Moodle 4.5

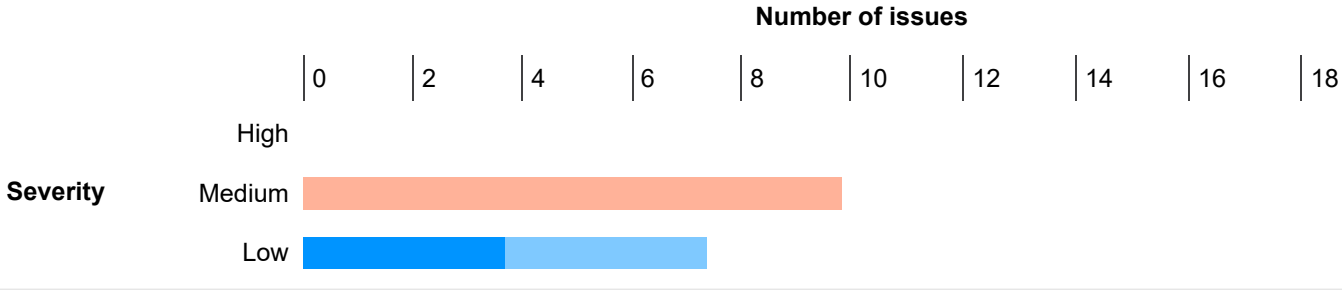
Burp Suite Professional

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low, Information or False Positive. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	0	0	0	0
	Medium	0	8	0	8
	Low	3	3	0	6
	Information	13	6	0	19
	False Positive	0	0	0	0

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

1. Session token in URL

1.1. https://moodledemo.eabyas.in:1443/
1.2. https://moodledemo.eabyas.in:1443/admin/search.php
1.3. https://moodledemo.eabyas.in:1443/calendar/view.php
1.4. https://moodledemo.eabyas.in:1443/grade/report/overview/index.php
1.5. https://moodledemo.eabyas.in:1443/message/output/popup/notifications.php
1.6. https://moodledemo.eabyas.in:1443/my/
1.7. https://moodledemo.eabyas.in:1443/my/courses.php
1.8. https://moodledemo.eabyas.in:1443/user/profile.php

2. Cookie without HttpOnly flag set

2.1. https://moodledemo.eabyas.in:1443/
2.2. https://moodledemo.eabyas.in:1443/login/index.php
2.3. https://moodledemo.eabyas.in:1443/robots.txt

3. Password field with autocomplete enabled

4. Unencrypted communications

5. Strict transport security not enforced

6. User agent-dependent response

6.1. http://moodledemo.eabyas.in:1443/
6.2. https://moodledemo.eabyas.in:1443/
6.3. https://moodledemo.eabyas.in:1443/admin/search.php

7. Duplicate cookies set

8. Cross-domain Referer leakage

8.1. https://moodledemo.eabyas.in:1443/
8.2. https://moodledemo.eabyas.in:1443/
8.3. https://moodledemo.eabyas.in:1443/
8.4. https://moodledemo.eabyas.in:1443/
8.5. https://moodledemo.eabyas.in:1443/calendar/view.php

9. Cross-domain script include

10. Frameable response (potential Clickjacking)

11. DOM data manipulation (DOM-based)

11.1. https://moodledemo.eabyas.in:1443/login/index.php
11.2. https://moodledemo.eabyas.in:1443/login/index.php

12. Email addresses disclosed

13. Private IP addresses disclosed

14. Cacheable HTTPS response

15. HTML does not specify charset

15.1. http://moodledemo.eabyas.in:1443/
15.2. http://moodledemo.eabyas.in:1443/robots.txt

16. TLS certificate

---

1. Session token in URL

There are 8 instances of this issue:

- /
- /admin/search.php
- /calendar/view.php

- /grade/report/overview/index.php
- /message/output/popup/notifications.php
- /my/
- /my/courses.php
- /user/profile.php

Issue background

Sensitive information within URLs may be logged in various locations, including the user's browser, the web server, and any forward or reverse proxy servers between the two endpoints. URLs may also be displayed on-screen, bookmarked or emailed around by users. They may be disclosed to third parties via the Referer header when any off-site links are followed. Placing session tokens into the URL increases the risk that they will be captured by an attacker.

Issue remediation

Applications should use an alternative mechanism for transmitting session tokens, such as HTTP cookies or hidden fields in forms that are submitted using the POST method.

Vulnerability classifications

- CWE-200: Information Exposure
- CWE-384: Session Fixation
- CWE-598: Information Exposure Through Query Strings in GET Request
- CAPEC-593: Session Hijacking

1.1. https://moodledemo.eabyas.in:1443/

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/**

Issue detail

The response contains the following links that appear to contain session tokens:

- https://moodledemo.eabyas.in:1443/login/logout.php?sesskey=LRaTMN9Yst

Request

```
GET /?redirect=0 HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

```
Cookie: MoodleSession=flgtj6vgus994pm6hm6jcquhub;
MOODLEID1_=sodium%3AbVCgXNGSinlR4DnRlQYDlPnKhrWWZdbi6VZItkgb8G191Ggv9dRLdA%2FkoTAF
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/my/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:16:03 GMT
Content-Type: text/html; charset=utf-8
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0, no-transform
Pragma: no-cache
Expires: Mon, 20 Aug 1969 09:23:00 GMT
Last-Modified: Mon, 28 Oct 2024 10:16:03 GMT
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="en" xml:lang="en">
<head>
<title>Home | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/image.php/boost/them
...[SNIP]...
</div>
<a href="https://moodledemo.eabyas.in:1443/login/logout.php?sesskey=LRaTMN9Yst" class="dropdown-item"
role="menuitem" tabindex="-1">

Log out

...[SNIP]...
</a> (<a href="https://moodledemo.eabyas.in:1443/login/logout.php?sesskey=LRaTMN9Yst">Log out</a>
...[SNIP]...
```

1.2. https://moodledemo.eabyas.in:1443/admin/search.php

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/admin/search.php**

Issue detail

The response contains the following links that appear to contain session tokens:

- https://moodledemo.eabyas.in:1443/login/logout.php?sesskey=u5ZdXFAr3V

Request

```
GET /admin/search.php HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=o8gp8vaeuk84pn6j8231lhreu4; MOODLEID1_=sodium%3A5Akqy5fY%2BRFnHV2JS4pBOcjzjSspI3p1mkHoNI9x%2BqunUPmgl0YoyBFvBRMG
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/my/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:16:29 GMT
Content-Type: text/html; charset=utf-8
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
Pragma: no-cache
Expires:
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="en" xml:lang="en">
<head>
<title>Search | Administration | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/i
...[SNIP]...
</div>
<a href="https://moodledemo.eabyas.in:1443/login/logout.php?sesskey=u5ZdXFAr3V" class="dropdown-item" role="menuitem" tabindex="-1">

Log out

...[SNIP]...
</a> (<a href="https://moodledemo.eabyas.in:1443/login/logout.php?sesskey=u5ZdXFAr3V">Log out</a>
...[SNIP]...
```

1.3. https://moodledemo.eabyas.in:1443/calendar/view.php

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/calendar/view.php**

Issue detail

The response contains the following links that appear to contain session tokens:

- https://moodledemo.eabyas.in:1443/login/logout.php?sesskey=Mv7EhKWLVb

Request

```
GET /calendar/view.php?view=month HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=k7j9v63h187ucbaoo8so2l035c; MOODLEID1_=sodium%3A8tkkqkVgnjuJTNONX1e9XrW6v9pc0LECPqEq4hvPb7aTgEjJ8u%2FHMbJ0%2Bi%2FT
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/my/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:17:02 GMT
Content-Type: text/html; charset=utf-8
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
Pragma: no-cache
Expires:
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="en" xml:lang="en">
<head>
<title>Moodle-Demo: Calendar: Detailed month view: October 2024 | Moodle-Demo</title>
<link rel="shortcut icon" href="https://
...[SNIP]...
</div>
<a href="https://moodledemo.eabyas.in:1443/login/logout.php?sesskey=Mv7EhKWLVb" class="dropdown-item" role="menuitem" tabindex="-1">
```

Log out

...[SNIP]...
 (Log out
...[SNIP]...

1.4. https://moodledemo.eabyas.in:1443/grade/report/overview/index.php

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/grade/report/overview/index.php**

Issue detail

The response contains the following links that appear to contain session tokens:

- https://moodledemo.eabyas.in:1443/login/logout.php?sesskey=RroF5KgSlQ

Request

```
GET /grade/report/overview/index.php HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=8s0mmu2aoo6jo2cs4mq5alrgh4; MOODLEID1_=sodium%3AnLMsSa%2FLUZDscGCUwq9X4uQjGc4i8blgQ8LVTPXcPJdzaltImgQ6T%2B9PKc0S
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/my/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:16:54 GMT
Content-Type: text/html; charset=utf-8
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
Pragma: no-cache
Expires:
```

```
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="en" xml:lang="en">
<head>
<title>Grades - Admin User | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/image
...[SNIP]...
</div>
<a href="https://moodledemo.eabyas.in:1443/login/logout.php?sesskey=RroF5KgSlQ" class="dropdown-item" role="menuitem"
tabindex="-1">

Log out

...[SNIP]...
</a> (<a href="https://moodledemo.eabyas.in:1443/login/logout.php?sesskey=RroF5KgSlQ">Log out</a>
...[SNIP]...
```

1.5. https://moodledemo.eabyas.in:1443/message/output/popup/notifications.php

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/message/output/popup/notifications.php**

Issue detail

The response contains the following links that appear to contain session tokens:

- https://moodledemo.eabyas.in:1443/login/logout.php?sesskey=7PhV80aMZi

Request

```
GET /message/output/popup/notifications.php HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=b0eelvepa5q8epdu26naaqd5n1;
MOODLEID1_=sodium%3AQr3691d6GC8Wyub%2FYS%2FSbvzp50DNu0mD3wnjg7oAUO1mV%2FkMnAcOgLzLO0iG
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/my/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:16:38 GMT
Content-Type: text/html; charset=utf-8
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
Pragma: no-cache
Expires:
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="en" xml:lang="en">
<head>
<title>Notifications | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/image.php/b
...[SNIP]...
</div>
<a href="https://moodledemo.eabyas.in:1443/login/logout.php?sesskey=7PhV80aMZi" class="dropdown-item"
role="menuitem" tabindex="-1">

Log out

...[SNIP]...
</a> (<a href="https://moodledemo.eabyas.in:1443/login/logout.php?sesskey=7PhV80aMZi">Log out</a>
...[SNIP]...
```

1.6. https://moodledemo.eabyas.in:1443/my/

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/my/**

Issue detail

The response contains the following links that appear to contain session tokens:

- https://moodledemo.eabyas.in:1443/login/logout.php?sesskey=XH0dAxmN3C

Request

```
GET /my/ HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
```

```
Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=7fp58pjiimqoi2fgeevotft4pt;
MOODLEID1_=sodium%3AkviQiL3VPxJNWKy4cBdERC4iK1XqGBodRPoWDNYf%2Bsks6FKEvH0%2Ber%2BOrp4e
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/login/index.php
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:15:54 GMT
Content-Type: text/html; charset=utf-8
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
Pragma: no-cache
Expires:
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="en" xml:lang="en">
<head>
<title>Dashboard | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/image.php/boost
...[SNIP]...
</div>
<a href="https://moodledemo.eabyas.in:1443/login/logout.php?sesskey=XH0dAxmN3C" class="dropdown-item"
role="menuitem" tabindex="-1">

Log out

...[SNIP]...
</a> (<a href="https://moodledemo.eabyas.in:1443/login/logout.php?sesskey=XH0dAxmN3C">Log out</a>
...[SNIP]...
```

1.7. https://moodledemo.eabyas.in:1443/my/courses.php

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/my/courses.php**

Issue detail

The response contains the following links that appear to contain session tokens:

- https://moodledemo.eabyas.in:1443/login/logout.php?sesskey=Qo9NiUS4jg

Request

```
GET /my/courses.php HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=7019j0vtqtn7drqkccq1lrkv2v; MOODLEID1_=sodium%3AsVAs9w8yriZH%2BpqjVzwsbxV84GT1nEsPhBzanL6NJ9m5JifyexrNXnjFXxOx
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/my/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:16:19 GMT
Content-Type: text/html; charset=utf-8
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
Pragma: no-cache
Expires:
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="en" xml:lang="en">
<head>
<title>My courses | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/image.php/boos
...[SNIP]...
</div>
<a href="https://moodledemo.eabyas.in:1443/login/logout.php?sesskey=Qo9NiUS4jg" class="dropdown-item" role="menuitem" tabindex="-1">

Log out

...[SNIP]...
</a> (<a href="https://moodledemo.eabyas.in:1443/login/logout.php?sesskey=Qo9NiUS4jg">Log out</a>
...[SNIP]...
```

1.8. https://moodledemo.eabyas.in:1443/user/profile.php

Summary

Severity: **Medium**

Confidence: **Firm**

Host: **https://moodledemo.eabyas.in:1443**

Path: **/user/profile.php**

Issue detail

The response contains the following links that appear to contain session tokens:

- https://moodledemo.eabyas.in:1443/login/logout.php?sesskey=gtgNT4qTOf

Request

```
GET /user/profile.php HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=ash87o9sok8s2kk9rrvojoldmc; MOODLEID1_=sodium%3AGCYo17XFoaMB9%2FHh38mwdC6rsUqnVlw9O%2BiXEDi%2FBebDw4fRfC4pwx2oDlgi
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/my/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:16:46 GMT
Content-Type: text/html; charset=utf-8
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
Pragma: no-cache
Expires:
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="en" xml:lang="en">
<head>
<title>Admin User: Public profile | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/them
...[SNIP]...
</div>
<a href="https://moodledemo.eabyas.in:1443/login/logout.php?sesskey=gtgNT4qTOf" class="dropdown-item" role="menuitem" tabindex="-1">
```

Log out

...[SNIP]...
 (Log out
...[SNIP]...

---

2. Cookie without HttpOnly flag set

There are 3 instances of this issue:

- /
- /login/index.php
- /robots.txt

Issue background

If the HttpOnly attribute is set on a cookie, then the cookie's value cannot be read or set by client-side JavaScript. This measure makes certain client-side attacks, such as cross-site scripting, slightly harder to exploit by preventing them from trivially capturing the cookie's value via an injected script.

Issue remediation

There is usually no good reason not to set the HttpOnly flag on all cookies. Unless you specifically require legitimate client-side scripts within your application to read or set a cookie's value, you should set the HttpOnly flag by including this attribute within the relevant Set-cookie directive.

You should be aware that the restrictions imposed by the HttpOnly flag can potentially be circumvented in some circumstances, and that numerous other serious attacks can be delivered by client-side script injection, aside from simple cookie stealing.

References

- Web Security Academy: Exploiting XSS vulnerabilities
- HttpOnly effectiveness

Vulnerability classifications

- CWE-16: Configuration
- CAPEC-31: Accessing/Intercepting/Modifying HTTP Cookies

2.1. https://moodledemo.eabyas.in:1443/

Summary

Severity:	**Low**
Confidence:	**Firm**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/**

Issue detail

The following cookie was issued by the application and does not have the HttpOnly flag set:

- **MoodleSession**

The cookie appears to contain a session token, which may increase the risk associated with this issue. You should review the contents of the cookie to determine its function.

Request

```
GET / HTTP/1.1
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:15:27 GMT
Content-Type: text/html; charset=utf-8
Set-Cookie: MoodleSession=hlkac3dvv4se0877uq0h6f122g; path=/; secure; SameSite=None
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0, no-transform
Pragma: no-cache
Expires: Mon, 20 Aug 1969 09:23:00 GMT
Last-Modified: Mon, 28 Oct 2024 10:15:27 GMT
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="en" xml:lang="en">
<head>
<title>Home | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/image.php/boost/them
...[SNIP]...
```

2.2. https://moodledemo.eabyas.in:1443/login/index.php

Summary

Severity: **Low**

Confidence: **Firm**

Host: **https://moodledemo.eabyas.in:1443**

Path: **/login/index.php**

Issue detail

The following cookies were issued by the application and do not have the HttpOnly flag set:

- **MoodleSession**
- MOODLEID1_

The highlighted cookie appears to contain a session token, which may increase the risk associated with this issue. You should review the contents of the cookies to determine their function.

Request

```
POST /login/index.php HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=dt21651hduer7rbq2n2keso9sd
Origin: https://moodledemo.eabyas.in:1443
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/login/index.php
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 87

anchor=&logintoken=K5GQ77miQ2vUg1F7ERVj6RcQ88o79Lxt&username=admin&password=Admin123%24
```

Response

```
HTTP/2 303 See Other
Server: nginx
Date: Mon, 28 Oct 2024 10:15:53 GMT
Content-Type: text/html; charset=utf-8
Location: https://moodledemo.eabyas.in:1443/login/index.php?testsession=2
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: MoodleSession=7fp58pjiimqoi2fgeevotft4pt; path=/; secure; SameSite=None
Set-Cookie: MOODLEID1_=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/; secure
Set-Cookie: MOODLEID1_=sodium%3AkviQiL3VPxJNWKy4cBdERC4iK1XqGBodRPoWDNYf%2Bsks6FKEvH0%2Ber%2BOrp4e; expires=Fri, 27-Dec-2024 10:15:53 GMT; Max-Age=5184000; path=/; secure
X-Redirect-By: Moodle
Content-Language: en

<!DOCTYPE html>
<html lang="en" xml:lang="en">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Redirect</title>
```

```
<style>
body {

...[SNIP]...
```

2.3. https://moodledemo.eabyas.in:1443/robots.txt

Summary

Severity:	**Low**
Confidence:	**Firm**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/robots.txt**

Issue detail

The following cookie was issued by the application and does not have the HttpOnly flag set:

- **MoodleSession**

The cookie appears to contain a session token, which may increase the risk associated with this issue. You should review the contents of the cookie to determine its function.

Request

```
GET /robots.txt HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:15:30 GMT
Content-Type: text/html; charset=utf-8
Set-Cookie: MoodleSession=8kar6ogi0lkbr1aflp1g7hq0ij; path=/; secure; SameSite=None
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0, no-transform
Pragma: no-cache
Expires: Mon, 20 Aug 1969 09:23:00 GMT
Last-Modified: Mon, 28 Oct 2024 10:15:30 GMT
Accept-Ranges: none

<!DOCTYPE html>
```

```
<html dir="ltr" lang="en" xml:lang="en">
<head>
<title>Home | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/image.php/boost/them
...[SNIP]...
```

---

3. Password field with autocomplete enabled

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/login/index.php**

Issue detail

The page contains a form with the following action URL:

- https://moodledemo.eabyas.in:1443/login/index.php

The form contains the following password field with autocomplete enabled:

- password

Issue background

Most browsers have a facility to remember user credentials that are entered into HTML forms. This function can be configured by the user and also by applications that employ user credentials. If the function is enabled, then credentials entered by the user are stored on their local computer and retrieved by the browser on future visits to the same application.

The stored credentials can be captured by an attacker who gains control over the user's computer. Further, an attacker who finds a separate application vulnerability such as cross-site scripting may be able to exploit this to retrieve a user's browser-stored credentials.

Issue remediation

To prevent browsers from storing credentials entered into HTML forms, include the attribute **autocomplete="off"** within the FORM tag (to protect all form fields) or within the relevant INPUT tags (to protect specific individual fields).

Please note that modern web browsers may ignore this directive. In spite of this there is a chance that not disabling autocomplete may cause problems obtaining PCI compliance.

Vulnerability classifications

- CWE-200: Information Exposure

Request

```
GET /login/index.php HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=8djrcfm00dkje2pmgvc4mtjjo1
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:15:48 GMT
Content-Type: text/html; charset=utf-8
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
Pragma: no-cache
Expires:
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="en" xml:lang="en">
<head>
<title>Log in to the site | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/image.
...[SNIP]...
</h1>
<form class="login-form" action="https://moodledemo.eabyas.in:1443/login/index.php" method="post" id="login">
<input id="anchor" type="hidden" name="anchor" value="">
...[SNIP]...
</label>
<input type="password" name="password" id="password" value="" class="form-control form-control-lg"
placeholder="Password" autocomplete="current-password">
</div>
...[SNIP]...
```

---

4. Unencrypted communications

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**http://moodledemo.eabyas.in:1443**
Path:	**/**

Issue description

The application allows users to connect to it over unencrypted connections. An attacker suitably positioned to view a legitimate user's network traffic could record and monitor their interactions with the application and obtain any information the user supplies. Furthermore, an attacker able to modify traffic could use the application as a platform for attacks against its users and third-party websites. Unencrypted connections have been exploited by ISPs and governments to track users, and to inject adverts and malicious JavaScript. Due to these concerns, web browser vendors are planning to visually flag unencrypted connections as hazardous.

To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Please note that using a mixture of encrypted and unencrypted communications is an ineffective defense against active attackers, because they can easily remove references to encrypted resources when these references are transmitted over an unencrypted connection.

Issue remediation

Applications should use transport-level encryption (SSL/TLS) to protect all communications passing between the client and the server. The Strict-Transport-Security HTTP header should be used to ensure that clients refuse to access the server over an insecure connection.

References

- Marking HTTP as non-secure
- Configuring Server-Side SSL/TLS
- HTTP Strict Transport Security

Vulnerability classifications

- CWE-326: Inadequate Encryption Strength
- CAPEC-94: Man in the Middle Attack
- CAPEC-157: Sniffing Attacks

---

5. Strict transport security not enforced

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/**

Issue detail

This issue was found in multiple locations under the reported path.

Issue background

The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.

To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic.This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Issue remediation

The application should instruct web browsers to only access the application using HTTPS. To do this, enable HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag if appropriate.

Note that because HSTS is a "trust on first use" (TOFU) protocol, a user who has never accessed the application will never have seen the HSTS header, and will therefore still be vulnerable to SSL stripping attacks. To mitigate this risk, you can optionally add the 'preload' flag to the HSTS header, and submit the domain for review by browser vendors.

References

- HTTP Strict Transport Security
- sslstrip
- HSTS Preload Form

Vulnerability classifications

- CWE-523: Unprotected Transport of Credentials
- CAPEC-94: Man in the Middle Attack
- CAPEC-157: Sniffing Attacks

Request

```
GET /?lang=am HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=9rdu4op2ra47d6nu7ava6po22t
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:15:38 GMT
Content-Type: text/html; charset=utf-8
Content-Language: am
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0, no-transform
Pragma: no-cache
```

```
Expires: Mon, 20 Aug 1969 09:23:00 GMT
Last-Modified: Mon, 28 Oct 2024 10:15:38 GMT
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="am" xml:lang="am">
<head>
<title>..... ..... | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/image.ph
...[SNIP]...
```

6. User agent-dependent response

There are 3 instances of this issue:

- http://moodledemo.eabyas.in:1443/
- https://moodledemo.eabyas.in:1443/
- https://moodledemo.eabyas.in:1443/admin/search.php

Issue description

Application responses may depend systematically on the value of the User-Agent header in requests. This behavior does not itself constitute a security vulnerability, but may point towards additional attack surface within the application, which may contain vulnerabilities.

This behavior often arises because applications provide different user interfaces for desktop and mobile users. Mobile interfaces have often been less thoroughly tested for vulnerabilities such as cross-site scripting, and often have simpler authentication and session handling mechanisms that may contain problems that are not present in the full interface.

To review the interface provided by the alternate User-Agent header, you can configure a match/replace rule in Burp Proxy to modify the User-Agent header in all requests, and then browse the application in the normal way using your normal browser.

Vulnerability classifications

- CWE-16: Configuration

6.1. http://moodledemo.eabyas.in:1443/

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**http://moodledemo.eabyas.in:1443**
Path:	**/**

Request 1

```
GET / HTTP/1.1
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 400 Bad Request
Server: nginx
Date: Mon, 28 Oct 2024 10:17:31 GMT
Content-Type: text/html
Content-Length: 650
Connection: close

<html>
<head><title>400 The plain HTTP request was sent to HTTPS port</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<center>The plain HTTP request was sent to HTTPS port</center>
...[SNIP]...
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

Request 2

```
GET / HTTP/1.1
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 2

```
HTTP/1.1 400 Bad Request
Server: nginx
```

```
Date: Mon, 28 Oct 2024 10:17:30 GMT
Content-Type: text/html
Content-Length: 248
Connection: close

<html>
<head><title>400 The plain HTTP request was sent to HTTPS port</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<center>The plain HTTP request was sent to HTTPS port</center>
...[SNIP]...
```

6.2. https://moodledemo.eabyas.in:1443/

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/**

Request 1

```
GET / HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:17:31 GMT
Content-Type: text/html; charset=utf-8
Set-Cookie: MoodleSession=vkg9sg6461t5b03ei4p0278gj7; path=/; secure; SameSite=None
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0, no-transform
Pragma: no-cache
Expires: Mon, 20 Aug 1969 09:23:00 GMT
Last-Modified: Mon, 28 Oct 2024 10:17:31 GMT
```

```
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="en" xml:lang="en">
<head>
<title>Home | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/image.php/boost/them
...[SNIP]...
<body id="page-site-index" class="limitedwidth format-site course path-site chrome dir-ltr lang-en yui-skin-sam yui3-skin-sam
moodledemo-eabyas-in--1443 pagelayout-frontpage course-1 context-2 notloggedin theme uses-drawers">
...[SNIP]...
```

Request 2

```
GET / HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1
Mobile/9B176 Safari/7534.48.3
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 2

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:17:30 GMT
Content-Type: text/html; charset=utf-8
Set-Cookie: MoodleSession=neo1uhmh1d8csbs009ornedet8; path=/; secure
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0, no-transform
Pragma: no-cache
Expires: Mon, 20 Aug 1969 09:23:00 GMT
Last-Modified: Mon, 28 Oct 2024 10:17:30 GMT
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="en" xml:lang="en">
<head>
<title>Home | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/image.php/boost/them
...[SNIP]...
<body id="page-site-index" class="limitedwidth format-site course path-site ios dir-ltr lang-en yui-skin-sam yui3-skin-sam
moodledemo-eabyas-in--1443 pagelayout-frontpage course-1 context-2 notloggedin theme uses-drawers">
...[SNIP]...
</div><div id="theme_switch_link"><a rel="nofollow" href="https://moodledemo.eabyas.in:1443/theme/switchdevice.php?
url=https%3A%2F%2Fmoodledemo.eabyas.in%3A1443%2F&amp;device=default&amp;sesskey=g3GftGBTEF">Switch to the
standard theme</a></div>
<script>
```

```
...[SNIP]...
<a href="https://moodle.com">
...[SNIP]...
```

6.3. https://moodledemo.eabyas.in:1443/admin/search.php

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/admin/search.php**

Request 1

```
GET /admin/search.php HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=d9slbslkr03e76idravbdualut; MOODLEID1_=sodium%3AAEbxRMV2LMuQZeOJqGYfEEhJlOCWJ%2B9R9FJqX9oKDjEP2QHDSXVNeqAgUiXn
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/my/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

Response 1

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:26:01 GMT
Content-Type: text/html; charset=utf-8
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
Pragma: no-cache
Expires:
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="en" xml:lang="en">
<head>
<title>Search | Administration | Moodle-Demo</title>
```

```
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/i
...[SNIP]...
<body id="page-admin-search" class="format-site admin path-admin chrome dir-ltr lang-en yui-skin-sam yui3-skin-sam
moodledemo-eabyas-in--1443 pagelayout-admin course-1 context-1 theme uses-drawers">
...[SNIP]...
<a
id="contacts-tab-671f66b96ccd2671f66b91ba406"
class="nav-link active"
href="#contacts-tab-panel-671f66b96ccd2671f66b91ba406"
data-toggle="tab"
data-action="show-contacts-section"
role="tab"

...[SNIP]...
<a
id="requests-tab-671f66b96ccd2671f66b91ba406"
class="nav-link"
href="#requests-tab-panel-671f66b96ccd2671f66b91ba406"
data-toggle="tab"
data-action="show-requests-section"
role="tab"

...[SNIP]...
```

Request 2

```
GET /admin/search.php HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1
Mobile/9B176 Safari/7534.48.3
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=d9slbslkr03e76idravbdualut;
MOODLEID1_=sodium%3AAEbxRMV2LMuQZeOJqGYfEEhJlOCWJ%2B9R9FJqX9oKDjEP2QHDSXVNeqAgUiXn
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/my/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

Response 2

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:25:59 GMT
Content-Type: text/html; charset=utf-8
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
Pragma: no-cache
Expires:
Accept-Ranges: none

<!DOCTYPE html>
```

```
<html dir="ltr" lang="en" xml:lang="en">
<head>
<title>Search | Administration | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/i
...[SNIP]...
<body id="page-admin-search" class="format-site admin path-admin ios dir-ltr lang-en yui-skin-sam yui3-skin-sam
moodledemo-eabyas-in--1443 pagelayout-admin course-1 context-1 theme uses-drawers">
...[SNIP]...
</div><div id="theme_switch_link"><a rel="nofollow" href="https://moodledemo.eabyas.in:1443/theme/switchdevice.php?
url=https%3A%2F%2Fmoodledemo.eabyas.in%3A1443%2Fadmin%2Fsearch.php%3Fquery&amp;device=default&amp;sesskey=tw6FB6nMBc">Switch to the standard theme</a></div>
<script>
...[SNIP]...
<a
id="contacts-tab-671f66b7a4e02671f66b75cd596"
class="nav-link active"
href="#contacts-tab-panel-671f66b7a4e02671f66b75cd596"
data-toggle="tab"
data-action="show-contacts-section"
role="tab"

...[SNIP]...
<a
id="requests-tab-671f66b7a4e02671f66b75cd596"
class="nav-link"
href="#requests-tab-panel-671f66b7a4e02671f66b75cd596"
data-toggle="tab"
data-action="show-requests-section"
role="tab"

...[SNIP]...
<a href="https://moodledemo.eabyas.in:1443/message/index.php">
...[SNIP]...
```

---

7. Duplicate cookies set

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/login/index.php**

Issue detail

The application attempted to set the following cookie to multiple values:

- **MOODLEID1_**

Issue background

The response contains two or more Set-Cookie headers that attempt to set the same cookie to different values. Browsers will only accept one of these values, typically the value in the last header. The presence of the duplicate headers may indicate a programming error.

Vulnerability classifications

- CWE-16: Configuration

Request 1

```
POST /login/index.php HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=dt21651hduer7rbq2n2keso9sd
Origin: https://moodledemo.eabyas.in:1443
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/login/index.php
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 87

anchor=&logintoken=K5GQ77miQ2vUg1F7ERVj6RcQ88o79Lxt&username=admin&password=Admin123%24
```

Response 1

```
HTTP/2 303 See Other
Server: nginx
Date: Mon, 28 Oct 2024 10:15:53 GMT
Content-Type: text/html; charset=utf-8
Location: https://moodledemo.eabyas.in:1443/login/index.php?testsession=2
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: MoodleSession=7fp58pjiimqoi2fgeevotft4pt; path=/; secure; SameSite=None
Set-Cookie: MOODLEID1_=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/; secure
Set-Cookie: MOODLEID1_=sodium%3AkviQiL3VPxJNWKy4cBdERC4iK1XqGBodRPoWDNYf%2Bsks6FKEvH0%2Ber%2BOrp4e; expires=Fri, 27-Dec-2024 10:15:53 GMT; Max-Age=5184000; path=/; secure
X-Redirect-By: Moodle
Content-Language: en

<!DOCTYPE html>
<html lang="en" xml:lang="en">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Redirect</title>
<style>
body {

...[SNIP]...
```

---

8. Cross-domain Referer leakage

There are 5 instances of this issue:

- /
- /
- /
- /
- /calendar/view.php

Issue background

When a web browser makes a request for a resource, it typically adds an HTTP header, called the "Referer" header, indicating the URL of the resource from which the request originated. This occurs in numerous situations, for example when a web page loads an image or script, or when a user clicks on a link or submits a form.

If the resource being requested resides on a different domain, then the Referer header is still generally included in the cross-domain request. If the originating URL contains any sensitive information within its query string, such as a session token, then this information will be transmitted to the other domain. If the other domain is not fully trusted by the application, then this may lead to a security compromise.

You should review the contents of the information being transmitted to other domains, and also determine whether those domains are fully trusted by the originating application.

Today's browsers may withhold the Referer header in some situations (for example, when loading a non-HTTPS resource from a page that was loaded over HTTPS, or when a Refresh directive is issued), but this behavior should not be relied upon to protect the originating URL from disclosure.

Note also that if users can author content within the application then an attacker may be able to inject links referring to a domain they control in order to capture data from URLs used within the application.

Issue remediation

Applications should never transmit any sensitive information within the URL query string. In addition to being leaked in the Referer header, such information may be logged in various locations and may be visible on-screen to untrusted parties. If placing sensitive information in the URL is unavoidable, consider using the Referer-Policy HTTP header to reduce the chance of it being disclosed to third parties.

References

- Referer Policy
- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-200: Information Exposure

8.1. https://moodledemo.eabyas.in:1443/

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/**

Issue detail

The page was loaded from a URL containing a query string:

- https://moodledemo.eabyas.in:1443/

The response contains the following links to other domains:

- https://cdn.jsdelivr.net/npm/mathjax@2.7.9/MathJax.js?delayStartupUntil=configured
- https://download.moodle.org/mobile?version=2024100700&lang=en&iosappid=633359593&androidappid=com.moodle.moodlemobile
- https://moodle.com/
- https://moodle.com/help/?utm_source=CTA-banner&utm_medium=platform&utm_campaign=name~Moodle4+cat~lms+mp~no

Request 1

```
GET /?redirect=0 HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=flgtj6vgus994pm6hm6jcquhub; MOODLEID1_=sodium%3AbVCgXNGSinlR4DnRlQYDlPnKhrWWZdbi6VZItkgb8G191Ggv9dRLdA%2FkoTAF
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/my/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:16:03 GMT
Content-Type: text/html; charset=utf-8
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0, no-transform
Pragma: no-cache
Expires: Mon, 20 Aug 1969 09:23:00 GMT
Last-Modified: Mon, 28 Oct 2024 10:16:03 GMT
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="en" xml:lang="en">
<head>
<title>Home | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/image.php/boost/them
...[SNIP]...
</script>
<script src="https://cdn.jsdelivr.net/npm/mathjax@2.7.9/MathJax.js?delayStartupUntil=configured"></script>
...[SNIP]...
```

```
<div>Powered by <a href="https://moodle.com">Moodle</a>
...[SNIP]...
```

8.2. https://moodledemo.eabyas.in:1443/

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/**

Issue detail

The page was loaded from a URL containing a query string:

- https://moodledemo.eabyas.in:1443/

The response contains the following links to other domains:

- https://cdn.jsdelivr.net/npm/mathjax@2.7.9/MathJax.js?delayStartupUntil=configured
- https://download.moodle.org/mobile?version=2024100700&lang=hi&iosappid=633359593&androidappid=com.moodle.moodlemobile
- https://moodle.com/

Request 1

```
GET /?lang=hi HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=t5q2m2u0mvlk7npm6c4dafve60
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:15:42 GMT
Content-Type: text/html; charset=utf-8
Content-Language: hi
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: no-store, no-cache, must-revalidate
```

```
Cache-Control: post-check=0, pre-check=0, no-transform
Pragma: no-cache
Expires: Mon, 20 Aug 1969 09:23:00 GMT
Last-Modified: Mon, 28 Oct 2024 10:15:42 GMT
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="hi" xml:lang="hi">
<head>
<title>..... ..... | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme
...[SNIP]...
</script>
<script src="https://cdn.jsdelivr.net/npm/mathjax@2.7.9/MathJax.js?delayStartupUntil=configured"></script>
...[SNIP]...
<div><a href="https://moodle.com">.....</a>
...[SNIP]...
```

8.3. https://moodledemo.eabyas.in:1443/

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/**

Issue detail

The page was loaded from a URL containing a query string:

- https://moodledemo.eabyas.in:1443/

The response contains the following links to other domains:

- https://cdn.jsdelivr.net/npm/mathjax@2.7.9/MathJax.js?delayStartupUntil=configured
- https://download.moodle.org/mobile?version=2024100700&lang=te&iosappid=633359593&androidappid=com.moodle.moodlemobile
- https://moodle.com/

Request 1

```
GET /?lang=te HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=1ensnt2s4fr4lqv0ipc5do1gdn
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
```

```
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:15:45 GMT
Content-Type: text/html; charset=utf-8
Content-Language: te
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0, no-transform
Pragma: no-cache
Expires: Mon, 20 Aug 1969 09:23:00 GMT
Last-Modified: Mon, 28 Oct 2024 10:15:45 GMT
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="te" xml:lang="te">
<head>
<title>..... | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/image.php/bo
...[SNIP]...
</script>
<script src="https://cdn.jsdelivr.net/npm/mathjax@2.7.9/MathJax.js?delayStartupUntil=configured"></script>
...[SNIP]...
<div>Powered by <a href="https://moodle.com">Moodle</a>
...[SNIP]...
```

8.4. https://moodledemo.eabyas.in:1443/

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/**

Issue detail

The page was loaded from a URL containing a query string:

- https://moodledemo.eabyas.in:1443/

The response contains the following links to other domains:

- https://cdn.jsdelivr.net/npm/mathjax@2.7.9/MathJax.js?delayStartupUntil=configured
- https://download.moodle.org/mobile?version=2024100700&lang=am&iosappid=633359593&androidappid=com.moodle.moodlemobile
- https://moodle.com/

Request 1

```
GET /?lang=am HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=9rdu4op2ra47d6nu7ava6po22t
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:15:38 GMT
Content-Type: text/html; charset=utf-8
Content-Language: am
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0, no-transform
Pragma: no-cache
Expires: Mon, 20 Aug 1969 09:23:00 GMT
Last-Modified: Mon, 28 Oct 2024 10:15:38 GMT
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="am" xml:lang="am">
<head>
<title>..... ..... | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/image.ph
...[SNIP]...
</script>
<script src="https://cdn.jsdelivr.net/npm/mathjax@2.7.9/MathJax.js?delayStartupUntil=configured"></script>
...[SNIP]...
<div>Powered by <a href="https://moodle.com">Moodle</a>
...[SNIP]...
```

8.5. https://moodledemo.eabyas.in:1443/calendar/view.php

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://moodledemo.eabyas.in:1443**

Path: **/calendar/view.php**

Issue detail

The page was loaded from a URL containing a query string:

- https://moodledemo.eabyas.in:1443/calendar/view.php

The response contains the following links to other domains:

- https://cdn.jsdelivr.net/npm/mathjax@2.7.9/MathJax.js?delayStartupUntil=configured
- https://docs.moodle.org/405/en/calendar/view
- https://download.moodle.org/mobile?version=2024100700&lang=en&iosappid=633359593&androidappid=com.moodle.moodlemobile
- https://moodle.com/
- https://moodle.com/help/?utm_source=CTA-banner&utm_medium=platform&utm_campaign=name~Moodle4+cat~lms+mp~no

Request 1

```
GET /calendar/view.php?view=month HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=k7j9v63h187ucbaoo8so2l035c; MOODLEID1_=sodium%3A8tkkqkVgnjuJTNONX1e9XrW6v9pc0LECPqEq4hvPb7aTgEjJ8u%2FHMbJ0%2Bi%2FT
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/my/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:17:02 GMT
Content-Type: text/html; charset=utf-8
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
Pragma: no-cache
Expires:
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="en" xml:lang="en">
<head>
<title>Moodle-Demo: Calendar: Detailed month view: October 2024 | Moodle-Demo</title>
<link rel="shortcut icon" href="https://
...[SNIP]...
```

```
</script>
<script src="https://cdn.jsdelivr.net/npm/mathjax@2.7.9/MathJax.js?delayStartupUntil=configured"></script>
...[SNIP]...
<div>Powered by <a href="https://moodle.com">Moodle</a>
...[SNIP]...
```

---

9. Cross-domain script include

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/**

Issue detail

The response dynamically includes the following script from another domain:

- https://cdn.jsdelivr.net/npm/mathjax@2.7.9/MathJax.js?delayStartupUntil=configured

This issue was found in multiple locations under the reported path.

Issue background

When an application includes a script from an external domain, this script is executed by the browser within the security context of the invoking application. The script can therefore do anything that the application's own scripts can do, such as accessing application data and performing actions within the context of the current user.

If you include a script from an external domain, then you are trusting that domain with the data and functionality of your application, and you are trusting the domain's own security to prevent an attacker from modifying the script to perform malicious actions within your application.

Issue remediation

Scripts should ideally not be included from untrusted domains. Applications that rely on static third-party scripts should consider using Subresource Integrity to make browsers verify them, or copying the contents of these scripts onto their own domain and including them from there. If that is not possible (e.g. for licensing reasons) then consider reimplementing the script's functionality within application code.

References

- Subresource Integrity

Vulnerability classifications

- CWE-829: Inclusion of Functionality from Untrusted Control Sphere

Request 1

```
GET /?lang=am HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
```

```
exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=9rdu4op2ra47d6nu7ava6po22t
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:15:38 GMT
Content-Type: text/html; charset=utf-8
Content-Language: am
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0, no-transform
Pragma: no-cache
Expires: Mon, 20 Aug 1969 09:23:00 GMT
Last-Modified: Mon, 28 Oct 2024 10:15:38 GMT
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="am" xml:lang="am">
<head>
<title>..... ..... | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/image.ph
...[SNIP]...
</script>
<script src="https://cdn.jsdelivr.net/npm/mathjax@2.7.9/MathJax.js?delayStartupUntil=configured"></script>
...[SNIP]...
```

Request 2

```
GET /?lang=te HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=1ensnt2s4fr4lqv0ipc5do1gdn
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 2

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:15:45 GMT
Content-Type: text/html; charset=utf-8
Content-Language: te
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0, no-transform
Pragma: no-cache
Expires: Mon, 20 Aug 1969 09:23:00 GMT
Last-Modified: Mon, 28 Oct 2024 10:15:45 GMT
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="te" xml:lang="te">
<head>
<title>..... | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/image.php/bo
...[SNIP]...
</script>
<script src="https://cdn.jsdelivr.net/npm/mathjax@2.7.9/MathJax.js?delayStartupUntil=configured"></script>
...[SNIP]...
```

Request 3

```
GET / HTTP/1.1
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 3

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:15:27 GMT
Content-Type: text/html; charset=utf-8
Set-Cookie: MoodleSession=hlkac3dvv4se0877uq0h6f122g; path=/; secure; SameSite=None
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0, no-transform
Pragma: no-cache
Expires: Mon, 20 Aug 1969 09:23:00 GMT
Last-Modified: Mon, 28 Oct 2024 10:15:27 GMT
```

```
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="en" xml:lang="en">
<head>
<title>Home | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/image.php/boost/them
...[SNIP]...
</script>
<script src="https://cdn.jsdelivr.net/npm/mathjax@2.7.9/MathJax.js?delayStartupUntil=configured"></script>
...[SNIP]...
```

---

10. Frameable response (potential Clickjacking)

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/**

Issue detail

This issue was found in multiple locations under the reported path.

Issue background

If a page fails to set an appropriate X-Frame-Options or Content-Security-Policy HTTP header, it might be possible for a page controlled by an attacker to load it within an iframe. This may enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defenses against cross-site request forgery, and may result in unauthorized actions.

Note that some applications attempt to prevent these attacks from within the HTML page itself, using "framebusting" code. However, this type of defense is normally ineffective and can usually be circumvented by a skilled attacker.

You should determine whether any functions accessible within frameable pages can be used by application users to perform any sensitive actions within the application.

Issue remediation

To effectively prevent framing attacks, the application should return a response header with the name **X-Frame-Options** and the value **DENY** to prevent framing altogether, or the value **SAMEORIGIN** to allow framing only by pages on the same origin as the response itself. Note that the SAMEORIGIN header can be partially bypassed if the application itself can be made to frame untrusted websites.

References

- Web Security Academy: Clickjacking
- X-Frame-Options

Vulnerability classifications

- CWE-693: Protection Mechanism Failure
- CAPEC-103: Clickjacking

Request 1

```
GET /?lang=am HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=9rdu4op2ra47d6nu7ava6po22t
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:15:38 GMT
Content-Type: text/html; charset=utf-8
Content-Language: am
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0, no-transform
Pragma: no-cache
Expires: Mon, 20 Aug 1969 09:23:00 GMT
Last-Modified: Mon, 28 Oct 2024 10:15:38 GMT
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="am" xml:lang="am">
<head>
<title>..... ..... | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/image.ph
...[SNIP]...
```

Request 2

```
GET / HTTP/1.1
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
```

```
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 2

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:15:27 GMT
Content-Type: text/html; charset=utf-8
Set-Cookie: MoodleSession=hlkac3dvv4se0877uq0h6f122g; path=/; secure; SameSite=None
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0, no-transform
Pragma: no-cache
Expires: Mon, 20 Aug 1969 09:23:00 GMT
Last-Modified: Mon, 28 Oct 2024 10:15:27 GMT
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="en" xml:lang="en">
<head>
<title>Home | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/image.php/boost/them
...[SNIP]...
```

Request 3

```
GET /?lang=te HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=1ensnt2s4fr4lqv0ipc5do1gdn
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 3

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:15:45 GMT
Content-Type: text/html; charset=utf-8
Content-Language: te
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: no-store, no-cache, must-revalidate
```

```
Cache-Control: post-check=0, pre-check=0, no-transform
Pragma: no-cache
Expires: Mon, 20 Aug 1969 09:23:00 GMT
Last-Modified: Mon, 28 Oct 2024 10:15:45 GMT
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="te" xml:lang="te">
<head>
<title>..... | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/image.php/bo
...[SNIP]...
```

---

11. DOM data manipulation (DOM-based)

There are 2 instances of this issue:

- /login/index.php
- /login/index.php

Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM data manipulation arises when a script writes controllable data to a field within the DOM that is used within the visible UI or client-side application logic. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will modify the appearance or behavior of the client-side UI. An attacker may be able to leverage this to perform virtual defacement of the application, or possibly to induce the user to perform unintended actions.

Burp Suite automatically identifies this issue using dynamic and static code analysis. Static analysis can lead to false positives that are not actually exploitable. If Burp Scanner has not provided any evidence resulting from dynamic analysis, you should review the relevant code and execution paths to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Issue remediation

The most effective way to avoid DOM-based DOM data manipulation vulnerabilities is not to dynamically write to DOM data fields any data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from being stored. In general, this is best achieved by using a whitelist of permitted values.

References

- Web Security Academy: DOM data manipulation

Vulnerability classifications

- CWE-20: Improper Input Validation
- CAPEC-153: Input Data Manipulation

11.1. https://moodledemo.eabyas.in:1443/login/index.php

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/login/index.php**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.hash** and passed to **the 'value' property of a DOM element**.

Request 1

```
GET /login/index.php HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=8djrcfm00dkje2pmgvc4mtjjo1
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:15:48 GMT
Content-Type: text/html; charset=utf-8
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
Pragma: no-cache
Expires:
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="en" xml:lang="en">
<head>
<title>Log in to the site | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/image.
...[SNIP]...
```

```
<script>document.getElementById('anchor').value = location.hash;</script>
...[SNIP]...
```

Static analysis

Data is read from **location.hash** and passed to **the 'value' property of a DOM element** via the following statement:

- `document.getElementById('anchor').value = location.hash;`

Dynamic analysis

Data is read from **location.hash** and passed to **input.value**.

The following value was injected into the source and reached the sink without any modification:

```
#okb45bhat9=okb45bhat9%27%22`'"/okb45bhat9/><okb45bhat9/\>ljl9405azo&
```

The stack trace at the source was:

```
at Object.nJKxK (<anonymous>:1:114787)
at Object._0x17d3d0 [as proxiedGetterCallback] (<anonymous>:1:660045)
at get hash [as hash] (<anonymous>:1:246001)
at https://moodledemo.eabyas.in:1443/login/index.php:53:72
```

The stack trace at the sink was:

```
at Object.lXJzh (<anonymous>:1:109484)
at Object.fzjsE (<anonymous>:1:615263)
at HTMLInputElement.set [as value] (<anonymous>:1:616030)
at https://moodledemo.eabyas.in:1443/login/index.php:53:61
```

11.2. https://moodledemo.eabyas.in:1443/login/index.php

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/login/index.php**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.hash** and passed to **the 'value' property of a DOM element**.

Request 1

```
GET /login/index.php HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=8djrcfm00dkje2pmgvc4mtjjo1
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:15:48 GMT
Content-Type: text/html; charset=utf-8
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
Pragma: no-cache
Expires:
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="en" xml:lang="en">
<head>
<title>Log in to the site | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/theme/image.
...[SNIP]...
<script>document.getElementById('anchor').value = location.hash;</script>
...[SNIP]...
```

Static analysis

Data is read from **location.hash** and passed to **the 'value' property of a DOM element** via the following statement:

- `document.getElementById('anchor').value = location.hash;`

Dynamic analysis

Data is read from **location.hash** and passed to **input.value**.

The following value was injected into the source and reached the sink without any modification:

```
#okb45bhat9=okb45bhat9%27%22`'"/okb45bhat9/><okb45bhat9/\>ljl9405azo&
```

The stack trace at the source was:

```
at Object.nJKxK (<anonymous>:1:114787)
at Object._0x17d3d0 [as proxiedGetterCallback] (<anonymous>:1:660045)
at get hash [as hash] (<anonymous>:1:246001)
at https://moodledemo.eabyas.in:1443/login/index.php:53:72
```

The stack trace at the sink was:

```
at Object.lXJzh (<anonymous>:1:109484)
at Object.fzjsE (<anonymous>:1:615263)
at HTMLInputElement.set [as value] (<anonymous>:1:616030)
at https://moodledemo.eabyas.in:1443/login/index.php:53:61
```

---

12. Email addresses disclosed

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/lib/javascript.php/1728980143/lib/requirejs/jquery-private.js**

Issue detail

The following email address was disclosed in the response:

- damyon@moodle.com

Issue background

The presence of email addresses within application responses does not necessarily constitute a security vulnerability. Email addresses may appear intentionally within contact information, and many applications (such as web mail) include arbitrary third-party email addresses within their core content.

However, email addresses of developers and other individuals (whether appearing on-screen or hidden within page source) may disclose information that is useful to an attacker; for example, they may represent usernames that can be used at the application's login, and they may be used in social engineering attacks against the organization's personnel. Unnecessary or excessive disclosure of email addresses may also lead to an increase in the volume of spam email received.

Issue remediation

Consider removing any email addresses that are unnecessary, or replacing personal addresses with anonymous mailbox addresses (such as helpdesk@example.com).

To reduce the quantity of spam sent to anonymous mailbox addresses, consider hiding the email address and instead providing a form that generates the email server-side, protected by a CAPTCHA if necessary.

References

- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-200: Information Exposure
- CAPEC-37: Retrieve Embedded Sensitive Data

Request 1

```
GET /lib/javascript.php/1728980143/lib/requirejs/jquery-private.js HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: */*
```

```
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=hlkac3dvv4se0877uq0h6f122g
Referer: https://moodledemo.eabyas.in:1443/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:15:28 GMT
Content-Type: application/javascript; charset=utf-8
Etag: "0c6e7143c267058f87b4bbcc6424d3fd99119007"
Content-Disposition: inline; filename="javascript.php"
Last-Modified: Tue, 15 Oct 2024 08:15:52 GMT
Expires: Sun, 26 Jan 2025 10:15:28 GMT
Pragma:
Cache-Control: public, max-age=7776000, immutable
Accept-Ranges: none
Vary: Accept-Encoding


/**
* This module depends on the real jquery - and returns the non-global version of it.
*
* @module jquery-private
* @package core
* @copyright 2015 Damyon Wiese <damyon@moodle.com>
*
...[SNIP]...
```

---

13. Private IP addresses disclosed

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/user/profile.php**

Issue detail

The following RFC 1918 IP address was disclosed in the response:

- 192.168.20.101

Issue background

RFC 1918 specifies ranges of IP addresses that are reserved for use in private networks and cannot be routed on the public Internet. Although various methods exist by which an attacker can determine the public IP addresses in use by an organization, the private addresses used internally cannot usually be determined in the same ways.

Discovering the private addresses used within an organization can help an attacker in carrying out network-layer attacks aiming to penetrate the organization's internal infrastructure.

Issue remediation

There is not usually any good reason to disclose the internal IP addresses used within an organization's infrastructure. If these are being returned in service banners or debug messages, then the relevant services should be configured to mask the private addresses. If they are being used to track back-end servers for load balancing purposes, then the addresses should be rewritten with innocuous identifiers from which an attacker cannot infer any useful information about the infrastructure.

References

- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-200: Information Exposure
- CAPEC-37: Retrieve Embedded Sensitive Data

Request 1

```
GET /user/profile.php HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=ash87o9sok8s2kk9rrvojoldmc; MOODLEID1_=sodium%3AGCYo17XFoaMB9%2FHh38mwdC6rsUqnVlw9O%2BiXEDi%2FBebDw4fRfC4pwx2oDlgi
Upgrade-Insecure-Requests: 1
Referer: https://moodledemo.eabyas.in:1443/my/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:16:46 GMT
Content-Type: text/html; charset=utf-8
Content-Language: en
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-Ua-Compatible: IE=edge
Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
Pragma: no-cache
Expires:
Accept-Ranges: none

<!DOCTYPE html>

<html dir="ltr" lang="en" xml:lang="en">
```

```
<head>
<title>Admin User: Public profile | Moodle-Demo</title>
<link rel="shortcut icon" href="https://moodledemo.eabyas.in:1443/them
...[SNIP]...
<a href="https://moodledemo.eabyas.in:1443/iplookup/index.php?ip=192.168.20.101&amp;user=2">192.168.20.101</a>
...[SNIP]...
```

---

14. Cacheable HTTPS response

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/lib/ajax/service-nologin.php**

Issue detail

This issue was found in multiple locations under the reported path.

Issue background

Unless directed otherwise, browsers may store a local cached copy of content received from web servers. Some browsers, including Internet Explorer, cache content accessed via HTTPS. If sensitive information in application responses is stored in the local cache, then this may be retrieved by other users who have access to the same computer at a future time.

Issue remediation

Applications should return caching directives instructing browsers not to store local copies of any sensitive data. Often, this can be achieved by configuring the web server to prevent caching for relevant paths within the web root. Alternatively, most web development platforms allow you to control the server's caching directives from within individual scripts. Ideally, the web server should return the following HTTP headers in all responses containing sensitive content:

- Cache-control: no-store
- Pragma: no-cache

References

- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-524: Information Exposure Through Caching
- CWE-525: Information Exposure Through Browser Caching
- CAPEC-37: Retrieve Embedded Sensitive Data

Request 1

```
GET /lib/ajax/service-nologin.php?
info=core_output_load_fontawesome_icon_system_map&cachekey=1728980143&args=%5B%7B%22index%22%3A0%2C%22methodname%22%3A%22core_output_load_fontawesome_icon_system_map%22%2C%22args%22%3A%7B%22themename%22%3A%22boost%22%7D%7D%5D HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
```

```
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=hlkac3dvv4se0877uq0h6f122g
X-Requested-With: XMLHttpRequest
Referer: https://moodledemo.eabyas.in:1443/
Content-Type: application/json
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:15:29 GMT
Content-Type: application/json; charset=utf-8
Expires: Sun, 26 Jan 2025 10:15:29 GMT
Pragma:
Cache-Control: public, max-age=7776000, immutable
Accept-Ranges: none

[{"error":false,"data":[{"component":"core","pix":"docs","to":"fa fa-circle-info"},{"component":"core","pix":"book","to":"fa fa-book"},
{"component":"core","pix":"help","to":"fa fa-circle-question text
...[SNIP]...
```

Request 2

```
GET /lib/ajax/service-nologin.php?
info=core_output_load_fontawesome_icon_system_map&cachekey=1728980143&args=%5B%7B%22index%22%3A0%2C%2
2methodname%22%3A%22core_output_load_fontawesome_icon_system_map%22%2C%22args%22%3A%7B%22themena
me%22%3A%22boost%22%7D%7D%5D HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=t5q2m2u0mvlk7npm6c4dafve60
X-Requested-With: XMLHttpRequest
Referer: https://moodledemo.eabyas.in:1443/
Content-Type: application/json
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 2

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:15:42 GMT
Content-Type: application/json; charset=utf-8
Expires: Sun, 26 Jan 2025 10:15:42 GMT
Pragma:
```

```
Cache-Control: public, max-age=7776000, immutable
Accept-Ranges: none

[{"error":false,"data":[{"component":"core","pix":"docs","to":"fa fa-circle-info"},{"component":"core","pix":"book","to":"fa fa-book"},
{"component":"core","pix":"help","to":"fa fa-circle-question text
...[SNIP]...
```

Request 3

```
GET /lib/ajax/service-nologin.php?
info=core_output_load_template_with_dependencies&cachekey=1728980143&args=%5B%7B%22index%22%3A0%2C%22m
ethodname%22%3A%22core_output_load_template_with_dependencies%22%2C%22args%22%3A%7B%22component%22
%3A%22core%22%2C%22template%22%3A%22loading%22%2C%22themename%22%3A%22boost%22%2C%22lang%22
%3A%22en%22%7D%7D%5D HTTP/2
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: MoodleSession=flgtj6vgus994pm6hm6jcquhub;
MOODLEID1_=sodium%3AbVCgXNGSinlR4DnRlQYDlPnKhrWWZdbi6VZltkgb8G191Ggv9dRLdA%2FkoTAF
X-Requested-With: XMLHttpRequest
Referer: https://moodledemo.eabyas.in:1443/?redirect=0
Content-Type: application/json
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 3

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 28 Oct 2024 10:16:05 GMT
Content-Type: application/json; charset=utf-8
Expires: Sun, 26 Jan 2025 10:16:05 GMT
Pragma:
Cache-Control: public, max-age=7776000, immutable
Accept-Ranges: none

[{"error":false,"data":{"templates":[{"component":"core","name":"loading","value":"\n\n<span class=\"loading-icon icon-no-
margin\">{{#pix}} i\/loading, core, {{#str}} loading {{\/str}} {{\/pix}}<\/spa
...[SNIP]...
```

---

15. HTML does not specify charset

There are 2 instances of this issue:

- /
- /robots.txt

Issue description

If a response states that it contains HTML content but does not specify a character set, then the browser may analyze the HTML and attempt to determine which character set it appears to be using. Even if the majority of the HTML actually employs a standard character set such as UTF-8, the presence of non-standard characters anywhere in the response may cause the browser to interpret the content using a different character set. This can have unexpected results, and can lead to cross-site scripting vulnerabilities in which non-standard encodings like UTF-7 can be used to bypass the application's defensive filters.

In most cases, the absence of a charset directive does not constitute a security flaw, particularly if the response contains static content. You should review the contents of affected responses, and the context in which they appear, to determine whether any vulnerability exists.

Issue remediation

For every response containing HTML content, the application should include within the Content-type header a directive specifying a standard recognized character set, for example **charset=ISO-8859-1**.

Vulnerability classifications

- CWE-16: Configuration
- CWE-436: Interpretation Conflict

15.1. http://moodledemo.eabyas.in:1443/

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**http://moodledemo.eabyas.in:1443**
Path:	**/**

Request 1

```
GET / HTTP/1.1
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="112", "Chromium";v="112"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 400 Bad Request
Server: nginx
Date: Mon, 28 Oct 2024 10:15:26 GMT
```

```
Content-Type: text/html
Content-Length: 650
Connection: close

<html>
<head><title>400 The plain HTTP request was sent to HTTPS port</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<center>The plain HTTP request was sent to HTTPS port</center>
...[SNIP]...
```

15.2. http://moodledemo.eabyas.in:1443/robots.txt

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**http://moodledemo.eabyas.in:1443**
Path:	**/robots.txt**

Request 1

```
GET /robots.txt HTTP/1.1
Host: moodledemo.eabyas.in:1443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 400 Bad Request
Server: nginx
Date: Mon, 28 Oct 2024 10:15:30 GMT
Content-Type: text/html
Content-Length: 650
Connection: close

<html>
<head><title>400 The plain HTTP request was sent to HTTPS port</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<center>The plain HTTP request was sent to HTTPS port</center>
...[SNIP]...
```

---

16. TLS certificate

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://moodledemo.eabyas.in:1443**
Path:	**/**

Issue detail

The server presented a valid, trusted TLS certificate. This issue is purely informational.

The server presented the following certificates:

Server certificate

Issued to:	*.eabyas.in, eabyas.in
Issued by:	Go Daddy Secure Certificate Authority - G2
Valid from:	Tue Jul 02 05:59:25 PDT 2024
Valid to:	Wed Jul 02 22:58:06 PDT 2025

Certificate chain #1

Issued to:	Go Daddy Secure Certificate Authority - G2
Issued by:	Go Daddy Root Certificate Authority - G2
Valid from:	Tue May 03 00:00:00 PDT 2011
Valid to:	Sat May 03 00:00:00 PDT 2031

Certificate chain #2

Issued to:	Go Daddy Root Certificate Authority - G2
Issued by:	Go Daddy Class 2 Certification Authority
Valid from:	Tue Dec 31 23:00:00 PST 2013
Valid to:	Fri May 30 00:00:00 PDT 2031

Certificate chain #3

Issued to:	Go Daddy Class 2 Certification Authority
Issued by:	Go Daddy Class 2 Certification Authority
Valid from:	Tue Jun 29 10:06:20 PDT 2004
Valid to:	Thu Jun 29 10:06:20 PDT 2034

Certificate chain #4

Issued to:	Go Daddy Class 2 Certification Authority
Issued by:	Go Daddy Class 2 Certification Authority
Valid from:	Tue Jun 29 10:06:20 PDT 2004
Valid to:	Thu Jun 29 10:06:20 PDT 2034

Issue background

TLS (or SSL) helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity. To serve this purpose, the server must present an TLS certificate that is valid for the server's hostname, is issued by a trusted authority and is valid for the current date. If any one of these requirements is not met, TLS connections to the server will not provide the full protection for which TLS is designed.

It should be noted that various attacks exist against TLS in general, and in the context of HTTPS web connections in particular. It may be possible for a determined and suitably-positioned attacker to compromise TLS connections without user detection even when a valid TLS certificate is used.

References

- SSL/TLS Configuration Guide

Vulnerability classifications

- CWE-295: Improper Certificate Validation
- CWE-326: Inadequate Encryption Strength
- CWE-327: Use of a Broken or Risky Cryptographic Algorithm

Report generated by Burp Suite web vulnerability scanner v2023.3.3, at Mon Oct 28 06:16:29 PDT 2024.