails/26

Request

```
GET / HTTP/1.1
Referer: https://muslimbibah.ssbmultiservices.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: muslimbibah.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

Content Security Policy (CSP)
https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

Implementing Content Security Policy
https://hacks.mozilla.org/2016/02/implementing-content-security-policy/

Outdated JavaScript libraries

You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.

Impact

Consult References for more information.

https://muslimbibah.ssbmultiservices.com/ Confidence: 95%

- **bootstrap.js 3.3.4**
  - URL: https://muslimbibah.ssbmultiservices.com/admin/
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - References:
    - https://github.com/twbs/bootstrap/releases

Request

```
GET /admin/ HTTP/1.1
Referer: https://muslimbibah.ssbmultiservices.com/
Cookie: ci_session=c585cfa9268c1753244567e4295eccd08ea181da
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
```

```
Host: muslimbibah.ssbmultiservices.com
Connection: Keep-alive
```

https://muslimbibah.ssbmultiservices.com/ Confidence: 95%

- **jQuery UI Dialog 1.12.1**
  - URL: https://muslimbibah.ssbmultiservices.com/search
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - References:
    - https://jqueryui.com/download/

Request

```
POST /search HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: https://muslimbibah.ssbmultiservices.com/
Cookie: ci_session=c585cfa9268c1753244567e4295eccd08ea181da
Content-Length: 66
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: muslimbibah.ssbmultiservices.com
Connection: Keep-alive

age1=16&age2=19&gender=male&living=1&religion=Muslim&tounge=Arabic
```

https://muslimbibah.ssbmultiservices.com/ Confidence: 95%

- **jQuery UI Tooltip 1.12.1**
  - URL: https://muslimbibah.ssbmultiservices.com/search
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - References:
    - https://jqueryui.com/download/

Request

```
POST /search HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: https://muslimbibah.ssbmultiservices.com/
Cookie: ci_session=c585cfa9268c1753244567e4295eccd08ea181da
Content-Length: 66
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
```

```
Host: muslimbibah.ssbmultiservices.com
Connection: Keep-alive

age1=16&age2=19&gender=male&living=1&religion=Muslim&tounge=Arabic
```

https://muslimbibah.ssbmultiservices.com/ Confidence: 95%

- **bootstrap.js 3.3.7**
  - URL: https://muslimbibah.ssbmultiservices.com/search
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - References:
    - https://github.com/twbs/bootstrap/releases

Request

```
POST /search HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: https://muslimbibah.ssbmultiservices.com/
Cookie: ci_session=c585cfa9268c1753244567e4295eccd08ea181da
Content-Length: 66
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: muslimbibah.ssbmultiservices.com
Connection: Keep-alive

age1=16&age2=19&gender=male&living=1&religion=Muslim&tounge=Arabic
```

Recommendation

Upgrade to the latest version.

Permissions-Policy header not implemented

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

Impact

https://muslimbibah.ssbmultiservices.com/

Locations without Permissions-Policy header:

- https://muslimbibah.ssbmultiservices.com/
- https://muslimbibah.ssbmultiservices.com/admin/
- https://muslimbibah.ssbmultiservices.com/search
- https://muslimbibah.ssbmultiservices.com/access
- https://muslimbibah.ssbmultiservices.com/Welcome/searchByid/2
- https://muslimbibah.ssbmultiservices.com/resources/demos/style.css
- https://muslimbibah.ssbmultiservices.com/Welcome2/complaint
- https://muslimbibah.ssbmultiservices.com/memberDetails/26
- https://muslimbibah.ssbmultiservices.com/Welcome2/complaintSend

Request

```
GET / HTTP/1.1
Referer: https://muslimbibah.ssbmultiservices.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: muslimbibah.ssbmultiservices.com
Connection: Keep-alive
```

References

Permissions-Policy / Feature-Policy (MDN)
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

Permissions Policy (W3C)
https://www.w3.org/TR/permissions-policy-1/

Possible server path disclosure (Unix)

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

https://muslimbibah.ssbmultiservices.com/

Pages with paths being disclosed:

- https://muslimbibah.ssbmultiservices.com/Welcome2/complaintSend
  /home/ssbmul5/muslimbibah.ssbmultiservices.com/application/controllers/Welcome2.php

Request

```
POST /Welcome2/complaintSend HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: https://muslimbibah.ssbmultiservices.com/Welcome2/complaint
Cookie: ci_session=c585cfa9268c1753244567e4295eccd08ea181da
Content-Length: 128
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
Host: muslimbibah.ssbmultiservices.com
Connection: Keep-alive

City=San%20Francisco&country=1&email=testing%40example.com&message=555&mycountry=1&name=BzenyKyK&ncode2=94102&number=987-65-4329
```

Recommendation

Prevent this information from being displayed to the user.

References

Full Path Disclosure
https://www.owasp.org/index.php/Full_Path_Disclosure

Reverse proxy detected

This server uses a reverse proxy, a load balancer or a CDN (Content Delivery Network) or it's hosted in a cloud provider. Acunetix detected this by sending various payloads and detecting changes in headers and body.

Impact

No impact is associated with this vulnerability.

https://muslimbibah.ssbmultiservices.com/

Detected reverse proxy: Apache httpd

Request

```
GET / HTTP/1.1
Max-Forwards: 0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: muslimbibah.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

None

Subresource Integrity (SRI) not implemented

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

Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha256, sha384 or sha512.

The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.

Impact

An attacker that has access or has hacked the hosting CDN can manipulate or replace the files.

https://muslimbibah.ssbmultiservices.com/

Pages where SRI is not implemented:

- https://muslimbibah.ssbmultiservices.com/
  Script SRC: **https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js**

- https://muslimbibah.ssbmultiservices.com/
  Script SRC: **https://code.jquery.com/jquery-1.12.4.js**

Request

```
GET / HTTP/1.1
Referer: https://muslimbibah.ssbmultiservices.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: muslimbibah.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Subresource Integrity (SRI).

For example, you can use the following <script> element to tell a browser that before executing the https://example.com/example-framework.js script, the browser must first compare the script to the expected hash, and verify that there's a match.

```
<script src="https://example.com/example-framework.js"
integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC"
crossorigin="anonymous"></script>
```

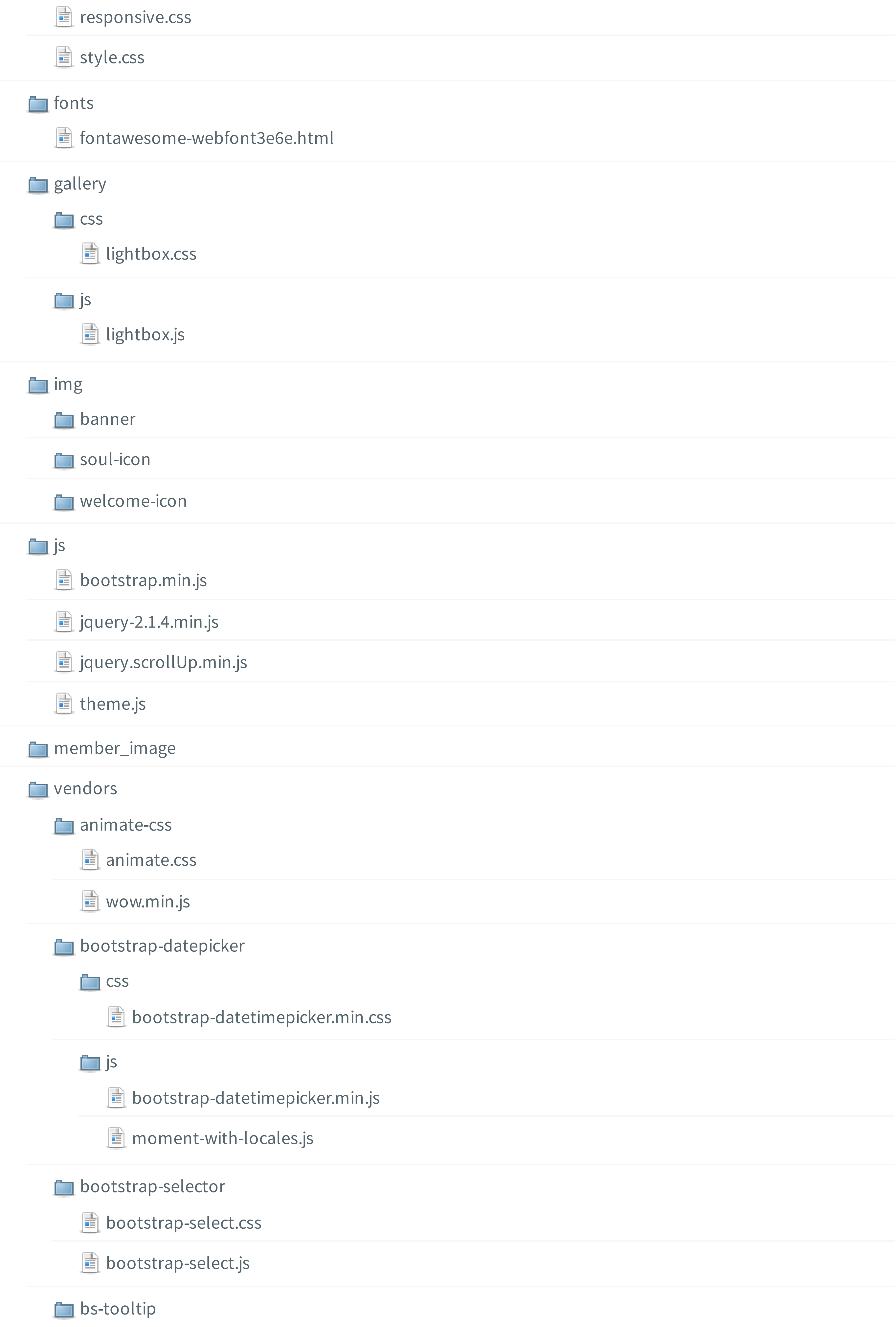
References

Subresource Integrity
https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

SRI Hash Generator
https://www.srihash.org/

Coverage

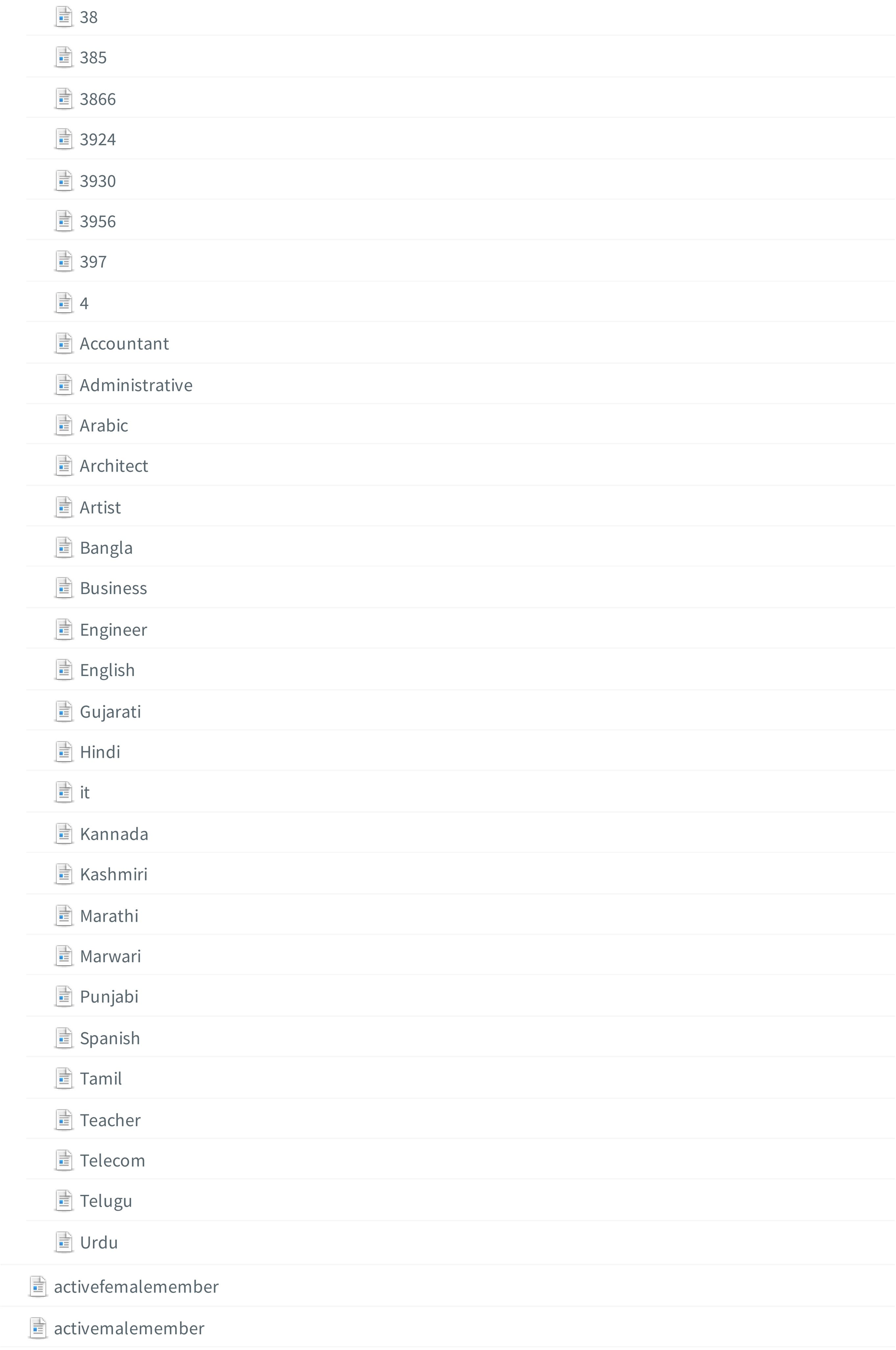
- https://muslimbibah.ssbmultiservices.com
  - #fragments
    - small-dialog
  - admin
  - cgi-sys
  - db
  - design
    - admin_panel
      - css
        - bootstrap.min.css
        - font-awesome.css
        - font.css
        - style-responsive.css
        - style.css
      - images
      - js
        - bootstrap.js
        - jquery.dcjqaccordion.2.7.js
        - jquery.nicescroll.js
        - jquery.scrollTo.js
        - jquery.slimscroll.js
        - jquery2.0.3.min.js
        - scripts.js
      - logo
      - slider
      - video_images
    - advertisement
    - css
      - bootstrap.min.css
      - font-awesome.min.css
      - primary.css



```
    responsive.css
    style.css
fonts
    fontawesome-webfont3e6e.html
gallery
    css
        lightbox.css
    js
        lightbox.js
img
    banner
    soul-icon
    welcome-icon
js
    bootstrap.min.js
    jquery-2.1.4.min.js
    jquery.scrollUp.min.js
    theme.js
member_image
vendors
    animate-css
        animate.css
        wow.min.js
    bootstrap-datepicker
        css
            bootstrap-datetimepicker.min.css
        js
            bootstrap-datetimepicker.min.js
            moment-with-locales.js
    bootstrap-selector
        bootstrap-select.css
        bootstrap-select.js
    bs-tooltip
    jquery.webui-popover.css
    jquery.webui-popover.min.js
counter-up
    jquery.counterup.min.js
    waypoints.min.js
image-dropdown
    dd.css
    flags.css
    jquery.dd.min.js
    skin2.css
jquery-ui
    jquery-ui.css
    jquery-ui.js
linears-icon
    style.css
magnific-popup
    jquery.magnific-popup.min.js
    magnific-popup.css
material-icon
    css
        materialdesignicons.min.css
    fonts
        materialdesignicons-webfont8d40.html
owl-carousel
    assets
        owl.carousel.css
    owl.carousel.min.js
revolution
    css
        layers.css
        navigation.css
        settings.css
    js
```

```
                extensions
                    revolution.extension.actions.min.js
                    revolution.extension.carousel.min.js
                    revolution.extension.kenburn.min.js
                    revolution.extension.layeranimation.min.js
                    revolution.extension.migration.min.js
                    revolution.extension.navigation.min.js
                    revolution.extension.parallax.min.js
                    revolution.extension.slideanims.min.js
                    revolution.extension.video.min.js
                jquery.themepunch.revolution.min.js
                jquery.themepunch.tools.min.js
    faq.js
mailman
memberDetails
    26
        #fragments
            small-dialog
    27
    37
    39
    41
    42
    46
    47
    48
    49
    50
    51
    53
    59
    60
    61
```

  - 62
  - 63
- resources
  - demos
    - style.css
- Welcome
  - getphonecode
    - 1
    - 2
    - 3
    - 4
    - 5
  - searchByid
    - 2
    - 5
  - searchMember
    - 1
    - 2
  - singleSearch
    - 10
    - 101
    - 107
    - 13
    - 131
    - 166
    - 178
    - 18
    - 191
    - 229
    - 230
    - 345
    - 348
    - 3605



- 38
- 385
- 3866
- 3924
- 3930
- 3956
- 397
- 4
- Accountant
- Administrative
- Arabic
- Architect
- Artist
- Bangla
- Business
- Engineer
- English
- Gujarati
- Hindi
- it
- Kannada
- Kashmiri
- Marathi
- Marwari
- Punjabi
- Spanish
- Tamil
- Teacher
- Telecom
- Telugu
- Urdu

activefemalemember

activemalemember

- femalememberbycase
- femalememberbycaste
- femalememberbylanguage
- femalememberbyreligion
- forget_pass
- forgetpassword
- malememberbycase
- malememberbycaste
- malememberbylanguage
- malememberbyreligion
- privacy_policy
- searchage
- searchcase
- searchcaste
- searchcity
- searchcountry
- searchlanguage
- searchmemberfemale
- searchmembermale
- searchprofession
- searchprofileid
- searchreligion
- terms_use

Welcome2

- complaint
  - #fragments
    - small-dialog
- complaintSend
- disclaimer
- faq
- feedback
- fraud_alert
- how

```
    membership_plan
    stay_safe
    testimonial
    verify_profile
about
access
composer.json
contact
index.php
license.txt
Login
registration
search
    #fragments
        small-dialog
story
```