Sri Lanka Institute of Information Technology

Cyber Security Assignment (2025)

Insecure Design

Bug Bounty Report- 01

IT23363366

TABLE OF CONTENT

1. Title

Report Title: Insecure Design
Reported By: Raahim Mahmooth
Platform: https://yeswehack.com/
Tested On: https://www.bookbeat.com/

2. Scope & Objective

The objective of this assessment was to evaluate the application's design and identify flaws that could lead to potential security issues even if the implementation appears correct. The focus was on identifying missing or weakly implemented security controls, particularly in authentication mechanisms, password policies, and API structures. This test aims to highlight insecure design patterns that might allow attackers to exploit the system or escalate privileges.

3. Enumeration and Reconnaissance

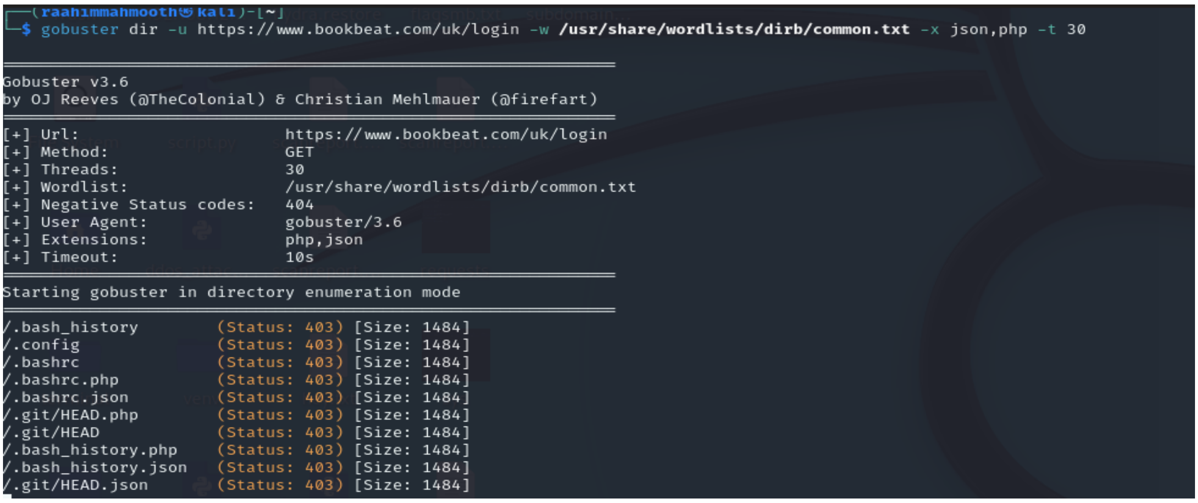
3.1 Tools Used

- Manual credential spraying on authentication endpoints
- Burp Suite for intercepting and modifying requests
- Postman for testing API endpoints
- Gobuster for directory and endpoint enumeration

3.2 Steps Taken

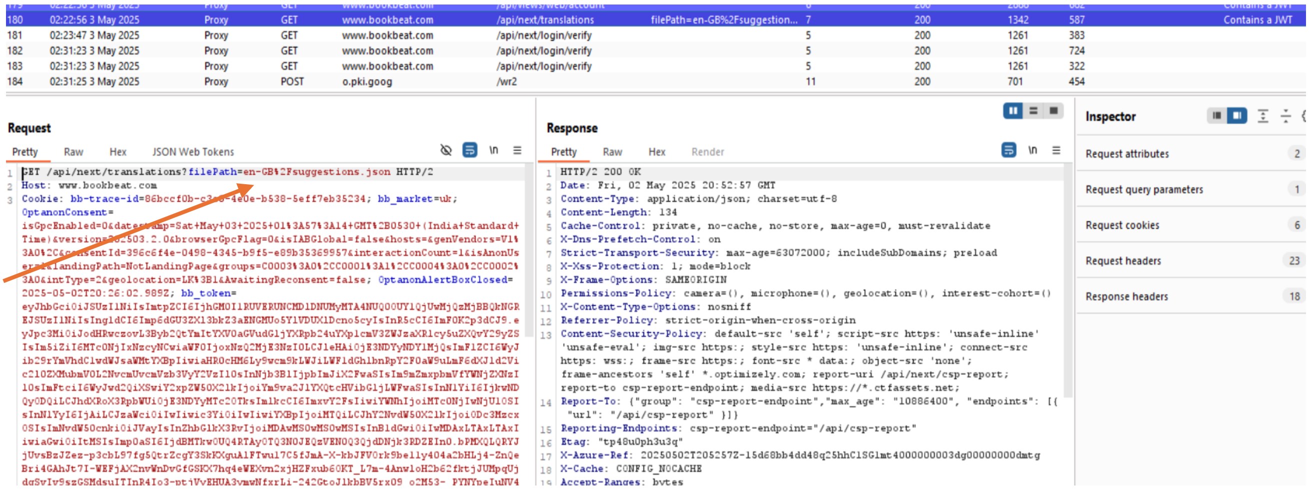
2.2.1 Assessed insecure API design. Gobuster enumeration returned no results. Manually identified the following endpoint using Burp Suite:

`GET /api/next/translations?filePath=en-GB%2Fbreadcrumbs.json`



```
┌──(raahimmahmooth㉿kali)-[~]
└─$ gobuster dir -u https://www.bookbeat.com/uk/login -w /usr/share/wordlists/dirb/common.txt -x json,php -t 30

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://www.bookbeat.com/uk/login
[+] Method:                  GET
[+] Threads:                 30
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,json
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.bash_history        (Status: 403) [Size: 1484]
/.config              (Status: 403) [Size: 1484]
/.bashrc              (Status: 403) [Size: 1484]
/.bashrc.php          (Status: 403) [Size: 1484]
/.bashrc.json         (Status: 403) [Size: 1484]
/.git/HEAD.php        (Status: 403) [Size: 1484]
/.git/HEAD            (Status: 403) [Size: 1484]
/.bash_history.php    (Status: 403) [Size: 1484]
/.bash_history.json   (Status: 403) [Size: 1484]
/.git/HEAD.json       (Status: 403) [Size: 1484]
```

Manual identification

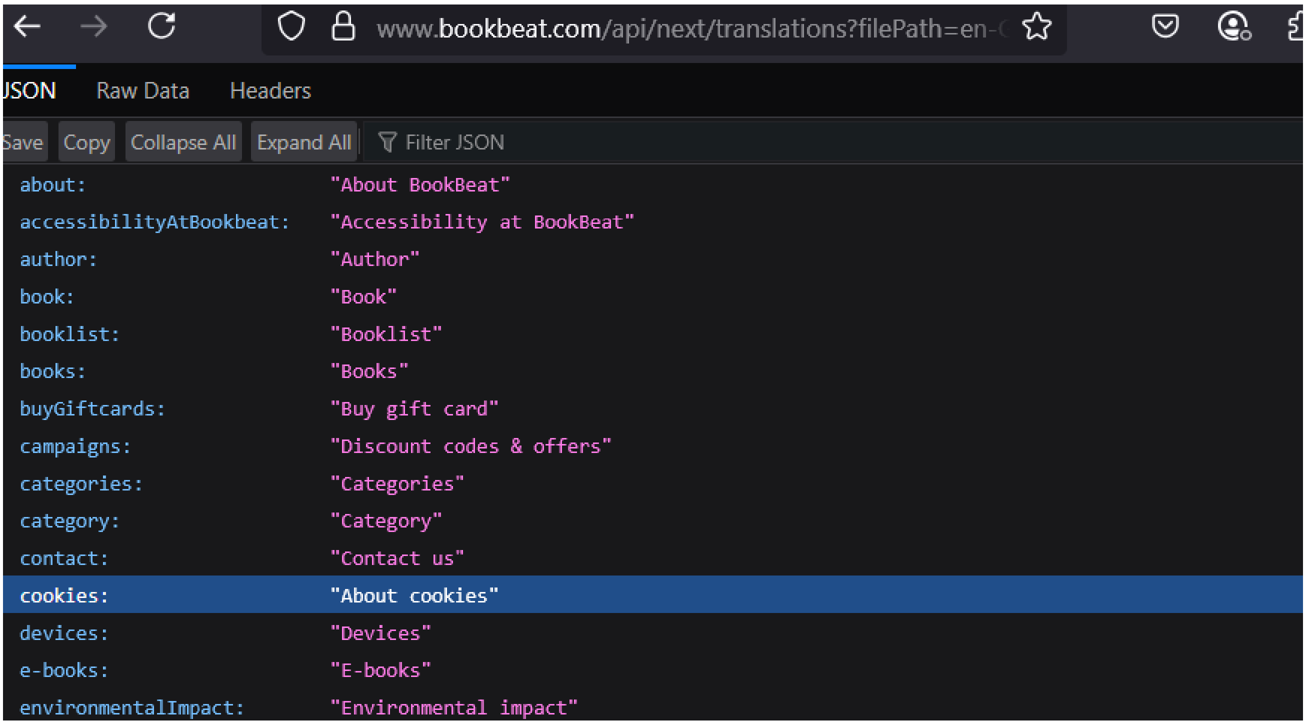


180	02:22:56 3 May 2025	Proxy	GET	www.bookbeat.com	/api/next/translations	filePath=en-GB%2Fsuggestion...	7	200	1342	587	Contains a JWT
181	02:23:47 3 May 2025	Proxy	GET	www.bookbeat.com	/api/next/login/verify		5	200	1261	383	
182	02:31:23 3 May 2025	Proxy	GET	www.bookbeat.com	/api/next/login/verify		5	200	1261	724	
183	02:31:23 3 May 2025	Proxy	GET	www.bookbeat.com	/api/next/login/verify		5	200	1261	322	
184	02:31:25 3 May 2025	Proxy	POST	o.pki.goog	/wr2		11	200	701	454	

```
GET /api/next/translations?filePath=en-GB%2Fsuggestions.json HTTP/2
Host: www.bookbeat.com
Cookie: bb-trace-id=86bccf0b-c3[illegible]-4e0e-b538-5eff7eb35234; bb_market=uk;
OptanonConsent=
isGpcEnabled=0&datestamp=Sat+May+03+2025+01%3A57%3A14+GMT%2B0530+(India+Standard+
Time)&version=202503.2.0&browserGpcFlag=0&isIABGlobal=false&hosts=&genVendors=V1%
3A0%2C&consentId=396c6f4e-0498-4345-b9f5-e89b35369957&interactionCount=1&isAnonUs
er=1&landingPath=NotLandingPage&groups=C0003%3A0%2CC0001%3A1%2CC0004%3A0%2CC0002%
3A0&intType=2&geolocation=LK%3B1&AwaitingReconsent=false; OptanonAlertBoxClosed=
2025-05-02T20:26:02.989Z; bb_token=
eyJhbGci0iJSUzI1NiIsImtpZCI6IjhGM0I1RUVERUNCMD1DNUMyMTA4NUQ0OUY1QjUwMjQzMjBBQkNGR
EJSUzI1NiIsIngldCI6Imp6dGU3ZX13bkZ3aENGMUo5Y1VDUX1Dcno5cyIsInR5cCI6ImF0K2p3dCJ9.e
yJpc3Mi0iJodHRwczovL3Byb2QtYmItYXV0aGVudGljYXRpb24uYXplcmV3ZWJzaXRlcy5uZXQvY29yZS
IsIm5iZiI6MTc0NjIxNzcyNCwiaWF0IjoxNzQ2MjE3NzI0LCJleHAi0jE3NDYyNDY1MjQsImF1ZCI6WyJ
ib29rYmVhdClwdWJsaWMtYXBpIiwiaHR0cHM6Ly9wcm9kLWJiLWF1dGhlbnRpY2F0aW9uLmF6dXJld2Vi
c210ZXMubmV0L2NvcmUvcmVzb3VyY2VzIl0sInNjb3BlIjpbImJiX2FwaSIsIm9mZmxpbmVfYWNjZXNzI
l0sImFtciI6WyJwd2QiXSwiY2xpZW50X2lkIjoiYm9va2J1YXQtcHVibGljLWFwaSIsInN1YiI6IjkwND
Qy0DQiLCJhdXRoX3RpbWUi0jE3NDYyMTc2OTksImlkcCI6ImxvY2FsIiwiYWNhIjoiMTc0NjIwNjU10SI
sInN1YyI6IjAiLCJzaWci0iIwIiwic3Yi0iIwIiwiYXBpIjoiMTQiLCJhY2NvdW50X2lkIjoi0Dc3Mzcx
0SIsImNvdW50cnki0iJVayIsInZhbGlkX3RvIjoiMDAwMS0wMS0wMSIsInBldGwi0iIwMDAxLTAxLTAxI
iwiaGwi0iItMSIsImp0aSI6IjdBMTkw0UQ4RTAy0TQ3N0JEQzVEN0Q3QjdDNjk3RDZEIn0.bPMXQLQRYJ
jUvsBzJZez-p3cbL97fg5QtrZcgY3SkKXguAlFTwul7C5fJmA-X-kbJFV0rk9belly404a2bHLj4-ZnQe
Bri4GAhJt7I-WEFjAX2nvWnDvGfGSKX7hq4eWEXvn2xjHZFxub60KT_L7m-4AnwloH2b62fktjJUMpqUj
dgSvIv9szGSMdsuITInR4Io3-ptjVvEHUA3vmwNfxrLi-242GtoJlkbBV5rx09 o2M53- PYNYpeIuNV4
```

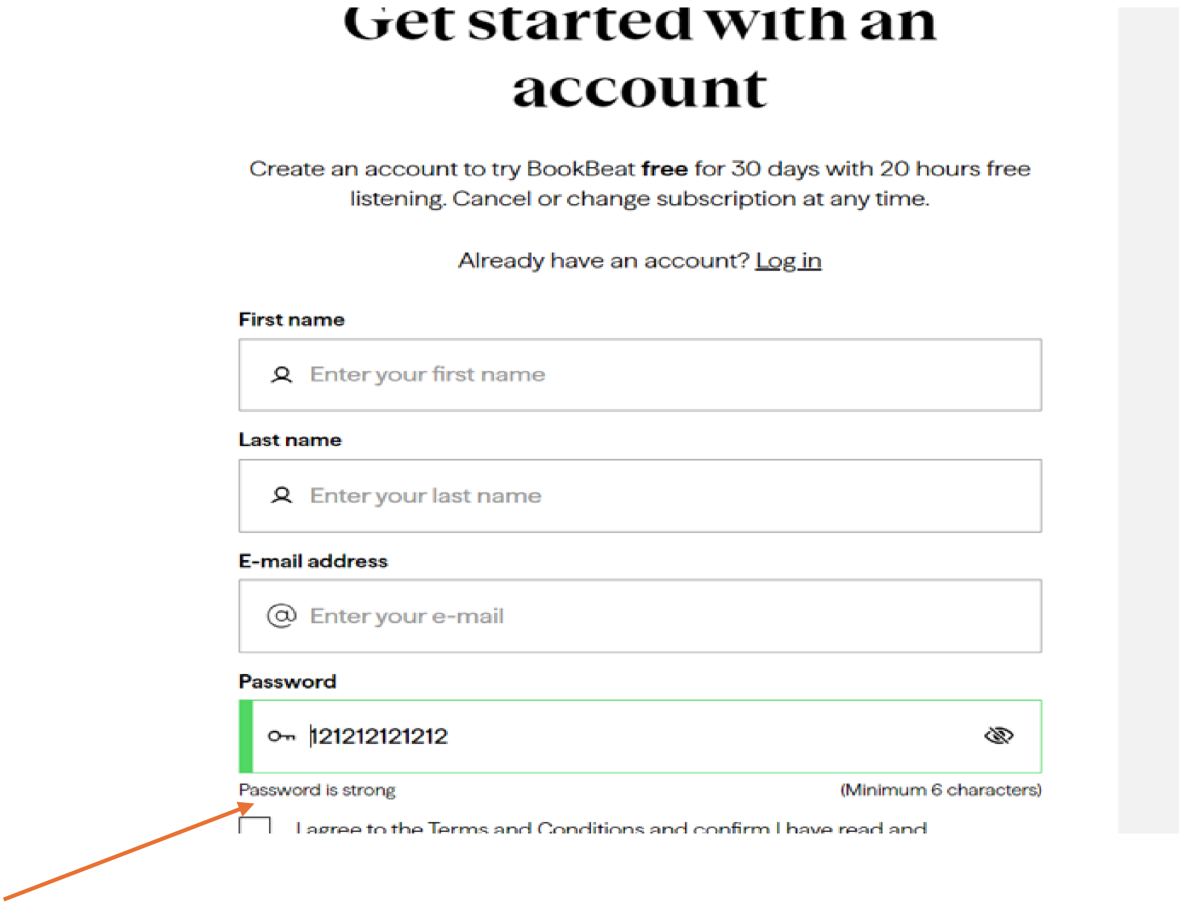
```
HTTP/2 200 OK
Date: Fri, 02 May 2025 20:52:57 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 134
Cache-Control: private, no-cache, no-store, max-age=0, must-revalidate
X-Dns-Prefetch-Control: on
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
X-Xss-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Permissions-Policy: camera=(), microphone=(), geolocation=(), interest-cohort=()
X-Content-Type-Options: nosniff
Referrer-Policy: strict-origin-when-cross-origin
Content-Security-Policy: default-src 'self'; script-src https: 'unsafe-inline'
'unsafe-eval'; img-src https:; style-src https: 'unsafe-inline'; connect-src
https: wss:; frame-src https:; font-src * data:; object-src 'none';
frame-ancestors 'self' *.optimizely.com; report-uri /api/next/csp-report;
report-to csp-report-endpoint; media-src https://*.ctfassets.net;
Report-To: {"group": "csp-report-endpoint","max_age": "10886400", "endpoints": [{
 "url": "/api/csp-report" }]}
Reporting-Endpoints: csp-report-endpoint="/api/csp-report"
Etag: "tp48u0ph3u3q"
X-Azure-Ref: 20250502T205257Z-15d68bb4dd48q25hhC1SG1mt4000000003dg00000000dmtg
X-Cache: CONFIG_NOCACHE
Accept-Ranges: bytes
```

Request attributes	2
Request query parameters	1
Request cookies	6
Request headers	23
Response headers	18



```
about:                      "About BookBeat"
accessibilityAtBookbeat:    "Accessibility at BookBeat"
author:                     "Author"
book:                       "Book"
booklist:                   "Booklist"
books:                      "Books"
buyGiftcards:               "Buy gift card"
campaigns:                  "Discount codes & offers"
categories:                 "Categories"
category:                   "Category"
contact:                    "Contact us"
cookies:                    "About cookies"
devices:                    "Devices"
e-books:                    "E-books"
environmentalImpact:        "Environmental impact"
```

__3.2.2__ Tested for logical flaws in authentication, including weak password policy enforcement. Identifying the application only enforces minimum length, not complexity



Get started with an account

Create an account to try BookBeat **free** for 30 days with 20 hours free listening. Cancel or change subscription at any time.

Already have an account? Log in

First name

Enter your first name

Last name

Enter your last name

E-mail address

Enter your e-mail

Password

121212121212

Password is strong (Minimum 6 characters)

□ I agree to the Terms and Conditions and confirm I have read and

4. Vulnerability Description

Insecure design represents systemic flaws in application architecture and the absence of necessary security controls. This vulnerability arises from design-level oversights, such as weak password policies, lack of access control validation, and insecure API structures. Insecure design **cannot be mitigated through implementation alone**, as the foundational security components are either missing or inadequate. (OWASP Top 10: A04 – Insecure Design-Critical vulnerability)

5. Affected Component

- API endpoint: `GET /api/next/translations?filePath=en-GB%2Fbreadcrumbs.json`
- Login page
- Password reset and registration mechanisms

6. Impact Assessment

Applications suffering from insecure design are highly susceptible to a wide range of attacks. Common exploitation scenarios include:

- **Broken Access Control:** Weak or missing role validation can allow unauthorized access to sensitive features.
- **Account Takeover via Weak Authentication:** Weak password policies combined with insecure login mechanisms (such as **login without password**) can allow attackers to access user accounts **if email accounts are compromised**(***single point of failure***).
- **API Misuse or Abuse:** Poorly designed endpoints with insecure input handling (e.g., ***unvalidated file paths or insecure methods***) can be leveraged for attacks like Path Traversal, SSRF, or information disclosure.
- **Bypass of CAPTCHA or Rate-Limiting Controls:** Without strong validation mechanisms, brute-force attacks and credential stuffing become feasible.

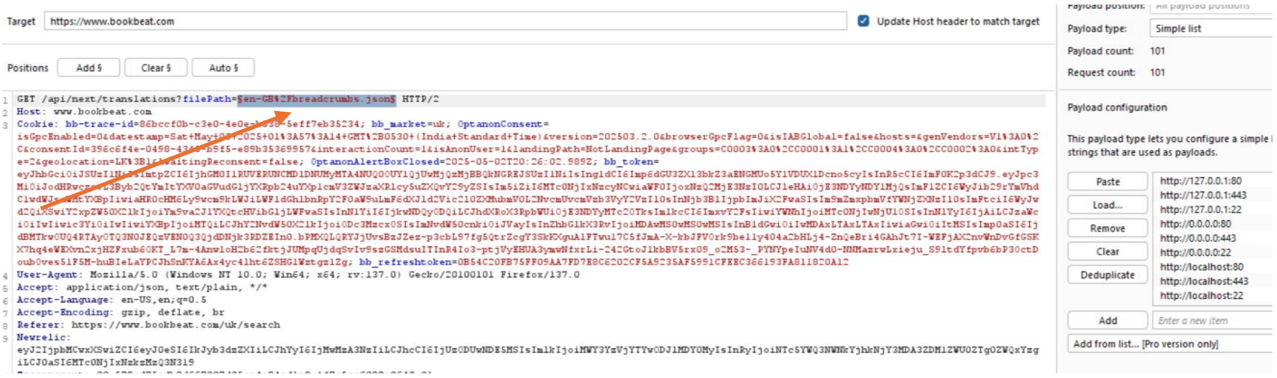
The design flaws *in Book beat's* authentication and API components can lead to account compromise, unauthorized data access, and potential full system breaches under targeted attacks

7. Proof of Concept (PoC)

1.0 – API Endpoint Analysis for any kind of insecure designs

Found API endpoint:*`GET /api/next/translations?filePath=en-GB%2Fbreadcrumbs.json`*

- **Tested for potential SSRF**-like behavior using burpsuit.



Target: https://www.bookbeat.com

☑ Update Host header to match target

```
GET /api/next/translations?filePath=§en-GB%2Fbreadcrumbs.json§ HTTP/2
Host: www.bookbeat.com
Cookie: bb-trace-id=86bccf0b-c3e0-4e0e-[illegible]-5eff7eb35234; bb_market=uk; OptanonConsent=
isGpcEnabled=0&datestamp=Sat+May+[illegible]+2025+01%3A57%3A14+GMT%2B0530+(India+Standard+Time)&version=202503.2.0&browserGpcFlag=0&isIABGlobal=false&hosts=&genVendors=V1%3A0%2
C&consentId=396c6f4e-0498-434[illegible]-b9f5-e89b35369957&interactionCount=1&isAnonUser=1&landingPath=NotLandingPage&groups=C0003%3A0%2CC0001%3A1%2CC0004%3A0%2CC0002%3A0&intTyp
e=2&geolocation=LK%3B1&[illegible]aitingReconsent=false; OptanonAlertBoxClosed=2025-05-02T20:26:02.989Z; bb_token=
eyJhbGciOiJSUzI1N[illegible]ImtpZCI6IjhGM0I1RUVERUNCMDlDNUMyMTA4NUQ0OUY1QjUwMjQzMjBBQkNGREJSUzI1NiIsIng1dCI6Imp6dGU3ZXl3bkZ3aENGMUo5YlVDUXlDcno5cyIsInR5cCI6ImF0K2p3dCJ9.eyJpc3
MiOiJodHRwcz[illegible]L3Byb2QtYmItYXV0aGVudGljYXRpb24uYXplcmV3ZWJzaXRlcy5uZXQvY29yZSIsIm5iZiI6MTc0NjIxNzcyNCwiaWF0IjoxNzQ2MjE3NzI0LCJleHAiOjE3NDYyNDY1MjQsImF1ZCI6WyJib29rYmVhd
ClwdWJs[illegible]tYXBpIiwiaHR0cHM6Ly9wcm9kLWJiLWF1dGhlbnRpY2F0aW9uLmF6dXJld2Vic2l0ZXMubmV0L2NvcmUvcmVzb3VyY2VzIl0sInNjb3BlIjpbImJiX2FwaSIsIm9mZmxpbmVfYWNjZXNzIl0sImFtciI6WyJw
d2QiXSwiY2xpZW50X2lkIjoiYm9va2JlYXQtcHVibGljLWFwaSIsInN1YiI6IjkwNDQyODQiLCJhdXRoX3RpbWUiOjE3NDYyMTc2OTksImlkcCI6ImxvY2FsIiwiYWNhIjoiMTc0NjIwNjU1OSIsInN1YyI6IjAiLCJzaWc
iOiIwIiwic3YiOiIwIiwiYXBpIjoiMTQiLCJhY2NvdW50X2lkIjoiODc3MzcxOSIsImNvdW50cnkiOiJVayIsInZhbGlkX3RvIjoiMDAwMS0wMS0wMSIsInBldGwiOiIwMDAxLTAxLTAxIiwiaGwiOiItMSIsImp0aSI6Ij
dBMTkw0UQ4RTAyOTQ3NOJEQzVENOQ3QjdDNjk3RDZEIn0.bPMXQLQRYJjUvsBzJZez-p3cbL97fg5QtrZcgY3SkKXguAlFTwul7C5fJmA-X-kbJFV0rk9belly404a2bHLj4-ZnQeBri4GAhJt7I-WEFjAX2nvWnDvGfGSK
X7hq4eWEXvn2xjHZFxub60KT_L7m-4AnwloH2b62fktjJUMpqUjdqSvIv9szGSMdsuITInR4Io3-ptjVyEHUA3ymwNfxrLi-242GtoJlkbBV5rx09_o2M53-_PYNYpeIuNV4d0-NNMazrwLxieju_S91tdYfpvb6bP30ctD
oub0ves51F5M-huBIeLaYPCJhSnKYA6Ax4yc4lht6ZSHGlWztgzlZg; bb_refreshtoken=0B54C20FB75FF09AA7FD7E8C6202CF5A9235AF5991CFEEC366193FA811820A12
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://www.bookbeat.com/uk/search
Newrelic:
eyJ2IjpbMCwxXSwiZCI6eyJ0eSI6IkJyb3dzZXIiLCJhYyI6IjMwMzA3NzIiLCJhcCI6IjUzODUwNDE5MSIsImlkIjoiMWY3YzVjYTYwODJlMDY0MyIsInRyIjoiNTc5YWQ3NWNkYjhkNjY3MDA3ZDM1ZWU0ZTg0ZWQxYzg
iLCJ0aSI6MTc0NjIxNzkzMzQ3N319
```

Payload position: All payload positions

Payload type: Simple list

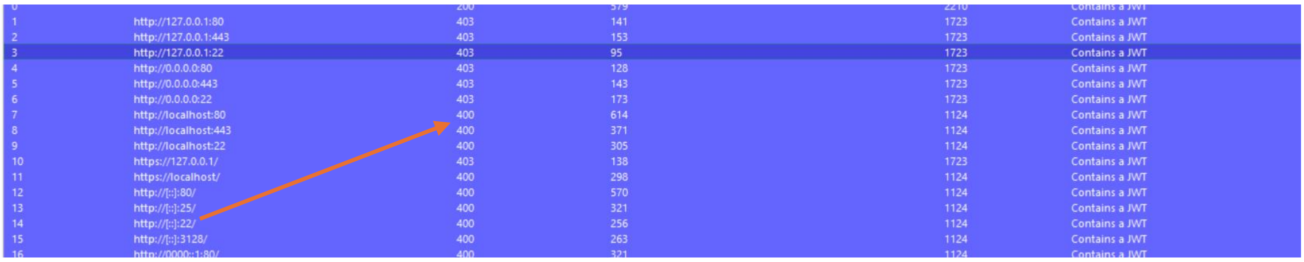
Payload count: 101

Request count: 101

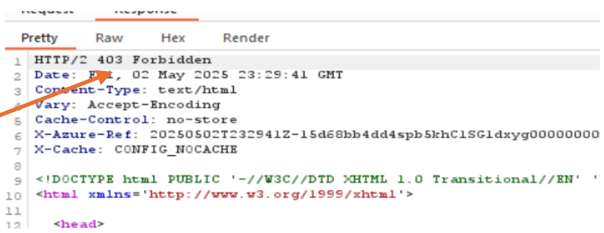
Payload configuration

This payload type lets you configure a simple l
strings that are used as payloads.

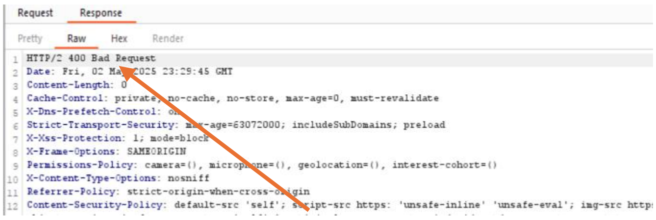
```
http://127.0.0.1:80
http://127.0.0.1:443
http://127.0.0.1:22
http://0.0.0.0:80
http://0.0.0.0:443
http://0.0.0.0:22
http://localhost:80
http://localhost:443
http://localhost:22
```



0		200	579	2210	Contains a JWT
1	http://127.0.0.1:80	403	141	1723	Contains a JWT
2	http://127.0.0.1:443	403	153	1723	Contains a JWT
3	http://127.0.0.1:22	403	95	1723	Contains a JWT
4	http://0.0.0.0:80	403	128	1723	Contains a JWT
5	http://0.0.0.0:443	403	143	1723	Contains a JWT
6	http://0.0.0.0:22	403	173	1723	Contains a JWT
7	http://localhost:80	400	614	1124	Contains a JWT
8	http://localhost:443	400	371	1124	Contains a JWT
9	http://localhost:22	400	305	1124	Contains a JWT
10	https://127.0.0.1/	403	138	1723	Contains a JWT
11	https://localhost/	400	298	1124	Contains a JWT
12	http://[::]:80/	400	570	1124	Contains a JWT
13	http://[::]:25/	400	321	1124	Contains a JWT
14	http://[::]:22/	400	256	1124	Contains a JWT
15	http://[::]:3128/	400	263	1124	Contains a JWT
16	http://0000::1:80/	400	321	1124	Contains a JWT

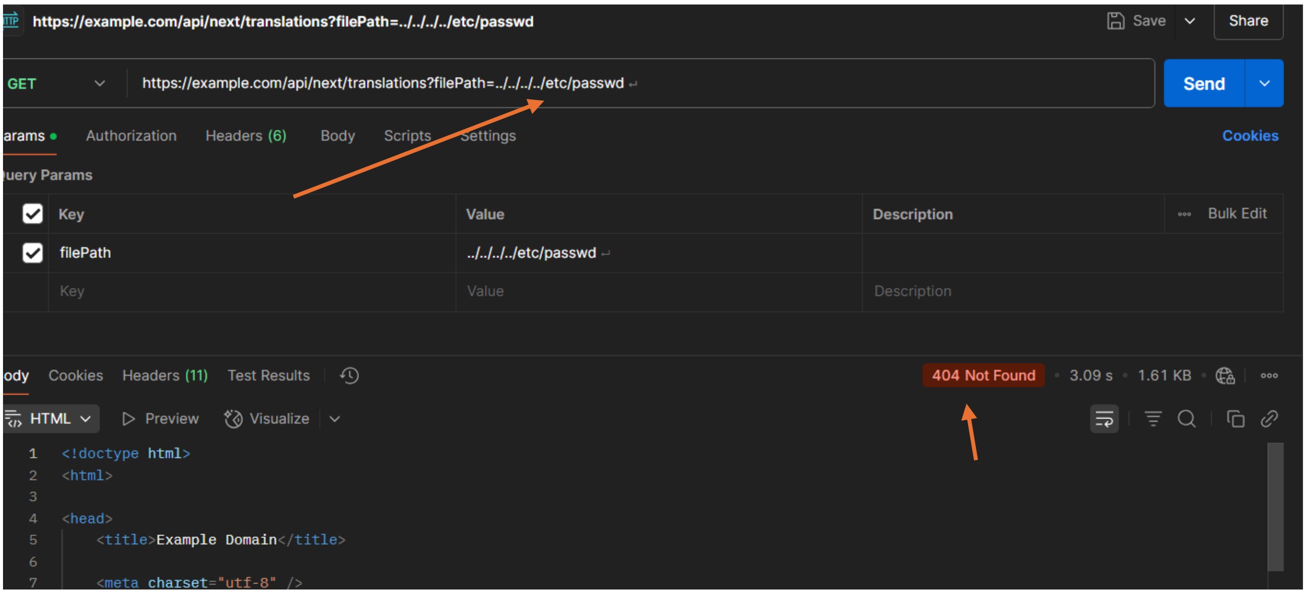


```
HTTP/2 403 Forbidden
Date: Fri, 02 May 2025 23:29:41 GMT
Content-Type: text/html
Vary: Accept-Encoding
Cache-Control: no-store
X-Azure-Ref: 20250502T232941Z-15d68bb4dd4spb5khC1SG1dxyg00000000
X-Cache: CONFIG_NOCACHE

<!DOCTYPE html PUBLIC '-//W3C//DTD XHTML 1.0 Transitional//EN' '
<html xmlns='http://www.w3.org/1999/xhtml'>

  <head>
```



```
HTTP/2 400 Bad Request
Date: Fri, 02 May 2025 23:29:45 GMT
Content-Length: 0
Cache-Control: private, no-cache, no-store, max-age=0, must-revalidate
X-Dns-Prefetch-Control: on
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
X-Xss-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Permissions-Policy: camera=(), microphone=(), geolocation=(), interest-cohort=()
X-Content-Type-Options: nosniff
Referrer-Policy: strict-origin-when-cross-origin
Content-Security-Policy: default-src 'self'; script-src https: 'unsafe-inline' 'unsafe-eval'; img-src http:
```

- **Attempted path traversal** by modifying `filePath` to values such as `../../../../etc/passwd` to test for insecure file access patterns. Endpoint behavior suggested poor input validation, though no sensitive data was disclosed within the test scope.



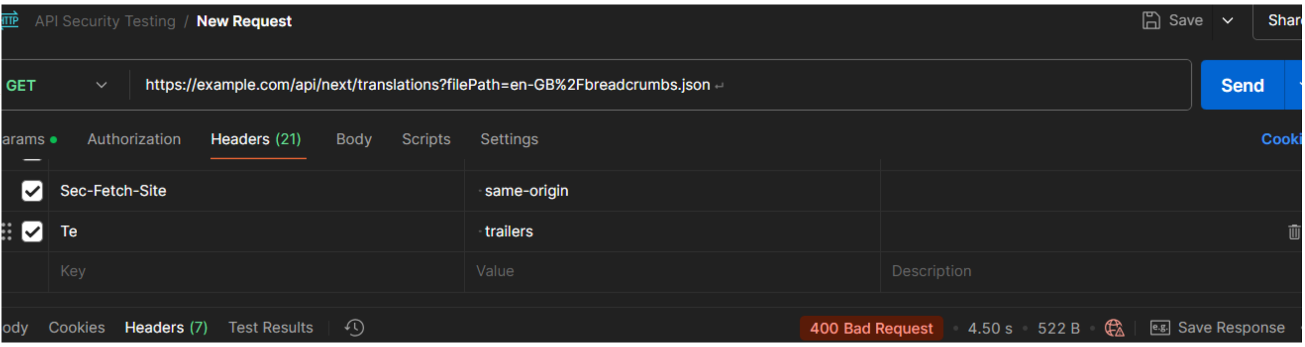
GET https://example.com/api/next/translations?filePath=../../../../etc/passwd

☑ Key	Value	Description
☑ filePath	../../../../etc/passwd	
Key	Value	Description

404 Not Found • 3.09 s • 1.61 KB

```
<!doctype html>
<html>

<head>
    <title>Example Domain</title>

    <meta charset="utf-8" />
```

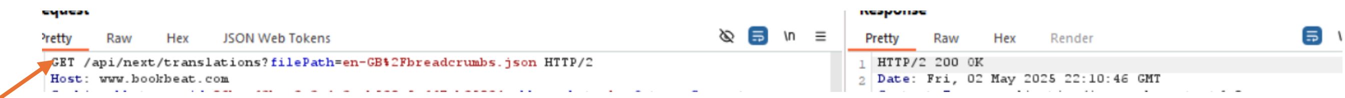
- **Insecure API Method Handling**
  Tested for misuse of HTTP methods (e.g., POST or DELETE used where GET should suffice). The current implementation shows signs of no insecure method validation. only the get method is allowed
  Get method(allowed)



GET https://example.com/api/next/translations?filePath=en-GB%2Fbreadcrumbs.json

☑ Sec-Fetch-Site	same-origin	
☑ Te	trailers	
Key	Value	Description

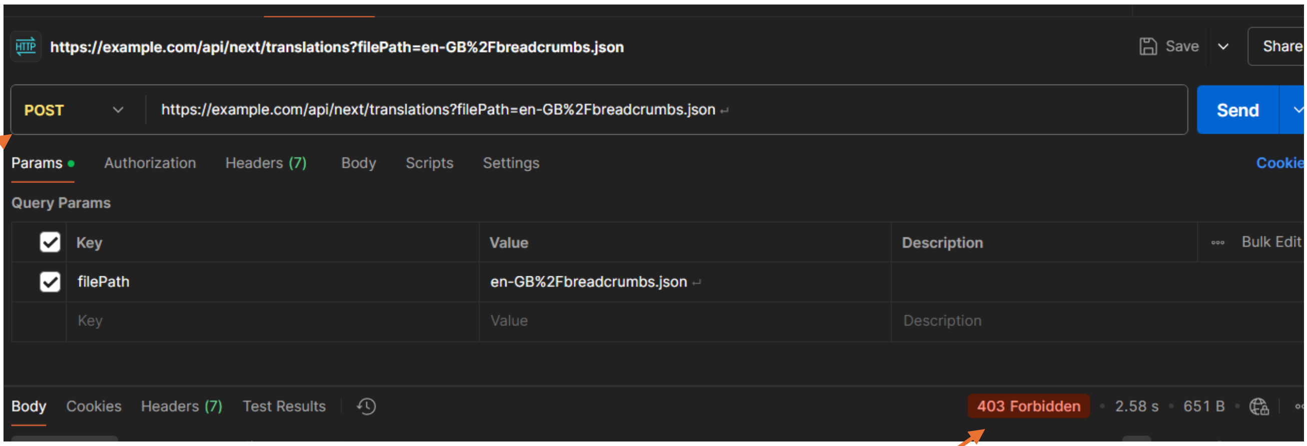
400 Bad Request • 4.50 s • 522 B



```
GET /api/next/translations?filePath=en-GB%2Fbreadcrumbs.json HTTP/2
Host: www.bookbeat.com
```

```
HTTP/2 200 OK
Date: Fri, 02 May 2025 22:10:46 GMT
```

Post method (Access denied)



https://example.com/api/next/translations?filePath=en-GB%2Fbreadcrumbs.json

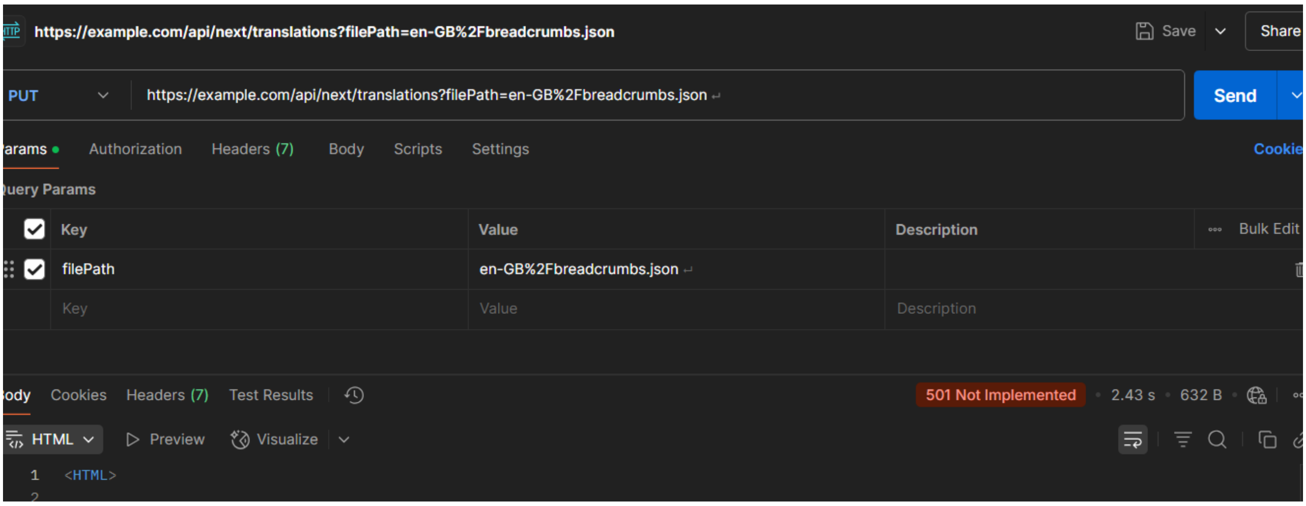
POST https://example.com/api/next/translations?filePath=en-GB%2Fbreadcrumbs.json

Query Params

	Key	Value	Description
☑	filePath	en-GB%2Fbreadcrumbs.json	
	Key	Value	Description

403 Forbidden • 2.58 s • 651 B

Put method (not implemented)



https://example.com/api/next/translations?filePath=en-GB%2Fbreadcrumbs.json

PUT https://example.com/api/next/translations?filePath=en-GB%2Fbreadcrumbs.json

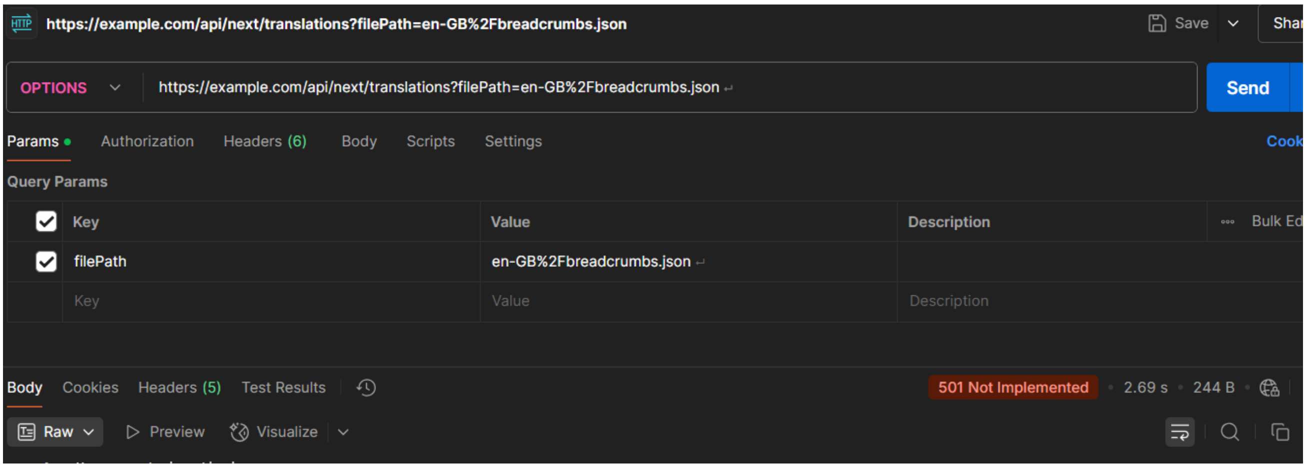
uery Params

	Key	Value	Description
☑	filePath	en-GB%2Fbreadcrumbs.json	
	Key	Value	Description

501 Not Implemented • 2.43 s • 632 B

```
<HTML>
```

Option method (unsupported)



https://example.com/api/next/translations?filePath=en-GB%2Fbreadcrumbs.json

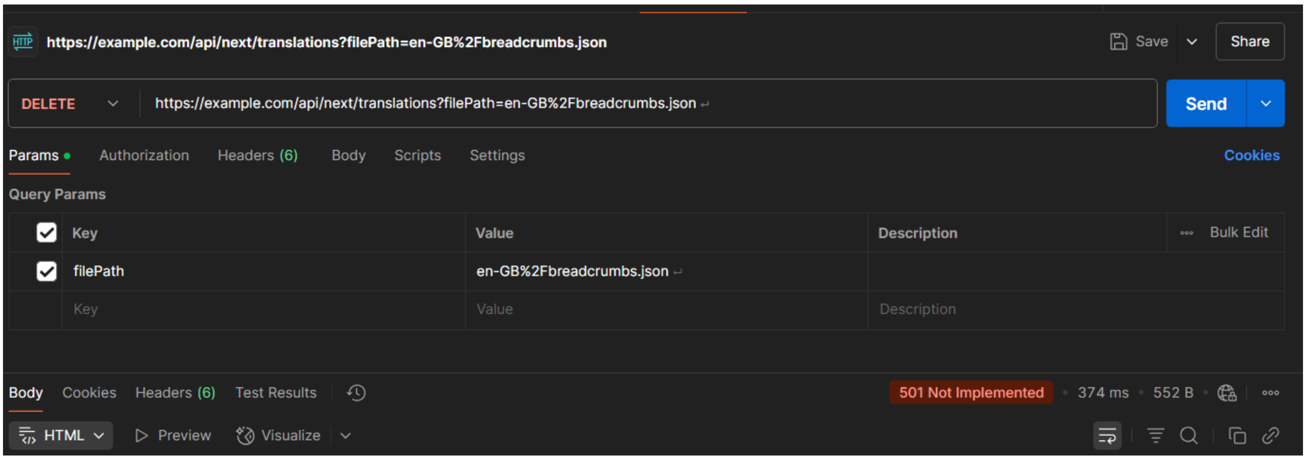
OPTIONS https://example.com/api/next/translations?filePath=en-GB%2Fbreadcrumbs.json

Query Params

	Key	Value	Description
☑	filePath	en-GB%2Fbreadcrumbs.json	
	Key	Value	Description

501 Not Implemented • 2.69 s • 244 B

Delete method (unsupported)



https://example.com/api/next/translations?filePath=en-GB%2Fbreadcrumbs.json

DELETE https://example.com/api/next/translations?filePath=en-GB%2Fbreadcrumbs.json

Query Params

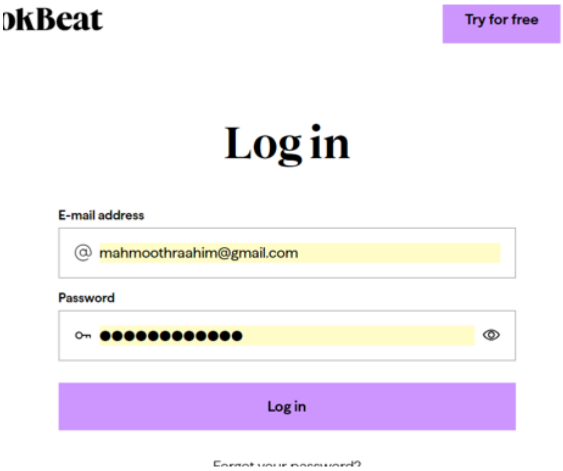
Key	Value	Description
☑ filePath	en-GB%2Fbreadcrumbs.json	
Key	Value	Description

501 Not Implemented · 374 ms · 552 B

- ❖ **The current implementation shows signs of no insecure method validation**

2.0 – Authentication Design Flaws

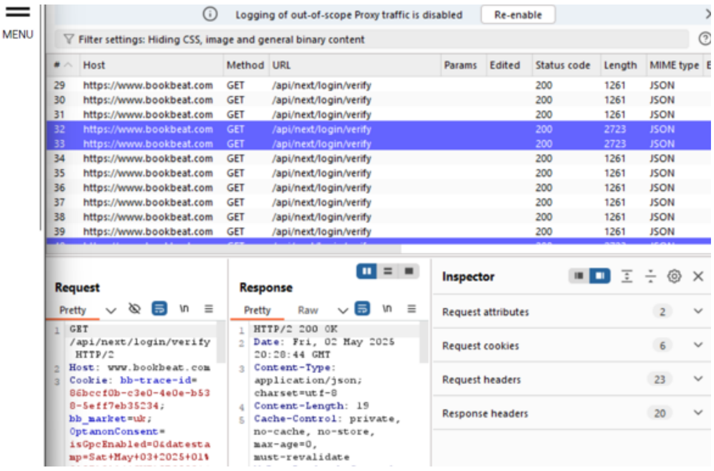
1.1 Exploited weak password policy. The **application only enforces minimum length, not complexity. Example: `112233445566` is accepted as a strong password**. Burp Suite was used to capture login request and attempt brute-force attempts. CAPTCHA is implemented after each login attempt, **making brute-force attacks harder but not impossible if CAPTCHA is bypassed**.



Log in

E-mail address: mahmoothraahim@gmail.com

Password: ●●●●●●●●●●●●



Logging of out-of-scope Proxy traffic is disabled

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type
29	https://www.bookbeat.com	GET	/api/next/login/verify			200	1261	JSON
30	https://www.bookbeat.com	GET	/api/next/login/verify			200	1261	JSON
31	https://www.bookbeat.com	GET	/api/next/login/verify			200	1261	JSON
32	https://www.bookbeat.com	GET	/api/next/login/verify			200	2723	JSON
33	https://www.bookbeat.com	GET	/api/next/login/verify			200	2723	JSON
34	https://www.bookbeat.com	GET	/api/next/login/verify			200	1261	JSON
35	https://www.bookbeat.com	GET	/api/next/login/verify			200	1261	JSON
36	https://www.bookbeat.com	GET	/api/next/login/verify			200	1261	JSON
37	https://www.bookbeat.com	GET	/api/next/login/verify			200	1261	JSON
38	https://www.bookbeat.com	GET	/api/next/login/verify			200	1261	JSON
39	https://www.bookbeat.com	GET	/api/next/login/verify			200	1261	JSON

Request

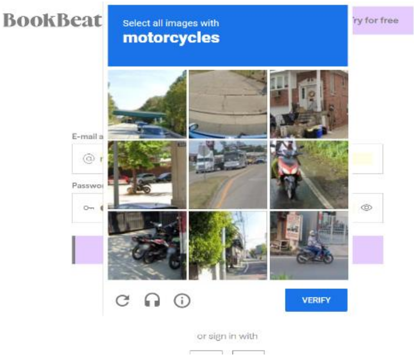
```
GET
/api/next/login/verify
 HTTP/2
Host: www.bookbeat.com
Cookie: bb-trace-id=
86bccf0b-c3e0-4e0e-b53
8-5eff7eb35234;
bb_market=uk;
OptanonConsent=
isGpcEnabled=0&datesta
mp=Sat+May+03+2025+01%
```

Response

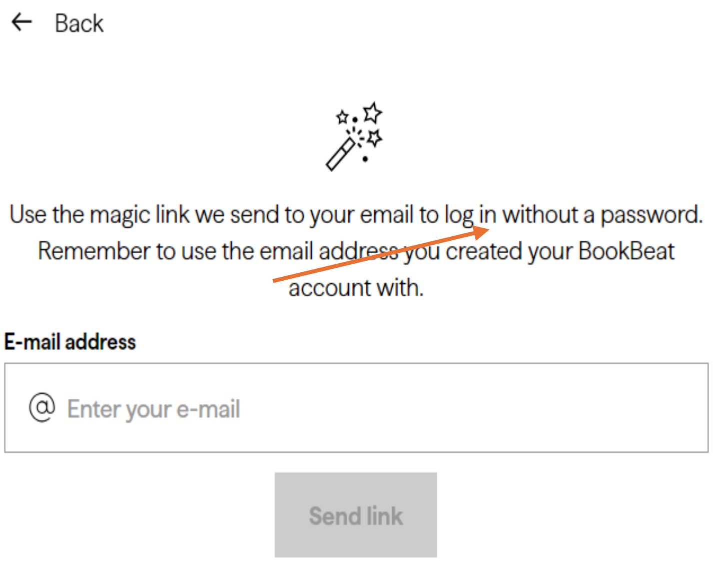
```
HTTP/2 200 OK
Date: Fri, 02 May 2025
20:28:44 GMT
Content-Type:
application/json;
charset=utf-8
Content-Length: 19
Cache-Control: private,
no-cache, no-store,
max-age=0,
must-revalidate
```

Inspector

Request attributes	2
Request cookies	6
Request headers	23
Response headers	20



1.2 Explored “Login Without Password” feature. Found that access could be granted via email alone. **If an attacker gains control of a user’s email** (e.g., through phishing or social engineering), they can **access the user’s Bookbeat account without a password**. This design weakens overall security posture and **increases the risk of account compromise**.



Use the magic link we send to your email to log in without a password. Remember to use the email address you created your BookBeat account with.

E-mail address

Enter your e-mail

Conclusion on Authentication Design Flaws:
While brute-forcing is mitigated via CAPTCHA, the weak password policy and insecure “login without password” design introduce severe risks. Attackers bypassing CAPTCHA or compromising a user’s email can gain unauthorized access, exposing users to significant threats.

8. Proposed Mitigation

To mitigate the **risks associated with insecure design**, the following actions should be considered:

Establish and follow a secure **software development lifecycle (SSDLC)** that includes input from security professionals to ensure that business logic and access controls are robustly designed. Use a valid library of secure design patterns for common components such as authentication, session management, and API interactions.

Apply threat modeling techniques during the design phase, particularly for high-value features like login flows, password resets, and API access. User stories should incorporate security criteria, and code should be validated through both unit and integration tests that reflect real-world misuse cases.

Ensure tier-based segregation within the system architecture and limit data/resource access based on clear authorization rules. Multi-tenancy should be securely isolated across all layers.

Add plausibility checks across application tiers and implement robust logging, rate limiting, and CAPTCHA that cannot be bypassed easily. Avoid offering login or reset flows that rely solely on email-based verification without multi-factor authentication (MFA).

9. Conclusion

This assessment revealed that Bookbeat suffers from several **design-level security issues, including a weak password policy and insecure authentication logic**. These vulnerabilities stem from foundational flaws in how security controls are conceptualized rather than implemented. While individual components such as CAPTCHA are in place, they are not sufficient to mitigate the risk introduced by poor design choices. Fixing these issues requires rethinking the application's authentication and access control strategies at the architectural level.

10. Reference

OWASP Top 10: A04 – Insecure Design