

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	bdana.ssbbmultiservices.com
Scan Type	Full Scan
Start Time	Jan 2, 2024, 12:26:58 PM GMT+8
Scan Duration	7 hours, 20 minutes
Requests	546377
Average Response Time	33ms
Maximum Response Time	14333ms
Application Build	v23.7.230728157



High



Medium



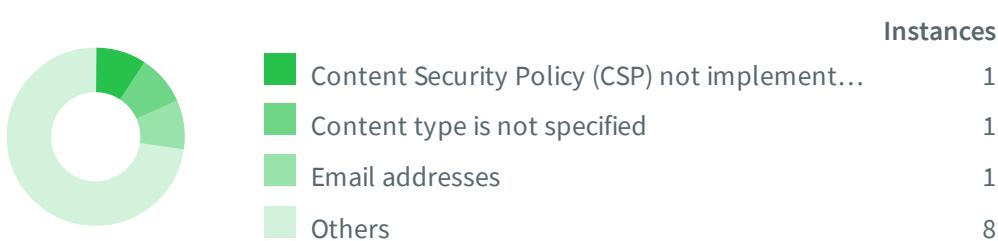
Low



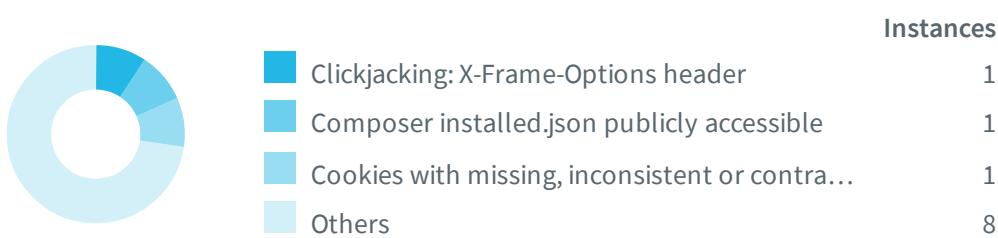
Informational

Severity	Vulnerabilities	Instances
❗ High	3	4
⚠ Medium	5	5
❗ Low	10	11
ℹ️ Informational	9	11
Total	27	31

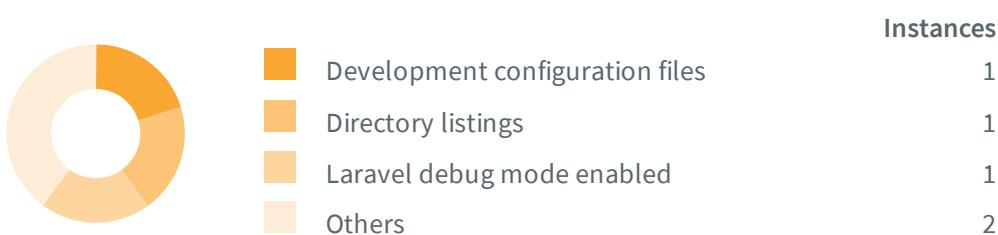
Informational



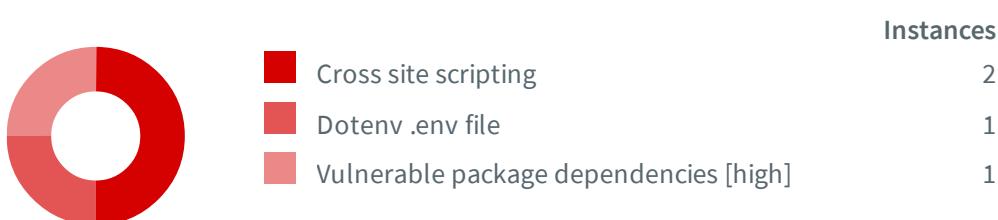
Low Severity



Medium Severity



High Severity



Impacts

SEVERITY	IMPACT
❗ High	2 Cross site scripting
❗ High	1 Dotenv .env file
❗ High	1 Vulnerable package dependencies [high]
❗ 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 package dependencies [medium]
❗ Low	1 Clickjacking: X-Frame-Options header
❗ Low	1 Composer installed.json publicly accessible
❗ Low	1 Cookies with missing, inconsistent or contradictory properties
❗ 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	2 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

SEVERITY**IMPACT**

 Informational	1	File uploads
 Informational	3	Outdated JavaScript libraries
 Informational	1	Permissions-Policy header not implemented
 Informational	1	Possible server path disclosure (Unix)
 Informational	1	Reverse proxy detected

Cross site scripting

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

Impact

Malicious JavaScript has access to all the same objects as the rest of the web page, including access to cookies and local storage, which are often used to store session tokens. If an attacker can obtain a user's session cookie, they can then impersonate that user.

Furthermore, JavaScript can read and make arbitrary modifications to the contents of a page being displayed to a user. Therefore, XSS in conjunction with some clever social engineering opens up a lot of possibilities for an attacker.

<https://bdana.ssbtmultiservices.com/index.php/subscribe-register-form>

URL encoded GET input **plan** was set to **0 onmouseover=moTt(95196) y=**

The input is reflected inside a tag parameter without quotes.

Request

```
GET /index.php/subscribe-register-form?plan=0%20onmouseover=moTt(95196)%20y= HTTP/1.1
Referer: https://bdana.ssbtmultiservices.com/
Cookie: PHPSESSID=4b5e7857595c78ff5af667c80e3168f1; XSRF-TOKEN=eyJpdiI6IkdkSUIzbjI4S0dxRkNPV0VHcTF3Qmc9PSIsInZhbHVlIjoibjhIY3d3em9xdGNRZldTQnZB0DZ0WDRDK3h1M1L5RHU5ZEJENlFOQWwwMuTPeUhCeVFLV3A1UE9lckYraVRkS2RFcVhVVjl3c3hSZHrtUEpkYitSdXVZVjZHaGoxcCt2UUxFyWm9JNJRtFVuQnczRkw5METXS1N0emhkYktkUEgiLCJtYWMi0iI2ZjUyYmQ5NjFjYTRkMGFlZTMzMjFkODgx0TkwNDIzZGM3ZTQyMDA5ZjgzNWRiNjdi0DA0MWxRjMjliNzYzNWRlIiwidGFnIjoiIn0%3D;
bangladesh_dental_association_of_north_america_session=eyJpdiI6ImhlVlnMLzZiUktYZlphZ3ZTRzg1Rmc9PSIsInZhbHVlIjoiWE55Qy91V0lyYjRiZXJTTVJDc2ZCYWxVdFJiMmVvbVl1a1ZoM0pGc0c4WG4wRU5XSzNDd1BhQnNaQzJTSmFBu9NUHdrYmFlQTNxMzMwVDlNZWY1T3dMZkZRQy9zV0dkWFVzdzFocU05ewlkQXE0SDI2N2lhnQnlhSENGeKhhRFIiLCJtYWMi0iI5N2NmZWE0NmQwNjQwNDU4NzU3MjA1MmNkNGFhMWRiNTRhMjNlOGYxMjVkJnWZmMzU3MTc3IiwidGFnIjoiIn0%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: bdana.ssbtmultiservices.com
Connection: Keep-alive
```

<https://bdana.ssbtmultiservices.com/subscribe-register-form>

URL encoded GET input **plan** was set to **0 onmouseover=kRrg(95566) y=**

The input is reflected inside a tag parameter without quotes.

Request

```
GET /subscribe-register-form?plan=0%20onmouseover=kRrg(95566)%20y= HTTP/1.1
Referer: https://bdana.ssbbmultiservices.com/
Cookie: PHPSESSID=6d40a857c8014cff0f5af1960f14d210; XSRF-
TOKEN=eyJpdiI6ImZKwFTbk5LbzCMEhudTJPYUuvTEE9PSIsInZhHVlIjoiVTFDZGlV0DRCSTNEYTZONENoNHAzUVBNcFA5MG
NSMFhxNTE5b215SkNKcmhVQnBieGdFTDJlMFhTTjl0YXNFVnhir0pSR3dnZUhMk9pY0lpdlFuawRMVm9RQjgvbk00WVdQaHJDZ2
lqaENBRkk3eWcycTJtaWJJenNNUR4SKUiLCJtYWMi0iI3NDFhNmZlNmI2YmU2YTI4MzQxMjhLYmU1YTMzZDc10GYyMzJmYTiYnj
QzMWE2NDM0MWVjNzIw0WY5NzljYTYYIiwidGFnIjoiIn0%3D;
bangladesh_dental_association_of_north_america_session=eyJpdiI6Inlmb2Y4eVN3Yjh4Z0xNSllqc3BUZHc9PSIsInZhHVlIjoiWFryUkZCUXZTTDRsemxvR2JzN2U0MXcx0VVZRkI2V3BuUGdtQjJuUDRwHy0c29GSFR4dmcvMWgzTkw3eVd4ckZoQ
3ZxWGY3ZjlwM1JHQmh5V1hmNTVmL1JnWVRxZVRaNG9xakVjV1Z6cER3cjFsbU9WaURjZXVzTHdDbTY5Z1YiLCJtYWMi0iJhYjEyN
jBhZTZkMTFlNTM1NzFlNzUzMDliYzkxMzRiMmJmYmNkYmMx0GF1MTcxYTQwZWZhNmM1ZTYx0GF1N2MzIiwidGFnIjoiIn0%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: bdana.ssbbmultiservices.com
Connection: Keep-alive
```

Recommendation

Apply context-dependent encoding and/or validation to user input rendered on a page

References

Cross-site Scripting (XSS) Attack - Acunetix

<https://www.acunetix.com/websitesecurity/cross-site-scripting/>

Types of XSS - Acunetix

<https://www.acunetix.com/websitesecurity/xss/>

XSS Filter Evasion Cheat Sheet

https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet

Excess XSS, a comprehensive tutorial on cross-site scripting

<https://excess-xss.com/>

Cross site scripting

https://en.wikipedia.org/wiki/Cross-site_scripting

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://bdana.ssbtmultiservices.com/>

Verified

File: `.env`

Pattern found:

`APP_ENV=`

Request

```
GET /.env HTTP/1.1
Cookie: PHPSESSID=c0f392e546a83e61122cfb5e9e95d0a8; XSRF-TOKEN=eyJpdiI6Iml6TWZLak5nSnFGd2p1b2t2S1hPN1E9PSIsInZhbHVlIjoiSE42dDBaQ2pRQ3QxMDB4ZHhlcnlVRmpoZ0RTN1duZpnTDZZVW8vRDJ0VUhqamNaQUZ00S9VUGkyc2xmamZlTHlt0EtyY0JZV2owVzFGWldjSXA3WnVkvXpuUDRGmzRuQvhXNElpUHdTmNxT0Q4WTFVSStMZEYwNGhCajVNeisiLCJtYWMi0iJkZjM5MDY3YTQyNTZiYWUyzTE50DA4YmRkODVkmWM4MDg00TQ0ZWM30TJkNmMwNmE3ZTNlYmFm0Tkx0WYwYzM2IiwidGFnIjoiIn0%3D;
bangladesh_dental_association_of_north_america_session=eyJpdiI6Inlw3JWN0M3QndDTVyzTldJWTNn0Hc9PSIsInZhbHVlIjoibjNrRXNmZ043eDVxNTJ1YjJPWDNocGU1WWYwd2VVb2JoZWpDSmZ0eE8vVEhLTGxDK3VKUSTmU0d6UmR0d1NCaTNseENNNUZLQUDWNWRMd0h0dWUrefFdjYUNjMC9oWHQxellr0XF5K3VIME4zQTU5RjV1ZDE0N1lteEdHa3BUQ2wiLCJtYWMi0iI4NTA3NzYyM2VkJNTE5YzI4MwYzYmM1M2U1NmRjNjRm0TcwZmVjMjVlNmQ3MDM0Y2EwNDY20DBkM2Qz0DlmMjYzIiwidGFnIjoiIn0%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: bdana.ssbtmultiservices.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://bdana.ssbtmultiservices.com/>

List of vulnerable **composer** packages:

Package: guzzlehttp/guzzle

Version: 7.4.0

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: 7.4.0

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: 7.4.0

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/1dd98b0564cb3f6bd16ce683cb755f94c10fbdb82>
- <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: 7.4.0

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/1dd98b0564cb3f6bd16ce683cb755f94c10fb82>
- <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: 7.4.0

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 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: 2.1.0

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

Package: guzzlehttp/psr7

Version: 2.1.0

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/http-psr7/security/advisories/GHSA-q7rv-6hp3-vh96>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=2022-24775>
- <https://github.com/guzzle/http-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/](mailto:announce@lists.fedoraproject.org/message/O35UN4IK6VS2LXSRWUDFWY7NI73RKY2U/)
- [https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/FJANwdxjze5BGLN4MQ4FEHV5LJ6CMKQF/](mailto:announce@lists.fedoraproject.org/message/FJANwdxjze5BGLN4MQ4FEHV5LJ6CMKQF/)

Package: symfony/http-kernel

Version: 5.3.10

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.

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://bdana.ssbbmultiservices.com/>

Development configuration files:

- <https://bdana.ssbbmultiservices.com/package.json>

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

- <https://bdanassbbmultiservices.com/composer.json>

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

- <https://bdana.ssbbmultiservices.com/composer.lock>

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

- <https://bdana.ssbbmultiservices.com/package-lock.json>

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

- <https://bdana.ssbbmultiservices.com/docker-compose.yml>

docker-compose.yml => Docker Compose configuration file. Docker Compose is a tool for defining and running multi-container Docker applications.

Request

```
GET /package.json HTTP/1.1
Cookie: PHPSESSID=c0f392e546a83e61122cfb5e9e95d0a8; XSRF-
TOKEN=eyJpdI6Iml6TWZLak5nSnFGd2p1b2t2S1hPN1E9PSIsInZhHVlIjoiSE42dBaQ2pRQ3QxMDB4ZHhlcnlVRmpoZ0RTN1
duZVpnTDZZVw8vRDJ0VUhqamNaQUZ00S9VUGkyc2xmamZlTHlt0EtyY0JZV2owVzFGWldjSXA3WnVkvXpuUDRGmzRuQvhXNElpUH
dHTmNxT0Q4WTFVSStMZEYwNGhCajVNeisiLCJtYWMi0iJkZjM5MDY3YTQyNTZiYWUyZTE50DA4YmRk0DVkMWM4MDg00TQ0ZWM30T
JkNmMwNmE3ZTNlYmFm0Tkx0WYwYzM2IiwidGFnIjoiIn0%3D;
bangladesh_dental_association_of_north_america_session=eyJpdI6InlWb3JWN0M3QndDTVyzTldJWTNn0Hc9PSIsInZhHVlIjoi
bJNrRXNmZ043eDVxNTJ1YjJPWDNocGU1WWYwd2VVb2JoZWpDSmZ0eE8vVEhLTGxDK3VKUSTmU0d6UmR0d1NCaTNseENNNUZLQ
UdWNWRM0h0dWUreFdjYUNjMC9oWHQxellr0XF5K3VIME4zQ TU5RjV1ZDE0N1lteEdHa3BUQ2wiLCJtYWMi0iI4NTA3nZyYm2V
kNTE5YzI4MWYzYmM1M2U1NmRjNjRm0TcwZmVjMjVlNmQ3MDM0Y2EwNDY20DBkM2Qz0DlmMjYzIiwidGFnIjoiIn0%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: bdana(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://bdana\(ssbmultiservices.com/](https://bdana(ssbmultiservices.com/)

Verified

Folders with directory listing enabled:

- [https://bdana\(ssbmultiservices.com/assets/](https://bdana(ssbmultiservices.com/assets/)
- [https://bdana\(ssbmultiservices.com/assets/website/](https://bdana(ssbmultiservices.com/assets/website/)
- [https://bdana\(ssbmultiservices.com/assets/website/fonts/](https://bdana(ssbmultiservices.com/assets/website/fonts/)
- [https://bdana\(ssbmultiservices.com/assets/website/fonts/fontawesome/](https://bdana(ssbmultiservices.com/assets/website/fonts/fontawesome/)
- [https://bdana\(ssbmultiservices.com/assets/website/fonts/fontawesome/css/](https://bdana(ssbmultiservices.com/assets/website/fonts/fontawesome/css/)
- [https://bdana\(ssbmultiservices.com/assets/toastr/](https://bdana(ssbmultiservices.com/assets/toastr/)

- <https://bdana.ssbumultiservices.com/assets/toastr/js/>
- <https://bdana.ssbumultiservices.com/assets/website/fonts/fontawesome/webfonts/>
- <https://bdana.ssbumultiservices.com/upload/>
- <https://bdana.ssbumultiservices.com/upload/about-us-image/>
- <https://bdana.ssbumultiservices.com/config/>
- <https://bdana.ssbumultiservices.com/database/>
- <https://bdana.ssbumultiservices.com/vendor/>
- <https://bdana.ssbumultiservices.com/resources/>
- <https://bdana.ssbumultiservices.com/storage/>
- <https://bdana.ssbumultiservices.com/tests/>
- <https://bdana.ssbumultiservices.com/upload/at-glance/>
- <https://bdana.ssbumultiservices.com/resources/css/>
- <https://bdana.ssbumultiservices.com/storage/app/>
- <https://bdana.ssbumultiservices.com/upload/banner-slider/>
- <https://bdana.ssbumultiservices.com/database/factories/>

Request

```
GET /assets/ HTTP/1.1
Cookie: PHPSESSID=c0f392e546a83e61122cfb5e9e95d0a8; XSRF-TOKEN=eyJpdiI6Iml6TWZLak5nSnFGd2p1b2t2S1hPN1E9PSIsInZhbHVlIjoiSE42dDBaQ2pRQ3QxMDB4ZHhlcnlVRmpoZ0RTN1duZVpnTDZZVW8vRDJ0VUhqamNaQUZ00S9VUGkyc2xmamZlTHlt0EtY0JZV2owVzFGWldjSXA3WnVkJXpuUDRGmzRuQVhXNElpUhdHTmNxT0Q4WTFVSStMZEYwNGhCajVNeisiLCJtYWMi0iJkZjM5MDY3YTQyNTZiYWUyZTE50DA4YmRk0DVkMWM4MDg00TQ0ZWM30TJkNmMwNmE3ZTNlYmFm0Tkx0WYwYzM2IiwidGFnIjoiIn0%3D;
bangladesh_dental_association_of_north_america_session=eyJpdiI6Inlw3JWN0M3QndDTVyzTldJWTNn0Hc9PSIsInZhbHVlIjoibjNrRXNmZ043eDVxNTJ1YjJPWDNocGU1WWYwd2VVb2JoZWpDSmZ0eE8vVEhLTGxDK3VKUStmU0d6UmR0d1NCaTNseENNNUZLQudWNWRMd0h0dWUreFdjYUNjMC9oWHQxellr0XF5K3VIME4zQTU5RjV1ZDE0N1lteEdHa3BUQ2wiLCJtYWMi0iI4NTA3NzYyM2VkJNT5YzI4MWYzYmM1M2U1NmRjNjRm0TcwZmVjMjVlNmQ3MDM0Y2EwNDY20DBkM2Qz0DlmMjYzIiwidGFnIjoiIn0%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: bdana.ssbumultiservices.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://bdana.ssbtmultiservices.com/>

Request

```
PUT /index.php HTTP/1.1
Cookie: PHPSESSID=c0f392e546a83e61122cfb5e9e95d0a8; XSRF-TOKEN=eyJpdiI6Iml6TwZLak5nSnFGd2p1b2t2S1hPN1E9PSIsInZhbHVlIjoISE42dBaQ2pRQ3QxMDB4ZHhlcnlVRmpoZ0RTN1duZVpnTDZZVw8vRDJ0VUhqamNaQUZ00S9VUGkyc2xmamZlTHlt0EtY0JZV2owVzFGWldjSXA3WnVkvXpuUDRGmzRuQvhXNElpUHdHTmNxT0Q4WTFVsstMZEYwNGhCajVNeisiLCJtYWMi0iJkZjM5MDY3YTQyNTZiYWUyZTE50DA4YmRk0DVkmwm4MDg00TQ0ZWM30TJkNmMwNmE3ZTNlYmFm0Tkx0WYwYzM2IiwidGFnIjoiIn0%3D;
bangladesh_dental_association_of_north_america_session=eyJpdiI6Inlw3JWN0M3QndDTVYzTldJwTNn0Hc9PSIsInZhbHVlIjoibjNrRXNmZ043eDVxNTJ1YjJPWDNocGU1WWYwd2VVb2JoZWpDSmZ0eE8vVEhLTGxDK3VKUStmU0d6UmR0d1NCaTNseENNNuZLQudWNWRMd0h0dWUreFdjYUNjMC9oWHQxellr0XF5K3VIME4zQTU5RjV1ZDE0N1lteEdHa3BUQ2wiLCJtYWMi0iI4NTA3NzYyM2VkNTE5YzI4MWYzYmM1M2U1NmRjNjRm0TcwZmVjMjVlNmQ3MDM0Y2EwNDY20DBkM2Qz0DlmMjYzIiwidGFnIjoiIn0%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: bdana.ssbtmultiservices.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://bdana.ssbtmultiservices.com/>

Request

```
GET /storage/logs/laravel.log HTTP/1.1
Cookie: PHPSESSID=c0f392e546a83e61122cfb5e9e95d0a8; XSRF-TOKEN=eyJpdiI6Iml6TWZLak5nSnFGd2p1b2t2S1hPN1E9PSIsInZhHVlIjoiSE42dBaQ2pRQ3QxMDB4ZHhlcnlVRmpoZ0RTN1duZVpnTDZZVW8vRDJ0VUhqamNaQUZ00S9VUGkyc2xmamZlTHlt0EtyY0JZV2owVzFGWldjSXA3WnVkJXpuUDRGmzRuQvhXNElpUhdHTmNxT0Q4WTFVsStMZEYwNGhCajVNeisiLCJtYWMi0iJkZjM5MDY3YTQyNTZiYWUyZTE50DA4YmRk0DVkMWM4MDg00TQ0ZWm30TJkNmMwNmE3ZTNlYmFm0Tkx0WYwYzM2IiwidGFnIjoiIn0%3D;
bangladesh_dental_association_of_north_america_session=eyJpdiI6Inlw3JWN0M3QndDTVyzTldJWTNn0Hc9PSIsInZhHVlIjoibjNrRXNmZ043eDVxNTJ1YjJPWDNocGU1WWYwd2VVb2JoZwpDSmZ0eE8vVEhLTGxDK3VKUStmU0d6UmR0d1NCaTNseENNNUZLQUDWNWRMd0h0dWUreFdjYUNjMC9oWHQxellr0XF5K3VIME4zQ TU5RjV1ZDE0N1lteEdHa3BUQ2wiLCJtYWMi0iI4NTA3NzYyM2VkNTE5YzI4MWYzYmM1M2U1NmRjNjRm0TcwZmVjMjVlNmQ3MDM0Y2EwNDY20DBkM2Qz0DlmMjYzIiwidGFnIjoiIn0%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: bdana.ssbtmultiservices.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>

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://bdana.ssbtmultiservices.com/>

List of vulnerable **composer** packages:

Package: laravel/framework

Version: 8.70.2

CVE: CVE-2021-43808

Title: Use of a Broken or Risky Cryptographic Algorithm

Description: Laravel is a web application framework. Laravel prior to versions 8.75.0, 7.30.6, and 6.20.42 contain a possible cross-site scripting (XSS) vulnerability in the Blade templating engine. A broken HTML element may be clicked and the user taken to another location in their browser due to XSS. This is due to the user being able to guess the parent placeholder SHA-1 hash by trying common names of sections. If the parent template contains an exploitable HTML structure an XSS vulnerability can be exposed. This vulnerability has been patched in versions 8.75.0, 7.30.6, and 6.20.42 by determining the parent placeholder at runtime and using a random hash that is unique to each request.

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

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

CWE: CWE-327

References:

- <https://github.com/laravel/framework/releases/tag/v6.20.42>
- <https://github.com/laravel/framework/commit/b8174169b1807f36de1837751599e2828ceddb9b>
- <https://github.com/laravel/framework/pull/39909>
- <https://github.com/laravel/framework/pull/39908>
- <https://github.com/laravel/framework/security/advisories/GHSA-66hf-2p6w-jqfw>
- <https://github.com/laravel/framework/pull/39906>
- <https://github.com/laravel/framework/releases/tag/v7.30.6>
- <https://github.com/laravel/framework/releases/tag/v8.75.0>

Package: symfony/http-kernel

Version: 5.3.10

CVE: CVE-2021-41267

Title: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')

Description: Symfony/Http-Kernel is the HTTP kernel component for Symfony, a PHP framework for web and console applications and a set of reusable PHP components. Headers that are not part of the "trusted_headers" allowed list

are ignored and protect users from "Cache poisoning" attacks. In Symfony 5.2, maintainers added support for the `X-Forwarded-Prefix` headers, but this header was accessible in SubRequest, even if it was not part of the "trusted_headers" allowed list. An attacker could leverage this opportunity to forge requests containing a `X-Forwarded-Prefix` header, leading to a web cache poisoning issue. Versions 5.3.12 and later have a patch to ensure that the `X-Forwarded-Prefix` header is not forwarded to subrequests when it is not trusted.

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

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

CWE: CWE-444

References:

- <https://github.com/symfony/symfony/security/advisories/GHSA-q3j3-w37x-hq2q>
- <https://github.com/symfony/symfony/releases/tag/v5.3.12>
- <https://github.com/symfony/symfony/commit/95dcf51682029e89450aee86267e3d553aa7c487>
- <https://github.com/symfony/symfony/pull/44243>

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://bdana\(ssbmultiservices.com/](https://bdana(ssbmultiservices.com/)

Paths without secure XFO header:

- <https://bdana.ssbumultiservices.com/>
- <https://bdana.ssbumultiservices.com/membership/login>
- <https://bdana.ssbumultiservices.com/about-us>
- <https://bdana.ssbumultiservices.com/reunion-detailes/constitution-gthntntr>
- <https://bdana.ssbumultiservices.com/advisory-committee>
- <https://bdana.ssbumultiservices.com/application-form>
- <https://bdana.ssbumultiservices.com/award>
- <https://bdana.ssbumultiservices.com/assets/website/fonts/fontawesome/webfonts/>
- <https://bdana.ssbumultiservices.com/upload/about-us-image/>
- <https://bdana.ssbumultiservices.com/css/app.css>
- <https://bdana.ssbumultiservices.com/js/app.js>
- <https://bdana.ssbumultiservices.com/blog>
- <https://bdana.ssbumultiservices.com/constitutions>
- <https://bdana.ssbumultiservices.com/contact-us>
- <https://bdana.ssbumultiservices.com/donate>
- <https://bdana.ssbumultiservices.com/events-news>
- <https://bdana.ssbumultiservices.com/free-member>
- <https://bdana.ssbumultiservices.com/single-news/niuyrk-banglades-presklab-ntun-kmitir-kache-dayitw-hstantr-61c647d1c9685>
- <https://bdana.ssbumultiservices.com/general-member>
- <https://bdana.ssbumultiservices.com/life-member>
- <https://bdana.ssbumultiservices.com/our-missions>

Request

```
GET / HTTP/1.1
Referer: https://bdana.ssbbmultiservices.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: bdana.ssbbmultiservices.com
Connection: Keep-alive
```

Recommendation

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

References

[The X-Frame-Options response header](#)

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

[Clickjacking](#)

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

[OWASP Clickjacking](#)

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

[Frame Buster Buster](#)

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

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://bdana.ssbbmultiservices.com/vendor/>

Request

```
GET /vendor/composer/installer.json HTTP/1.1
Cookie: PHPSESSID=6d40a857c8014cff0f5af1960f14d210; XSRF-
TOKEN=eyJpdiI6InM5UjVDRXQ5WUg0M0g2Wnh6VmtmTkE9PSIsInZhbHVlIjoibGNVV2w3VUlFUWhBcDZhD2greFJLbCtNNHFkSX
poWitZd3pUWkRJTDhpZllYaWtSbk5Ia3htc2hXUXRDbkRzdktFSHk4dGxQbkhRZExGSjhIS0xUQmtXVXZ2M0NXRm9lU2NLZWRBaX
dscFVLbTRjQXl6aU1TVkVNcGVDQ0pCQuclCJtYWMi0iI0NDEzNzU4MTQ5ZGzINDYzMDE3MzU2MmJiMmYwY2E2MzI0MDJkMWY3Yz
FhNTYzMmNmYmE1NzcwZTQ4Mzzh0WE3IiwidGFnIjoiIn0%3D;
bangladesh_dental_association_of_north_america_session=eyJpdiI6IkFyMU1INXV5Tld4aWVwKzBnN2I5MwC9PSIsInZhbHVlIjoiTTThTL3FNSmJKKy90aFFIV0VJRTBqYWhMbEcYzmVrSGorbzE1ZWRZZnhGS3h5UHBIV1VGcjM20WF6Y3Zkc2Z1aVU5b
3Y5azQrZDNRUWFKMm9KNUFibytVaVZWVkrS0luTnlUdWxaQmthZhhKRmtvYjBDQitTbUhCNERTNVc0bzgiLCJtYWMi0iI4MTE0
DMzMTIzMThlOTIzZTlxZDnhZGQ3NzA5ZTljMzA5MzA3NmI1NDRhMzIwZWy3N2Jk0TMzZmIy0WQ5YmY1IiwidGFnIjoiIn0%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: bdana(ssbmultiservices).com
Connection: Keep-alive
```

Recommendation

Restrict access to vendors directory

References

[Composer Basic usage](#)

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

Cookies with missing, inconsistent or contradictory properties

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

Impact

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

List of cookies with missing, inconsistent or contradictory properties:

- <https://bdana.ssbtmultiservices.com/>

Cookie was set with:

Set-Cookie: PHPSESSID=c0f392e546a83e61122cfb5e9e95d0a8; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://bdana.ssbtmultiservices.com/>

Cookie was set with:

Set-Cookie: PHPSESSID=b187fa8759e656a16ab01d7cccd4e5e89; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://bdana.ssbtmultiservices.com/about-us>

Cookie was set with:

Set-Cookie: PHPSESSID=b001100828c4e093ecba92a4705369d2; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://bdana.ssbtmultiservices.com/award>

Cookie was set with:

Set-Cookie: PHPSESSID=f90f02f61bf9fc7932eb28e9bbef982b; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://bdana.ssbtmultiservices.com/blog>

Cookie was set with:

Set-Cookie: PHPSESSID=a7c2e95e7a83d8e7892c56be014aa092; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://bdana.ssbtmultiservices.com/contact-us>

Cookie was set with:

Set-Cookie: PHPSESSID=b0acde8024553b2d72eba49e7bf535e3; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://bdana.ssbtmultiservices.com/contact-us/message>

Cookie was set with:

Set-Cookie: PHPSESSID=a7962c0705b7c8d3b30ea60b44997e3f; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://bdana.ssbtmultiservices.com/events-news>

Cookie was set with:

Set-Cookie: PHPSESSID=77c420d62f652c5201e67b453de26a45; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://bdana.ssbtmultiservices.com/index.php>

Cookie was set with:

Set-Cookie: PHPSESSID=81f6d93afc139d2b10063b9823311c1b; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://bdana.ssbtmultiservices.com/photo-gallery>

Cookie was set with:

Set-Cookie: PHPSESSID=789b37a8cf07f5f27b100e21096568c4; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://bdana.ssbbmultiservices.com/privacy-policy>

Cookie was set with:

```
Set-Cookie: PHPSESSID=4e8dd57eaa70100bf04b456f78deb531; path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://bdana.ssbbmultiservices.com/term-of-service>

Cookie was set with:

```
Set-Cookie: PHPSESSID=4592603ca3207cca9ed9e5e7ffa14168; path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://bdana.ssbbmultiservices.com/video-gallery>

Cookie was set with:

```
Set-Cookie: PHPSESSID=aa9ba2fd4d81aedc5683cb3ac01ed4e3; path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and

sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://bdanassbmultiservices.com/contact-us/>

Cookie was set with:

```
Set-Cookie: PHPSESSID=a974c07f06df9cc549cd010aa1e5ab63; path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://bdanassbmultiservices.com/reunion-detailes/inauguration>

Cookie was set with:

```
Set-Cookie: PHPSESSID=1b0bd4911652c5b54cf3168c383841a9; path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://bdanassbmultiservices.com/index.php/contact-us/message>

Cookie was set with:

```
Set-Cookie: PHPSESSID=d782e9ed7f0ab070a9d8dff373cc6b34; path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://bdana.ssbumultiservices.com/reunion-detailes/constitution-ghtntntr>

Cookie was set with:

Set-Cookie: PHPSESSID=578af00e769dc592e0f4b38f0bec7aa6; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://bdana.ssbumultiservices.com/reunion-detailes/punrmilnee-2017>

Cookie was set with:

Set-Cookie: PHPSESSID=bf5b450109e7107e6fcb858e7bd800cb; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://bdana.ssbumultiservices.com/reunion-detailes/vyes-voice-ovishiek>

Cookie was set with:

Set-Cookie: PHPSESSID=0bbafab75885851d08d72dbdcf7d5961; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://bdana.ssbumultiservices.com/single-news/brnadhz-ayojne-niuyrk-banglades-presklaber-ntun-kmiti-ovishikt-61be2c819eaaa>

Cookie was set with:

Set-Cookie: PHPSESSID=bf5f919850df3598f84c54bc498ba418; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://bdana.ssbtmultiservices.com/single-news/kovid-19-e-kshtigrst-pribarer-majhe-bak-er-khadz-samgree-bitrn-60083c947d971>

Cookie was set with:

Set-Cookie: PHPSESSID=2e83f4642dde56183132c31beaf91566; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

Request

```
GET / HTTP/1.1
Referer: https://bdana.ssbtmultiservices.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: bdana.ssbtmultiservices.com
Connection: Keep-alive
```

Recommendation

Ensure that the cookies configuration complies with the applicable standards.

References

[MDN | Set-Cookie](#)

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

[Securing cookies with cookie prefixes](#)

<https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/>

[Cookies: HTTP State Management Mechanism](#)

<https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05>

[SameSite Updates - The Chromium Projects](#)

<https://www.chromium.org/updates/same-site>

[draft-west-first-party-cookies-07: Same-site Cookies](#)

<https://tools.ietf.org/html/draft-west-first-party-cookies-07>

Cookies without 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://bdana.ssbbmultiservices.com/>

Verified

Cookies without HttpOnly flag set:

- <https://bdana.ssbbmultiservices.com/>

Set-Cookie: PHPSESSID=c0f392e546a83e61122cfb5e9e95d0a8; path=/

- <https://bdana.ssbbmultiservices.com/>

Set-Cookie: XSRF-TOKEN=eyJpdiI6Iml6TWZLak5nSnFGd2p1b2t2S1hPN1E9PSIsInZhbHVlIjoiSE42dDBaQ2pRQ3QxMDB4ZHlcnlVRmpoZ0RTN1duZVpnTDZZVW8vRDJ0VUhqamNaQUZ00S9VUGkyc2xmamZlTHlt0EtyY0JZV2owVzFGWldjSXA3WnVkJXpuUDRGmzRuQVhXNElpUHdHTmNxT0Q4WTFVSStMZEYwNGhCajVNeisiLCJtYWMi0iJkZjM5MDY3YTQyNTZiYWUyZTE50DA4YmRkODVkmWM4MDg00TQ0ZWM30TJkNmMwNmE3ZTNlYmFmOTkx0WYwYzM2IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:27:30 GMT; Max-Age=7200; path=/; samesite=lax

- <https://bdana.ssbsmultiservices.com/membership/login>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IkowRnAvWkFGVWZNN2NUZmxNaDNPaFE9PSIsInZhbHVlIjoicXh0QTFScUU2R1JLdmFsZmcvb2hvLzM2T1RVUHpGNi93Sn1QMzZlWHhhaEpj0Hh20FIwTDI4U3pGemYzTHRvUmFnVzNyaGF0V1UzSHgzMDFjT3FTTitUR2lSRUh1UTJFdmcM3liREp6Y0wxVDAxpXplTHQ5MmJHREFzKzJTQUkiLCJtYWMi0iI2ZmJiZjUwYTkzZmJmJAxYTc5Y2RLMDM2MzgxMDRmODZmMzJkNGQ2NGU5NmY10TZLYWM0YWQ3ZjMwMW E2MGRmIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:30:32 GMT; Max-Age=7200; path=/; samesite=lax

- <https://bdana.ssbsmultiservices.com/about-us>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6ImtJUTNSSXdZODNyaHJkdndYMllnWUE9PSIsInZhbHVlIjoivGsyYXVHRDBDYXVDL3VVa0kwK2FWQ1BRNWZZQzZuQm12c2N6MXRQMFJMYVhUbm9lt1RVaXhGeTh1ZkxvZ2sxZklqRjhxaEFpYUhJcUU4NndVYjNzbnh0amJjcFVFa21IVWtaZmxYV1dpQ3hjaDVlnkFWV2ovK0pqeGdzRGFlSU0iLCJtYWMi0iJiMDFmNTg5ZWVmZjA1MTk5ZmU4MzE4ZTJhZDc30DAyNDdjNmQ0YTM1MjNjMTY10DBiMzkzNzBmODljMjdiYmE4IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:30:34 GMT; Max-Age=7200; path=/; samesite=lax

- <https://bdana.ssbsmultiservices.com/reunion-detailes/constitution-gthntnr>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IndFZEZua3ZGYXZzK2FQRlhoSkIxUXc9PSIsInZhbHVlIjoizW9CdHR0aFQvYW5tU21peHB1QklWNk9hMG5aTDdST29lwWhodGFrYUxJMVF5bHBGS2ZRTGZUTEVBU1NDc2Y3bXU2aFBpS1NsZzYycw5td1psdUU3WGs1Vz1TY2NLN01iRGJoNlArRGx4ZUk40WJxcE52VDFRa0Js0VFnM3RrK0YiLCJtYWMi0iJhMThhM2ViNmY1MzJmMjExYWY4N2M40GUzNTA2ZTk3NTEyYzZhMDAxNzIyZTUzNGZiZjE5MTgzMWEx0TMxNmNiIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:30:43 GMT; Max-Age=7200; path=/; samesite=lax

- <https://bdana.ssbsmultiservices.com/advisory-committee>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6InphZmx5R0lGczg1bmc5cW15cjRraFE9PSIsInZhbHVlIjoic1JWenMxYjFGUE1wcnBaZE9KK2lFajBudUVHNld0S2pvQVlkchVCcndPM2crZnNHQ2JiY0VNbFUxRzBRTW130VorZHhzYzg4NW96eGx6MzlBaXj2VTfJeXJmQjUxZ1RoRlRGdlJaNzBNZEZ2akhJVXJdcXhSZ25La094a3lSWHEiLCJtYWMi0iI0YmEyMGQ5NmRkMjI4NTc4MjhmnjRhZDliNDJlYjYyYmM1YzNlNTAzYTQyM2Y3NTFjOWYzNTBmNDhhZTQ5M2I4IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:30:47 GMT; Max-Age=7200; path=/; samesite=lax

- [https://bdana\(ssbmultiservices.com/application-from](https://bdana(ssbmultiservices.com/application-from)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IlhmZHNlK2VSMTg0RDR6Q1RQNWRN0FE9PSIsInZhbHVlIjoiTDLKalVEa1FRdXJRRncwKzVhYjBacXd6MVZ0Mm9Gam1wVEFkeW4rVC9TeXY4T1BUTTJ1WEN0ajJwenBWQzRRYjZBUExwZnczK0p4ZC9TNk5hQll0cnBjVmLUUpUTTRaY0x3SEtXR1N5cWRCSFaYzUyTzhZcE1VeDJIVncrL0giLCJtYWMi0iI2ZjNhMTAyZTY2YmU2NTc50TY2YTFmYzAxZjVLZDdiNmNmNzIzM2ZmYTgz0WQ1Yzg4ZWIZmM4NTJkNzY3M2FkIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:30:48 GMT; Max-Age=7200; path=/; samesite=lax

- [https://bdana\(ssbmultiservices.com/award](https://bdana(ssbmultiservices.com/award)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6ImJzTlJNZEVBQU81NnNjMnNHbHVPR1E9PSIsInZhbHVlIjoiaVU4VDVTMVcxY295V1cydW1tQkV3Q3I4aXFubFU30W1LTDR1QWo5eGpPcXRHUBpRGJFRXA0WjNYbmtWRWxsVENMNXFZRkVxNkpnQU5uUWxBSk04bnlpb0NrNFFqS2VpaENwYjZpbS9rdWl5cmM0VXdMc0RaUm8zUU5nSVRlc2wiLCJtYWMi0iI5NTE1Nzk1MWM50DU4NTllMTcx0DQyMTc3MGNlNjhMGZhMzliMGQwZmI4ZTY1MjI0ZTU3MTgxY2M2MDZlY2JlIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:30:48 GMT; Max-Age=7200; path=/; samesite=lax

- [https://bdana\(ssbmultiservices.com/blog](https://bdana(ssbmultiservices.com/blog)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6Ik9oYnErNkdLNlp0RHZ0SWcrekLSVnc9PSIsInZhbHVlIjoivmFYTxPTFVtKzNSaXR2ck81YVhPUlY3am1yaGFQd3BsSVZ0dSt5RVBkSmVQSnYzanM5TGYxQXd0T0RNSWRoVks1TlVNKy9wdm8vUw5TME9xU0s2dHNlbHV6dENEMkl0RkFIYUw0akhNSWVNWGZSSlJyMEZucEE3Y2FXTVpVZjUiLCJtYWMi0iI1ZGYxMGJlMzhLYzkxMmFiN2FkMjQwMThjMTlhZDQ2MmE5NTFkMDk4MmFlZjE4NTg4NmM5MzJhM2UzMWQ4M2UxIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:37:33 GMT; Max-Age=7200; path=/; samesite=lax

- [https://bdana\(ssbmultiservices.com/constitutions](https://bdana(ssbmultiservices.com/constitutions)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IjhSbzY3TTlEZFNlYUthT0gzZGFzcWc9PSIsInZhbHVlIjoic1M1RXh1a3hmZnM4NEdoLzIzS0hhU2NUVWIxR3RsaklsbFFmM1RLLeFpGdnhXZlZLb0QxZ2xVVU1zdmwvVlJaei9aMjR6TjB3TVY0ME9QQUNkVGU5MVYwckdEQjdmZVkJ3ejJFeVhocVVrQzIxTmcvNzh4Z3JqWURQVE8wb1J0M0wiLCJtYWMi0iIwNjExM2FhYTc0Yzc1MTE0NWIXY2YzZDYzYmIxYTc5MDMzMjExNzJjMmVlMWM1NmUyNDgx0DRmZjNmNGIzZjI4IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:37:34 GMT; Max-Age=7200; path=/; samesite=lax

- [https://bdana\(ssbmultiservices.com/application-message-send](https://bdana(ssbmultiservices.com/application-message-send)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IlBwa0dQOXlpWTg5NFZRZ09uN1VXSHc9PSIsInZhbHVlIjoiRWhMcEhr0GRXS3llUKF1YWMrdEdMaEJqTk9HWVRDb0lLSDAxVHhWc1JY0UhqL2EzY0RzZkJ2S00xTGdycGsrMkF1aDFaQnBrQuh2UFJ1R3BPcFlHZzY5ZWJidGk1VS9zNDVhY0pMeS9BZ3RTYzJJWFqMG5PMkF0MVNZcjRYS1MiLCJtYWMi0iJkMDY5MDA0ZTBjYzA3YzA4ZWI0NDZjN2Rj0TMyZjA2NjRiZjA50DM1NzZlMmI3YjMzYjNiYjAzMDExMTljYzQ4IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:37:40 GMT; Max-Age=7200; path=/; samesite=lax

- [https://bdana\(ssbmultiservices.com/contact-us](https://bdana(ssbmultiservices.com/contact-us)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IldkYlBBMGJZN2lPZ01lRXhsQkxl0UE9PSIsInZhbHVlIjoiOXY4WFR0L1xdytQL1kwSTgxUjRmb1dJU2o5cHJIRUZJeUYwZi8wNzBCVmpMajRizzkrVzRsK2R4ak95TGZQN3JFMDhnUFE3cFZqNUJyL3V60DJvc0RGSkJMdklnNVpEQWEwQ09KblgzTTJJazF4QTI4dk00T1FZVWoySDRTeUMiLCJtYWMi0iJmZWQ0MTBjZTA2M2JlNjQ1MDhhMzQ0MmU0YzJkZjQ2ZWIzzjI1MzRiMDU1MTUwNjYzNzc4ZmFiYzY4NzllMmRlIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:37:41 GMT; Max-Age=7200; path=/; samesite=lax

- [https://bdana\(ssbmultiservices.com/contact-us/message](https://bdana(ssbmultiservices.com/contact-us/message)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6ImppeWZuQzZYTmZVNmtYWmNzMhhNMVE9PSIsInZhbHVlIjoiibEZBV05NuM5lZEg3UXdEbFR2YzdPTGVHTWJBRFlIQ2pMc0lhMG1ld1lFMGRL0DhQbEE3bmNDWCthWC83SThds9tTnhNMXJjMWdRTjRUdlJSZ1BDbEtFRnZzd2xz0FJUK0hRN2tvZDFaNmQvaGZ4YzFxYk8rWHVlMWVldHF5QXQiLCJtYWMi0iI5YmZiYjEzODFm0WUwNGVkNDVi0DRlNTA4NzI5ZjBiNDM2MzY1ZThlMGY3MGY20TkwoGFiMTZmYmVjZmMyN2RjIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:39:24 GMT; Max-Age=7200; path=/; samesite=lax

- [https://bdana\(ssbmultiservices.com/donate](https://bdana(ssbmultiservices.com/donate)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IjlickhnZ0M1dEtCOENFOVFoN2tKZUE9PSIsInZhbHVlIjoiYzdFb3lMcEh1SWVZcnJncmUrNFMrMm8xdzNQSGRm0HoxR2pFUHpEckdXbFlGTy9mTEFlRVI0YlBVK09EYVFYRTVBVzdMb0ZQc2JZSStLR2xMeks4Q1B0YlRlVG1Cbkowb1p1NTFGQ2ZzY01SVDN6enBwSE9yYTltZXJIRDh3USsiLCJtYWMi0iJhNTkwZTkxMWIwMDU1NTU0ZDg5NjQzMTkzNmE0ZDBhMTc4NGJh0GI4ZmE0MjZkODcy0TM0Zjc0Y2Ji0TdmZjk2IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:39:25 GMT; Max-Age=7200; path=/; samesite=lax

- <https://bdana.ssbservices.com/events-news>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6InJoanpBdnh4allBTXg1Wm1oQWhkc2c9PSIsInZhbHVlIjoiTmtSMDJCbWhGMnlMbFY5bkxuTFB2M3NrRDZpdytGc1JQL0t4RDNqemxqVLY30G1RY1I1czBKYmNtL0poV0F0ellsNzZGWNRuRmdJZmkzUmZjNVZZNnN3MFI2MkVhMGZzQ21iTkZsb2JFY2pLZXVvcLY5K3R4TTljUGZoQm550FAiLCJtYWMi0iI5MTAwMDfkZjRhMjAyMzE0ZTZm0TjhMDI0MTM1YTQ30ThmMWM3ZTg4MGI2MjNiMjY1Mjh1MmIxZDc3Mjgw0DEyIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:39:25 GMT; Max-Age=7200; path=/; samesite=lax

- <https://bdana.ssbservices.com/free-member>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6Imp0M0IvcFppVWNBSUZudytxeG5kUnc9PSIsInZhbHVlIjoiemw2ellZQ3dRTSs1ZE0wM2xLc3RuaGJkZVN0dXJkYm0xS1hoTmNBcEF5MVZKUUltE9FZG41cUFCTVkzZmV0ahIvcHBPCsyenRK0VZXRErudj1SMWFxVGNuUlgrcnViekVaTFA1Tk5KU0pmd0l3d0h0RTU3MjJSbVBFEkIvbzAiLCJtYWMi0iI5NWZh0WQ0NTEy0DgwMGQx0WEy0DIyNGRi0GE4MDlkMzVmZWQ0NTg3NTM50GM2ZjZjYzQ0ZWE5YzFlNGQzYWRIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:39:25 GMT; Max-Age=7200; path=/; samesite=lax

- <https://bdana.ssbservices.com/single-news/niuyrk-banglades-presklab-ntun-kmitir-kache-dayitw-hstanr-61c647d1c9685>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IjdQSjlEbkyvNTFuM2F0RzdzbzJCTnc9PSIsInZhbHVlIjoiL2VJd3hxbjB1MTd0UFcreVhYK0lMQkNZNnMxSzgzTTReanNJUmR4alR6Qnp5QXR4RmhLTHk4ZlQvVGo1QlFBRHI0NXAzY3VkyWFFa0V0MHJ5ZTMzaHsekJRUGl10Xc4Vkdhl0tWcnJnR000aURaNjdMd0xVemdUR0Z4c253bysiLCJtYWMi0iIyYmU4MDQzMGIzY2I3NjlmNjNiZWI0ZjQ0ZjVkn2Uy0DUwMDhmNTU30GNm0GYxM2JkZDk1MTRl0TMxM2MzYjFiiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:40:56 GMT; Max-Age=7200; path=/; samesite=lax

- <https://bdana.ssbservices.com/general-member>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6Ijlo0TZkQy80TwpmSDlvd2RBTTAzK1E9PSIsInZhbHVlIjoiVWhTV0JuUVB3WmVnZFVXeWR3Q0VmY3JuSVFYMTRqcnp6Q096SjVSTFlHeDFTcnA4RULPaFNISnk4VUZVazJBelhjZzRsMnpEWFhkcuLRUEJJQjNxTmpDVWRi0XhQaGMwVmRsU1VvMDUyckViM0NWTlA2VTBGcDNUUzRIUzBEEd24iLCJtYWMi0iI3MTlhZjgzNzA0MjA2ZjNlZjYxMDJmZjljNDViYjdMmM2ZTzmMjQyN2JmNjRhMDViYTI3NjAz0DgzYWQx0GNmIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:41:31 GMT; Max-Age=7200; path=/; samesite=lax

- <https://bdana.ssbbmultiservices.com/life-member>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6ImNYaDRhcDczSlQvRG1MYmpYMLB2NlE9PSIsInZhbHVlIjoiQTRXK2tNOVRKcmVIWUNDTy9GdlFTTlgxamsvNGZDdkFyenpUSENnSDJZVUh1d3dQcVFrU0h2NTZxRwdUVERaWndGakE5UjZhVw1haXNpRGhidndMRjVQeTNPb1hzelgzeEJialhmMFpNZE42ZnYzQ3VSjFtUlRLdmxxZDFQeVgiLCJtYWMi0iIzYmE0MjE5ZjQ2MDdhYzE30TYyZmU20DI10GVlZDk50GZlZmFhNWUxZmE1MWJiMzFhYjQ5ZmFlNjczOWI30DgyIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:41:32 GMT; Max-Age=7200; path=/; samesite=lax

- <https://bdana.ssbbmultiservices.com/our-missions>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IkFvchZDRkVuUm82aTZPT1JNMFpVdWc9PSIsInZhbHVlIjoicnhWdVlWbzlSTGlpbUdScHRNT3NzaE1VV1liNkIyREhCL2d6aDBoN0tZV096QnJ2Q0dEdzM4Zkl3NkJll3l3V0UzbjY5MVhvRENsbw1zY1o1TFZ0bzV1R1o4Q3Q1VXdvK2htNm9HY2Y1ayti0VVzMnpqYWtqQnJFRFlzdGpiTzAiLCJtYWMi0iJkYTgxZGEzNGU2MTk40WY10GQ2YmY1MTlkYjAzYmFiYmYwYjNjMWFhMGViY2ZmNmU5YTAzNzBm0DYzZGY20TBjIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:41:35 GMT; Max-Age=7200; path=/; samesite=lax

- <https://bdana.ssbbmultiservices.com/our-vissions>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IkpqM2pQTUDCR0JHbkFaVGNRK1JnVWc9PSIsInZhbHVlIjoiMHVCTWpFT08zU3Vqb2ZDQVBGEtNb2ZFTjdTVXUxbHZDT2pFSE5JdXhhYTFhSWZZVVRFcU02Z0o3NDM5RnNzTFVXMkdPY3FtR25wM1ZTbTQ0UK1sWCtOcjZQcUZjaXc5Qk9wSUwwaUxNTFdCSlBRWGRZNjUzczFnZG43cFlpSmMiLCJtYWMi0iJmZjEzMzliZGRhYWFMDFiZjI2ZGY5MWE3YTgyMWRlMDIxNTYyMTNlNDM1YWI5OTI1MGM5NWIwN2QzNTA50DU0IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:41:35 GMT; Max-Age=7200; path=/; samesite=lax

Request

GET / HTTP/1.1
 Referer: <https://bdana.ssbbmultiservices.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: bdana.ssbbmultiservices.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://bdana.ssbumultiservices.com/>

Verified

Cookies without Secure flag set:

- <https://bdana.ssbumultiservices.com/>

Set-Cookie: PHPSESSID=c0f392e546a83e61122cfb5e9e95d0a8; path=/

- <https://bdana.ssbumultiservices.com/>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6Iml6TWZLak5nSnFGd2p1b2t2S1hPN1E9PSIsInZhbHVlIjoISE42dBaQ2pRQ3QxMDB4ZHhlcnlVRmpoZ0RTN1duZVpnTDZZW8vRDJ0VUhqamNaQUZ00S9VUGkyc2xmamZlTHlt0EtyY0JZV2owVzFGWldjSXA3WnVkvXpuUDRGmzRuQVhXNElpUHdHTmNxT0Q4WTFVSStMZEYwNGhCajVNeisiLCJtYWMi0iJkZjM5MDY3YTQyNTZiYWUyZTE50DA4YmRk0DVkMWM4MDg00TQ0ZWM30TjkNmMwNmE3ZTNlYmFm0Tkx0WYwYzM2IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:27:30 GMT; Max-Age=7200; path=/; samesite=lax

- <https://bdana.ssbumultiservices.com/>

Set-Cookie:

bangladesh_dental_association_of_north_america_session=eyJpdiI6InlWb3JWN0M3QndDTVYzTldJWTNn0Hc9PSIsInZhbHVlIjoibjNrRXNmZ043eDvxNTJ1YjJPWDNocGU1WWYwd2Vvb2JoZWpDSmZ0eE8vVEhLTGxDK3VKUSTmU0d6UmR0d1NCaTNseENNUZLQUdWNWRMd0h0dWUreFdjYUNjMC9oWHQxellr

0XF5K3VIME4zQ TU5RjV1ZDE0N1lteEdHa3BUQ2wiLCJtYWMi0iI4NTA3NzYyM2VkNTE5YzI4MWYzYmM1M
2U1NmRjNjRm0TcwZmVjMjVlNmQ3MDM0Y2EwNDY20DBkM2Qz0DlmMjYzIiwidGFnIjoiIn0%3D;
expires=Tue, 02-Jan-2024 06:27:30 GMT; Max-Age=7200; path=/; httponly;
samesite=lax

- <https://bdana.ssbservices.com/membership/login>

Set-Cookie: XSRF-TOKEN=eyJpdiI6IkowRnAvWkFGVWZNN2NUZmxNaDNPaFE9PSIsInZhbHVlIjoicXh0QTFScUU2R1JLdmFsZmcvb2hvLzM2T1RVUHpGNi93SnLQMzZlWHhhaEpj0Hh20FIwTDI4U3pGemYzTHRvUmFnVzNyaGF0V1UzSHgzMDFjT3FTTitUR2lSRUh1UTJFd mhCM3liREp6Y0wxVDAxbXplTHQ5MmJHREFzKzJTQUkiLCJtYWMi0iI2ZmJiZjUwYTkzZmMjAxYTc5Y2R1MDM2MzgxMDRm0DZmMzJkNGQ2NGU5NmY10TZLYWM0YWQ3ZjMwMW E2MGRmIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:30:32 GMT; Max-Age=7200; path=/; samesite=lax

- <https://bdana.ssbservices.com/membership/login>

Set-Cookie: bangladesh_dental_association_of_north_america_session=eyJpdiI6IjE5QzV2WhhZVUh2Nm5GbDlnTnByYWc9PSIsInZhbHVlIjoitTDNrQ1hoY0xtZ2R30UdsZ1BmKzZ4MjhkM0F0ZFcyV2pnSwg20E9mS21DM1Zyb2w5eTVMZVltRE5JQ2ZzanVYdnRtR0R5bXU5dmpHU05LRnd2b0NvZGRRdktGc2pG0EppUzdMVE9rb01zdHQ3R2RBaTBtR1gvU0JWVlb3SDVBNGIiLCJtYWMi0iIxM2EyMjZmYmY2YTdmNGIzYjVhNDVky2U40DAz0DZiYmI0NWU30TkxBkY2I4ZTAxNjBjYWI0Mzk2MGIzNDI3IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:30:32 GMT; Max-Age=7200; path=/; httponly; samesite=lax

- <https://bdana.ssbservices.com/about-us>

Set-Cookie: XSRF-TOKEN=eyJpdiI6ImtJUTNSSXdZ0DNyaHJkdndYMllnWUE9PSIsInZhbHVlIjoivGsYXVHRDBDYXVDL3VVa0kwK2FWQ1BRNWZZQzZuQm12c2N6MXRQMFJMYVhUb m9lt1RVaXhGeTh1ZkxvZ2sxZklqRjhxaEFpYUhJcUU4NndVYjNzbnh0amJjcFVFa21IVWtaZmxYV1dpQ3hjaDVlnkFWV2ovK0pqeGdzRGflsu0iLCJtYWMi0iJiMDFmNTg5ZWVmZjA1MTk5ZmU4MzE4ZTJhZDc30DAyNDdjNmQ0YTM1MjNjMTY10DBiMzkzNzBm0DljMjdiYmE4IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:30:34 GMT; Max-Age=7200; path=/; samesite=lax

- <https://bdana.ssbservices.com/about-us>

Set-Cookie: bangladesh_dental_association_of_north_america_session=eyJpdiI6Ik9lcG1STmNybEc zdX

pzVU5HZEUwTFE9PSIsInZhbHVlIjoiNU9ZaDlPYmVLZXrVQ015R1BzSnJxd2JJU3RtVzZ5QUNNV2xBM0d
mb1dCS1hoWUhCbTA0Z1F3WG93SlkxMEZDRFlDdmNZd0kxV0xUenZzK3BibFZQc3Y5Y1BXeGwwSUza0tp
WGxMbFl3MVhBMnV4SGhIN2FVNXhreGliNTFySW8iLCJtYWMi0iJm0DVjZWZhMjRlNzkzNTIwZTU50DZhY
mY0NGUzYjhM2ZiZWZhZDhmMDkxYTYYjI3Mjk0Mzk4MTdlNjQ1MzRkIiwidGFnIjoiIn0%3D;
expires=Tue, 02-Jan-2024 06:30:34 GMT; Max-Age=7200; path=/; httponly;
samesite=lax

- <https://bdana.ssbumultiservices.com/reunion-detailes/constitution-gthntntr>

Set-Cookie: XSRF-TOKEN=eyJpdiI6IndFZEZua3ZGYXZzK2FQRlhoSkIxUXc9PSIsInZhbHVlIjoiZW9CdHR0aFQvYW5tU21peHB1QklWNk9hMG5aTDdST29lWWhodGFrYUxJMVF5bHBGS2ZRTGZUTEVBU1NDc2Y3bXU2aFBpS1NsZzYycw5td1psdUU3WGs1VzlTY2NLN01iRGJoNlArRGx4ZUk40WJxcE52VDFRa0Js0VFnM3RrK0YiLCJtYWMi0iJhMThhM2ViNmY1MzMjMjExYWY4N2M40GUzNTA2ZTk3NTEyYzZhMDAxNzIyZTUzNGZiZjE5MTgzMWEx0TMxNmNiIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:30:43 GMT; Max-Age=7200; path=/; samesite=lax

- <https://bdana.ssbumultiservices.com/reunion-detailes/constitution-gthntntr>

Set-Cookie: bangladesh_dental_association_of_north_america_session=eyJpdiI6InFTdUVGN1FPYUx4Vk02c09GSDFtVXc9PSIsInZhbHVlIjoiZlNhVw9qby9sYlpkWGRyNDMwWGTDbG5PZjFLVTJRa0RwcUF2Vjh0RTZWZkpSSmpvc0l2ZkYzaEYx0U1ERnNzK3hvbE9aQjNNajJGTUJlTWxjWUhIQUg2UEpNTnBYTmZHzzhnU3NBT1pSS1ZTYWorak9hSlBvWG9aSlNYazzTcVYiLCJtYWMi0iJlNWQwMDc4YmZlMGZLYTViZTRj0GJhNmY3MWVlZDg3NzM4ZmUxMjdjYTU2NDliZDZjMGNjY2FkZTY5N2iZDViiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:30:43 GMT; Max-Age=7200; path=/; httponly; samesite=lax

- <https://bdana.ssbumultiservices.com/advisory-committee>

Set-Cookie: XSRF-TOKEN=eyJpdiI6InphZmx5R0lGczg1bmc5cW15cjRraFE9PSIsInZhbHVlIjoiclJWenMxYjFGUE1wcnBaZE9KK2lFajBudUVHNwd0S2pvQVlkchVCndPM2crZnNHQ2JiY0VNbFUxRzBRTW130VorZHzYzg4NW96eGx6MzlBaXJ2VTFJeXJmQjUxZ1RoR1RGdlJaNzBNZEZ2akhJVXJDcXhSZ25La094a3lSWHEiLCJtYWMi0iI0YmEyMGQ5NmRkMjI4NTc4MjhMnjRhZDliNDJlYjYyYmM1YzNlNTAzYTQyM2Y3NTFj0WYzNTBmNDhhZTQ5M2I4IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:30:47 GMT; Max-Age=7200; path=/; samesite=lax

- <https://bdana.ssbumultiservices.com/advisory-committee>

Set-Cookie:

bangladesh_dental_association_of_north_america_session=eyJpdiI6Ik1PYjc2T2NkSGlCNi9wTy9RSTV4QUE9PSIsInZhbHVlIjoi0UROZjBF0EhmbnVuSmxz0TVTSWxvT1FBbFhzK202aEVNNy9nREcwWHNmNzh20HovSjRCeWRmS01KTGgvY09EdEtXcTVWSkV6S1Rva1ZHFl4QXVUcTNXKzhHeFFod0IvWW1vV3VCdWM2cFVV0EFZQ3k5SFRxcEJxbEpGV0FVUjUiLCJtYWMi0iI2N2Y0YmZlMDhhNjFmMTQ4YjExNjdiNWQ3YTQ0ZTcw0WEyM2ZiMGY0NzMxZWIzMzJj0WM1YTZhNGVkJzJhZTMyIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:30:47 GMT; Max-Age=7200; path=/; httponly; samesite=lax

- <https://bdana.ssbtmultiservices.com/application-from>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IlhmZHNlK2VSMTg0RDR6QlRQNWRN0FE9PSIsInZhbHVlIjoiTDlKalVEa1FRdXJRRncwKzVhYjBacXd6MVZ0Mm9Gam1wVEFkeW4rVC9TeXY4TlBUTTJ1WEN0ajJwenBWQzRRYjZBUExwZnczK0p4ZC9TNk5hQll0cnBjVmLU0UpUTTRaY0x3SEtXR1N5cWRCSEFaYzUyTzhZcE1VeDJIVncrL0giLCJtYWMi0iI2ZjNhMTAyZTY2YmU2NTc50TY2YTFmYzAxZjVlZDdiNmNmNzIzM2ZmYTgz0WQ1Yzg4ZWIZMmY4NTJkNzY3M2FkIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:30:48 GMT; Max-Age=7200; path=/; samesite=lax

- <https://bdana.ssbtmultiservices.com/application-from>

Set-Cookie:

bangladesh_dental_association_of_north_america_session=eyJpdiI6IjB3NFRNbFhYVWxDVzRNWU1RM1V5WHc9PSIsInZhbHVlIjoiCKNYR3JWeVB2akRseGFjYmJMUKk0T3VJ0GJFRzUyV09CaWlndVhmRpGWURaU0dNWtDjQ011WGU4emNzWmNXWmll3pLQ25RZ1lMSkxmTGx3T0NscXFkVFA2UUdwbXM3ViuZ1FkRFRYMUUpzQVAx0HQyUU9wRnhHZUJwdmg3eXgiLCJtYWMi0iI10GIzYzk4MDY1Y2VmY2E0M2JlNTNjZGRhOGNlYmViZGY3NTM1MWQyNDIxZThmMDQ1NzVjNjE40DkyYzA4Y2E1IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:30:48 GMT; Max-Age=7200; path=/; httponly; samesite=lax

- <https://bdana.ssbtmultiservices.com/membership/login>

Set-Cookie:

bangladesh_dental_association_of_north_america_session=eyJpdiI6Im5zeGNvWVBQM1B6N0IzZFB6cmZStLE9PSIsInZhbHVlIjoiUjJCaytXczhLTGV0R25jQ3Y0ZS9LdFhncjBpQWtwcmx4eWxPRlY1ZTAvMmVZUkhVa1JJQQUlkajZPbzhCbjhybWlmYVNvdGxya2pCK3JESStXMF15NVZPNmRDTnNiV2FMSzla d0x0MW5qcW5qMW5mZ1AyNhl0dFVrZVERb2tCd2ciLCJtYWMi0iJj0GRmZTYxY2I0N2E0YTgzNzAxZDdhY2YyZmM2M2Uw0WUwMjMyYjQ0MmJmMDcwZwVhNTRmZWE5YzUzZTk30TY0IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:30:52 GMT; Max-Age=7200; path=/; httponly; samesite=lax

- <https://bdana.ssbtmultiservices.com/membership/login>

Set-Cookie:

bangladesh_dental_association_of_north_america_session=eyJpdiI6InFPYUVDeUlZVmdlNS
tDRFFNZGFMZWc9PSIsInZhHVlIjoiVTBaeTU2U05wcXJpNGpxRkI3bjJnbVRc1lqb2pud3B0TFhsaHV
uQzJhWXFubHl2bjR2bGp3b2ZBdHBnbkFNQmtvc1dYdVBxYThkbkdqS25tblRHdm1mY0szdytyLzhEVUox
RTZMek80c2cxVllYanNJvNE0UktUOUxkZG1DaUkiLCJtYWMi0iJhMWQ2MjM3MTczYjcyYWNhNTZiNzUyZ
WJiZmFhMzU1MDhiNGVhMzk5NTAwNDIzzjcxYzkwMGNiZGI5ZGI00GQ5IiwidGFnIjoiIn0%3D;
expires=Tue, 02-Jan-2024 06:30:52 GMT; Max-Age=7200; path=/; httponly;
samesite=lax

- <https://bdana.ssbtmultiservices.com/award>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6ImJzTlJNZEVBQU81NnNjMnNHbHVPR1E9PSIsInZhHVlIjoiaVU4VDVTMVcxY295V1c
ydW1tQkV3Q3I4aXFubFU30W1LTDRlQWo5eGpPcXRHUDpRGJFRXA0WjNYbmtWRWxsVENMNxFZRkVxNkpn
QU5uUWxBSk04bnlpb0NrNFFqS2VpaENwYjZpbS9rdWl5cmM0VXdMc0RaUm8zUU5nSVRlc2wiLCJtYWMi0
iI5NTE1Nzk1MWM50DU4NTllMTcx0DQyMTc3MGNlNjhMGZhMzliMGQwZmI4ZTY1MjI0ZTU3MTgxY2M2MD
ZLY2JlIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:30:48 GMT; Max-Age=7200;
path=/; samesite=lax

- <https://bdana.ssbtmultiservices.com/award>

Set-Cookie:

bangladesh_dental_association_of_north_america_session=eyJpdiI6ImExak05Uzh0aVh5Tz
JTVmE3eVpCZUE9PSIsInZhHVlIjoidEZrMkd0QmFSMThKeHBYK2Nt0HpGRjd1UFNteTh2aXpkBXBmdTI
yVmF0QUtpaE41YjRiUW1KNC8yZE8xanhH0UNKQmtKU1RoVC9TUVFmVWtXU0pFUHZXRkozc0RmVWY1MFdV
Qi95MVNqQ1M0bXJqd2lwQzZjWkljWnUyVlkWUYiLCJtYWMi0iI3MjU1NmJiNDFkZTQxNjc4YjFlZWUyM
TcyZTdiYjkxYmMyZmQyMjhm0DUxMzRkZGQ4MmU0NDY3NDgyMzg3YTBkIiwidGFnIjoiIn0%3D;
expires=Tue, 02-Jan-2024 06:30:48 GMT; Max-Age=7200; path=/; httponly;
samesite=lax

- <https://bdana.ssbtmultiservices.com/application-message-send>

Set-Cookie:

bangladesh_dental_association_of_north_america_session=eyJpdiI6Ik56Q0VlSkF6c1Vpa2
1QRHBlyU90MVE9PSIsInZhHVlIjoiWEdoSFVMbWdqU2R3MG94Rm1vUwNPY3g4dEMxNkdSZ2owSldQdXg
wRkNRWG1KdlgyUjNidld5dnNLeXFxrzJVQ2Zj0VFJUkZaaUYyNHVRSFJZY3Z4YwlITkUrdU9vcytCcGld
NURibEZFNmdpNDNSYTvnZDlTRmhQMuxWclZBM28iLCJtYWMi0iIzMTBkMzY4NTA40WQ3YjY3YTg4MmM2Z
WQ20WQxNDNkNWY5MjU40TVmYzIwNTIxMmU2YjM0ZjVlYzdiYjg4MGVkJiwidGFnIjoiIn0%3D;

expires=Tue, 02-Jan-2024 06:31:49 GMT; Max-Age=7200; path=/; httponly;
samesite=lax

- <https://bdana.ssbbmultiservices.com/application-message-send>

Set-Cookie:

bangladesh_dental_association_of_north_america_session=eyJpdiI6InhNcVFGWG1RQXA0OD
NWL3dPMDdWMFE9PSIsInZhbHVlIjoicEdobjR4Lzlod0Rv0jRsbGRlM2JKRzhrS1Q3Q3hVVzdHbE8vTld
HYiswTUxSKy9KQnNEaVY4cFJaZTRrRFFqUlZQ0XdrVFNYUUhLUFN0MTFGTjNPRVFmdGZYd2piT0JpQytL
VGFlbTBhdFI3b2RKQXg5Ui9hNjM5TWlHN2JDNFIIiLCJtYWMi0iJhNDMz0GVhZTBj0TRLmjhiNjkz0Tc1N
TExYmIx0Tlm0Dg3M2Y5MWI5NGFl0DdmZTdk0GQ1MjcyZmNjYmZlOTdkIiwidGFnIjoiIn0%3D;
expires=Tue, 02-Jan-2024 06:31:49 GMT; Max-Age=7200; path=/; httponly;
samesite=lax

- <https://bdana.ssbbmultiservices.com/application-message-send>

Set-Cookie:

bangladesh_dental_association_of_north_america_session=eyJpdiI6InRnSVFMNG5GK0J0SU
FQaFVmejBmNnc9PSIsInZhbHVlIjoiNmVlbGpaVzlhU2s4UEzoNTd3Vkx0eEhnTVNwZFh5T1FJeExxeWl
0UUUFHQlhNcmthdTd1QXdLeWw2ZURjM0k0bmhqeU00bVhya0pGV1l0NVk4WHVJbEcrMUVLR2NiRkwwcHc4
Yw1xNG94S1lqTFl3LzN2Q0FyWDVCL0VJNnVKL3oiLCJtYWMi0iJkYjk0NWfmZGI30GU4MThiMzhmNjlmM
mEwNTQxZjcwNTI20DNmZjI0MzUwNwU4MzMwNDdj0ThhM2M1MmZkNzZhIiwidGFnIjoiIn0%3D;
expires=Tue, 02-Jan-2024 06:31:49 GMT; Max-Age=7200; path=/; httponly;
samesite=lax

- <https://bdana.ssbbmultiservices.com/application-message-send>

Set-Cookie:

bangladesh_dental_association_of_north_america_session=eyJpdiI6ImVBcG5S0VZIMFJXSX
FHbXhiNTlxQXc9PSIsInZhbHVlIjoiSUNYcUt4cGlSSUFrl1I0K3hJYUVFRzJ4blV4aVJadGdNNUNS1p
RTmh1RFo4azJ1cGlmQ0x3eDlLbWhTVTB2Y3o4Mmo2WGxpYWs4ckNuVStoaFdaew9GazJvekNhMURQeXBn
TTkrRFQrbUhhQWp0clRXc1RZVmozSVVkrDRzS2QiLCJtYWMi0iIx0WY1ZDExNThmZjM1Mjg2MzY2NDgwZ
jU3MmQ2YWVlMjZlYjQ3NjQwNzMyMjJjYWNhZWQwZGU0MTFhMTE2ZTU2IiwidGFnIjoiIn0%3D;
expires=Tue, 02-Jan-2024 06:31:49 GMT; Max-Age=7200; path=/; httponly;
samesite=lax

Request

GET / HTTP/1.1
Referer: <https://bdana.ssbbmultiservices.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: bdana.ssbbmultiservices.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://bdana.ssbbmultiservices.com/>

Documentation files:

- <https://bdana.ssbbmultiservices.com/> **README.md**

File contents (first 100 characters):

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

Request

```
GET /README.md HTTP/1.1
Cookie: PHPSESSID=c0f392e546a83e61122cfb5e9e95d0a8; XSRF-TOKEN=eyJpdiI6Iml6TWZLak5nSnFGd2p1b2t2S1hPN1E9PSISInZhHVlIjoISE42dBaQ2pRQ3QxMDB4ZHhlcnlVRmpoZ0RTN1duZVpnTDZZVW8vRDJ0VUhqamNaQUZ0OS9VUGkyc2xmamZlTHlT0EtyY0JZV2owVzFGWldjSXA3WnVkJkZjM5MDY3YTQyNTZiYWUyZTE50DA4YmRkODVkJkMWM4MDg00TQ0ZWm30TJkNmMwNmE3ZTNlYmFmOTkx0WYwYzM2IiwidGFnIjoiIn0%3D; bangladesh_dental_association_of_north_america_session=eyJpdiI6InlWb3JWN0M3QndDTVYzTldJWTNn0Hc9PSISInZhHVlIjoibjNrRXNmZ043eDVxNTJ1YjJPWDNocGU1WWYwd2VVb2JoZwpDSmZ0eE8vVEhLTGxDK3VKUStmU0d6UmR0d1NCaTNseENNNUZLQUdWNRMd0h0dWUreFdjYUNjMC9oWHQxellr0XF5K3VIME4zQ TU5RjV1ZDE0N1lteEdHa3BUQ2wiLCJtYWMi0iI4NTA3NzYyM2VkJNTE5YzI4MWYzYmM1M2U1NmRjNjRm0TcwZmVjMjVlNmQ3MDM0Y2EwNDY20DBkM2Qz0DlmMjYzIiwidGFnIjoiIn0%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: bdana.ssbbmultiservices.com
Connection: Keep-alive

Recommendation

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

HTTP Strict Transport Security (HSTS) not implemented

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

Impact

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

<https://bdana.ssbbmultiservices.com/>

URLs where HSTS is not enabled:

- <https://bdana.ssbbmultiservices.com/>
- <https://bdana.ssbbmultiservices.com/membership/login>
- <https://bdana.ssbbmultiservices.com/about-us>
- <https://bdana.ssbbmultiservices.com/reunion-detailes/constitution-gthntntr>
- <https://bdana.ssbbmultiservices.com/advisory-committee>
- <https://bdana.ssbbmultiservices.com/application-form>
- <https://bdana.ssbbmultiservices.com/award>
- <https://bdana.ssbbmultiservices.com/assets/website/fonts/fontawesome/webfonts/>
- <https://bdana.ssbbmultiservices.com/upload/about-us-image/>
- <https://bdana.ssbbmultiservices.com/css/app.css>
- <https://bdana.ssbbmultiservices.com/js/app.js>
- <https://bdana.ssbbmultiservices.com/blog>
- <https://bdana.ssbbmultiservices.com/constitutions>
- <https://bdana.ssbbmultiservices.com/contact-us>
- <https://bdana.ssbbmultiservices.com/donate>
- <https://bdana.ssbbmultiservices.com/events-news>
- <https://bdana.ssbbmultiservices.com/free-member>

- <https://bdana.ssbumultiservices.com/single-news/niuyrk-banglades-presklab-ntun-kmitir-kache-dayitw-hstantr-61c647d1c9685>
- <https://bdana.ssbumultiservices.com/general-member>
- <https://bdana.ssbumultiservices.com/life-member>
- <https://bdana.ssbumultiservices.com/our-missions>

Request

```
GET / HTTP/1.1
Referer: https://bdana.ssbumultiservices.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: bdana.ssbumultiservices.com
Connection: Keep-alive
```

Recommendation

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

References

hstspreload.org

<https://hstspreload.org/>

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

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

Insecure Inline Frame (iframe)

The web page was found to be using an Inline Frame ("iframe") to embed a resource, such as a different web page. The Inline Frame is either configured insecurely, or not as securely as expected. This vulnerability alert is based on the origin of the embedded resource and the iframe's sandbox attribute, which can be used to apply security restrictions as well as exceptions to these restrictions.

Impact

When a web page uses an insecurely configured iframe to embed another web page, the latter may manipulate the former, and trick its visitors into performing unwanted actions.

<https://bdana.ssbbmultiservices.com/>

Verified

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

Request

```
GET / HTTP/1.1
Referer: https://bdana.ssbbmultiservices.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: bdana.ssbbmultiservices.com
Connection: Keep-alive
```

<https://bdana.ssbbmultiservices.com/contact-us>

Verified

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

Request

```
GET /contact-us HTTP/1.1
Referer: https://bdana.ssbbmultiservices.com/
Cookie: PHPSESSID=c0f392e546a83e61122cfb5e9e95d0a8; XSRF-TOKEN=eyJpdiI6IitqNUMraWY0cTVWOGtocEJLR3lVb1E9PSIsInZhbHVljoIRDhSNU9BRUZFTFNkTjhvWFR2cUVGaUNVbmtxaFR5TGNXVlxTmZDKzU20HQ0M0t0eVVtSmrnUnZFRXhTN2xjUTc4WEJwRWF5NGF3WUtqdERLRkVaSHlwUEJ2anZtRHJsMlp3MWg1ZmMvd9rZktoZnM0bFNVbWtFdFk0STJhT2YiLCJtYWMi0iJlNjdiY2JlY2E1YmY3YjFjOTBiMmQ4ZTQyNWJkZjIyYjMyNjcy0WM2NDzzmE5ZWU3MzNiYmIyZGQyYT5MDUyIiwidGFnIjoiIn0%3D; bangladesh_dental_association_of_north_america_session=eyJpdiI6IkhmNHdUZ2U5SDlCSmJ3VnPczNSQUE9PSIsInZhbHVljoIYUp4M1hPQXRCCZVB4RE1kTTFPBfKxUk5nUE5BNxl0V0xiS0NmM3RUeDJZR2JVVERxVi9qdm1BQXZuMwLDbDRoRngre1lKWDZjMjIvcJhTXFoN1pGV1d0UE1qSjJ6YXhBTTlhQ21yUzhubGtveElpNmhwEwh5TExEWj1MMEpBTXgiLCJtYWMi0iI1N2ExYjcxMzUzN2RmMzM5MWI4ZDczMmZLZjA3MDUwMWQ2YjNhYzA40Dg1MjIwYTizY2RjNTkwNmRlmjVmNzhiIiwidGFnIjoiIn0%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: bdana.ssbbmultiservices.com
Connection: Keep-alive
```

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>

[HTML Standard: iframe](#)

<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>

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://bdana.ssbtmultiservices.com/>

Possible sensitive directories:

- <https://bdana.ssbtmultiservices.com/upload>
- <https://bdana.ssbtmultiservices.com/database>
- <https://bdana.ssbtmultiservices.com/config>
- <https://bdana.ssbtmultiservices.com/tests>

Request

```
GET /upload/ HTTP/1.1
Cookie: PHPSESSID=c0f392e546a83e61122cfb5e9e95d0a8; XSRF-
TOKEN=eyJpdiI6Iml6TWzLak5nSnFGd2p1b2t2S1hPN1E9PSIsInZhbHVlIjoiSE42dBaQ2pRQ3QxMDB4ZHhlcnlVRmpoZ0RTN1
duZVpnTDZZVw8vRDJ0VUhqamNaQUZ00S9VUGkyc2xmamZlTHlt0EtyY0JZV2owVzFGWldjSXA3WnVkvXpuUDRGmzRuQvhXNElpUH
dHTmNxT0Q4WTFVSStMZEYwNGhCajVNNeisiLCJtYWMi0iJkZjM5MDY3YTQyNTZiYWUyZTE50DA4YmRk0DVkMWM4MDg00TQ0ZWM30
JkNmMwNmE3ZTNlYmFm0Tkx0WYwYzM2IiwidGFnIjoiIn0%3D;
bangladesh_dental_association_of_north_america_session=eyJpdiI6Inlw3JWN0M3QndDTVyzTldJWTNn0Hc9PSIsI
nZhbHVlIjoibjNrRXNmZ043eDVxNTJ1YjJPWDNocGU1WWYwd2VVb2JoZWpDSmZ0eE8vVEhLTGxDK3VKUSTmU0d6UmR0d1NCaTNse
ENNNUZLQUDWNWRMd0h0dWUreFdjYUNjMC9oWHQxellr0XF5K3VIME4zQTU5RjV1ZDE0N1lteEdHa3BUQ2wiLCJtYWMi0iI4NTA3N
zYyM2VkJNTE5YzI4MWYzYmM1M2U1NmRjNjRmOTcwZmVjMjVlNmQ3MDM0Y2EwNDY20DBkM2Qz0DlmMjYzIiwidGFnIjoiIn0%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: bdana.ssbtmultiservices.com
```

Recommendation

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

References

[Web Server Security and Database Server Security](#)

<https://www.acunetix.com/websitetesecurity/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://bdana.ssbtmultiservices.com/>

Possible sensitive files:

- <https://bdana.ssbtmultiservices.com/web.config>

Request

```
GET /web.config HTTP/1.1
Accept: weufmqsv/gqpj
Cookie: PHPSESSID=c0f392e546a83e61122cfb5e9e95d0a8; XSRF-TOKEN=eyJpdiI6ImL6TwZLak5nSnFGd2p1b2t2S1hPN1E9PSIsInZhbHVlIjoISE42dBaQ2pRQ3QxMDB4ZHhlcnlVRmpoZ0RTN1duZVpnTDZZVw8vRDJ0VUhqamNaQUZ00S9VUGkyc2xmamZlTHlt0EtY0JZV2owVzFGWldjSXA3WnVkJXpuUDRGMzRuQVhXNElpUHdHTmNxT0Q4WTFVSttMZEYwNGhCajVNeisiLCJtYWMi0iJkZjM5MDY3YTQyNTZiYWUyZTE50DA4YmRk0DVkMWM4MDg00TQ0ZWM30TJkNmMwNmE3ZTNlYmFm0Tkx0WYwYzM2IiwidGFnIjoiIn0%3D;
bangladesh_dental_association_of_north_america_session=eyJpdiI6Inlw3JWN0M3QndDTVYzTldJwTNn0Hc9PSIsInZhbHVlIjoibjNrRXNmZ043eDVxNTJ1YjJPWDNocGU1WWYwd2VVb2JoZWpDSmZ0eE8vVEhLTGxDK3VKUSTmU0d6UmR0d1NCaTNseENNNuZLQudwNWRMd0h0dWUreFdjYUNjMC9oWHQxellr0XF5K3VIME4zQTU5RjV1ZDE0N1lteEdHa3BUQ2wiLCJtYWMi0iI4NTA3NzYyM2VkJNTE5YzI4MWYzYmM1M2U1NmRjNjRm0TcwZmVjMjVlNmQ3MDM0Y2EwNDY20DBkM2Qz0DlmMjYzIiwidGFnIjoiIn0%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: bdana.ssbbmultiservices.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/websitetecurity/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 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://bdana.ssbbmultiservices.com/**](https://bdana.ssbbmultiservices.com/)

Paths without CSP header:

- <https://bdana.ssbumultiservices.com/>
- <https://bdana.ssbumultiservices.com/membership/login>
- <https://bdana.ssbumultiservices.com/about-us>
- <https://bdana.ssbumultiservices.com/reunion-detailes/constitution-gthntntr>
- <https://bdana.ssbumultiservices.com/advisory-committee>
- <https://bdana.ssbumultiservices.com/application-form>
- <https://bdana.ssbumultiservices.com/award>
- <https://bdana.ssbumultiservices.com/assets/website/fonts/fontawesome/webfonts/>
- <https://bdana.ssbumultiservices.com/upload/about-us-image/>
- <https://bdana.ssbumultiservices.com/css/app.css>
- <https://bdana.ssbumultiservices.com/js/app.js>
- <https://bdana.ssbumultiservices.com/blog>
- <https://bdana.ssbumultiservices.com/constitutions>
- <https://bdana.ssbumultiservices.com/contact-us>
- <https://bdana.ssbumultiservices.com/donate>
- <https://bdana.ssbumultiservices.com/events-news>
- <https://bdana.ssbumultiservices.com/free-member>
- <https://bdana.ssbumultiservices.com/single-news/niuyrk-banglades-presklab-ntun-kmitir-kache-dayitw-hstantr-61c647d1c9685>
- <https://bdana.ssbumultiservices.com/general-member>
- <https://bdana.ssbumultiservices.com/life-member>
- <https://bdana.ssbumultiservices.com/our-missions>

Request

```
GET / HTTP/1.1
Referer: https://bdana.ssbbmultiservices.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: bdana.ssbbmultiservices.com
Connection: Keep-alive
```

Recommendation

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

References

[Content Security Policy \(CSP\)](#)

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

[Implementing Content Security Policy](#)

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

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://bdana.ssbbmultiservices.com/>

Verified

Pages where the content-type header is not specified:

- <https://bdana.ssbbmultiservices.com/README.md>
- <https://bdana.ssbbmultiservices.com/.env>
- <https://bdana.ssbbmultiservices.com/composer.lock>
- <https://bdana.ssbbmultiservices.com/docker-compose.yml>
- <https://bdana.ssbbmultiservices.com/web.config>
- https://bdana.ssbbmultiservices.com/resources/sass/_variables.scss

- <https://bdana.ssbtmultiservices.com/resources/sass/app.scss>

Request

```
GET /README.md HTTP/1.1
Referer: https://bdana.ssbtmultiservices.com/
Cookie: PHPSESSID=6d40a857c8014cff0f5af1960f14d210; XSRF-TOKEN=eyJpdiI6ImNnV1F5T3JoS3BaQ1Z0YVWMT3JKUUE9PSIsInZhbHVljoizWNZvKRuekd4bkdmRDl60FBWdlhxM1FYbjUrbnpwCegvN1JiYVlSK1Q3N0VBYXpRWXZyRXhqWVh0ZEz2Qjhva2FtejZzZmZ5NW5VVDh3VWtWTrnNTNE5yV1VQ0GNUSG42TjF6R2E3cjNsBzJMdVgyMUNURW1EZ2IzYlJUbzNNK1ciLCJtYWMi0iJjNDgzMzc3ZTA0Njg2Zjh1MmZlYjhjNjI4M2E4MDdkYzk00TU4YmUyMDMxDzbkNjU4MDAzZDU0Y2M50DI4NDEwIiwidGFnIjoiIn0%3D;
bangladesh_dental_association_of_north_america_session=eyJpdiI6ImNhcFB3bEFsZFgvVXA3MFNQaUJZN2c9PSIsInZhbHVljoibXFaSzZiYS9Ya1V2bVBZVXhtT2F6TjkvaEJ40GV3cEpjUEdkeEFhaW1EU1Qyb2JMUHozYk1UUndQaENN0S84cExGtnVDMVhsY0ZDcjhhTmZWVkNpM2JjL1NkalBxdXpuZ1dZRjRMdHhSc0w5Tm5SNTRjUkRFcUdzNXlSa1BFNjciLCJtYWMi0iJi0WVjNWMwMzMyY2IxYmNiMjI30DJjZTNiZjc2MDc0MTQ5NTZiNjFkOTQwNjI0NjczMDVhYzYzNTI2YmI5MzAwIiwidGFnIjoiIn0%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: bdana.ssbtmultiservices.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://bdana.ssbtmultiservices.com/>

Emails found:

- <https://bdana.ssbtmultiservices.com/>
bdana@gmail.com

- <https://bdana.ssbumultiservices.com/about-us>
bdana@gmail.com
- <https://bdana.ssbumultiservices.com/reunion-detailes/constitution-gthntntr>
bdana@gmail.com
- <https://bdana.ssbumultiservices.com/advisory-committee>
bdana@gmail.com
- <https://bdana.ssbumultiservices.com/application-from>
bdana@gmail.com
- <https://bdana.ssbumultiservices.com/award>
bdana@gmail.com
- <https://bdana.ssbumultiservices.com/blog>
bdana@gmail.com
- <https://bdana.ssbumultiservices.com/constitutions>
bdana@gmail.com
- <https://bdana.ssbumultiservices.com/contact-us>
bdana@gmail.com
- <https://bdana.ssbumultiservices.com/donate>
bdana@gmail.com
- <https://bdana.ssbumultiservices.com/events-news>
bdana@gmail.com
- <https://bdana.ssbumultiservices.com/free-member>
bdana@gmail.com
- <https://bdana.ssbumultiservices.com/single-news/niuyrk-banglades-presklab-ntun-kmitir-kache-dayitw-hstantr-61c647d1c9685>
bdana@gmail.com
- <https://bdana.ssbumultiservices.com/general-member>
bdana@gmail.com
- <https://bdana.ssbumultiservices.com/life-member>
bdana@gmail.com
- <https://bdana.ssbumultiservices.com/our-missions>
bdana@gmail.com
- <https://bdana.ssbumultiservices.com/our-vissions>
bdana@gmail.com
- <https://bdana.ssbumultiservices.com/photo-gallery>
bdana@gmail.com
- <https://bdana.ssbumultiservices.com/privacy-policy>
bdana@gmail.com
- <https://bdana.ssbumultiservices.com/publications>
bdana@gmail.com
- <https://bdana.ssbumultiservices.com/register-plan>
bdana@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: bdana.ssbbmultiservices.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

File uploads

These pages allows visitors to upload files to the server. Various web applications allow users to upload files (such as pictures, images, sounds, ...). Uploaded files may pose a significant risk if not handled correctly. A remote attacker could send a multipart/form-data POST request with a specially-crafted filename or mime type and execute arbitrary code.

Impact

If the uploaded files are not safely checked an attacker may upload malicious files.

<https://bdana.ssbbmultiservices.com/>

Pages with file upload forms:

- <https://bdana.ssbbmultiservices.com/application-form>

```
Form name: <empty>
Form action: https://bdana.ssbbmultiservices.com/application-message-send
Form method: POST
Form file input: profile_img [file]
```

- <https://bdanasssbmultiservices.com/update-info>

```
Form name: <empty>
Form action: https://bdana.ssbbmultiservices.com/update-info-send
Form method: POST
Form file input: imageupload [file]
```

- <https://bdana.ssbbmultiservices.com/subscribe-register-form>

```
Form name: <empty>
Form action: https://bdana.ssbbmultiservices.com/subscribe-user-data
Form method: POST
Form file input: profile_img [file]
```

- <https://bdana.ssbbmultiservices.com/index.php/application-from>

```
Form name: <empty>
Form action: https://bdana.ssbbmultiservices.com/index.php/application-message-send
Form method: POST
Form file input: profile_img [file]
```

- <https://bdana.ssbbmultiservices.com/membership-overview>

```
Form name: <empty>
Form action: https://bdana.ssbbmultiservices.com/application-message-send
Form method: POST
Form file input: profile_img [file]
```

- <https://bdana.ssbbmultiservices.com/membership-renew>

```
Form name: <empty>
Form action: https://bdana.ssbbmultiservices.com/application-message-send
Form method: POST
Form file input: profile_img [file]
```

- <https://bdana.ssbbmultiservices.com/index.php/update-info>

```
Form name: <empty>
Form action: https://bdana.ssbbmultiservices.com/index.php/update-info-send
Form method: POST
Form file input: imageupload [file]
```

- <https://bdana.ssbbmultiservices.com/index.php/subscribe-register-form>

```
Form name: <empty>
Form action: https://bdana.ssbbmultiservices.com/index.php/subscribe-user-data
Form method: POST
Form file input: profile_img [file]
```

- <https://bdana.ssbbmultiservices.com/index.php/membership-overview>

```
Form name: <empty>
Form action: https://bdana.ssbbmultiservices.com/index.php/application-message-send
```

```
Form method: POST
Form file input: profile_img [file]

• https://bdana.ssbbmultiservices.com/index.php/membership-renew

    Form name: <empty>
    Form action: https://bdana.ssbbmultiservices.com/index.php/application-message-
    send
    Form method: POST
    Form file input: profile_img [file]
```

Request

```
GET /application-from HTTP/1.1
Referer: https://bdana.ssbbmultiservices.com/
Cookie: PHPSESSID=c0f392e546a83e61122cfb5e9e95d0a8; XSRF-
TOKEN=eyJpdii6IndFZEZua3ZGYXZzK2FQRlhoSkIxUXc9PSIsInZhbHVlIjoiZW9CdHR0aFQvYW5tU21peHB1QklWNk9hMG5aTD
dSt29lWWhodGFrYUxJMVF5bHBGS2ZRTGZUTEVBU1NDc2Y3bXU2aFBpS1NsZzYycw5td1psdUU3WGs1VzlTY2NLN01iRGJoNlArRG
x4ZUk40WJxcE52VDFRa0Js0VFnM3RrK0YiLCJtYWMi0iJhMThhM2ViNmY1MzJmMjExYWy4N2M40GUzNTA2ZTk3NTEyYzZhMDAxNz
IyZTUzNGZiZjE5MTgzMWEx0TMxNmNiIiwidGFnIjoiIn0%3D;
bangladesh_dental_association_of_north_america_session=eyJpdii6InFTdUVGN1FPYUx4Vk02c09GSDftVXc9PSIsI
nZhbHVlIjoiZlNhVw9qby9sYlpkWGRyNDMwWGtDbG5PZjFLVTJRa0RwcUF2Vjh0RTZWZkpSSmprc0l2ZkYzaEYx0U1ERnNzK3hvb
E9aQjNNajJGTUJlTWxjWUhIQUg2UEpNTnBYTmZHZZhnU3NBT1pSS1ZTYWorak9hSlBvWG9aS1NYazzTcVYiLCJtYWMi0iJlNWQwM
Dc4YmZlMGZlYTViZTRj0GJhNmY3MWVlZDg3NzM4ZmUxMjdjYTU2NDliZDzMGNjY2FkZTY5N2ZiZDViIiwidGFnIjoiIn0%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: bdana.ssbbmultiservices.com
Connection: Keep-alive
```

Recommendation

Restrict file types accepted for upload: check the file extension and only allow certain files to be uploaded. Use a whitelist approach instead of a blacklist. Check for double extensions such as .php.png. Check for files without a filename like .htaccess (on ASP.NET, check for configuration files like web.config). Change the permissions on the upload folder so the files within it are not executable. If possible, rename the files that are uploaded.

Outdated JavaScript libraries

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

Impact

Consult References for more information.

<https://bdana.ssbtmultiservices.com/>

Confidence: 95%

- **jQuery 3.5.1**

- URL: <https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js>
- Detection method: The library's name and version were determined based on the file's CDN URI.
- References:
 - <https://code.jquery.com/>

Request

```
GET / HTTP/1.1
Referer: https://bdana.ssbtmultiservices.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: bdana.ssbtmultiservices.com
Connection: Keep-alive
```

<https://bdana.ssbtmultiservices.com/>

Confidence: 95%

- **bootstrap.js 4.5.2**

- URL: <https://bdana.ssbtmultiservices.com/>
- Detection method: The library's name and version were determined based on its dynamic behavior.
- References:
 - <https://github.com/twbs/bootstrap/releases>

Request

```
GET / HTTP/1.1
Referer: https://bdana.ssbtmultiservices.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: bdana.ssbtmultiservices.com
Connection: Keep-alive
```

<https://bdana.ssbtmultiservices.com/>

Confidence: 95%

- **slick 1.5.9**

- URL: <https://bdana.ssbbmultiservices.com/assets/website/slick-slider/slick.min.js>
- Detection method: The library's name and version were determined based on the file's contents.
- References:
 - <https://github.com/kenwheeler/slick/tags>

Request

```
GET /assets/website/slick-slider/slick.min.js HTTP/1.1
Referer: https://bdana.ssbbmultiservices.com/
Cookie: PHPSESSID=4b5e7857595c78ff5af667c80e3168f1; XSRF-TOKEN=eyJpdiI6ImNWzlxY0RPMzRubnZ2lJVU203ZVE9PSIsInZhbHVlIjoiVnRldGZudEt0aEErN1l3KzIxUnBSZVljWm1HVFIdYyN2ZHvlorYlhnb3g2N0F6RmxNwne4Mkh1SzSbTZ2MjFDd3d5R0Vqdm16L3VVWldGaXdZNms4dXVsSUNGTXRsUjRhSENFSkdMQTcrMHFubm0zWUlhcmEvWHRSUGxQNWQiLCJtYWMi0iJlYWJlNjk0NGI1MThlMDk4YjBmNTdmMjJlMDc5YzYwNGIwYjExYWZmYjdkZGI20DljMjU5NWFiNmFiZTc2MDlhIiwidGFnIjoiIn0%3D;
bangladesh_dental_association_of_north_america_session=eyJpdiI6IlJ2eTJpcnJ0TUR4eTdEaHI5eWhielE9PSIsInZhbHVlIjoiZkNocjAvZW9vcFFUSEh6MVJ0UUJDdGtZRitXNE1t0XlgZmlVL0xQbnJYcUZVWh0SExRdHl0ckQ5QUl4YVRxTTlk0FNqVWd3elUyNFdw0ENhZLY2MuTZVJiay84di94NjZQSXQyckxPRzlDclJuUXdjbj1Jy0Wtoa01YYVQ3NEEiLCJtYWMi0iJl0DUyNjJhY2Y50WIzNTc2MDI3YThlM2FkNDY40GQ4ZDU1MTAxYjU20GQ4ZTUx0GZiZjFiMzQzZmQ5ZDNmMzAxIiwidGFnIjoiIn0%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: bdana.ssbbmultiservices.com
Connection: Keep-alive
```

Recommendation

Upgrade to the latest version.

Permissions-Policy header not implemented

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

Impact

<https://bdana.ssbbmultiservices.com/>

Locations without Permissions-Policy header:

- <https://bdana.ssbbmultiservices.com/>
- <https://bdana.ssbbmultiservices.com/membership/login>
- <https://bdana.ssbbmultiservices.com/about-us>

- <https://bdana.ssbumultiservices.com/reunion-detailes/constitution-ghtntntr>
- <https://bdana.ssbumultiservices.com/advisory-committee>
- <https://bdana.ssbumultiservices.com/application-from>
- <https://bdana.ssbumultiservices.com/award>
- <https://bdana.ssbumultiservices.com/assets/website/fonts/fontawesome/webfonts/>
- <https://bdana.ssbumultiservices.com/application-message-send>
- <https://bdana.ssbumultiservices.com/upload/about-us-image/>
- <https://bdana.ssbumultiservices.com/css/app.css>
- <https://bdana.ssbumultiservices.com/js/app.js>
- <https://bdana.ssbumultiservices.com/blog>
- <https://bdana.ssbumultiservices.com/constitutions>
- <https://bdana.ssbumultiservices.com/contact-us>
- <https://bdana.ssbumultiservices.com/donate>
- <https://bdana.ssbumultiservices.com/events-news>
- <https://bdana.ssbumultiservices.com/free-member>
- <https://bdana.ssbumultiservices.com/donation>
- <https://bdana.ssbumultiservices.com/single-news/niuyrk-banglades-presklab-ntun-kmitir-kache-dayitw-hstantr-61c647d1c9685>
- <https://bdana.ssbumultiservices.com/general-member>

Request

```
GET / HTTP/1.1
Referer: https://bdana.ssbumultiservices.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: bdana.ssbumultiservices.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://bdana.ssbtmultiservices.com/>

Pages with paths being disclosed:

- <https://bdana.ssbtmultiservices.com/contact-us/message>
`/home/ssbmul5/bdana.ssbtmultiservices.com/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php`
- <https://bdana.ssbtmultiservices.com/update-info-send>
`/home/ssbmul5/bdana.ssbtmultiservices.com/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php`
- <https://bdana.ssbtmultiservices.com/donation>
`/home/ssbmul5/bdana.ssbtmultiservices.com/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php`
- <https://bdana.ssbtmultiservices.com/password/email>
`/home/ssbmul5/bdana.ssbtmultiservices.com/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php`
- <https://bdana.ssbtmultiservices.com/membership/password/email>
`/home/ssbmul5/bdana.ssbtmultiservices.com/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php`
- <https://bdana.ssbtmultiservices.com/index.php/contact-us/message>
`/home/ssbmul5/bdana.ssbtmultiservices.com/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php`
- <https://bdana.ssbtmultiservices.com/application-message-send>
`/home/ssbmul5/bdana.ssbtmultiservices.com/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php`
- <https://bdana.ssbtmultiservices.com/subscribe-user-data>
`/home/ssbmul5/bdana.ssbtmultiservices.com/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php`
- <https://bdana.ssbtmultiservices.com/index.php/update-info-send>
`/home/ssbmul5/bdana.ssbtmultiservices.com/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php`
- <https://bdana.ssbtmultiservices.com/index.php/donation>
`/home/ssbmul5/bdana.ssbtmultiservices.com/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php`
- <https://bdana.ssbtmultiservices.com/index.php/membership/password/email>
`/home/ssbmul5/bdana.ssbtmultiservices.com/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php`
- <https://bdana.ssbtmultiservices.com/index.php/application-message-send>
`/home/ssbmul5/bdana.ssbtmultiservices.com/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php`

- <https://bdana.ssbumultiservices.com/index.php/subscribe-user-data>
`/home/ssbumul5/bdana.ssbumultiservices.com/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php`

Request

```
GET /contact-us/message HTTP/1.1
Referer: https://bdana.ssbumultiservices.com/contact-us
Cookie: PHPSESSID=6d40a857c8014cff0f5af1960f14d210; XSRF-TOKEN=eyJpdiI6IlZjcVlTN3BLKzZla1JENjFkSU9ja1E9PSIsInZhbHVlIjoiUy9p0Ct0dmJiTEk1UE5LakNTalNiTzRNY2JrZn15Z3ltdly1NDJEWlVQaFVrU0JRb3BHYzg0UHExNTB1Nm9qZ1pDQjJyVkvzT0V4NEM20Ho2UGHZQ0hFNU1TTkpyTG9oUlBTWpLTUhRaUMwTWJwVEtENut3RWRJaFVJZm92UKiLCJtYWMi0iJhYjQzMGIyMThlMzZmNjVhNjVlYTNiYjNlMDVmNjFhNDVkJTE3NTVjOWViODUwYzhkZDUyMzgxYzk4Yjk3YTdmIiwidGFnIjoiIn0%3D;
bangladesh_dental_association_of_north_america_session=eyJpdiI6Im12NUJMb09keXp2bWgzZ3BNV3h2N3c9PSIsInZhbHVlIjoiOFdaeUNrSDE2M0N6c3l3aTl4MwlQNHFjbHZJeG1walZsZDZ2R0p6NndRdkVCRW11ZGMrTXZ1QlMwY3dYNWoreTd4MFV4c3J0Z0laK2FMGtXK0N2NzNIcXR3emUxS1l0bTZFaTV5dDQzSUdS0DAwb3oxL3ptSGM0enY4WjhREiLCJtYWMi0iJmZDFhMGI0TQyMWIyODA0YTg5Y2RhZDJkYTA4YmEyM2Yz0DVh0TE40TQwZGJk0TlkMmI0YzVkgQwN2RjYzQ0IiwidGFnIjoiIn0%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: bdana.ssbumultiservices.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

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://bdana.ssbtmultiservices.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: bdana.ssbtmultiservices.com
Connection: Keep-alive
```

Recommendation

None

Subresource Integrity (SRI) not implemented

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

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

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

Impact

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

<https://bdana.ssbtmultiservices.com/>

Pages where SRI is not implemented:

- <https://bdana.ssbtmultiservices.com/>
Script SRC: <https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js>
- <https://bdana.ssbtmultiservices.com/>
Script SRC: <https://www.jqueryscript.net/demo/Text-Scrolling-Plugin-for-jQuery-Marquee/jquery.marquee.js?v=3>

Request

```
GET / HTTP/1.1
Referer: https://bdana.ssbtmultiservices.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: bdana.ssbtmultiservices.com
Connection: Keep-alive
```

Recommendation

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

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

```
<script src="https://example.com/example-framework.js"
integrity="sha384-oqVuAfXRKap7fdgccY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQholwx4JwY8wC"
crossorigin="anonymous"></script>
```

References

Subresource Integrity

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

SRI Hash Generator

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

Coverage

https://bdana.ssbbmultiservices.com

Inputs

GET iv, value, mac, tag

_ignition

Inputs

GET iv, value, mac, tag

health-check

Inputs

GET iv, value, mac, tag

assets

Inputs

GET iv, value, mac, tag

admin

Inputs

GET iv, value, mac, tag

images

Inputs

GET iv, value, mac, tag

logo

Inputs

GET iv, value, mac, tag

toastr

Inputs

GET iv, value, mac, tag

js

toastr.min.js

website

Inputs

GET iv, value, mac, tag

css

card-style.css

 loader.css

 style.css

 subscription.css

 fonts

 fontawesome

 CSS

 all.css

 webfonts

 Inputs

 GET

iv, value, mac, tag

 grid-gallery

 GridHorizontal.js

 imagesloaded.pkgd.min.js

 jquery.scripttop.min.css

 lightbox.css

 lightbox.js

 image

 Inputs

 GET

iv, value, mac, tag

 js

 imask.min.js

 main.js

 payment-plugin.js

 progressbar.js

 sweet-alert.min.js

 owl-carousel

 owl.carousel.min.css

 owl.carousel.min.js

 owl.theme.default.min.css

 pdf

 Inputs

 GET

iv, value, mac, tag

 slick-slider

	 slick.main.css
	 slick.min.js
	 slick.theme.min.css
 cgi-sys	
	 Inputs
	 iv, value, mac, tag
 config	
	 Inputs
	 iv, value, mac, tag
 contact-us	
	 Inputs
	 iv, value, mac, tag
	 message
	 Inputs
	 iv, value, mac, tag
	 iv, value, mac, tag
	 _token, email, message, name, phone, subject, submit
 css	
	 Inputs
	 iv, value, mac, tag
	 app.css
 database	
	 Inputs
	 iv, value, mac, tag
 factories	
	 Inputs
	 iv, value, mac, tag
 migrations	
	 Inputs
	 iv, value, mac, tag
 seeders	
	 Inputs
	 iv, value, mac, tag

 bdana_bdanssyye.sql
 Inputs
GET iv, value, mac, tag

 executive-detailes

 abdul-hamid
 Inputs
GET iv, value, mac, tag

 abdur-rouf-dilip
 Inputs
GET iv, value, mac, tag

 abu-noman-shakil
 Inputs
GET iv, value, mac, tag

 aftab-jony
 Inputs
GET iv, value, mac, tag

 amin-mack
 Inputs
GET iv, value, mac, tag

 anowar-hossain
 Inputs
GET iv, value, mac, tag

 azizul-chowdhury
 Inputs
GET iv, value, mac, tag

 babu-khan
 Inputs
GET iv, value, mac, tag

 badrul-haque
 Inputs
GET iv, value, mac, tag

 fahad-solaiman
 Inputs
GET iv, value, mac, tag

 femd-rocky

 Inputs

 GET iv, value, mac, tag

 harun-bhuiyan

 Inputs

 GET iv, value, mac, tag

 isteak-rumi

 Inputs

 GET iv, value, mac, tag

 joshi-choudhury

 Inputs

 GET iv, value, mac, tag

 kamruzzaman-bacchu

 Inputs

 GET iv, value, mac, tag

 m-a-aziz

 Inputs

 GET iv, value, mac, tag

 m-r-khandaker-santu

 Inputs

 GET iv, value, mac, tag

 mahmud-badsha

 Inputs

 GET iv, value, mac, tag

 masud-rana-topon

 Inputs

 GET iv, value, mac, tag

 mazeda-a-uddin

 Inputs

 GET iv, value, mac, tag

 md-azad

 Inputs

 GET iv, value, mac, tag

 md-humayun-kabir

 Inputs

GET iv, value, mac, tag

 md-kashem

 Inputs

GET iv, value, mac, tag

 mir-nizamul-haque

 Inputs

GET iv, value, mac, tag

 mohammad-idris

 Inputs

GET iv, value, mac, tag

 mohammed-alam-nomi

 Inputs

GET iv, value, mac, tag

 mohammed-salim-haroun

 Inputs

GET iv, value, mac, tag

 mohammed-uddin-alamgir

 Inputs

GET iv, value, mac, tag

 moin-choudhury

 Inputs

GET iv, value, mac, tag

 moinul-islam

 Inputs

GET iv, value, mac, tag

 monsur-chowdhury

 Inputs

GET iv, value, mac, tag

 morshed-sm-masud

 Inputs

GET iv, value, mac, tag

 nazmun-nahar-rahman



GET iv, value, mac, tag

 nilufar-shereen



GET iv, value, mac, tag

 nurul-amin-babu



GET iv, value, mac, tag

 sajjad-hossain



GET iv, value, mac, tag

 samiur-rahman



GET iv, value, mac, tag

 sanatan-shil



GET iv, value, mac, tag

 sarwar-chaudri



GET iv, value, mac, tag

 shafiuddin-miah



GET iv, value, mac, tag

 shah-chisty



GET iv, value, mac, tag

 shahriar-arif



GET iv, value, mac, tag

 shakhawat-biswas



GET iv, value, mac, tag

 shamol-c-nath

 Inputs

GET iv, value, mac, tag

 shoag-azam

 Inputs

GET iv, value, mac, tag

 subal-debnath

 Inputs

GET iv, value, mac, tag

 tohidul-islam-roni

 Inputs

GET iv, value, mac, tag

 towhid-shiblee

 Inputs

GET iv, value, mac, tag

 z-r-chowdhury-litu

 Inputs

GET iv, value, mac, tag

 zakir-h-chowdhury

 Inputs

GET iv, value, mac, tag

 index.php

 Inputs

GET iv, value, mac, tag

 contact-us

 Inputs

GET iv, value, mac, tag

 message

 Inputs

GET iv, value, mac, tag

POST iv, value, mac, tag

POST _token, email, message, name, phone, subject, submit

 executive-detailes

 abdul-hamid



Inputs

GET iv, value, mac, tag



abdur-rouf-dilip



Inputs

GET iv, value, mac, tag



abu-noman-shakil



Inputs

GET iv, value, mac, tag



aftab-jony



Inputs

GET iv, value, mac, tag



amin-mack



Inputs

GET iv, value, mac, tag

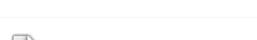


anowar-hossain



Inputs

GET iv, value, mac, tag



azizul-chowdhury



Inputs

GET iv, value, mac, tag



babu-khan



Inputs

GET iv, value, mac, tag



fahad-solaiman



Inputs

GET iv, value, mac, tag



femd-rocky



Inputs

GET iv, value, mac, tag



harun-bhuiyan



Inputs

GET iv, value, mac, tag



istea-k-rumi



GET iv, value, mac, tag



joshi-choudhury



GET iv, value, mac, tag



kamruzzaman-bacchu



GET iv, value, mac, tag



m-a-aziz



GET iv, value, mac, tag



m-r-khandaker-santu



GET iv, value, mac, tag



mahmud-badsha



GET iv, value, mac, tag



masud-rana-topon



GET iv, value, mac, tag



mazeda-a-uddin



GET iv, value, mac, tag



md-azad



GET iv, value, mac, tag



md-humayun-kabir



GET iv, value, mac, tag



md-kashem



Inputs

GET iv, value, mac, tag

mir-nizamul-haque



GET iv, value, mac, tag

mohammad-idris



GET iv, value, mac, tag

mohammed-alam-nomi



GET iv, value, mac, tag

mohammed-salim-haroun



GET iv, value, mac, tag

mohammed-uddin-alamgir



GET iv, value, mac, tag

moin-choudhury



GET iv, value, mac, tag

moinul-islam



GET iv, value, mac, tag

monsur-chowdhury



GET iv, value, mac, tag

morshed-sm-masud



GET iv, value, mac, tag

nazmun-nahar-rahman



GET iv, value, mac, tag

nilufar-shereen



Inputs

GET iv, value, mac, tag

nurul-amin-babu



Inputs

GET iv, value, mac, tag

sajjad-hossain



Inputs

GET iv, value, mac, tag

samiur-rahman



Inputs

GET iv, value, mac, tag

sanatan-shil



Inputs

GET iv, value, mac, tag

sarwar-chaudri



Inputs

GET iv, value, mac, tag

shafiuddin-miah



Inputs

GET iv, value, mac, tag

shah-chisty



Inputs

GET iv, value, mac, tag

shahriar-arif



Inputs

GET iv, value, mac, tag

shakhawat-biswas



Inputs

GET iv, value, mac, tag

shamol-c-nath



Inputs

GET iv, value, mac, tag

shoag-azam



Inputs

GET iv, value, mac, tag



subal-debnath



Inputs

GET iv, value, mac, tag



tohidul-islam-roni



Inputs

GET iv, value, mac, tag



towhid-shiblee



Inputs

GET iv, value, mac, tag



z-r-chowdhury-litu



Inputs

GET iv, value, mac, tag



zakir-h-chowdhury



Inputs

GET iv, value, mac, tag



member-detailes

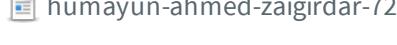


farhana-yeasmin-rita-70



Inputs

GET iv, value, mac, tag



humayun-ahmed-zaigirdar-72



Inputs

GET iv, value, mac, tag



khanam-chowdhury-43



Inputs

GET iv, value, mac, tag



md-sajib-prodhan-23



Inputs

GET iv, value, mac, tag



rahim-islam-prodhan-18



Inputs

GET iv, value, mac, tag

 rahim-islam-prodhan-33



GET iv, value, mac, tag

 tarek-khan-17



GET iv, value, mac, tag

 membership



GET iv, value, mac, tag

 password

 email



POST iv, value, mac, tag

POST _token, email

POST _token, email

GET iv, value, mac, tag

 reset



GET iv, value, mac, tag

 login



POST iv, value, mac, tag

POST _token, email, password

POST _token, email, password, remember

GET iv, value, mac, tag

 reunion-detailes

 constitution-ghntntr



GET iv, value, mac, tag

 inauguration



GET iv, value, mac, tag

 punrmilnee-2017



Inputs

GET iv, value, mac, tag



vyes-voice-ovishek



Inputs

GET iv, value, mac, tag



single-news

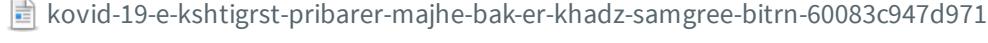


brnadhz-ayojne-niuyrk-banglades-presklaber-ntun-kmiti-ovishikt-61be2c819eaaa



Inputs

GET iv, value, mac, tag



kovid-19-e-kshtigrst-pribarer-majhe-bak-er-khadz-samgree-bitrn-60083c947d971



Inputs

GET iv, value, mac, tag



late-fazle-rashid-61bbe3f717299



Inputs

GET iv, value, mac, tag



niuizrk-banglades-pres-klab-fjle-rseed-purshkar2018-pelen-mnjur-ahmed-61bbe0316b76d



Inputs

GET iv, value, mac, tag



niuizrk-banglades-pres-klab-fjle-rseed-purshkar2018-pelen-mnjur-ahmed-61bc1ea61506e



Inputs

GET iv, value, mac, tag



niuizrk-banglades-pres-klab-fjle-rseed-purshkar2018-pelen-mnjur-ahmed-61be28f8a84d8



Inputs

GET iv, value, mac, tag

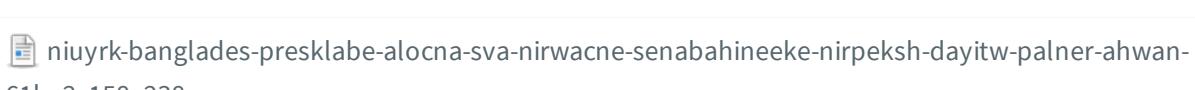


niuyrk-banglades-presklab-ntun-kmitir-kache-dayitw-hstantr-61c647d1c9685

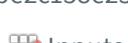


Inputs

GET iv, value, mac, tag



niuyrk-banglades-presklabe-alocna-sva-nirwacne-senabahineke-nirpeksh-dayitw-palner-ahwan-61be2c158e238



Inputs

GET iv, value, mac, tag



niuyrk-banglades-presklaber-nb-nirwacit-kmitir-ovishek-pesadaritw-bjay-rakhar-ongoeekar-61be32ea7e7b3



Inputs

GET iv, value, mac, tag

 niuyrk-banglades-presklaber-ntun-kmiti-abu-taher-svapti-mnoyar-smpadk-61c16f7ef1107

 Inputs

GET iv, value, mac, tag

 niuyrk-banglades-presklaber-ntun-kmiti-svapti-da-wajed-smpadk-mnoyarul-61be2f7d893c4

 Inputs

GET iv, value, mac, tag

 niuyrk-banglades-presklaber-sadharn-sva-oo-nirwacn-9-nvembr-votar-talika-cudant-61be2e220c91b

 Inputs

GET iv, value, mac, tag

 niuyrk-banglades-presklaber-sadharn-sva-oo-nirwacn-9i-nvembr-61be2d57b1513

 Inputs

GET iv, value, mac, tag

 about-us

 Inputs

GET iv, value, mac, tag

 advisory-committee

 Inputs

GET iv, value, mac, tag

 application-from

 Inputs

GET iv, value, mac, tag

 application-message-send

 Inputs

GET iv, value, mac, tag

POST iv, value, mac, tag

POST _token, address, associate, business_name, business_nature, city, email, experience, facebook, fax, general, incorporated_date, information, instagram, life_member, linkedin, other_social, owner_name, phone, profile_img, state, telephone, twitter, website, zipcode

 award

 Inputs

GET iv, value, mac, tag

 blog

 Inputs

GET iv, value, mac, tag

 constitutions

 Inputs

GET iv, value, mac, tag

 contact-us

 Inputs

GET iv, value, mac, tag

 donate

 Inputs

GET iv, value, mac, tag

 donation

 Inputs

GET iv, value, mac, tag

POST iv, value, mac, tag

POST _token, card_name, card_number, current_url, cvv, expire_date, id, payment_method, price

 events-news

 Inputs

GET iv, value, mac, tag

 executive-committee

 Inputs

GET iv, value, mac, tag

 free-member

 Inputs

GET iv, value, mac, tag

 general-member

 Inputs

GET iv, value, mac, tag

 life-member

 Inputs

GET iv, value, mac, tag

 membership-overview

 Inputs

GET iv, value, mac, tag

 membership-renew

 Inputs

GET iv, value, mac, tag

 message-president

 Inputs

GET iv, value, mac, tag

 message-secretary

 Inputs

GET iv, value, mac, tag

 our-missions

 Inputs

GET iv, value, mac, tag

 our-vissions

 Inputs

GET iv, value, mac, tag

 photo-gallery

 Inputs

GET iv, value, mac, tag

 privacy-policy

 Inputs

GET iv, value, mac, tag

 publications

 Inputs

GET iv, value, mac, tag

 register-plan

 Inputs

GET iv, value, mac, tag

 subscribe-register-form

 Inputs

GET iv, value, mac, tag

GET plan

 subscribe-user-data

 Inputs

POST iv, value, mac, tag

POST _token, city, confirm_password, country, email, facebook, fname, information, lname, mname, other_social, password, phone, profile_img, splan, state, twitter, usa_address, yearOfBirth, zipcode

GET iv, value, mac, tag

term-of-service

Inputs

GET iv, value, mac, tag

update-info

Inputs

GET iv, value, mac, tag

update-info-send

Inputs

GET iv, value, mac, tag

POST iv, value, mac, tag

POST _token, email, imageupload, memberId, message, name, phone, subject, submit

video-gallery

Inputs

GET iv, value, mac, tag

GET page

jbba

Inputs

GET iv, value, mac, tag

membership-renew

Inputs

GET iv, value, mac, tag

js

Inputs

GET iv, value, mac, tag

app.js

mailman

Inputs

GET iv, value, mac, tag

archives

Inputs

GET iv, value, mac, tag

📁 member-detailes

📄 farhana-yeasmin-rita-70

📝 Inputs

GET iv, value, mac, tag

📄 humayun-ahmed-zaigirdar-72

📝 Inputs

GET iv, value, mac, tag

📄 khanam-chowdhury-43

📝 Inputs

GET iv, value, mac, tag

📄 md-sajib-prodhan-23

📝 Inputs

GET iv, value, mac, tag

📄 rahim-islam-prodhan-18

📝 Inputs

GET iv, value, mac, tag

📄 rahim-islam-prodhan-33

📝 Inputs

GET iv, value, mac, tag

📄 tarek-khan-17

📝 Inputs

GET iv, value, mac, tag

📁 membership

📝 Inputs

GET iv, value, mac, tag

📁 password

📝 Inputs

GET iv, value, mac, tag

📄 email

📝 Inputs

POST iv, value, mac, tag

POST _token, email

POST _token, email

GET iv, value, mac, tag

reset

Inputs

GET iv, value, mac, tag

login

Inputs

POST iv, value, mac, tag

POST _token, email, password

POST _token, email, password, remember

GET iv, value, mac, tag

password

Inputs

GET iv, value, mac, tag

email

Inputs

POST iv, value, mac, tag

POST _token, email

POST _token, email

GET iv, value, mac, tag

reset

Inputs

GET iv, value, mac, tag

resources

Inputs

GET iv, value, mac, tag

css

Inputs

GET iv, value, mac, tag

js

Inputs

GET iv, value, mac, tag

lang

Inputs

GET iv, value, mac, tag

 sass

 Inputs

GET iv, value, mac, tag

 _variables.scss

 Inputs

GET iv, value, mac, tag

 app.scss

 Inputs

GET iv, value, mac, tag

 views

 Inputs

GET iv, value, mac, tag

 reunion-detailes

 constitution-gthntntr

 Inputs

GET iv, value, mac, tag

 inauguration

 Inputs

GET iv, value, mac, tag

 punrmilnee-2017

 Inputs

GET iv, value, mac, tag

 vyes-voice-ovishek

 Inputs

GET iv, value, mac, tag

 single-news

 brnadhz-ayojne-niuyrk-banglades-presklaber-ntun-kmiti-ovishikt-61be2c819eaaa

 Inputs

GET iv, value, mac, tag

 kovid-19-e-kshtigrst-pribarer-majhe-bak-er-khadz-samgree-bitrn-60083c947d971

 Inputs

GET iv, value, mac, tag

 late-fazle-rashid-61bbe3f717299

 Inputs

GET iv, value, mac, tag

 niuizrk-banglades-pres-klab-fjle-rseed-purshkar2018-pelen-mnjur-ahmed-61bbe0316b76d

 Inputs

GET iv, value, mac, tag

 niuizrk-banglades-pres-klab-fjle-rseed-purshkar2018-pelen-mnjur-ahmed-61bc1ea61506e

 Inputs

GET iv, value, mac, tag

 niuizrk-banglades-pres-klab-fjle-rseed-purshkar2018-pelen-mnjur-ahmed-61be28f8a84d8

 Inputs

GET iv, value, mac, tag

 niuyrk-banglades-presklab-ntun-kmitir-kache-dayitw-hstantr-61c647d1c9685

 Inputs

GET iv, value, mac, tag

 niuyrk-banglades-presklabe-alocna-sva-nirwacne-senabahineke-nirpeksh-dayitw-palner-ahwan-61be2c158e238

 Inputs

GET iv, value, mac, tag

 niuyrk-banglades-presklaber-nb-nirwacit-kmitir-ovishek-pesadaritw-bjay-rakhar-ongoeekar-61be32ea7e7b3

 Inputs

GET iv, value, mac, tag

 niuyrk-banglades-presklaber-ntun-kmiti-abu-taher-svapti-mnoyar-smpadk-61c16f7ef1107

 Inputs

GET iv, value, mac, tag

 niuyrk-banglades-presklaber-ntun-kmiti-svapti-da-wajed-smpadk-mnoyarul-61be2f7d893c4

 Inputs

GET iv, value, mac, tag

 niuyrk-banglades-presklaber-sadharn-sva-oo-nirwacn-9-nvembr-votar-talika-cudant-61be2e220c91b

 Inputs

GET iv, value, mac, tag

 niuyrk-banglades-presklaber-sadharn-sva-oo-nirwacn-9i-nvembr-61be2d57b1513

 Inputs

GET iv, value, mac, tag

storage	
Inputs	 GET iv, value, mac, tag
app	
Inputs	 GET iv, value, mac, tag
framework	
Inputs	 GET iv, value, mac, tag
logs	
Inputs	 GET iv, value, mac, tag
tests	
Inputs	 GET iv, value, mac, tag
upload	
Inputs	 GET iv, value, mac, tag
about-page	
Inputs	 GET iv, value, mac, tag
about-us-image	
Inputs	 GET iv, value, mac, tag
at-glance	
Inputs	 GET iv, value, mac, tag
banner-slider	
Inputs	 GET iv, value, mac, tag
ex-committee	
Inputs	 GET iv, value, mac, tag
member-renew	



GET iv, value, mac, tag

members-message



GET iv, value, mac, tag

photo-gallery



GET iv, value, mac, tag

post-image



GET iv, value, mac, tag

publication-constitution



GET iv, value, mac, tag

reunion



GET iv, value, mac, tag

slider



GET iv, value, mac, tag

subscribe-users



GET iv, value, mac, tag

vendor



GET iv, value, mac, tag

asm89



GET iv, value, mac, tag

bin



GET iv, value, mac, tag

brick



Inputs

GET iv, value, mac, tag



composer



GET iv, value, mac, tag



dflydev



GET iv, value, mac, tag



doctrine



GET iv, value, mac, tag



dragonmantank



GET iv, value, mac, tag



egulias



GET iv, value, mac, tag



facade



GET iv, value, mac, tag



fakerphp



GET iv, value, mac, tag



fideloper



GET iv, value, mac, tag



filp



GET iv, value, mac, tag



fruitcake



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





GET iv, value, mac, tag

📁 nunomaduro



GET iv, value, mac, tag

📁 opis



GET iv, value, mac, tag

📁 paypal



GET iv, value, mac, tag

📁 phar-io



GET iv, value, mac, tag

📁 phpdocumentor



GET iv, value, mac, tag

📁 phoption



GET iv, value, mac, tag

📁 phpspec



GET iv, value, mac, tag

📁 phpunit



GET iv, value, mac, tag

📁 psr



GET iv, value, mac, tag

📁 psy



GET iv, value, mac, tag

📁 ralouphie



Inputs

GET iv, value, mac, tag



ramsey



GET iv, value, mac, tag



sebastian



GET iv, value, mac, tag



swiftmailer



GET iv, value, mac, tag



symfony



GET iv, value, mac, tag



theseer



GET iv, value, mac, tag



tjjsverkoyen



GET iv, value, mac, tag



vlucas



GET iv, value, mac, tag



voku



GET iv, value, mac, tag



webmozart



GET iv, value, mac, tag



autoload.php



GET iv, value, mac, tag



.env



Inputs

GET iv, value, mac, tag



about-us



Inputs

GET iv, value, mac, tag



advisory-committee



Inputs

GET iv, value, mac, tag



application-from



Inputs

GET iv, value, mac, tag



application-message-send



Inputs

GET iv, value, mac, tag

POST iv, value, mac, tag

POST _token, address, associate, business_name, business_nature, city, email, experience, facebook, fax, general, incorporated_date, information, instagram, life_member, linkedin, other_social, owner_name, phone, profile_img, state, telephone, twitter, website, zipcode



award



Inputs

GET iv, value, mac, tag



blog



Inputs

GET iv, value, mac, tag



composer.json



Inputs

GET iv, value, mac, tag



composer.lock



Inputs

GET iv, value, mac, tag



constitutions



Inputs

GET iv, value, mac, tag



contact-us



GET iv, value, mac, tag



GET iv, value, mac, tag



GET iv, value, mac, tag



POST iv, value, mac, tag

POST _token, price, id, current_url, payment_method, card_name, card_number, expire_date, cvv

POST _token, card_name, card_number, current_url, cvv, expire_date, id, payment_method, price

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



 Inputs
POST iv, value, mac, tag
POST _token, email, password
POST _token, email, password, remember
GET iv, value, mac, tag
  membership-overview
 Inputs
GET iv, value, mac, tag
  membership-renew
 Inputs
GET iv, value, mac, tag
  message-president
 Inputs
GET iv, value, mac, tag
  message-secretary
 Inputs
GET iv, value, mac, tag
  our-missions
 Inputs
GET iv, value, mac, tag
  our-vissions
 Inputs
GET iv, value, mac, tag
  package-lock.json
 Inputs
GET iv, value, mac, tag
  package.json
 Inputs
GET iv, value, mac, tag
  photo-gallery
 Inputs
GET iv, value, mac, tag
  privacy-policy



Inputs

GET iv, value, mac, tag



Inputs

GET iv, value, mac, tag



Inputs

GET iv, value, mac, tag



Inputs

GET iv, value, mac, tag



Inputs

GET iv, value, mac, tag



Inputs

GET iv, value, mac, tag

GET plan



Inputs

POST iv, value, mac, tag

POST _token, city, confirm_password, country, email, facebook, fname, information, lname, mname, other_social, password, phone, profile_img, splan, state, twitter, usa_address, yearOfBirth, zipcode

GET iv, value, mac, tag



..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..

..</