

Comprehensive Report



Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Scan Detail

Target	banglamobile.ssbmultiservices.com
Scan Type	Full Scan
Start Time	Jan 2, 2024, 12:26:35 PM GMT+8
Scan Duration	2 hours, 27 minutes
Requests	319710
Average Response Time	33ms
Maximum Response Time	4906ms
Application Build	v23.7.230728157



High



Medium



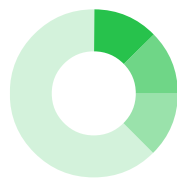
Low



Informational

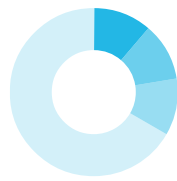
Severity	Vulnerabilities	Instances
High	2	2
Medium	7	7
Low	9	9
Informational	7	8
Total	25	26

Informational



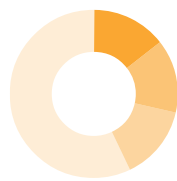
Instances	
Content Security Policy (CSP) not implement...	1
Content type is not specified	1
Email addresses	1
Others	5

Low Severity



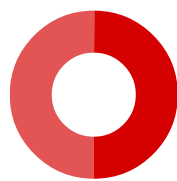
Instances	
Clickjacking: X-Frame-Options header	1
Composer installed.json publicly accessible	1
Cookies without HttpOnly flag set	1
Others	6

Medium Severity


























Instances	
Active Mixed Content over HTTPS	1
Development configuration files	1
Directory listings	1
Others	4

High Severity



Instances	
Dotenv .env file	1
Vulnerable package dependencies [high]	1

Impacts

SEVERITY	IMPACT
 High	1 Dotenv .env file
 High	1 Vulnerable package dependencies [high]
 Medium	1 Active Mixed Content over HTTPS
 Medium	1 Development configuration files
 Medium	1 Directory listings
 Medium	1 Laravel debug mode enabled
 Medium	1 Laravel log file publicly accessible
 Medium	1 Vulnerable JavaScript libraries
 Medium	1 Vulnerable package dependencies [medium]
 Low	1 Clickjacking: X-Frame-Options header
 Low	1 Composer installed.json publicly accessible
 Low	1 Cookies without HttpOnly flag set
 Low	1 Cookies without Secure flag set
 Low	1 Documentation files
 Low	1 HTTP Strict Transport Security (HSTS) not implemented
 Low	1 Insecure Inline Frame (iframe)
 Low	1 Possible sensitive directories
 Low	1 Possible sensitive files
 Informational	1 Content Security Policy (CSP) not implemented
 Informational	1 Content type is not specified
 Informational	1 Email addresses
 Informational	1 Permissions-Policy header not implemented
 Informational	1 Possible server path disclosure (Unix)

 Informational 1 Reverse proxy detected

Dotenv .env file

A dotenv file (.env) was found in this directory. Dotenv files are used to load environment variables from a .env file into the running process.

This file 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://banglamobile.ssbmultiservices.com/>

Verified

File: .env

Pattern found:

```
APP_ENV=
```

Request

```
GET /.env HTTP/1.1
Cookie: XSRF-
TOKEN=eyJpdjI6IiIyYmVhbnR3dWUxucVA0RW9jMjdyTmc9PSIsInZhbnVlIjoIR050NXlnekhreGx0eUFyUlVqSlBRclREZm4vUDJDYmZy
MmVzbEpRNERCSGprMWRDcm05U2tZa1Fha0ZnQSt0S1JERTdwZ2wxY01SNU9qZFhMVGFhGaVFHVG5LQ2x3MStENzhHUUV2RDVHTjBOMm9lck
VRN3R2MFh0aE1SmNiNVoiLCJtYWMiOiI2NmY30GE4MTk2NTNlNmZmNmNlZTBmN2ZjZmU2YTQ3Y2Y2YmYxOWE2ZjhhMzhjODFiNDQ2NjQz
NjZlZWUyYWE5IiwidGFuIjoIIn0%3D;
bangla_mobile_session=eyJpdjI6IiIyYmVhbnR3dWUxucVA0RW9jMjdyTmc9PSIsInZhbnVlIjoIR050NXlnekhreGx0eUFyUlVqSlBRclREZm4vUDJDYmZy
TFgzN2JES05TWXRpb29DYTEwXWJmWmE0Y3hYdEhQXFla0RibWNSU0tIcmVLM2JYSkhKVXJ3U1ZpOUVYUVBqVnFpL1JYNnYvVEM0Z3Izbnw
QreENCZ04rdmVSN0VRNw1WT1lyek9aMlNucFgiLCJtYWMiOiI2NmY30GE4MTk2NTNlNmZmNmNlZTBmN2ZjZmU2YTQ3Y2Y2YmYxOWE2ZjhhMzhjODFiNDQ2NjQz
NjZlZWUyYWE5IiwidGFuIjoIIn0%3D
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: banglamobile.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

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

Vulnerable package dependencies [high]

One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package.

Impact

The impact of this vulnerability is different for each vulnerable package. It's recommended to investigate each vulnerable package individually.

<https://banglamobile.ssbmultiservices.com/>

List of vulnerable **composer** packages:

Package: guzzlehttp/guzzle

Version: 7.4.1

CVE: CVE-2022-29248

Title: Reliance on Cookies without Validation and Integrity Checking

Description: Guzzle is a PHP HTTP client. Guzzle prior to versions 6.5.6 and 7.4.3 contains a vulnerability with the cookie middleware. The vulnerability is that it is not checked if the cookie domain equals the domain of the server which sets the cookie via the Set-Cookie header, allowing a malicious server to set cookies for unrelated domains. The cookie middleware is disabled by default, so most library consumers will not be affected by this issue. Only those who manually add the cookie middleware to the handler stack or construct the client with ['cookies' => true] are affected. Moreover, those who do not use the same Guzzle client to call multiple domains and have disabled redirect forwarding are not affected by this vulnerability. Guzzle versions 6.5.6 and 7.4.3 contain a patch for this issue. As a workaround, turn off the cookie middleware.

CVSS V2: AV:N/AC:M/Au:N/C:P/I:P/A:N

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N

CWE: CWE-565

References:

- <https://github.com/guzzle/guzzle/commit/74a8602c6faec9ef74b7a9391ac82c5e65b1cdab>
- <https://github.com/guzzle/guzzle/pull/3018>
- <https://github.com/guzzle/guzzle/security/advisories/GHSA-cwmx-hcrq-mhc3>
- <https://www.drupal.org/sa-core-2022-010>
- <https://www.debian.org/security/2022/dsa-5246>

Package: guzzlehttp/guzzle

Version: 7.4.1

CVE: CVE-2022-31043

Title: Improper Removal of Sensitive Information Before Storage or Transfer

Description: Guzzle is an open source PHP HTTP client. In affected versions `Authorization` headers on requests are sensitive information. On making a request using the `https` scheme to a server which responds with a redirect to a URI with the `http` scheme, we should not forward the `Authorization` header on. This is much the same as to how we don't forward on the header if the host changes. Prior to this fix, `https` to `http` downgrades did not result in the `Authorization` header being removed, only changes to the host. Affected Guzzle 7 users should upgrade to Guzzle 7.4.4 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.7 or 7.4.4. Users unable to upgrade may consider an alternative approach which would be to use their own redirect middleware. Alternately users may simply disable redirects all together if redirects are not expected or required.

CVSS V2: AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CWE: CWE-212

References:

- <https://github.com/guzzle/guzzle/security/advisories/GHSA-w248-ffj2-4v5q>
- <https://github.com/guzzle/guzzle/commit/e3ff079b22820c2029d4c2a87796b6a0b8716ad8>
- <https://www.rfc-editor.org/rfc/rfc9110.html#name-redirection-3xx>
- <https://www.drupal.org/sa-core-2022-011>
- <https://www.debian.org/security/2022/dsa-5246>

Package: guzzlehttp/guzzle

Version: 7.4.1

CVE: CVE-2022-31091

Title: Exposure of Sensitive Information to an Unauthorized Actor

Description: Guzzle, an extensible PHP HTTP client. `Authorization` and `Cookie` headers on requests are sensitive information. In affected versions on making a request which responds with a redirect to a URI with a different port, if we choose to follow it, we should remove the `Authorization` and `Cookie` headers from the request, before containing. Previously, we would only consider a change in host or scheme. Affected Guzzle 7 users should upgrade to Guzzle 7.4.5 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.8 or 7.4.5. Note that a partial fix was implemented in Guzzle 7.4.2, where a change in host would trigger removal of the curl-added Authorization header, however this earlier fix did not cover change in scheme or change in port. An alternative approach would be to use your own redirect middleware, rather than ours, if you are unable to upgrade. If you do not require or expect redirects to be followed, one should simply disable redirects all together.

CVSS V2: AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

CWE: CWE-200

References:

- <https://github.com/guzzle/guzzle/commit/1dd98b0564cb3f6bd16ce683cb755f94c10fbd82>
- <https://github.com/guzzle/guzzle/security/advisories/GHSA-q559-8m2m-g699>
- <https://www.debian.org/security/2022/dsa-5246>
- <https://security.gentoo.org/glsa/202305-24>

Package: guzzlehttp/guzzle

Version: 7.4.1

CVE: CVE-2022-31090

Title: Improper Removal of Sensitive Information Before Storage or Transfer

Description: Guzzle, an extensible PHP HTTP client. `Authorization` headers on requests are sensitive information. In affected versions when using our Curl handler, it is possible to use the `CURLOPT_HTTPAUTH` option to specify an `Authorization` header. On making a request which responds with a redirect to a URI with a different origin (change in host, scheme or port), if we choose to follow it, we should remove the `CURLOPT_HTTPAUTH` option before continuing, stopping curl from appending the `Authorization` header to the new request. Affected Guzzle 7 users should upgrade to Guzzle 7.4.5 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.8 or 7.4.5. Note that a partial fix was implemented in Guzzle 7.4.2, where a change in host would trigger removal of the curl-added Authorization header, however this earlier fix did not cover change in scheme or change in port. If you do not require or expect redirects to be followed, one should simply disable redirects all together. Alternatively, one can specify to use the Guzzle steam handler backend, rather than curl.

CVSS V2: AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

CWE: CWE-212

References:

- <https://github.com/guzzle/guzzle/commit/1dd98b0564cb3f6bd16ce683cb755f94c10fbd82>
- <https://github.com/guzzle/guzzle/security/advisories/GHSA-25mq-v84q-4j7r>
- <https://www.debian.org/security/2022/dsa-5246>
- <https://security.gentoo.org/glsa/202305-24>

Package: guzzlehttp/guzzle

Version: 7.4.1

CVE: CVE-2022-31042

Title: Improper Removal of Sensitive Information Before Storage or Transfer

Description: Guzzle is an open source PHP HTTP client. In affected versions the `Cookie` headers on requests are sensitive information. On making a request using the `https` scheme to a server which responds with a redirect to a URI with the `http` scheme, or on making a request to a server which responds with a redirect to a a URI to a different host, we should not forward the `Cookie` header on. Prior to this fix, only cookies that were managed by our cookie middleware would be safely removed, and any `Cookie` header manually added to the initial request would not be stripped. We now always strip it, and allow the cookie middleware to re-add any cookies that it deems should be there. Affected Guzzle 7 users should upgrade to Guzzle 7.4.4 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.7 or 7.4.4. Users unable to upgrade may consider an alternative approach to use your own redirect middleware, rather than ours. If you do not require or expect redirects to be followed, one should simply disable redirects all together.

CVSS V2: AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CWE: CWE-212

References:

- <https://github.com/guzzle/guzzle/security/advisories/GHSA-f2wf-25xc-69c9>
- <https://github.com/guzzle/guzzle/commit/e3ff079b22820c2029d4c2a87796b6a0b8716ad8>
- <https://www.rfc-editor.org/rfc/rfc9110.html#name-redirection-3xx>
- <https://www.drupal.org/sa-core-2022-011>
- <https://www.debian.org/security/2022/dsa-5246>

Package: guzzlehttp/psr7

Version: 1.8.3

CVE: CVE-2022-24775

Title: Improper Input Validation

Description: guzzlehttp/psr7 is a PSR-7 HTTP message library. Versions prior to 1.8.4 and 2.1.1 are vulnerable to improper header parsing. An attacker could sneak in a new line character and pass untrusted values. The issue is patched in 1.8.4 and 2.1.1. There are currently no known workarounds.

CVSS V2: AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

CWE: CWE-20

References:

- <https://github.com/guzzle/psr7/security/advisories/GHSA-q7rv-6hp3-vh96>
- <https://github.com/guzzle/psr7/pull/485/commits/e55afaa3fc138c89adf3b55a8ba20dc60d17f1f1>
- <https://github.com/guzzle/psr7/pull/486/commits/9a96d9db668b485361ed9de7b5bf1e54895df1dc>
- <https://www.drupal.org/sa-core-2022-006>

Package: guzzlehttp/psr7

Version: 1.8.3

CVE: CVE-2023-29197

Title: Interpretation Conflict

Description: guzzlehttp/psr7 is a PSR-7 HTTP message library implementation in PHP. Affected versions are subject to improper header parsing. An attacker could sneak in a newline (\n) into both the header names and values. While the specification states that \r\n\r\n is used to terminate the header list, many servers in the wild will also accept \n\n. This is a follow-up to CVE-2022-24775 where the fix was incomplete. The issue has been patched in versions 1.9.1 and 2.4.5. There are no known workarounds for this vulnerability. Users are advised to upgrade.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

CWE: CWE-436

References:

- <https://github.com/guzzle/psr7/security/advisories/GHSA-q7rv-6hp3-vh96>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=2022-24775>
- <https://github.com/guzzle/psr7/security/advisories/GHSA-wxmh-65f7-jcvw>
- <https://www.rfc-editor.org/rfc/rfc7230#section-3.2.4>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/O35UN4IK6VS2LXSRWUDFWY7NI73RKY2U/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/FJANWDXJZE5BGLN4MQ4FEHV5LJ6CMKQF/>

Package: spatie/browsershot

Version: 3.52.3

CVE: CVE-2022-43983

Title: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Description: Browsershot version 3.57.2 allows an external attacker to remotely obtain arbitrary local files. This is possible because the application does not validate that the HTML content passed to the Browsershot::html method does not contain URL's that use the file:// protocol.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N

CWE: CWE-79

References:

- <https://fluidattacks.com/advisories/khalid/>
- <https://github.com/spatie/browsershot/>

Package: spatie/browsershot

Version: 3.52.3

CVE: CVE-2022-41706

Title: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Description: Browsershot version 3.57.2 allows an external attacker to remotely obtain arbitrary local files. This is possible because the application does not validate the URL protocol passed to the Browsershot::url method.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N

CWE: CWE-79

References:

- <https://github.com/spatie/browsershot/>

- <https://fluidattacks.com/advisories/eminem/>

Package: spatie/browsershot

Version: 3.52.3

CVE: CVE-2022-43984

Title: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Description: Browsershot version 3.57.3 allows an external attacker to remotely obtain arbitrary local files. This is possible because the application does not validate that the JS content imported from an external source passed to the Browsershot::html method does not contain URLs that use the file:// protocol.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N

CWE: CWE-79

References:

- <https://fluidattacks.com/advisories/malone/>
- <https://github.com/spatie/browsershot/>

Package: symfony/http-kernel

Version: 5.4.2

CVE: CVE-2022-24894

Title: Improper Authorization

Description: Symfony is a PHP framework for web and console applications and a set of reusable PHP components. The Symfony HTTP cache system, acts as a reverse proxy: It caches entire responses (including headers) and returns them to the clients. In a recent change in the `AbstractSessionListener`, the response might contain a `Set-Cookie` header. If the Symfony HTTP cache system is enabled, this response might be stored and return to the next clients. An attacker can use this vulnerability to retrieve the victim's session. This issue has been patched and is available for branch 4.4.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CWE: CWE-285

References:

- <https://github.com/symfony/symfony/commit/d2f6322af9444ac5cd1ef3ac6f280dbef7f9d1fb>
- <https://github.com/symfony/symfony/security/advisories/GHSA-h7vf-5wrv-9fhv>
- <https://lists.debian.org/debian-lts-announce/2023/07/msg00014.html>

Recommendation

It's recommended to update the vulnerable packages to the latest version (if a fix exists). If a fix does not exist, you may want to suggest changes that address the vulnerability to the package maintainer or remove the package from your dependency tree.

Active Mixed Content over HTTPS

Active Content is a resource which can run in the context of your page and moreover can alter the entire page. If the HTTPS page includes active content like scripts or stylesheets retrieved through regular, cleartext HTTP, then the connection is only partially encrypted. The unencrypted content is accessible to sniffers.

Impact

A man-in-the-middle attacker can intercept the request for the HTTP content and also rewrite the response to include malicious codes. Malicious active content can steal the user's credentials, acquire sensitive data about the user, or attempt to install malware on the user's system (by leveraging vulnerabilities in the browser or its plugins, for example), and therefore the connection is not safeguarded anymore.

<https://banglamobile.ssbmultiservices.com/>

The following issues were detected:

- The tag **link** references the resource <http://fonts.googleapis.com/css?family=Monda>
- The tag **link** references the resource <http://fonts.googleapis.com/css?family=Doppio+One>

Request

```
GET / HTTP/1.1
Referer: https://banglamobile.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: banglamobile.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

There are two technologies to defense against the mixed content issues: - HTTP Strict Transport Security (HSTS) is a mechanism that enforces secure resource retrieval, even in the face of user mistakes (attempting to access your web site on port 80) and implementation errors (your developers place an insecure link into a secure page) - Content Security Policy (CSP) can be used to block insecure resource retrieval from third-party web sites - Last but not least, you can use "protocol relative URLs" to have the user's browser automatically choose HTTP or HTTPS as appropriate, depending on which protocol the user is connected with. For example: A protocol relative URL to load an style would look like `>link rel="stylesheet" href="//example.com/style.css"/<`. Same for scripts `>script type="text/javascript" src="//example.com/code.js"</script<` The browser will automatically add either "http:" or "https:" to the start of the URL, whichever is appropriate.

References

[MDN: Mixed Content](https://developer.mozilla.org/en-US/docs/Web/Security/Mixed_content)

https://developer.mozilla.org/en-US/docs/Web/Security/Mixed_content

[What is mixed content?](https://web.dev/what-is-mixed-content/)

<https://web.dev/what-is-mixed-content/>

[Fixing mixed content](https://web.dev/fixing-mixed-content/)

<https://web.dev/fixing-mixed-content/>

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://banglamobile.ssbmultiservices.com/>

Development configuration files:

- <https://banglamobile.ssbmultiservices.com/package.json>

`package.json` => Grunt configuration file. Grunt is a JavaScript task runner.

- <https://banglamobile.ssbmultiservices.com/composer.json>

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

- <https://banglamobile.ssbmultiservices.com/composer.lock>

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

- <https://banglamobile.ssbmultiservices.com/package-lock.json>

`package-lock.json` => npm file. This file keeps track of the exact version of every package that is installed.

- <https://banglamobile.ssbmultiservices.com/.styleci.yml>

`.styleci.yml` => StyleCI configuration file

Request

GET /package.json HTTP/1.1

Cookie: XSRF-

TOKEN=eyJpdiI6IiN1T0E5YW5GVtN5RERjUWtaeVNqRUE9PSIsInZhbnVlIjoIWDdtZFI4WTZD0TRoUzJhdjBkVVgyUWdxcWkwUjZuM1FVUFNBNUY5ako3aU5tM2RQaWRnc1Z6OFJ0TUNrVepMUENOVzdCS2U1YnV5YXhJYXlBQTVmMlhQbDFVYWdQs2dRcG1XcWRlTHVCSHhTcDNsYzE3cFR6Vz16NWhjMFNnZk4iLCJtYWMiOiI1ZTE5ZmI2ZTBkYzgyNTdjMTUyZjAxN2E1NDZjMmU0YjRhMzA2ZmIwYzZmMzI0ZDg5ZWY2NWE2MGUyNGI4YmZjIiwidGFuIjoIIn0%3D;

bangla_mobile_session=eyJpdiI6InNvWUJrelIrRktQeU5sM0ljTFpXeUE9PSIsInZhbnVlIjoIQTU3TnZDaFlXNHVOWDFHL2hSQUF1SWWhMc3hWUTdV0EI4OXAvMFA4VXozd3JXSnrRmtNdHdwYlBLNWllTnlJcEdab3Z4V3h5MjJvUXpmVVQzRUFTeCsraG54YjhlVWp6TEw1cER0eXVWZSt2VzRnYi93WFhTWnllODliNzhXVGsiLCJtYWMiOiI1ZTY1NGQ2MDgxNjUwOGJkYWRkNTU5MGNjNjNhNzU3NjRlNWU0MWRiZTE1NGRkMzk1MjhlMWE3Mzk1NGQ1YmY5IiwidGFuIjoIIn0%3D

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: banglamobile.ssbmultiservices.com
Connection: Keep-alive

Recommendation

Remove or restrict access to all configuration files accessible 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://banglamobile.ssbmultiservices.com/> Verified

Folders with directory listing enabled:

- <https://banglamobile.ssbmultiservices.com/front/>
- <https://banglamobile.ssbmultiservices.com/front/assets/>
- <https://banglamobile.ssbmultiservices.com/front/assets/css/>
- <https://banglamobile.ssbmultiservices.com/toastr/>
- <https://banglamobile.ssbmultiservices.com/toastr/css/>
- <https://banglamobile.ssbmultiservices.com/uploads/>
- <https://banglamobile.ssbmultiservices.com/uploads/paybill/large/>
- <https://banglamobile.ssbmultiservices.com/uploads/paybill/>
- <https://banglamobile.ssbmultiservices.com/upload/>
- <https://banglamobile.ssbmultiservices.com/upload/header-footer/>
- <https://banglamobile.ssbmultiservices.com/admin/>
- <https://banglamobile.ssbmultiservices.com/front/assets/grid-gallery/>
- <https://banglamobile.ssbmultiservices.com/toastr/js/>
- <https://banglamobile.ssbmultiservices.com/vendor/>
- <https://banglamobile.ssbmultiservices.com/uploads/product/>
- <https://banglamobile.ssbmultiservices.com/front/assets/js/>
- <https://banglamobile.ssbmultiservices.com/upload/about-us-image/>
- <https://banglamobile.ssbmultiservices.com/uploads/hot-deals/>
- <https://banglamobile.ssbmultiservices.com/uploads/hot-deals/large/>
- <https://banglamobile.ssbmultiservices.com/vendor/bin/>

- <https://banglamobile.ssbmultiservices.com/admin/assets/>

Request

```
GET /front/ HTTP/1.1
Cookie: XSRF-
TOKEN=eyJpdii6ImI6c2kt60VcxcUFUcFpWSEErOU1lakE9PSIsInZhbHVlIjoieEVCUE5sVTJpYmp3VUVnTlQwQW0xRkRtdGxtN1RBZERo
dVBaelVZa0EYam4rSVBlckJldjJOUFZ0anJuZitVV1Z0eGNVR1BhdWVYLzBKQVhmcFY3ZmoyMHFNdk4xWfo5SXF6YlBaQmRQNklwSVdoaw
9WdC9JZWNPbVRFWHFANViiLCJtYWMiOiI00WY1ZTVkZDAzZjkyNWIXNWUwOTljMmY3MDFkZjI1ODM4YzAzZjI0YzFLMzUxNDk4MTc3MGFj
NzZkMzJiOTMlIiwidGFuIjoieIn0%3D;
bangla_mobile_session=eyJpdii6ImI6c2kt60VcxcUFUcFpWSEErOU1lakE9PSIsInZhbHVlIjoibG5KeEFhU3lxZk1kc3dBemRPNFpw
eWpZczFsNHhQVU43a0lPMLFkN0tQ0U9zbWM2dElBeEhvMGx5bitiZXZCbCtH0XRid2JrUUFBTfZVVHJmZ2RCZEx0TkRNS01pSHhIZkxTcE
JmQUc5eDZnRWR5aTV0SEt2Z2k2ZFRHai9UTnQiLCJtYWMiOiIjInGU3ZjlhNmI0NjMxNzE2N2ZiMmIXODU3N2VmOWIyMmI1N2EzNmMzZGQ5
NmE0NTAwZmI4ZmQ5Nzg0NTczY2UwIiwidGFuIjoieIn0%3D
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: banglamobile.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>

Laravel debug mode enabled

The web application uses Laravel framework. Laravel Debug mode is enabled. Debug mode should be turned off in production environment, as it leads to disclosure of sensitive information about the web application.

Impact

The web application in debug mode discloses sensitive information. This information can be used to launch further attacks.

<https://banglamobile.ssbmultiservices.com/>

Request

```
PUT /index.php HTTP/1.1
Cookie: XSRF-
TOKEN=eyJpdiI6IlN1T0E5YW5GVtN5RERjUWtaeVNqRUE9PSIsInZhbnVlIjoiwDdtZFI4WTZD0TRoUzJhdjBkVVgyUWdxcWkwUjZuM1FV
UFNBNUY5ako3aU5tM2RQaWRncLZ60FJ0TUNrVEpMUENOVzdCS2U1YnV5YXhJYXlBQTVmMlhQbDFVYWdqS2dRcG1XcWRlTHVCSHhTcDNsYz
E3cFR6VzI6NVhjMFNnZk4iLCJtYWMiOiI1ZTE5ZmI2ZTBkYzgyNTdjMTUyZjAxN2E1NDZjMmU0YjRhMzA2ZmIwYzZmMzI0ZDg5ZWY2NWE2
MGUyNGI4YmZjIiwidGFuIjoIIn0%3D;
bangla_mobile_session=eyJpdiI6InNvWUJrelIrRktQeU5sM0ljTFpXeUE9PSIsInZhbnVlIjoIQTR3TnZDaFlXNHVOWDFHL2hSQUF1
SWhmC3hwUTdV0EI4OXAvMFA4VXozd3JXSnrRmtNdHdwYlBLNWllTnlJcEdab3Z4V3h5MjJvUXpmVVQzRUFTeCsraG54YjhlVWp6TEw1cE
R0eXVWZSt2VzRnYi93WFhTWnllODliNzhXVGsiLCJtYWMiOiI1ZTY1NGQ2MDgxNjUwOGJkYWRkNTU5MGNjNjNhNzU3NjRlNWU0MWRiZTE1
NGRkMzk1MjhlMWE3Mzk1NGQ1YmY5IiwidGFuIjoIIn0%3D
Content-Length: 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: banglamobile.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Disable the debug mode by setting APP_DEBUG to false

References

Error Handling

<https://laravel.com/docs/7.x/errors#configuration>

Laravel log file publicly accessible

Laravel is a popular PHP web application framework. A publicly accessible Laravel log file (/storage/logs/laravel.log) was found in this directory.

This file 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

The Laravel log file may disclose sensitive information. This information can be used to launch further attacks.

<https://banglamobile.ssbmultiservices.com/>

Request

```
GET /storage/logs/laravel.log HTTP/1.1
Cookie: XSRF-
TOKEN=eyJpdiI6IlN1T0E5YW5GVtN5RERjUWtaeVNqRUE9PSIsInZhbnVlIjoiwDdtZFI4WTZD0TRoUzJhdjBkVVgyUWdxcWkwUjZuM1FV
```


UFNBNUY5ako3aU5tM2RQaWRncLZ60FJ0TUNrVEpMUENOVzdCS2U1YnV5YXhJYXlBQTVmMlhQbDFVYWdqS2dRcG1XcWRLTHVCSHhTcDNsYzE3cFR6Vzl6NVhjMFNnZk4iLCJtYWMiOiI1ZTE5ZmI2ZTBkYzgyNTdjMTUyZjAxN2E1NDZjMmU0YjRhMzA2ZmIwYzZmMzI0ZDg5ZWY2NWE2MGUyNGI4YmZjIiwidGFnIjoiIn0%3D;

bangla_mobile_session=eyJpdiI6InNvWUJrelIrRktQeU5sM0ljTFpXeUE9PSIsInZhbnVlIjoiQTR3TnZDaFlXNHVOWDFHL2hSQUF1SWhMc3hWUTdV0EI4OXAvMFA4VXozd3JXSnrRmtNdHdwYlBLNWllTnJcEdab3Z4V3h5MjJvUXpmVVQzRUFTeCsraG54YjhlVWp6TEw1cER0eXVWZSt2VzRnYi93WFhTWnllODliNzhXVGsiLCJtYWMiOiI1ZTY1NGQ2MDgxNjUwOGJkYWRkNTU5MGNjNjNhNzU3NjRlNWU0MWRiZTE1NGRkMzk1MjhlMWE3Mzk1NGQ1YmY5IiwidGFnIjoiIn0%3D

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: banglamobile.ssbmultiservices.com

Connection: Keep-alive

Recommendation

Remove or restrict access from the internet to this type of files.

References

[Laravel Logging](https://laravel.com/docs/5.6/logging)
<https://laravel.com/docs/5.6/logging>

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://banglamobile.ssbmultiservices.com/> Confidence: 95%

- **jQuery 3.3.1**
 - URL: <https://banglamobile.ssbmultiservices.com/>
 - Detection method: The library's name and version were determined based on its dynamic behavior.
 - 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://banglamobile.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: banglamobile.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Upgrade to the latest version.

Vulnerable package dependencies [medium]

One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package.

Impact

The impact of this vulnerability is different for each vulnerable package. It's recommended to investigate each vulnerable package individually.

<https://banglamobile.ssbmultiservices.com/>

List of vulnerable **composer** packages:

Package: spatie/browsershot

Version: 3.52.3

CVE: CVE-2020-7790

Title: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Description: This affects the package spatie/browsershot from 0.0.0. By specifying a URL in the file:// protocol an attacker is able to include arbitrary files in the resultant PDF.

CVSS V2: AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CWE: CWE-22

References:

- <https://snyk.io/vuln/SNYK-PHP-SPATIEBROWSERSHOT-1037064>
- <https://github.com/spatie/browsershot/issues/441%23issue-735049731>

Recommendation

It's recommended to update the vulnerable packages to the latest version (if a fix exists). If a fix does not exist, you may want to suggest changes that address the vulnerability to the package maintainer or remove the package from your dependency tree.

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://banglamobile.ssbmultiservices.com/>

Paths without secure XFO header:

- <https://banglamobile.ssbmultiservices.com/>
- <https://banglamobile.ssbmultiservices.com/serarch>
- <https://banglamobile.ssbmultiservices.com/product/view/blood-pressure-formula>

- <https://banglamobile.ssbmultiservices.com/uploads/paybill/large/>
- <https://banglamobile.ssbmultiservices.com/pay-bill/ultra-men-power>
- <https://banglamobile.ssbmultiservices.com/upload/header-footer/>
- <https://banglamobile.ssbmultiservices.com/admin/>
- <https://banglamobile.ssbmultiservices.com/products/category/accessories-61e26ea54ea5b>
- <https://banglamobile.ssbmultiservices.com/about-us>
- <https://banglamobile.ssbmultiservices.com/contact>
- <https://banglamobile.ssbmultiservices.com/customer-service>
- <https://banglamobile.ssbmultiservices.com/vendor/autoload.php>
- <https://banglamobile.ssbmultiservices.com/wishlist/40c3c9cc2212888b799a8b3b8a6c8152>
- <https://banglamobile.ssbmultiservices.com/feature-products>
- <https://banglamobile.ssbmultiservices.com/hot-deals>
- <https://banglamobile.ssbmultiservices.com/how-we-work>
- <https://banglamobile.ssbmultiservices.com/pay-bill>
- <https://banglamobile.ssbmultiservices.com/privacy-policy>
- <https://banglamobile.ssbmultiservices.com/return-refund>
- <https://banglamobile.ssbmultiservices.com/terms-service>
- <https://banglamobile.ssbmultiservices.com/why-choose-us>

Request

GET / HTTP/1.1
Referer: <https://banglamobile.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: banglamobile.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)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

[Clickjacking](https://en.wikipedia.org/wiki/Clickjacking)

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

[OWASP Clickjacking](https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html)

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

[Frame Buster Buster](https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)

<https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed>

Composer installed.json publicly accessible

A `installed.json` file was discovered. Composer is a tool for dependency management in PHP. It allows you to declare the libraries your project depends on and it will manage (install/update) them for you. After installing the dependencies, Composer stores the list of them in a special file for internal purposes.

As the file is publicly accessible, it leads to disclosure of information about components used by the web application.

Impact

`installed.json` discloses sensitive information. This information can be used to launch further attacks.

<https://banglamobile.ssbmultiservices.com/vendor/>

Request

```
GET /vendor/composer/installed.json HTTP/1.1
Cookie: XSRF-
TOKEN=eyJpdjI6Im9IMjRiZEtZSkthQ0UxN3cvRFlIMWc9PSIsInZhbnVlIjoibDJVNUVFQ016QmJia1hZNmKxUkxrTGZpdUlGN3VaaG5qRHFV0ZaM0ZUOXpSbDNyaU9MZVNSL1F60ENCNmVjTG11clg0R1dRVFlPVU9iS3A1MHdo0XJYVERyUHhCZhdGL1lLajFnMEdHLzFBTytdXJSWmJ1cXEyaVweXp4a28iLCJtYWMiOiI1ZGE0ZWZMA5MjRlZTIwMDI1OWJmZDgxN2IxMTZlNjNhNGNjMzRmYzNlZmIxMTc0NTY1OWY4YmZjMzllMzIxIiwidGFuIjoiaW0%3D;
bangla_mobile_session=eyJpdjI6Im9IMjRiZEtZSkthQ0UxN3cvRFlIMWc9PSIsInZhbnVlIjoibDJVNUVFQ016QmJia1hZNmKxUkxrTGZpdUlGN3VaaG5qRHFV0ZaM0ZUOXpSbDNyaU9MZVNSL1F60ENCNmVjTG11clg0R1dRVFlPVU9iS3A1MHdo0XJYVERyUHhCZhdGL1lLajFnMEdHLzFBTytdXJSWmJ1cXEyaVweXp4a28iLCJtYWMiOiI1ZGE0ZWZMA5MjRlZTIwMDI1OWJmZDgxN2IxMTZlNjNhNGNjMzRmYzNlZmIxMTc0NTY1OWY4YmZjMzllMzIxIiwidGFuIjoiaW0%3D
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
```

Recommendation

Restrict access to vendors directory

References

[Composer Basic usage](#)

<https://getcomposer.org/doc/01-basic-usage.md>

Cookies without HttpOnly flag set

One or more cookies don't have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Impact

Cookies can be accessed by client-side scripts.

<https://banglamobile.ssbmultiservices.com/> Verified

Cookies without HttpOnly flag set:

- <https://banglamobile.ssbmultiservices.com/>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IiN1T0E5YW5GVNT5RERjUWtaeVNqRUE9PSIsInZhbnVlIjoieWdDdtZFI4WTZD0TRoUzJhdjBkV
VgyUWdxwkwUjZuM1FVUFNBNUY5ako3aU5tM2RQaWRnciZ60FJ0TUNrVEpMUEN0VzdCS2U1YnV5YXhJYXlBQTVm
MlhQbDFVYWdqS2dRcG1XcWRlTHVCShhTcDNsYzE3cFR6VzI6NVhjMFNnZk4iLCJtYWMiOiI1ZTE5ZmI2ZTBkYzg
yNTdjMTUyZjAxN2E1NDZjMmU0YjRhMzA2ZmIwYzZmMzI0ZDg5ZWY2NWE2MGUyNGI4YmZjIiwidGFuIjoieWdDdtZFI4WTZD0TRoUzJhdjBkV
; expires=Tue, 02-Jan-2024 06:26:37 GMT; Max-Age=7200; path=/; samesite=lax

- <https://banglamobile.ssbmultiservices.com/serarch>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6ImI6ckt60VcxUcFpWSEErOU1lakE9PSIsInZhbnVlIjoieWdDdtZFI4WTZD0TRoUzJhdjBkV
W0xRkRtdGxtN1RBZERodVBaelVZa0Eyam4rSVBlckJldjJ0UFZ0anJuZitVV1Z0eGNVR1BhdWVyLzBKQVhmcFY3
ZmoyMHFNdk4xWfo5SXF6YlBaQmRQNklwSVdoaw9WdC9JZWNPbVRFWHFaNViiLCJtYWMiOiI00WY1ZTVkZDAzZjk

yNWIXNWUw0TljMmY3MDFkZjI10DM4YzAzZjI0YzFlMzUxNDk4MTc3MGFjNzZkMzJiOTM1IiwidGFnIjoiIn0%3D
; expires=Tue, 02-Jan-2024 06:27:47 GMT; Max-Age=7200; path=/; samesite=lax

- <https://banglamobile.ssbmultiservices.com/product/view/blood-pressure-formula>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6ImJsU3psUlZvODM2K0lTSWxZTGLBZEE9PSIsInZhbnVlIjoiUHHWeGxYUovcmFZSnBwVjJRS
EtXTxdHem52UUFDbStaRm9LN05HUVBTWxhoa3JlYjNmMlpEUFczYjJ0aU90ZGV0bGY4SHRiWutyMzcRdURHVFFS
eEdPNHhR0FFydG5KVW9zb1RndmxWwG9VQjk0QXNYMlBabTZHa0w3aEFGUloiLCJtYWMiOiIxNGJjZjJiMWMYMTd
lMTE5NDY2ZmJhMWQ0MTM2NWY1MTFmOTZmOTMzMmY2Q4Nzk4YWI5ZGJiZWUyM2QzYmY5IiwidGFnIjoiIn0%3D
; expires=Tue, 02-Jan-2024 06:28:13 GMT; Max-Age=7200; path=/; samesite=lax

- <https://banglamobile.ssbmultiservices.com/pay-bill/ultra-men-power>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IjU2ZlNjNTBEdkFlTzZ4OGJiaC9KQ3c9PSIsInZhbnVlIjoieG45TFV3cUJmckttaEZ3aERRa
jR0Mk43QlFLSGJSN1ZtYwZa3FpTnBVSHN2NFNIeGRyZkZkSzRhclJpOGh5QmJDQThVOHpmc2lJc1JiZFltWDE1
T2lXdW44N2dTc0ZKVTg4emU3eGN5bWlzcFpQbHNyYVMwR3FuSEpxZWtob0giLCJtYWMiOiJjYjI3YmE3Zjg2NjE
yMDRkY2RmNWVkyZWZkNGMzYjY2NzM2ZGRiYmRhZGJjMTMzOGY1ZjdiYzY0ODk0MGJkZGI2IiwidGFnIjoiIn0%3D
; expires=Tue, 02-Jan-2024 06:29:05 GMT; Max-Age=7200; path=/; samesite=lax

- <https://banglamobile.ssbmultiservices.com/serarch>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6Im81ZGdMYU0zcFFka0krQWwxM1NCR2c9PSIsInZhbnVlIjoiUXFtTWU0UmRQODRjdGpIbFRtS
2xPcHVPL2JaUERZe1AwYUxCZTFsRGFjZTVwRFpPOHoxK0Z2M1ord0lndkVXZmRzQjFEYjErSVpDK3QzYUk0d2xy
bU4reVQ5Ky9UL2hmRDY3RlhPR1VpMmxxaHZQT05TRFVlOVhRdE8yZEdQaVYiLCJtYWMiOiIzYzY0ZTUwZjYyOGF
mNzA1MjYyZGI4OGU4MTA1NTA0NjgwODQ1ODJjZmYwNmFkNGU3MDllOTlhODllZTMzZjhmIiwidGFnIjoiIn0%3D
; expires=Tue, 02-Jan-2024 06:27:46 GMT; Max-Age=7200; path=/; samesite=lax

- <https://banglamobile.ssbmultiservices.com/products/category/accessories-61e26ea54ea5b>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6ImFkc2V0cHEXTHFTSjUrdVoyZElRb2c9PSIsInZhbnVlIjoieHp2UUhrT3dnMHR4TXdLb1V3T
1dlVzE3ZE5Yd0NLc0lQalQzSFVDT0hsZzRZQ0VYcHBmUDl2TTL5ULe4ZWlyVmU2UkZRT0hGZGR0ZzFYnjZ2SVRk
NEQ3TjB3eXE5L3FKV0ZxcjNFl1o1NVVtQ1Z4NUZyYjRrM3h1L3dhbWRBbngiLCJtYWMiOiI4MGmxZWm0Nzk1N2Q
zYWQzZTY4ODQ1YmExNzA2Yjg2MGY3Nj1jNzZlMmNiNTUzNjA1MWZlNmU2YjlkMWY2OTQ0IiwidGFnIjoiIn0%3D
; expires=Tue, 02-Jan-2024 06:29:43 GMT; Max-Age=7200; path=/; samesite=lax

- <https://banglamobile.ssbmultiservices.com/wishlist>

TOKEN=eyJpdiI6IlN4RXJpbW5WM0JjNFFxdkRNMlJ2SVE9PSIsInZhbnVlIjoieU1JT0Jkb2ZyZjRtcXcyMkNTN21sVHNWS1drL0VhcFFeK1BhRThhWnN2NFhsRndkZ21VM0oybEhwYXE0eFNqNkFuc0hlLQUE0UTZzRVR0aXZQTWp0eHVhR3dYZjdJc3ZDbGhoTzZsRXlTNUJCakZkTzE0cmdLOVvk0QitlbHFFZTMiLCJtYWMiOiI2NDc3YzllNGZkNWE5MWMwMyNzRmZDY3MzY5ODAzMWEwZXZWNlNjZjNDA0YTA5NGU0ODYyMDM3ODdiN2I0ZWl1OTQwIiwidGFuIjoieIn0%3D; expires=Tue, 02-Jan-2024 06:28:27 GMT; Max-Age=7200; path=/; samesite=lax

- TOKEN=eyJpdiI6IjZjRlRlbWxiaXAvckwvWFJRcHRPV0E9PSIsInZhbnVlIjoIjWp4Q3JxRldXOdCvcnEzZFdBW
HFEZHL0SS9RNnVkY0thdFVWNVVRbis0Zm1SUE5VV3ljM0VqMnRycEdmblQzRThoYlV3R1lPbm1Za2pqZWVZ1Bx
Z2IINmZyEGtBWxllV21FazF4Qjk1Q2NxQ2xwYVpNQkKFwVnKbHJGelpURGQiLCJtYWMiOiI5MjMyYTY30TE0MjA
0MmVLZmYwYWNlYzcyMzZmMwNTg2ZGI4YzkyOGZiYTUzNDQ1Njc20ThiMDkwYWY3YTJhYzYzIiwidGFuIjoIIn0%3D
; expires=Tue, 02-Jan-2024 06:30:25 GMT; Max-Age=7200; path=/; samesite=lax

- TOKEN=eyJpdjI6Ikw2V2VtR0h2QVJhQmoweGE1ZHNQZ1E9PSIsInZhbnVlIjoiIn2ZRnEwOTJHUUVVNDh0bEt2M
XphTzEzU2FZYlFQTctMa2pzV2Z3MlEzRDFZU0FCcHBGZ0xJZDBnU3pUK3lMVWw5RDRrZXF6RGdKdU56SWRlZ3U2
ektKRzNmb1UrK29QekZVWGFnTWZoLlFGeUdjM29nSmhyMw54SkdCMLBYV2oiLCJtYWMiOiI0YmU50DE4NzQ0MmJ
kNGNhYWE3ODcwY2E4MWEyMGYyYjZkMTQ4Y2U1NmUyNzlkNDEyZTQzNjNkYjI0OWU1YzI3IiwidGFnIjoiIn0%3D
; expires=Tue, 02-Jan-2024 06:30:25 GMT; Max-Age=7200; path=/; samesite=lax

- TOKEN=eyJpdjI6IjI5bjNBZyB4citiKMHHYVxkxLSGxxWlE9PSIsInZhbnHVLIjoivkZyTFVKJnhHV1IvYUdmMjd1Q
lorRlpFOGVENXI2eXpPT0laOFFlWGlwNlRHaVdvWXERCudVbE9SUUVuQmxYNmYNG9XNVVKUG5wY0wvZGRJZkM4WjQ0
NjdJUUVud2IxUmhId2tMdVpTV08vUWNuU3ZtNlB5aUg1RjNXcXN4REZhOVQiLCJtYWMiOiJiYTVMmWY2MzkwMTN
mZjRkYTNNKjYiZmZmNjNjYjlyYzg2NzdjNDUyYTQ0OTYyOTllZjFkZDg1YTI4YTIXMjJhIiwidGFniJoiIn0%3D
; expires=Tue, 02-Jan-2024 06:30:26 GMT; Max-Age=7200; path=/; samesite=lax

- TOKEN=eyJpdiI6InNmMXRVQ3dCUXhVaFVJR09ySULiOWc9PSIsInZhbnVlIjoiMGVYdXEvaFnlMWlmRWRSMTI5U
GRjQ1Q4aDFGWDNwRjBYRGNVVUFsMEh0YS91NkNqYVw6NUtTZWZhaemp4a085dXZjMGc2aFA1ZUxxS3hjM0Fibk10
Nk5zZ01YdStjMnJPN2xJTjBYRVMvdGVWYzluWjVuSXA4RnluZm1nQy9BaTkiLCJtYWMiOiIzNThkZGVhMGYyYTE
2MGJiY2M4MGE3Y2YzMWVmMTljOTg2N2UwNGNjNjc4YjBlZGQyNmI1NTlkYzU0NThlZmQ2IiwidGFuIjoiIn0%3D
; expires=Tue, 02-Jan-2024 06:30:39 GMT; Max-Age=7200; path=/; samesite=lax

- <https://banglamobile.ssbmultiservices.com/feature-products>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IkIhYWN1b2VpRFJkUUU3OEZ6U25LWUE9PSIsInZhbnVlIjoiYkhxcml6SjMwZnVVCYktGSzFhRzArSGF2YnJaK2g1ZXhlQWlGbDltMmw1UEJML2ptZjhtOWlseXRwbU1tcG5FbUl4aTFnSWM2WFAzVmVnVkZxMkNiNG10dVdxN0lqb2lqTTM3a0NuR3Evm80MWF5Zmg0Y0FiS0dUNEppaldYQ3giLCJtYWMiOiJiMWMYyJIZGVhZjhhkNDk2NjA4NjUxZTQ3MmVKNDBlNzA5ZDJjMzI0MGFlNzU4ODgyMjI5MTYzYjZiNmFkM2U0IiwidGFuIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:31:12 GMT; Max-Age=7200; path=/; samesite=lax

- <https://banglamobile.ssbmultiservices.com/hot-deals>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IkRSM3NiNnN0YVV3ZGRvK056Y0kxWnc9PSIsInZhbnVlIjoiVENRV1lydW5vNWxHVFN2R1FENEN1N0libTd0N2pyOGZzRy9KczVwRjFoVy9MSHJqOFhOT1EvSwpTVk5ubnZZZG95aVRBRjBFN3hGUmk4cm15UEhKeEI3WW1JaEc4T2N6bHY4b1BvVWhRwk92RHRSNnZ6VE4yOGt2NlhhTlZGdGgiLCJtYWMiOiJhNDFmMDY0MDcxNzY4YjhiZDEwNmVkZGM2YTU4ZmQ5Mjg2MDljN2VhYTE3OTc2NTM3YmI4MTdlNjI5NGYyMWU5IiwidGFuIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:31:13 GMT; Max-Age=7200; path=/; samesite=lax

- <https://banglamobile.ssbmultiservices.com/how-we-work>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6InRuaGM1c1VJTlo4Z1ZTQkZWtGJQYwc9PSIsInZhbnVlIjoiK2l6NFVYzmdjanVoVlJENEJvRHc2aEsvWjM1eGFUbUxUMkp1VHE4Q29oTnJRQXZiUEpLRDV4QVlNVmRmNXdscXVZaXN4OEZwNW0wTlBHdEZCTDBWeDZuYWJaQmZya01YaWlHUKM10Fd0NkF2K1RENytdSMvTwhBb1p3dGJtYloiLCJtYWMiOiI5MDdjOWY1NjNiNjNlMDg1MDg3MjllNTM1MDliYjRiOGVmZTViODQyZTMwZmY0MzY1MmFlMWZkOTdkYWMTU2IiwidGFuIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:31:22 GMT; Max-Age=7200; path=/; samesite=lax

- <https://banglamobile.ssbmultiservices.com/pay-bill>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IjNlYjFQa1l2a0RTRHAXYnRPM3NuSXc9PSIsInZhbnVlIjoiiekZFRDFCRLNST05xaG5wNG1YUllKWMjM5Fl6empabmVk0TRsTm5KVm9nN1hsR082TXdiQkkwdG5tVlJ6SmFWMm5RRjBZa0R1MGxKRG9ETmc3S2Fs d2Jkb2M1cTVQRUNxTno3RkozN3p6Q1kyNm1oVHFxU2lFVW85WlF1UDlQRlYiLCJtYWMiOiJjODJlMWUzNTFmMmJlNjc3ZWZiYzg0ODkzYW4NThlZmRlMWZkOTk0MmU1MmFiZDU2MDQ1YTIyZTkzYzE4N2U5IiwidGFuIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:31:23 GMT; Max-Age=7200; path=/; samesite=lax

- <https://banglamobile.ssbmultiservices.com/privacy-policy>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6Ii9DeHNpaVFkYnh1VDkwM0UwSk03c3c9PSIsInZhbnVlIjoiODR1OGVqTVM1UjBuSXprK1pwb1V6QmRlSSstIZmJYRkdjQitvZTRHbVUydjlyZGtNNjMxcUc5Z2orUXErb3BRRmhGQ3NRWUxwQjQvTURXNGFKS25q

Set-Cookie: XSRF-

TOKEN=eyJpdjI6ImtFMkh3OVcwaHI2a0R2cEtqR0xFU0E9PSIsInZhbnVlIjoicDlxWjBJQTZFUHpJV2lxQit2U
DQzVitUUmlsenJpeFNLNlZKdWpUcTlpRXQrVjh0aE9tSnNQYzBDbmNPcmRxVTZPS0tPdDQ4amVZYmZUOGpyNTlF
YWZHaDZTMXJRWW1xZDhXclFna3hPTzhXN0ZLY21yanVMZTNXdnB6dnI5YzQiLCJtYWMiOiJjZmFiYjM1ZmY3OTd
iYWIzZjc2YjBlZTk4YmE3ZjMwODY4MGJlZDZjNjI3ODYwNTYxYzNhMTZlMDk2ZDVjZGJhIiwidGFuIjoiIn0%3D
; expires=Tue, 02-Jan-2024 06:31:30 GMT; Max-Age=7200; path=/; samesite=lax

Request

GET / HTTP/1.1

Referer: https://banglamobile.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: banglamobile.ssbmultiservices.com

Connection: Keep-alive

Recommendation

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

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://banglamobile.ssbmultiservices.com/>

Verified

Cookies without Secure flag set:

- https://banglamobile.ssbmultiservices.com/

Set-Cookie: XSRF-

TOKEN=eyJpdjI6ImlNlT0E5YW5GVtN5RERjUWtaeVNqRUE9PSIsInZhbnVlIjoiwDdtZFI4WTZD0TRoUzJhdjBkV
VgyUWdxWkwUjZuM1FVUFNBNUY5ako3aU5tM2RQaWRnczZ6OFJ0TUNrVEpMUENOVzdCS2U1YnV5YXhJYXlBQTVm
MlhQbDFVYWdqS2dRcG1XcWRlTHVCSHhTcDNsYzE3cFR6VzI6NVhjMFNnZk4iLCJtYWMiOiI1ZTE5ZmI2ZTBkYzgy

yNTdjMTUyZjAxN2E1NDZjMmU0YjRhMzA2ZmIwYzZmMzI0ZDg5ZWY2NWE2MGUyNGI4YmZjIiwidGFnIjoiIn0%3D
; expires=Tue, 02-Jan-2024 06:26:37 GMT; Max-Age=7200; path=/; samesite=lax

- <https://banglamobile.ssbmultiservices.com/>

Set-Cookie:

bangla_mobile_session=eyJpdiI6InNvWUJrelIrRktQeU5sM0ljTFpXeUE9PSIsInZhbHVlIjoiQTR3TnZDa
FLXNHVOWDFHL2hSQUF1SWhMc3hWUTdV0EI4OXAvMFA4VXozd3JXSnrRmtNdHdwYlBLNWllTnlJcEdab3Z4V3h5
MjJvUXpmVVQzRUFTeCsraG54YjhlVVp6TEwlcER0eXVWZSt2VzRnYi93WFhTWnllODliNzhXVGsiLCJtYWMiOiI
1ZTY1NGQ2MDgxNjUwOGJkYWRkNTU5MGNjNjNhNzU3NjRlNWU0MWRiZTE1NGRkMzk1MjhlMWE3Mzk1NGQ1YmY5Ii
widGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:26:37 GMT; Max-Age=7200; path=/;
httponly; samesite=lax

- <https://banglamobile.ssbmultiservices.com/serarch>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6ImI6c6kt60VcxcUFUcFpWSEErOU1lakE9PSIsInZhbHVlIjoieEVCUE5sVTJpYmp3VUUnTlQwQ
W0xRkRtdGxtN1RBZERodVBaelVZa0Eyam4rSVBlckJldjJ0UFZ0anJuZitVV1Z0eGNVR1BhdWVyLzBKQVhmcFY3
ZmoyMHFNdk4xWfo5SXF6YlBaQmRQNklwSVdoaw9WdC9JZWNPbVRFWHFfaNVIiLCJtYWMiOiI0OWY1ZTVkZDAzZjk
yNWIXNWUwOTljMmY3MDFkZjI1ODM4YzAzZjI0YzFLMzUxNDk4MTC3MGFjNzZkMzJiOTM1IiwidGFnIjoiIn0%3D
; expires=Tue, 02-Jan-2024 06:27:47 GMT; Max-Age=7200; path=/; samesite=lax

- <https://banglamobile.ssbmultiservices.com/serarch>

Set-Cookie:

bangla_mobile_session=eyJpdiI6InBUU1B00WJPULJHwLZkelRtelkSWc9PSIsInZhbHVlIjoibG5KeEFhU
3lxZk1kc3dBemRPNFpWeWpZczFsNHhQVU43a0lPMLFkN0tQ0U9zbWM2dElBeEhvMGx5bitiZXZCbCtH0XRid2Jr
UUFBTfZVVHJmZ2RCZEx0TkrNS0lpSHhIZkxTcEJmQUc5eDZnRWR5aTV0SEt2Z2k2ZFRHai9UTnQiLCJtYWMiOiI
iNGU3ZjlhNmI0NjMxNzE2N2ZiMmIXODU3N2VmOWIyMmI1N2EzNmMzZGQ5NmE0NTAwZmI4ZmQ5Nzg0NTczY2UwIi
widGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:27:47 GMT; Max-Age=7200; path=/;
httponly; samesite=lax

- <https://banglamobile.ssbmultiservices.com/product/view/blood-pressure-formula>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6ImJsU3psUlZvODM2K0lTSWxZTGlBZEE9PSIsInZhbHVlIjoiUHhWeGxkYUovcmFZSnBwVjJRS
EtXTXhHem52UUFDdbStaRm9LN05HUVBTWxhoa3JlYjNmMlpEUFczYjJ0aU90ZGV0bGY4SHRiWUtyMzcrcdURHVFFS
eEdPNHhR0FFydG5KVW9zb1RndmxWWG9VQjk0QXNYMlBabTZHa0w3aEFGUloiLCJtYWMiOiIxNGJjZjJiMwMyMTd
lMTE5NDY2ZmJhMWQ0MTM2NWY1MTFmOTZmOTMzZmM2Y2Q4Nzk4YWI5ZGJiZWUyM2QzYmY5IiwidGFnIjoiIn0%3D
; expires=Tue, 02-Jan-2024 06:28:13 GMT; Max-Age=7200; path=/; samesite=lax

- <https://banglamobile.ssbmultiservices.com/product/view/blood-pressure-formula>

Set-Cookie:

```
bangla_mobile_session=eyJpdiI6InNVU3JtTTVDZTd4dk9SNEhIcHUxUGc9PSIsInZhbHVlIjoicEc3V3N1U
Vp3NExybmZhdXR0WSttUU40K3V0YnVRVzJLcUN6M3F4anRrcmt3QUh6c0N4amZyQklFWTRRRWo1dmsxdnNpaVJN
Ui9ReGxmQkUzOFpwTHBad1BTSW1NdUgyM0x2akVxY1hyOW5kN0daay9wYkx5Rn14UXJ6cCtUL2siLCJtYWMiOiJ
lZGQ3OWQwNzgzZTU3ZmY3YmEwMzE3OTVkd0TE4MzAwMjg0MDJkZjc4YTdmY2ZiZjkyMmMzYzc3N2EyMzE4Zjk4Ii
widGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:13 GMT; Max-Age=7200; path=/;
httponly; samesite=lax
```

- <https://banglamobile.ssbmultiservices.com/wishlist>

Set-Cookie:

```
bangla_mobile_session=eyJpdiI6IkhhUGpxQkhxcHphU1EyRzJqcE8yVnc9PSIsInZhbHVlIjoicEc3V3N1U
Vpzd1hGc2VFNXZDMi9ITTU1VXhwOWxGSGJWTKJqYWdCcURnTURKL1NBNUV3WG0xZm9kMm1mS2JiSTk1ZmtIdFJP
Vmo0S3ZCVUx3MDcyUjJoa0tLa3RSGVlN09YcURjRXo2VDlFRTZ3TVJnRWZUY01taUR3dFZuVVEiLCJtYWMiOiJ
kOWZiMDAxYzhkZWZkODE3OWFiN2EzNjZkNjA3ZGRiODAxZGM4YWQ1ZjgyNTI1MGExYTdhZWE4MTQwNDBkZTE3Ii
widGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:30 GMT; Max-Age=7200; path=/;
httponly; samesite=lax
```

- <https://banglamobile.ssbmultiservices.com/pay-bill/ultra-men-power>

Set-Cookie: XSRF-

```
TOKEN=eyJpdiI6IjU2ZlNjNTBEdkFlTzZ4OGJiaC9KQ3c9PSIsInZhbHVlIjoieG45TFV3cUJmcktttaEZ3aERRa
jR0Mk43QlFLSGJSN1ZtYw1Za3FpTnBVSHN2NFNIeGRyZkZkSzRhclJpOGh5QmJDQThVbHpmc2lJclJiZFltWDE1
T21XdW44N2d2Tc0ZKVTg4emU3eGN5bW1zcFpQbHNyYmVmR3FuSEpxZWtob0giLCJtYWMiOiJjYjY3YmE3Zjg2NjE
yMDRkY2RmNWVhYmZkNGMzYjY2NzZGRiYmRhZGJjMTMzOGY1ZjdiYzY0ODk0MGJkZGI2IiwidGFnIjoiIn0%3D
; expires=Tue, 02-Jan-2024 06:29:05 GMT; Max-Age=7200; path=/; samesite=lax
```

- <https://banglamobile.ssbmultiservices.com/pay-bill/ultra-men-power>

Set-Cookie:

```
bangla_mobile_session=eyJpdiI6IkppSURnLzN1S0VQMHhTTVFuNUk1T3c9PSIsInZhbHVlIjoicEc3V3N1U
Vp3NExybmZhdXR0WSttUU40K3V0YnVRVzJLcUN6M3F4anRrcmt3QUh6c0N4amZyQklFWTRRRWo1dmsxdnNpaVJN
Ui9ReGxmQkUzOFpwTHBad1BTSW1NdUgyM0x2akVxY1hyOW5kN0daay9wYkx5Rn14UXJ6cCtUL2siLCJtYWMiOiJ
lZGQ3OWQwNzgzZTU3ZmY3YmEwMzE3OTVkd0TE4MzAwMjg0MDJkZjc4YTdmY2ZiZjkyMmMzYzc3N2EyMzE4Zjk4Ii
widGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:29:05 GMT; Max-Age=7200; path=/;
httponly; samesite=lax
```

- <https://banglamobile.ssbmultiservices.com/wishlist>

bangla_mobile_session=eyJpdiiI6ILVRS3BtY0lLa3ZlSVF2MHVCenRZYXc9PSIsInZhbnHVLIjoiT1lGa1lFQjh2bjQ3OUxiNENQU0ljVjh6aEN5WG9YQ3gyT05HN0lQRGh4amNvVW50dk80d0RkWWlaNm1tOTNNND25ZOUQ2U05YNkRMSzNhbmEp5SnFU0EdUVnEvUXVMedGwUVdyNLZWtnY0BGI0ZEUwSFZGc2lyQ1ZBMGoyejFocEsiLCJtYWMiOiJlM2IyYWI5ZjAwYmNmYmZkNmU0NDhhNjU3MTE0NWVlMGQ1NGUxMjU4ZDlmN2YyN2Q5NGQ1ZTk3NWQ1ZjcxBjZmIiwidGFuIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:29:28 GMT; Max-Age=7200; path=/; httponly; samesite=lax

- Set-Cookie: XSRF-

TOKEN=eyJpdiI6Im81ZGdMYU0zcFFka0krQWwxM1NCR2c9PSIsInZhbnVlIjoiUXFtTW0UmRQ0DRjdGpIbFRtS2xPcHVPL2JaUERZelAwYUxCZTFsRGFjZTVwRFpPOHoxK0Z2M1ord0lndkVXZmRzQjFEYjErSVpDK3QzYUk0d2xybU4reVQ5Ky9UL2hmRDY3RlhPR1VpMmxxaHZQT05TRFVlOVhRdE8yZEdQaVYiLCJtYWMiOiIiZyZm0ZTUwZjYyOGFmNzA1MjYyZGI4OGU4MTA1NTA0NjgwODQ1ODJjZmYwNmFkNGU3MDllOThhODllZTMzZjhmIiwidGFmIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:27:46 GMT; Max-Age=7200; path=/; samesite=lax

- Set-Cookie:

bangla_mobile_session=eyJpdiI6Ik1lRXU4bWQ0aUV6WwtqTEZCV0Fla3c9PSIsInZhbnHVlIjoiSFNFdHZ6N1hWMFRWN1F3d2hDMXp4c2M4VHpaN0pJRnppV0tSd3dlR0g3dWN6WWEUDlCZVVPNUZFYXlxZlZUUDF2ZHLJNGorblZHdit5YjRuNUG2emM2cHlCQ1FyaGFZbmFpalpZdU9zU1R0dG96WVB0SEl0eUE1Y1UvSFFsVHIiLCJtYWMiOiIwNGJiNDZlMzA2YjdkNDU2YWRhZDQ0MjhiYjgxMzNmMzI5MTBiMzIxN2VmNWY1ZjA4ODY1NWUwYTRkNjIxYjc2IiwidGFuIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:27:46 GMT; Max-Age=7200; path=/; httponly; samesite=lax

- Set-Cookie: XSRF-

TOKEN=eyJpdii6ImFkc2V0cHEXTHFTSjUrdVoyZELRb2c9PSIsInZhbnVlIjoieHp2UUhRt3dnMHR4TXdlbVl3T1dlVzE3ZE5Yd0NLc0lQalQzSFVDTh0sZzRZQ0VYcHBmUDl2Tl5ULE4ZWlyVmU2UkZRT0hGZGR0ZzFYnJZ2SVRkNEQ3TjB3eXE5L3FKV0ZxcjNFl1o1NVVtQ1Z4NUZyYjRrM3h1L3dhbWRBbngiLCJtYWMiOiI4MGMxZW0nZk1N2QzYWQzZTY4ODQ1YmExNzA2Yjg2MGY3NjllNzZlMmNiNTUzNjA1MWZlNmU2YjlkMmWY20TQ0IiwidGFuIjoieIn0%3D; expires=Tue, 02-Jan-2024 06:29:43 GMT; Max-Age=7200; path=/; samesite=lax

- Set-Cookie:

bangla_mobile_session=eyJpdjI6Ii9sVTdCWFd0UTd0Tmg1ZllkS3hockE9PSIsInZhbnVlIjoiaKzB5NWp0c1M3QUJwK5pWZvVz1lMXo2RGZrK285L1RGWctralllQWJBME9XZF1DOHBTbEd0WDd0TMXYvREpKUXo2MwllKz10bEJNVHV5ZUNuTFVoUkhqK3J5ZVczSWF1SGR2Nm1Kb285bnBESlpVUTlrTFo1a0t1VEtuMURGN3UiLCJtYWMiOiJ

kMWU2YTFm0DNkNzE2NzEzYzIx0Dg4ZDUz0GE0ZDQ0ZDYxYTMzMzE1MDBhZjUzZjg1NTJjMzU4NmRiZDgyMTA1Ii
widGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:29:43 GMT; Max-Age=7200; path=/;
httponly; samesite=lax

- <https://banglamobile.ssbmultiservices.com/wishlist>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IlN4RXJpbW5WM0JjNFFxdkRNM1J2SVE9PSIsInZhbHVlIjoieU1JT0Jkb2ZyZjRtcXcyMkNTN
21sVHNWS1drL0VhcFFeK1BhRThhWnN2NFhsRndkZ21VM0oybEhwYXE0eFNqNkFuc0hlQUE0UTZzRVR0aXZQTWp0
eHVIR3dYZjdJc3ZDbGhoTzZsRXlTNUJCaKZkTzE0cmdLOVlk0QitlbHFFZTMiLCJtYWMiOiI2NDc3YzllNGZkNWE
5MWMYnZRMZDY3MzY5ODA3MWEhZWNlNjZjNDA0YTA5NGU0ODYyMDM3ODdiN2I0ZWl1OTQwIiwidGFnIjoiIn0%3D
; expires=Tue, 02-Jan-2024 06:28:27 GMT; Max-Age=7200; path=/; samesite=lax

- <https://banglamobile.ssbmultiservices.com/wishlist>

Set-Cookie:

bangla_mobile_session=eyJpdiI6IkZlc1paUndZMGZGc2ZxMkgwUWpaSnc9PSIsInZhbHVlIjoieWxiWTDdCS
lFCbVhKTU1qd2FsRmVvMzVzVGZ1bHMWY93UjFTT2RxNEtSWVg4RHRBemlpdjBMNktYdXNISUYxZU8xTjlsS3Zn
dzhrZ2thSWV1Zy9wOVRRSzJ2K0dsaEZ4UzhCL2VLTDJIBU10RG1mb3lwVWk5SR2VGVSENNR1BNUS8iLCJtYWMiOiJ
kNTc4NDIyYTYiNTcwZDJjNTJjY2E1ZDIyMGExN2YyZGU1Zjg3ZDgyZGRkMWEhZWNlNjZjNDA0YTA5NGU0ODYyMDM3ODdiN2I0ZWl1OTQwIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:27 GMT; Max-Age=7200; path=/;
httponly; samesite=lax

- <https://banglamobile.ssbmultiservices.com/about-us>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IjZjRlRlbWxiaXAvckwvWFJRcHRPV0E9PSIsInZhbHVlIjoieWp4Q3JxRldXb0cvcnEzZFdBW
HFEZHloSS9RNNvKYOthdFVWNVVRbis0Zm1SUE5VV3ljM0VqMnRycEdmblQzRThoY1V3R1lPbm1Za2pqZWNVZ1Bx
Z21lNmZyEgTlV21FazF4Qjk1Q2NzQ2xwYVpNqKJFVWNBHJGelpURGQiLCJtYWMiOiI5MjMyYTY30TE0MjA
0MmVLZmYwYWNlYzcyMzZGI4YzkyOGZiYTUzNDQ1Njc20ThiMDkwYWY3YTJhYzYzIiwidGFnIjoiIn0%3D
; expires=Tue, 02-Jan-2024 06:30:25 GMT; Max-Age=7200; path=/; samesite=lax

- <https://banglamobile.ssbmultiservices.com/about-us>

Set-Cookie:

bangla_mobile_session=eyJpdiI6ImVrNFhpd1p0Q1FpbXExdnZkYWlPTXc9PSIsInZhbHVlIjoiekc0NmJFQ
m9vVTR10EJLdmZV3BHUEFVTy9lMU9IRGNEMGVpUWFXymZkRUwrcFFtcmFqLzB2Ykc2USt0SFZVM0d3VGZXWElo
NThEdDQrZHJiakYzVzJ0UnZuZ2xEU0JCVE9ucG4vUUJSbU0wdndwTC9CZEVReExKN2g0NGlEN0oiLCJtYWMiOiI
4MDk40TIyZjdjN2YzNmIwNTk4YzJkZmJjMmU0ZTk2YzJlOGQ2NGZkZTYxMGZmODJmMGZhYTFhMzE2MmQ5ODgzIi
widGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:30:25 GMT; Max-Age=7200; path=/;
httponly; samesite=lax

- <https://banglamobile.ssbmultiservices.com/contact>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IkW2V2VtR0h2QVJhQmoweGE1ZHNQZ1E9PSIsInZhbmVlIjoiN2ZRSnEwOTJHUUVlNDh0bEt2M
XphTzEzU2FZYlFQTctMa2pzV2Z3MlEzRDFZU0FCcHBGZ0xJZDBuU3pUK3lMVWw5RDdrZXF6RGdKdU56SWRIZ3U2
ektKRzNmb1UrK29QekZVWGFnTWZoLlFGeUdjM29nSmhyMw4SkdCMLBYV2oiLCJtYWMiOiI0YmU5ODE4NzQ0MmJ
kNGNhYWE3ODcwY2E4MWEyMGYyYjZkMTQ4Y2U1NmUyNzlkNDEyZTQzNjNkYjI0WU1Yzc3IiwidGFuIjoiIn0%3D
; expires=Tue, 02-Jan-2024 06:30:25 GMT; Max-Age=7200; path=/; samesite=lax

- <https://banglamobile.ssbmultiservices.com/contact>

Set-Cookie:

bangla_mobile_session=eyJpdiI6IlJzckdyRGh2VFliaVhZbzBQK0F6NEE9PSIsInZhbmVlIjoiZhdDN0c1V
ldkMG8weTJzMXBQU95UFpjMms3SEJYQzJRYjBpT1RwQXJCRTQ4ZWY1RlZJM2RkQVlORVNPT1ladDNHNGhlYlJz
SHdUUUozWlBSZ2RsZU5TSTI1WVdqM0hxRlcwVWV6UzIzQ0VZcUptZ2FXV05pcmxJNEtLQzVwUUEiLCJtYWMiOiI
2OGQ0M2I5MDZhNTZjODg0ODk3Mjc5YzAxZmU2ZjdMzYzMDA2MjRlOWU10TE5ZDM4ODI3YzYyN2Y0YzdiZjKxIi
widGFuIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:30:25 GMT; Max-Age=7200; path=/;
httponly; samesite=lax

- <https://banglamobile.ssbmultiservices.com/customer-service>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IjI5bjNBZ3B4citKMhYVYkxLSGxxWlE9PSIsInZhbmVlIjoiVkJyTFVKNjhHV1IvYUdmMjd1Q
lorRlpF0GVENXI2eXpPT0la0FFlWGlwNlRHaVdvWxErcUdVbE9SZUVuQmxYNG9XNVVKUG5wY0wvZGRJZkM4WjQ0
NjdJUVNud2IxUmhId2tMdVpTV08vUWNUU3ZtNlB5aUg1RjNxcXN4REZhOVQiLCJtYWMiOiJiYTVMmWY2MzkwMTN
mZjRkYTnkYjZiZmZmNjNjYjYjYzYzNzZjNDUyYTQ0OTYyOTllZjFkZDg1YTI4YTIxMjJhIiwidGFuIjoiIn0%3D
; expires=Tue, 02-Jan-2024 06:30:26 GMT; Max-Age=7200; path=/; samesite=lax

Request

GET / HTTP/1.1
Referer: <https://banglamobile.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: banglamobile.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://banglamobile.ssbmultiservices.com/>

Documentation files:

- <https://banglamobile.ssbmultiservices.com/README.md>

File contents (first 100 characters):

```
<p align="center"><a href="https://laravel.com" target="_blank">

Verified

An iframe tag references an external resource, and no sandbox attribute is set.

## Request

```
GET /contact HTTP/1.1
Referer: https://banglamobile.ssbmultiservices.com/
Cookie: XSRF-
TOKEN=eyJpdjI6ImFkc2V0cHEXTHFTSjUrdVoyZElRb2c9PSIsInZhbnVlIjoieHp2UUhrT3dnMHR4TXdlbV3T1dVzE3ZE5Yd0NLc01Q
a1QzSFVDT0hsZzRZQ0VYcHBmUDl2TTL5U1E4ZWlyVmU2UkZRT0hGZGR0ZzFYNjZ2SVRkNEQ3TjB3eXE5L3FKV0ZxcjNFl1o1NVVtQ1Z4NU
ZyYjRrM3h1L3d3bWRBbngiLCJtYWMiOiI4MGxZWm0Nzk1N2QzYWQzZTY4ODQ1YmExNzA2Yjg2MGY3NjllNzZlMmNiNTUzNjA1MWZlNmU2
YjlkMWY2OTQ0IiwidGFuIjoieH0%3D;
bangla_mobile_session=eyJpdjI6ImFkc2V0cHEXTHFTSjUrdVoyZElRb2c9PSIsInZhbnVlIjoieHp2UUhrT3dnMHR4TXdlbV3T1dVzE3ZE5Yd0NLc01Q
MXo2RGZrK285L1RGWCtrallIQWJBME9XZFlDOHBTbEd0WDdTMXYvREpKUXo2MmWlKzL0bEJNVHV5ZUNuTFVoUkhqK3J5ZVczSWFLSGR2Nm
lKb285bnBESlpVUTlrTFo1a0tlVEtuMURGN3UiLCJtYWMiOiI4MGxZWm0Nzk1N2QzYWQzZTY4ODQ1YmExNzA2Yjg2MGY3NjllNzZlMmNiNTUzNjA1MWZlNmU2
ZjUzZjgINTJjMzU4NmRiZDgyMTA1IiwidGFuIjoieH0%3D
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
```

## Recommendation

---

Review the iframe's purpose and environment, and use the sandbox attribute to secure the iframe while applying sandbox directives to ease security restrictions if necessary.

## References

---

[MDN | iframe: The Inline Frame Element](https://developer.mozilla.org/en-US/docs/Web/HTML/Element/iframe)

<https://developer.mozilla.org/en-US/docs/Web/HTML/Element/iframe>

[HTML Standard: iframe](https://html.spec.whatwg.org/multipage/iframe-embed-object.html#the-iframe-element)

<https://html.spec.whatwg.org/multipage/iframe-embed-object.html#the-iframe-element>

[HTML 5.2: 4.7. Embedded content](https://www.w3.org/TR/html52/semantics-embedded-content.html#element-attrdef-iframe-sandbox)

<https://www.w3.org/TR/html52/semantics-embedded-content.html#element-attrdef-iframe-sandbox>

## 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://banglamobile.ssbmultiservices.com/>**

Possible sensitive directories:

- <https://banglamobile.ssbmultiservices.com/uploads>
- <https://banglamobile.ssbmultiservices.com/upload>
- <https://banglamobile.ssbmultiservices.com/admin>
- <https://banglamobile.ssbmultiservices.com/database>
- <https://banglamobile.ssbmultiservices.com/config>
- <https://banglamobile.ssbmultiservices.com/tests>

## Request

---

GET /uploads/ HTTP/1.1

Cookie: XSRF-

TOKEN=eyJpdii6IjU2ZLNjNTBEkFLtZz40GJiaC9K0k3c9PSIsInZhbmHVLIjoieG45TFV3cUJmckttaEZ3aERRajR0Mk43QlFLSGJSN1ZtYwLWZa3FpTnBvSHN2NFNIeGRyZkZkSzRhcLJpOGh5QmJDQThV0Hpmc2lJc1JiZjFltWDE1T2lXdw44N2dTc0ZKVtG4emU3eGN5bWlzcFpQbHNYaVMwR3FuSEpxZWtob0giLCJtYWMiOiJjYjI3YmE3Zjg2NjEyMDRkY2RmNWVkyZWZkNGMzYjY2NzM2ZGRiYmRhZGJjMTMzOGY1ZjdiYzY0ODk0MGJkZGI2IiwidGFuIjoiiIn0%3D;  
 bangla\_mobile\_session=eyJpdii6IkpSURnLzN1S0VQMhHTTVFuNUk1T3c9PSIsInZhbmHVLIjoieG45TFV3cUJmckttaEZ3aERRajR0Mk43QlFLSGJSN1ZtYwLWZa3FpTnBvSHN2NFNIeGRyZkZkSzRhcLJpOGh5QmJDQThV0Hpmc2lJc1JiZjFltWDE1T2lXdw44N2dTc0ZKVtG4emU3eGN5bWlzcFpQbHNYaVMwR3FuSEpxZWtob0giLCJtYWMiOiJjYjI3YmE3Zjg2NjEyMDRkY2RmNWVkyZWZkNGMzYjY2NzM2ZGRiYmRhZGJjMTMzOGY1ZjdiYzY0ODk0MGJkZGI2IiwidGFuIjoiiIn0%3D;  
 bm5GM1RzWkRrBDbtSVF5emJpD2VTSnZsSUNlMEhrcnFTRThic3JjVWdoa09zUXRBSUhZVkJibWRIK1bWJ4ZTRMZFB3YURHtm5VUjRRU3VPVFRKbHREOGdhSGc1TURJRXRzZE81Qm8rQWEiLCJtYWMiOiI0OTVmMDBkNzQ2N2I0MGY5Zjc2N2QyZjIyNGM3ODU2MzRlNWJkMWQ3ZTk1MGJhN2E2MGFjNDQyZmJiYTYzZDM0IiwidGFuIjoiiIn0%3D  
 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: banglamobile.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/>

## Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

## Impact

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

<https://banglamobile.ssbmultiservices.com/>

### Possible sensitive files:

- <https://banglamobile.ssbmultiservices.com/web.config>

## Request

```
GET /web.config HTTP/1.1
Accept: lyfzwdn/vjik
Cookie: XSRF-
TOKEN=eyJpdiiI6IjU2ZLNJNTBEdkFlTzZ40GJiaC9KQ3c9PSIsInZhbnVlIjoieG45TFV3cUJmckttaEZ3aERRajR0Mk43QlFLSGJSN1ZtYWwLa3FpTnBVSHN2NFNIeGRyekZkSzRhclJpOGh5OmdDQThtV0Hpmc2LjclJiZFltWDE1T21XdW44N2dTc0ZKVtq4emU3eGN5bWlzcfPqbH
```

NYaVMwR3FuSEpxZWtob0giLCJtYWMiOiJjYjI3YmE3Zjg2NjEyMDRkY2RmNWVhYmZkNGMzYjY2NzMTZGRiYmRhZGJjMTMzOGY1ZjdiYzY0ODk0MGJkZGI2IiwidGFnIjoiIn0%3D;  
bangla\_mobile\_session=eyJpdiI6IlVRS3BtY01La3Z1SVF2MHVCenRZYXc9PSIsInZhbnVlIjoiT1lGa1lFQjh2bjQ3OUxiNENQU0ljVjh6aEN5WG9YQ3gyT05HN0lQRGh4amNvVW50dk80d0RkWWlaNm1t0TNNd25Z0UQ2U05YNkRMSzNhEp5SnFU0EdUVnEvUXVMeDgwUVdyNlZWt0Y0bG10ZEUwSFZGc21yQ1ZBMGoyejFocEsiLCJtYWMiOiJlM2IyYWI5ZjAwYmNmYmZkNmU0NDhhNjU3MTE0NWVlMGQ1NGUxMjU4ZDZmN2YyN2Q5NGQ1ZTk3NWQ1ZjcxMjZmIiwidGFnIjoiIn0%3D  
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: banglamobile.ssbmultiservices.com  
Connection: Keep-alive

## Recommendation

Restrict access to this file or remove it from the website.

## References

[Web Server Security and Database Server Security](https://www.acunetix.com/websitesecurity/webserver-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://banglamobile.ssbmultiservices.com/>

Paths without CSP header:

- <https://banglamobile.ssbmultiservices.com/>
- <https://banglamobile.ssbmultiservices.com/product/view/blood-pressure-formula>
- <https://banglamobile.ssbmultiservices.com/uploads/paybill/large/>
- <https://banglamobile.ssbmultiservices.com/pay-bill/ultra-men-power>
- <https://banglamobile.ssbmultiservices.com/upload/header-footer/>
- <https://banglamobile.ssbmultiservices.com/admin/>
- <https://banglamobile.ssbmultiservices.com/products/category/accessories-61e26ea54ea5b>
- <https://banglamobile.ssbmultiservices.com/about-us>
- <https://banglamobile.ssbmultiservices.com/contact>
- <https://banglamobile.ssbmultiservices.com/customer-service>
- <https://banglamobile.ssbmultiservices.com/vendor/autoload.php>
- <https://banglamobile.ssbmultiservices.com/feature-products>
- <https://banglamobile.ssbmultiservices.com/hot-deals>
- <https://banglamobile.ssbmultiservices.com/how-we-work>
- <https://banglamobile.ssbmultiservices.com/pay-bill>
- <https://banglamobile.ssbmultiservices.com/privacy-policy>
- <https://banglamobile.ssbmultiservices.com/return-refund>
- <https://banglamobile.ssbmultiservices.com/terms-service>
- <https://banglamobile.ssbmultiservices.com/why-choose-us>
- <https://banglamobile.ssbmultiservices.com/product/view/digestive-engyme>
- <https://banglamobile.ssbmultiservices.com/index.php>

## Request

---

GET / HTTP/1.1  
Referer: https://banglamobile.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: banglamobile.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)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>

### [Implementing Content Security Policy](https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)

<https://hacks.mozilla.org/2016/02/implementing-content-security-policy/>

# Content type is not specified

These page(s) does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems.

## Impact

None

<https://banglamobile.ssbmultiservices.com/>

Verified

Pages where the content-type header is not specified:

- <https://banglamobile.ssbmultiservices.com/.styleci.yml>
- <https://banglamobile.ssbmultiservices.com/composer.lock>
- <https://banglamobile.ssbmultiservices.com/README.md>
- <https://banglamobile.ssbmultiservices.com/.env>
- <https://banglamobile.ssbmultiservices.com/.env.live>
- <https://banglamobile.ssbmultiservices.com/web.config>
- <https://banglamobile.ssbmultiservices.com/vendor/bin/carbon>
- <https://banglamobile.ssbmultiservices.com/vendor/bin/php-parse>



- <https://banglamobile.ssbmultiservices.com/vendor/bin/phpunit>
- <https://banglamobile.ssbmultiservices.com/vendor/bin/psys>
- <https://banglamobile.ssbmultiservices.com/vendor/bin/var-dump-server>
- <https://banglamobile.ssbmultiservices.com/vendor/bin/patch-type-declarations>

## Request

```
GET /.styleci.yml HTTP/1.1
Referer: https://banglamobile.ssbmultiservices.com/
Cookie: XSRF-
TOKEN=eyJpdiI6Ii9DeHNpaVFkYnh1VDkwM0UwSk03c3c9PSIsInZhbnVlIjoiodR10GVqTVM1UjBuSXprK1pwb1V6QmRlSStIZmJYRkdj
QitvZTRHbVUydjlyZGtNNjMxcUc5Z2orUXErb3BRRmhGQ3NRWUxwQjQvTURXNGFKS25qbGF4Ym9INFQrMGpsZlpwSFRrVWlmSkc2bDBWQl
JReEttQTJ2cEFGclB0Qm0iLCJtYWMiOiI3MGRiNmM0YmZhYmMyNGY4YTNkYjc2OGRkOWUwMTU3NTZkNmNhNzcyYTgyZjFmYTEyNmYwYTRm
ZDUyYzBlOWExIiwidGFuIjoiaW0%3D;
bangla_mobile_session=eyJpdiI6IktlYlpl4MFRNc1ArME5TekRPbnlwdkE9PSIsInZhbnVlIjoiTU5pQStSRHlZcklUWG92K0E3d1F4
VDg3Nk83NG16V6K5QYitIewVBTvdrVHNIN3hIQnJucFY1azZhWUhmMXJzaDlnUTdqbfVHRVZSeFU0ak9YT0NjT240NDFhdi8vTTZYbzZ0OW
dWUjZCZlk2Z2ZmXk2pSMWlNaFJrSW80T2xCeG8iLCJtYWMiOiI3MGRiNmM0YmZhYmMyNGY4YTNkYjc2OGRkOWUwMTU3NTZkNmNhNzcyYTgyZjFmYTEyNmYwYTRm
YzZwNGRjYjUyYUxNDUzZGU2ZjIiIiwidGFuIjoiaW0%3D
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: banglamobile.ssbmultiservices.com
Connection: Keep-alive
```

## Recommendation

Set a Content-Type header value for these page(s).

# Email addresses

One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

## Impact

Email addresses posted on Web sites may attract spam.

### <https://banglamobile.ssbmultiservices.com/>

Emails found:

- <https://banglamobile.ssbmultiservices.com/banglamobileny@gmail.com>
- <https://banglamobile.ssbmultiservices.com/digitalonetravel@gmail.com>

- <https://banglamobile.ssbmultiservices.com/serarch>  
**banglamobileny@gmail.com**
- <https://banglamobile.ssbmultiservices.com/serarch>  
**digitalonetravel@gmail.com**
- <https://banglamobile.ssbmultiservices.com/product/view/blood-pressure-formula>  
**banglamobileny@gmail.com**
- <https://banglamobile.ssbmultiservices.com/product/view/blood-pressure-formula>  
**digitalonetravel@gmail.com**
- <https://banglamobile.ssbmultiservices.com/pay-bill/ultra-men-power>  
**banglamobileny@gmail.com**
- <https://banglamobile.ssbmultiservices.com/pay-bill/ultra-men-power>  
**digitalonetravel@gmail.com**
- <https://banglamobile.ssbmultiservices.com/products/category/accessories-61e26ea54ea5b>  
**banglamobileny@gmail.com**
- <https://banglamobile.ssbmultiservices.com/products/category/accessories-61e26ea54ea5b>  
**digitalonetravel@gmail.com**
- <https://banglamobile.ssbmultiservices.com/about-us>  
**banglamobileny@gmail.com**
- <https://banglamobile.ssbmultiservices.com/about-us>  
**digitalonetravel@gmail.com**
- <https://banglamobile.ssbmultiservices.com/contact>  
**banglamobileny@gmail.com**
- <https://banglamobile.ssbmultiservices.com/contact>  
**digitalonetravel@gmail.com**
- <https://banglamobile.ssbmultiservices.com/customer-service>  
**banglamobileny@gmail.com**
- <https://banglamobile.ssbmultiservices.com/customer-service>  
**digitalonetravel@gmail.com**
- <https://banglamobile.ssbmultiservices.com/feature-products>  
**banglamobileny@gmail.com**
- <https://banglamobile.ssbmultiservices.com/feature-products>  
**digitalonetravel@gmail.com**
- <https://banglamobile.ssbmultiservices.com/hot-deals>  
**banglamobileny@gmail.com**
- <https://banglamobile.ssbmultiservices.com/hot-deals>  
**digitalonetravel@gmail.com**
- <https://banglamobile.ssbmultiservices.com/how-we-work>  
**banglamobileny@gmail.com**

## Request

---

GET / HTTP/1.1

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: banglamobile.ssbmultiservices.com

Connection: Keep-alive

## Recommendation

---

Check references for details on how to solve this problem.

## References

---

[Anti-spam techniques](https://en.wikipedia.org/wiki/Anti-spam_techniques)

[https://en.wikipedia.org/wiki/Anti-spam\\_techniques](https://en.wikipedia.org/wiki/Anti-spam_techniques)

# 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://banglamobile.ssbmultiservices.com/>**

Locations without Permissions-Policy header:

- <https://banglamobile.ssbmultiservices.com/>
- <https://banglamobile.ssbmultiservices.com/serarch>
- <https://banglamobile.ssbmultiservices.com/product/view/blood-pressure-formula>
- <https://banglamobile.ssbmultiservices.com/wishlist>
- <https://banglamobile.ssbmultiservices.com/uploads/paybill/large/>
- <https://banglamobile.ssbmultiservices.com/pay-bill/ultra-men-power>
- <https://banglamobile.ssbmultiservices.com/upload/header-footer/>
- <https://banglamobile.ssbmultiservices.com/admin/>
- <https://banglamobile.ssbmultiservices.com/products/category/accessories-61e26ea54ea5b>
- <https://banglamobile.ssbmultiservices.com/about-us>
- <https://banglamobile.ssbmultiservices.com/contact>
- <https://banglamobile.ssbmultiservices.com/customer-service>
- <https://banglamobile.ssbmultiservices.com/wishlist/40c3c9cc2212888b799a8b3b8a6c8152>
- <https://banglamobile.ssbmultiservices.com/vendor/autoload.php>
- <https://banglamobile.ssbmultiservices.com/feature-products>
- <https://banglamobile.ssbmultiservices.com/hot-deals>
- <https://banglamobile.ssbmultiservices.com/how-we-work>
- <https://banglamobile.ssbmultiservices.com/pay-bill>
- <https://banglamobile.ssbmultiservices.com/privacy-policy>
- <https://banglamobile.ssbmultiservices.com/return-refund>
- <https://banglamobile.ssbmultiservices.com/terms-service>

## Request

---

GET / HTTP/1.1  
Referer: https://banglamobile.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: banglamobile.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://banglamobile.ssbmultiservices.com/>

Pages with paths being disclosed:

- <https://banglamobile.ssbmultiservices.com/contact-mail/home/ssbmul5/banglamobile.ssbmultiservices.com/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php>
- <https://banglamobile.ssbmultiservices.com/password/email/home/ssbmul5/banglamobile.ssbmultiservices.com/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php>
- <https://banglamobile.ssbmultiservices.com/serarch/home/ssbmul5/banglamobile.ssbmultiservices.com/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php>
- <https://banglamobile.ssbmultiservices.com/wishlist/610f952b087ae4beb70d637b7e2755ef/home/ssbmul5/banglamobile.ssbmultiservices.com/vendor/bumbummen99/shoppingcart/src/Cart.php>
- <https://banglamobile.ssbmultiservices.com/products/category/home/ssbmul5/banglamobile.ssbmultiservices.com/app/Http/Controllers/Front/ViewProductController.php>

- <https://banglamobile.ssbmultiservices.com/index.php/serarch/home/ssbmul5/banglamobile.ssbmultiservices.com/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php>
- <https://banglamobile.ssbmultiservices.com/index.php/contact-mail/home/ssbmul5/banglamobile.ssbmultiservices.com/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php>
- <https://banglamobile.ssbmultiservices.com/index.php/wishlist/610f952b087ae4beb70d637b7e2755ef/home/ssbmul5/banglamobile.ssbmultiservices.com/vendor/bumbummen99/shoppingcart/src/Cart.php>
- <https://banglamobile.ssbmultiservices.com/index.php/products/category/home/ssbmul5/banglamobile.ssbmultiservices.com/app/Http/Controllers/Front/ViewProductController.php>
- <https://banglamobile.ssbmultiservices.com/wishlist/40c3c9cc2212888b799a8b3b8a6c8152/home/ssbmul5/banglamobile.ssbmultiservices.com/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php>
- <https://banglamobile.ssbmultiservices.com/wishlist/4ace7efbcc6e608a26017e98cee400f4/home/ssbmul5/banglamobile.ssbmultiservices.com/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php>
- <https://banglamobile.ssbmultiservices.com/wishlist/610f952b087ae4beb70d637b7e2755ef/home/ssbmul5/banglamobile.ssbmultiservices.com/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php>
- <https://banglamobile.ssbmultiservices.com/index.php/wishlist/610f952b087ae4beb70d637b7e2755ef/home/ssbmul5/banglamobile.ssbmultiservices.com/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php>

## Request

```
GET /contact-mail HTTP/1.1
Referer: https://banglamobile.ssbmultiservices.com/contact
Cookie: XSRF-
TOKEN=eyJpdiI6IlJENDlxMXBVMlRlTUN0a2JlWDJJclE9PSIsInZhbmVlIjoiri0c1U3VqYllFcFp5QUd0MWRlTlLQYUt0SjBBTis1bEFUaWFGbk1HV0VVUUwcvlRaU9m0EEvWxVFeXnc3JoZHBGTHVDRnpERURCdVZkV3J4UjNlMnAweVlobjJLYmxza2JsKzBOUnR2N0NGWUt0YTMvaGoyaEQvMDhhk3ZVb3AiLCJtYWMiOiIzYjFkOWU0WQ1ZTVmNTJmMjBjNDdjZGYyODQzZWZmMjQ4NDUzMDZiYjIwMjJmZjFmNDNlYjdiNzdkYjk0NWZjIiwidGFuIjoiriIn0%3D;
bangla_mobile_session=eyJpdiI6InloU2Jab3BWSVh5NysxMUZ1Tkglb2c9PSIsInZhbmVlIjoia1RaelNmVlZYmRkZB5NWR0M2piMjhxVzK30EJRmVBpVXRSLnNhHlKRm1FWG1tb3lneGxXb1p6emwxUU9lcGU4R0JPCvdBMEhoMm1ndFYwQlI0bXdCdKpjSHA2SGFhZU9sWmNMDXg0ZVlvaFE5dXdVczgwYm51cnk4VElhdhUilCJtYWMiOiJkZjBlZDY0ZWZiMWQyMTRlM2E4OTExYzk4Zjg4M2EzYzAxNjQyZjJlZDdmMDk5ZDc5MDI0WU5YzExMWZkNjJlIiwidGFuIjoiriIn0%3D
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: banglamobile.ssbmultiservices.com
Connection: Keep-alive
```

## Recommendation

Prevent this information from being displayed to the user.

## References

## Full Path Disclosure

[https://www.owasp.org/index.php/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://banglamobile.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: banglamobile.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.

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

Pages where SRI is not implemented:

- ## Request

<https://banglamobile.ssbmultiservices.com/wishlist/40c3c9cc2212888b799a8b3b8a6c8152>

Pages where SRI is not implemented:

- ## Request

47

## 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/uxy9rx7HNQlGYl1kPzQh01wx4JwY8wC"
crossorigin="anonymous"></script>
```

## References

---

### [Subresource Integrity](https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity)

[https://developer.mozilla.org/en-US/docs/Web/Security/Subresource\\_Integrity](https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity)

### [SRI Hash Generator](https://www.srihash.org/)

<https://www.srihash.org/>



# Coverage

https://banglamobile.ssbmultiservices.com

Inputs

GET iv, value, mac, tag

\_ignition

Inputs

GET iv, value, mac, tag

health-check

Inputs

GET iv, value, mac, tag

admin

Inputs

GET iv, value, mac, tag

assets

Inputs

GET iv, value, mac, tag

css

Inputs

GET iv, value, mac, tag

fonts

Inputs

GET iv, value, mac, tag

images

Inputs

GET iv, value, mac, tag

scripts

Inputs

GET iv, value, mac, tag

cgi-sys

Inputs

GET iv, value, mac, tag

config

Inputs

GET iv, value, mac, tag

database

Inputs

GET iv, value, mac, tag

front

Inputs

GET iv, value, mac, tag

assets

Inputs

GET iv, value, mac, tag

css

custom.css

flexslider.css

menu.css

responsive.css

style.css

grid-gallery

GridHorizontal.js

imagesloaded.pkgd.min.js

jquery.scripthead.min.css

lightbox.css

lightbox.js

images

Inputs

GET iv, value, mac, tag

js

custom.js

easing.js

jquery.min.js

move-top.js

nav-hover.js

nav.js

script.js

owl-carousel

owl.carousel.min.js

index.php



Inputs

GET

iv, value, mac, tag



pay-bill



Inputs

GET

iv, value, mac, tag



ultra-men-power



Inputs

GET

iv, value, mac, tag



ultra-men-powers



Inputs

GET

iv, value, mac, tag



product



Inputs

GET

iv, value, mac, tag



view



blood-pressure-formula



Inputs

GET

iv, value, mac, tag



digestive-engyme



Inputs

GET

iv, value, mac, tag



ginseng-plant



Inputs

GET

iv, value, mac, tag



herbal-oil



Inputs

GET

iv, value, mac, tag



joint-formula



Inputs

GET

iv, value, mac, tag



joint-relief



Inputs

GET

iv, value, mac, tag

















low-t-booster



Inputs

GET

iv, value, mac, tag

|                                                                                                                |                     |
|----------------------------------------------------------------------------------------------------------------|---------------------|
|  medicated                      |                     |
|  Inputs                       |                     |
|                               | iv, value, mac, tag |
|  men-formula                  |                     |
|  Inputs                       |                     |
|                               | iv, value, mac, tag |
|  men-power-hand-watch         |                     |
|  Inputs                       |                     |
|                               | iv, value, mac, tag |
|  rhemulein-pain-reliever-oil  |                     |
|  Inputs                       |                     |
|                               | iv, value, mac, tag |
|  skin-care                    |                     |
|  Inputs                       |                     |
|                               | iv, value, mac, tag |
|  supper-nice-watch            |                     |
|  Inputs                      |                     |
|                             | iv, value, mac, tag |
|  test                       |                     |
|  Inputs                     |                     |
|                             | iv, value, mac, tag |
|  time-max-time-max-time-max |                     |
|  Inputs                     |                     |
|                             | iv, value, mac, tag |
|  ultra-men-power            |                     |
|  Inputs                     |                     |
|                             | iv, value, mac, tag |
|  ultra-men-power-one        |                     |
|  Inputs                     |                     |
|                             | iv, value, mac, tag |
|  ultra-men-power-watch      |                     |
|  Inputs                     |                     |
|                             | iv, value, mac, tag |
|  ultra-men-watch            |                     |
|  Inputs                     |                     |
|                             | iv, value, mac, tag |

 ultra-power-watch

 Inputs

**GET** iv, value, mac, tag

 vision-support

 Inputs

**GET** iv, value, mac, tag

 view

 Inputs

**GET** iv, value, mac, tag

 products

 Inputs

**GET** iv, value, mac, tag

 category

 accessories-61e26ea54ea5b

 Inputs

**GET** iv, value, mac, tag

 mobile-phone-61e26e5798d5d

 Inputs

**GET** iv, value, mac, tag

 nokia-61e2a5a572ba0

 Inputs

**GET** iv, value, mac, tag

 sumsung-61e2bacb0de2e

 Inputs

**GET** iv, value, mac, tag

 tablet-61e26e8802be8

 Inputs

**GET** iv, value, mac, tag

 watch-61e26e954f067

 Inputs

**GET** iv, value, mac, tag

 category

 Inputs

**GET** iv, value, mac, tag

 wishlist

## Inputs

**GET** iv, value, mac, tag

---

 610f952b087ae4beb70d637b7e2755ef

## Inputs

**GET** iv, value, mac, tag

---

**POST** iv, value, mac, tag

---

**POST** \_method, \_token

---

 about-us

## Inputs

**GET** iv, value, mac, tag

---

 contact

## Inputs

**GET** iv, value, mac, tag

---

 contact-mail

## Inputs

**GET** iv, value, mac, tag

---

**POST** iv, value, mac, tag

---

**POST** \_token, email, name, phone, subject

---

 customer-service

## Inputs

**GET** iv, value, mac, tag

---

 feature-products

## Inputs

**GET** iv, value, mac, tag

---

 hot-deals

## Inputs

**GET** iv, value, mac, tag

---

 how-we-work

## Inputs

**GET** iv, value, mac, tag

---

 pay-bill

## Inputs

**GET** iv, value, mac, tag

---

 privacy-policy

## Inputs

 iv, value, mac, tag

 product

 Inputs

 iv, value, mac, tag

 products

 Inputs

 iv, value, mac, tag

 page

 return-refund

 Inputs

 iv, value, mac, tag

 serarch

 Inputs


 iv, value, mac, tag

 \_token, search

 \_token, search

 page

 iv, value, mac, tag

 terms-service

 Inputs

 iv, value, mac, tag

 why-choose-us

 Inputs

 iv, value, mac, tag

 wishlist

 Inputs

 iv, value, mac, tag

 iv, value, mac, tag

 \_token, productId, qty

 js

 Inputs

 iv, value, mac, tag

 mailman

 Inputs

 iv, value, mac, tag

## password

### Inputs

**GET** iv, value, mac, tag

## email

### Inputs

**POST** iv, value, mac, tag

**POST** \_token, email

**GET** iv, value, mac, tag

## reset

### Inputs

**GET** iv, value, mac, tag

## pay-bill

### Inputs

**GET** iv, value, mac, tag

## ultra-men-power

### Inputs

**GET** iv, value, mac, tag

## ultra-men-powers

### Inputs

**GET** iv, value, mac, tag

## product

### Inputs

**GET** iv, value, mac, tag

## view

### Inputs

**GET** iv, value, mac, tag

## blood-pressure-formula

### Inputs

**GET** iv, value, mac, tag

## digestive-engyme

### Inputs

**GET** iv, value, mac, tag

## ginseng-plant

### Inputs

**GET** iv, value, mac, tag

## herbal-oil





GET iv, value, mac, tag



GET iv, value, mac, tag



GET iv, value, mac, tag



GET iv, value, mac, tag



GET iv, value, mac, tag



GET iv, value, mac, tag



GET iv, value, mac, tag



GET iv, value, mac, tag



GET iv, value, mac, tag



GET iv, value, mac, tag



GET iv, value, mac, tag



GET iv, value, mac, tag

 ultra-men-power

 Inputs

**GET** iv, value, mac, tag

---

 ultra-men-power-one

 Inputs

**GET** iv, value, mac, tag

---

 ultra-men-power-watch

 Inputs

**GET** iv, value, mac, tag

---

 ultra-men-watch

 Inputs

**GET** iv, value, mac, tag

---

 ultra-power-watch

 Inputs

**GET** iv, value, mac, tag

---

 vision-support

 Inputs

**GET** iv, value, mac, tag

---

 view

 Inputs

**GET** iv, value, mac, tag

---

 products

 Inputs

**GET** iv, value, mac, tag

---

 category

 Inputs

**GET** iv, value, mac, tag

---

 accessories-61e26ea54ea5b

 Inputs

**GET** iv, value, mac, tag

---

 mobile-phone-61e26e5798d5d

 Inputs

**GET** iv, value, mac, tag

---

 nokia-61e2a5a572ba0

 Inputs

**GET** iv, value, mac, tag

 sumsung-61e2bacb0de2e

 Inputs

**GET** iv, value, mac, tag

 tablet-61e26e8802be8

 Inputs

**GET** iv, value, mac, tag

 watch-61e26e954f067

 Inputs

**GET** iv, value, mac, tag

 category

 Inputs

**GET** iv, value, mac, tag

 resources

 Inputs

**GET** iv, value, mac, tag

 storage

 Inputs

**GET** iv, value, mac, tag

 tests

 Inputs

**GET** iv, value, mac, tag

 toastr

 Inputs

**GET** iv, value, mac, tag

 css

 Inputs

**GET** iv, value, mac, tag

 toastr.min.css

 js

 Inputs

**GET** iv, value, mac, tag

 toastr.min.js

 upload

 Inputs

**GET** iv, value, mac, tag

about-us-image

Inputs

GET iv, value, mac, tag

---

header-footer

Inputs

GET iv, value, mac, tag

---

photo-gallery

Inputs

GET iv, value, mac, tag

---

uploads

Inputs

GET iv, value, mac, tag

---

home-slider

Inputs

GET iv, value, mac, tag

---

hot-deals

Inputs

GET iv, value, mac, tag

---

large

Inputs

GET iv, value, mac, tag

---

paybill

Inputs

GET iv, value, mac, tag

---

large

Inputs

GET iv, value, mac, tag

---

product-gallery

Inputs

GET iv, value, mac, tag

---

large

Inputs

GET iv, value, mac, tag

---

product

Inputs

GET iv, value, mac, tag

 78186.webp

 Inputs

**GET** iv, value, mac, tag

 vendor

 Inputs

**GET** iv, value, mac, tag

 asm89

 Inputs

**GET** iv, value, mac, tag

 bin

 Inputs

**GET** iv, value, mac, tag

 carbon

 Inputs

**GET** iv, value, mac, tag

 carbon.bat


 Inputs

**GET** iv, value, mac, tag

 patch-type-declarations

 Inputs

**GET** iv, value, mac, tag

 patch-type-declarations.bat

 Inputs

**GET** iv, value, mac, tag

 php-parse

 Inputs

**GET** iv, value, mac, tag

 php-parse.bat

 Inputs

**GET** iv, value, mac, tag

 phpunit


 Inputs

**GET** iv, value, mac, tag

 phpunit.bat

 Inputs

 iv, value, mac, tag

 psysh

 Inputs

 iv, value, mac, tag

 psysh.bat

 Inputs

 iv, value, mac, tag

 var-dump-server

 Inputs

 iv, value, mac, tag

 var-dump-server.bat

 Inputs

 iv, value, mac, tag

 brick

 Inputs

 iv, value, mac, tag

 bumbummen99

 Inputs

 iv, value, mac, tag

 composer

 Inputs

 iv, value, mac, tag

 dflydev

 Inputs

 iv, value, mac, tag

 doctrine

 Inputs

 iv, value, mac, tag

 dragonmantank

 Inputs

 iv, value, mac, tag

 egulias

 Inputs

 iv, value, mac, tag

 facade



GET iv, value, mac, tag



GET iv, value, mac, tag



GET iv, value, mac, tag



GET iv, value, mac, tag



GET iv, value, mac, tag



GET iv, value, mac, tag



GET iv, value, mac, tag



GET iv, value, mac, tag



GET iv, value, mac, tag



GET iv, value, mac, tag



GET iv, value, mac, tag




GET iv, value, mac, tag


 monolog


 Inputs

 GET iv, value, mac, tag


---

 myclabs

 Inputs

 GET iv, value, mac, tag

---

 nesbot

 Inputs

 GET iv, value, mac, tag

---


 nette


 Inputs

 GET iv, value, mac, tag

---

 nicmart

 Inputs

 GET iv, value, mac, tag


---


 nikic


 Inputs

 GET iv, value, mac, tag

---

 nunomaduro

 Inputs

 GET iv, value, mac, tag

---

 opis

 Inputs

 GET iv, value, mac, tag


---


 phar-io


 Inputs

 GET iv, value, mac, tag


---


 phpdocumentor


 Inputs

 GET iv, value, mac, tag


---


 phpoption


 Inputs

 GET iv, value, mac, tag




---

 phpspec

 Inputs




 GET iv, value, mac, tag






 phpunit  
 Inputs  
 GET iv, value, mac, tag

 psr  
 Inputs  
 GET iv, value, mac, tag




 psy  
 Inputs  
 GET iv, value, mac, tag




 ralouphie  
 Inputs  
 GET iv, value, mac, tag




 ramsey  
 Inputs  
 GET iv, value, mac, tag




 sebastian  
 Inputs  
 GET iv, value, mac, tag



 spatie  
 Inputs  
 GET iv, value, mac, tag

 swiftmailer  
 Inputs  
 GET iv, value, mac, tag

 symfony  
 Inputs  
 GET iv, value, mac, tag

 theseer  
 Inputs  
 GET iv, value, mac, tag

 tijsverkoyen  
 Inputs  
 GET iv, value, mac, tag

 vlucas  


 iv, value, mac, tag

 voku

 Inputs

 iv, value, mac, tag

 webmozart

 Inputs

 iv, value, mac, tag

 autoload.php

 Inputs

 iv, value, mac, tag

 wishlist

 Inputs

 iv, value, mac, tag

 081abfa36a6db7cd604996a9996107ab

 Inputs

 \_method, \_token

 40c3c9cc2212888b799a8b3b8a6c8152

 Inputs

 iv, value, mac, tag

 iv, value, mac, tag

 \_method, \_token


 4ace7efbcc6e608a26017e98cee400f4

 Inputs

 iv, value, mac, tag

 iv, value, mac, tag

 \_method, \_token

 610f952b087ae4beb70d637b7e2755ef

 Inputs

 iv, value, mac, tag

 iv, value, mac, tag

 \_method, \_token

 \_ignition

 Inputs

 iv, value, mac, tag

 .env



Inputs

**GET** iv, value, mac, tag

---



.env.live



Inputs

**GET** iv, value, mac, tag

---



.styleci.yml



Inputs

**GET** iv, value, mac, tag

---



about-us



Inputs

**GET** iv, value, mac, tag

---



composer.json



Inputs

**GET** iv, value, mac, tag

---



composer.lock



Inputs

**GET** iv, value, mac, tag

---



contact



Inputs

**GET** iv, value, mac, tag

---



contact-mail



Inputs

**GET** iv, value, mac, tag

**POST** iv, value, mac, tag

**POST** \_token, email, name, phone, subject

---



customer-service



Inputs

**GET** iv, value, mac, tag

---



feature-products



Inputs

**GET** iv, value, mac, tag

---



hot-deals



Inputs

**GET** iv, value, mac, tag

---



how-we-work



Inputs

GET

iv, value, mac, tag



index.php



Inputs

GET

iv, value, mac, tag



login



Inputs

POST

iv, value, mac, tag

POST

\_token, email, password

POST

\_token, email, password

GET

iv, value, mac, tag



package-lock.json



Inputs

GET

iv, value, mac, tag



package.json



Inputs

GET

iv, value, mac, tag



password



Inputs

GET

iv, value, mac, tag



pay-bill



Inputs

GET

iv, value, mac, tag



privacy-policy



Inputs

GET

iv, value, mac, tag



product



Inputs

GET

iv, value, mac, tag



products



Inputs

GET

iv, value, mac, tag

GET

page



README.md



Inputs

**GET** iv, value, mac, tag

---

 return-refund

 Inputs

**GET** iv, value, mac, tag

---

 robots.txt

 Inputs

**GET** iv, value, mac, tag

---

 serarch

 Inputs

**POST** iv, value, mac, tag

**POST** \_token, search

**POST** \_token, search

**GET** page

**GET** iv, value, mac, tag


---

 sitemap.xml

 Inputs

**GET** iv, value, mac, tag

---

 terms-service

 Inputs

**GET** iv, value, mac, tag

---

 web.config

 Inputs

**GET** iv, value, mac, tag

---