

API Security Testing - Missing Security Headers & Token Exposure

Recently, as part of my continuous learning in cybersecurity, I performed a basic API penetration test on a sample application. The goal was to understand common API security weaknesses and how they impact overall system security.

Here are some of the key issues I identified and what they mean:

1. Insecure Authentication Method (Using GET Instead of POST)-Failed

The API was accepting login credentials through a GET request, meaning the username and password were visible in the URL.

This is insecure because:

- URLs are stored in browser history
- They can appear in server logs
- They may leak through referrers
- Sensitive data becomes easily exposed

Proper authentication workflows must use POST, where credentials are sent in the request body and can be protected using TLS/HTTPS.

The screenshot shows the Postman interface with a successful API call. At the top, the URL is `http://192.168.1.107/v1/users.php?format=json&username=securestore&password=securestore`. Below it, the method is set to `GET`. The `Headers` tab shows several headers, including `Content-Type: application/json`, `Accept: */*`, and `User-Agent: PostmanRuntime/7.29.0`. The `Body` tab displays a JSON response with the following content:

```
1 {  
2   "code": 1,  
3   "status": 200,  
4   "data": {  
5     "username": "securestore",  
6     "emailid": "securestore@gmail.com",  
7     "token": "212174768840da1c6a1604c8b485a0ee"  
8   }  
}
```

The response status is `200 OK` with a duration of `233 ms` and a size of `346 B`. The JSON response body is also shown in the `Body` tab.

screenshot of Postman showing 200 OK for a GET request with sensitive data.

2. Server Version Disclosure (Information Leakage)-Failed

The server response headers exposed the full server version:

Apache/2.4.18 (Ubuntu)

Attackers can use this information to:

- Identify known vulnerabilities for that exact version
- Tailor exploits more effectively
- Plan targeted attacks

Servers should disable unnecessary header disclosure to limit recon and fingerprinting.

Response

Pretty	Raw	Hex	Render
1 HTTP/1.1 200 OK			
2 Date: Wed, 19 Nov 2025 06:32:42 GMT			
3 Server: Apache/2.4.18 (Ubuntu)			
4 Content-Length: 134			
5 Connection: close			
6 Content-Type: application/json; charset=utf-8			
7			
8 {			
"code":1,			
"status":200,			
"data":{			
"username":"securestore",			
"emailid":"securestore@gmail.com",			
"token":"212174768840dalc6a1604c8b485a0ee"			
}			
}			

API response from the repeater showing the Server version.

API Returns Sensitive Data in Response (Sensitive Data Exposure)

3. Sensitive Data Exposure- Failed

- Email address

- Authentication token
- Username

This allows account takeover if the token is valid.

The API returns sensitive user information, including username, email ID, and authentication token in plaintext JSON. This is a direct sensitive data exposure vulnerability and could lead to account takeover if intercepted or replayed.

```
[
  "code":1,
  "status":200,
  "data":{
    "username":"securestore",
    "emailid":"securestore@gmail.com",
    "token":"212174768840dalc6a1604c8b485a0ee"
  }
]
```

Exposed username ,email id and token in the response.

4. Missing Security Headers (CSP, HSTS, XSS Protections)-Failed

The API and website lacked essential security headers:

- **Content Security Policy (CSP)** - helps prevent XSS
- **HSTS (HTTP Strict Transport Security)** - forces HTTPS
- **X-Frame-Options / X-Content-Type-Options** - prevent clickjacking & MIME sniffing

These headers form the foundation of modern web security.

Without these headers:

- The site could be loaded over HTTP and here it can lead to the token leakage.
- Man-in-the-middle attacks become easier
- XSS risks increase
- Session security is weaker

5. Username Enumeration Risk-Passed

The API didn't respond differently depending on whether the username existed.

Example:

- Valid username + wrong password = "Password incorrect"
- Invalid username = "User does not exist"

This behaviour allows attackers to:

- Confirm valid usernames
- Prepare targeted brute-force attacks
- Reduce effort required for credential stuffing

A secure system should always return a generic error message such as: "Invalid username or password" like below.

Response

Pretty	Raw	Hex	Render
HTTP/1.1 401 Unauthorized			
Date: Wed, 19 Nov 2025 06:57:02 GMT			
Server: Apache/2.4.18 (Ubuntu)			
Content-Length: 61			
Connection: close			
Content-Type: application/json; charset=utf-8			
{			
"code": 4,			
"status": 401,			
"data": "Invalid Username or Password"			
}			

6. No Rate Limiting => Password Brute Force Vulnerability-Failed

There was no rate limiting or lockout mechanism on login attempts.
Using an intruder attack, I noticed:

- Response sizes changed when the correct character was used
- This can leak information during brute-force attempts
- Attackers can automate login attempts at scale

Proper protections include:

- Rate limiting (429 Too Many Requests)
- Account lockout
- CAPTCHA
- Monitoring abnormal login behaviour

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. In the top navigation bar, the 'Payloads' tab is highlighted. Below the tabs, there are sections for 'Payload Sets' and 'Payload Options [Simple list]'. The 'Payload Sets' section shows a payload set named '1' with a payload count of 7. The 'Payload Options [Simple list]' section shows a list of payloads: a, b, c, d, e, f, g. There are buttons for Paste, Load..., Remove, Clear, and Deduplicate. At the bottom, there are 'Add', 'Enter a new item', and 'Add from list ...' buttons. The 'Payload Processing' section below it is currently empty.

Screenshot showing the payload

Screenshot of the Postman interface showing the 'Positions' tab for an attack setup.

Attack type: Sniper

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://192.168.1.107

```
1 GET /v1/users.php?format=json&username=securestore&password=securestore$fs HTTP/1.1
2 User-Agent: PostmanRuntime/7.49.1
3 Accept: /*
4 Cache-Control: no-cache
5 Postman-Token: a0cb14ef-d8bf-4bd2-ba9b-7041fdc74d87
6 Host: 192.168.1.107
7 Accept-Encoding: gzip, deflate
8 Connection: close
```

Screenshot showing modified password with attack position markers.

6. Intruder attack of http://192.168.1.107 - Temporary attack - Not saved to project file

Attack Save Columns

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request ^	Payload	Status	Error	Timeout	Length	Comment
0		401	<input type="checkbox"/>	<input type="checkbox"/>	245	
1	a	401	<input type="checkbox"/>	<input type="checkbox"/>	245	
2	b	401	<input type="checkbox"/>	<input type="checkbox"/>	245	
3	c	401	<input type="checkbox"/>	<input type="checkbox"/>	245	
4	d	401	<input type="checkbox"/>	<input type="checkbox"/>	245	
5	e	200	<input type="checkbox"/>	<input type="checkbox"/>	309	
6	f	401	<input type="checkbox"/>	<input type="checkbox"/>	245	
7	g	401	<input type="checkbox"/>	<input type="checkbox"/>	245	

Request Response

Pretty Raw Hex

```
1 GET /v1/users.php?format=json&username=securestore&password=securestore$fs HTTP/1.1
2 User-Agent: PostmanRuntime/7.49.1
3 Accept: /*
4 Cache-Control: no-cache
5 Postman-Token: a0cb14ef-d8bf-4bd2-ba9b-7041fdc74d87
6 Host: 192.168.1.107
7 Accept-Encoding: gzip, deflate
8 Connection: close
9
10
```

0 matches

Attack result showing different status and length parameters for letter e, confirming the letter is correct.

Conclusion

This self-driven API security assessment helped strengthen my understanding of:

- API attack surfaces
- Authentication weaknesses
- Header security
- Enumeration risks
- Brute-force defence mechanisms

API security is a critical component of modern application security, and even small misconfigurations can significantly increase risk. I am continuing to explore more areas of penetration testing and API hardening as part of my learning journey