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.

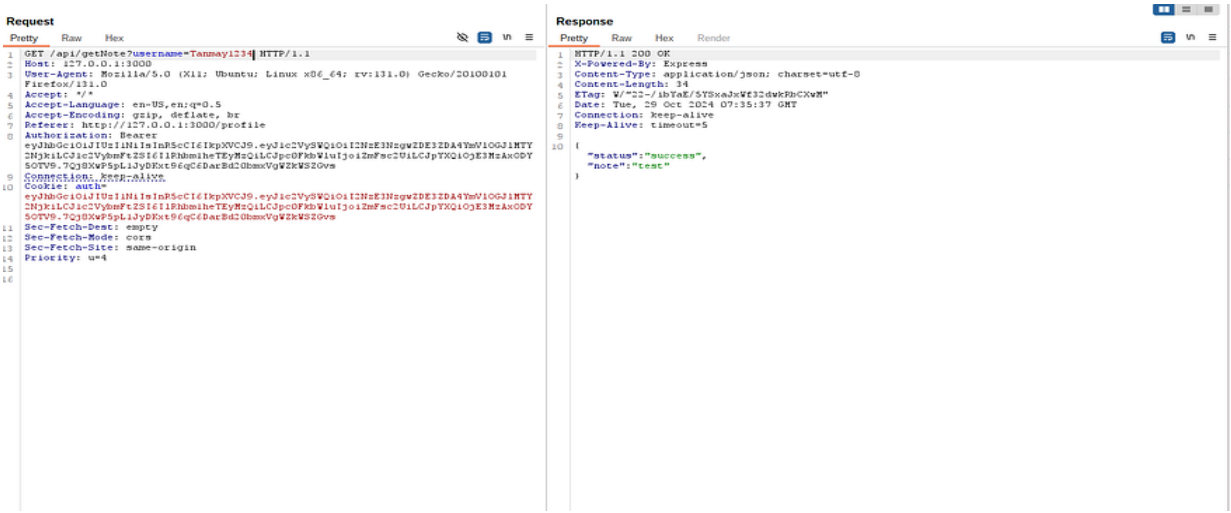
OWASP API Top 10 (2023)

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

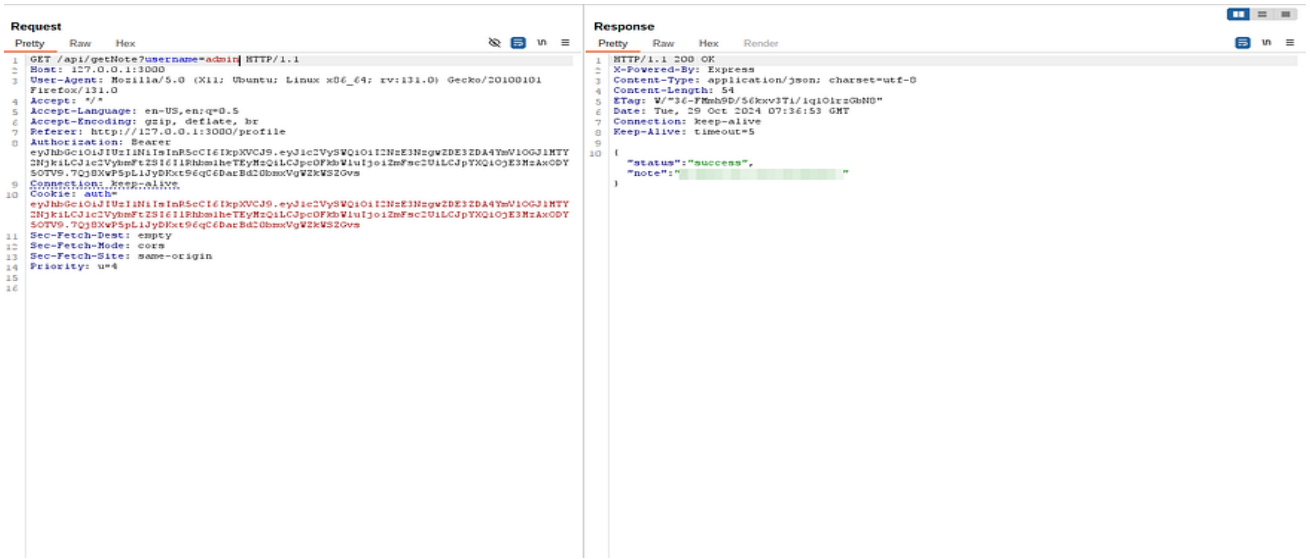
- 0xa1: Broken Object Level Authorization (Autorización a nivel de objeto rota)
- 0xa2: Broken Authentication (Autenticación rota)
- 0xa3: Broken Object Property Level Authorization (Autorización a nivel de propiedad de objeto rota)
- 0xa4: Unrestricted Resource Consumption (Consumo de recursos sin restricciones)
- 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.

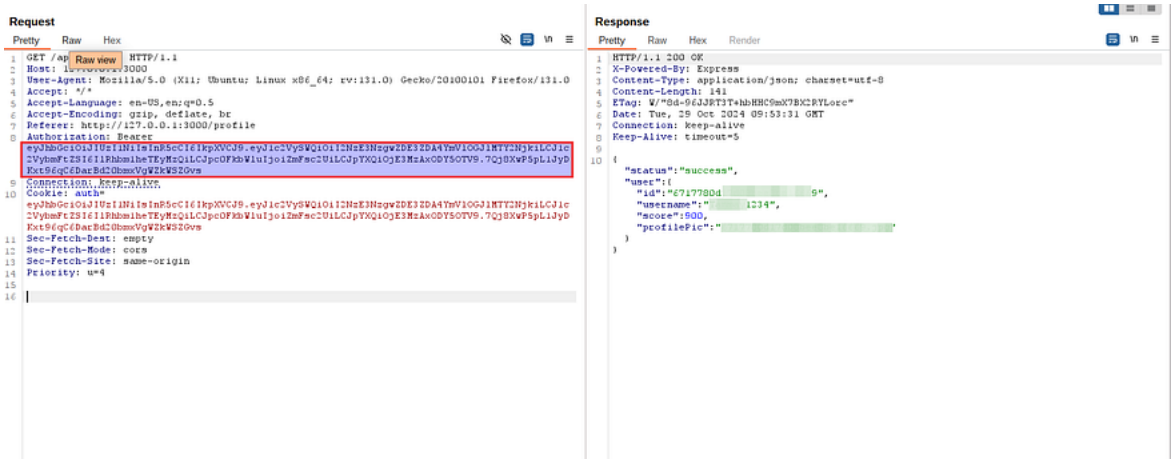


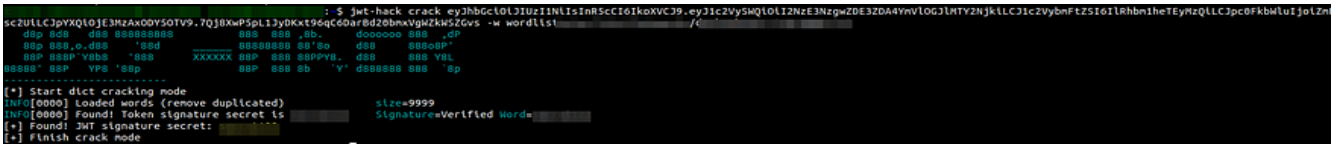
root1	100
admin	0
test	0
Tanmay	0
user	0
root	0
admin1	0



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.





eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOiI2NzE3NzgwZDE3ZDA4YmVlOGJlMTY2NjkiLCJ1c2VybmFtZSI6IlRhbm1heTEyMzQiLCJpc0FkbWluIjoidHJ1ZSIsImlhdCI6MTczMDE4Njk5NX0.wnTXQaD8o85pNx3YYN6sYTHmRhH5od9uhvozD1JXHfs

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

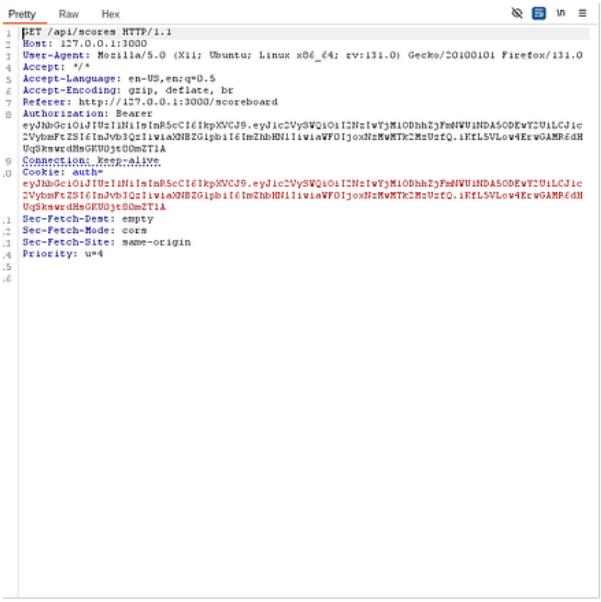
```
{
  "userId": "6717780d17d08bee8be16669",
  "username": "Tanmay1234",
  "isAdmin": "true",
  "iat": 1730186995
}
```

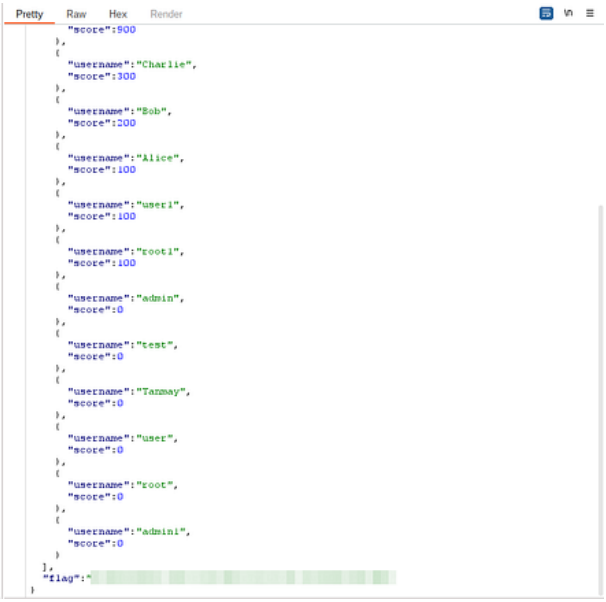
VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  
) secret base64 encoded
```

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.





API4:2023 Unrestricted Resource Consumption

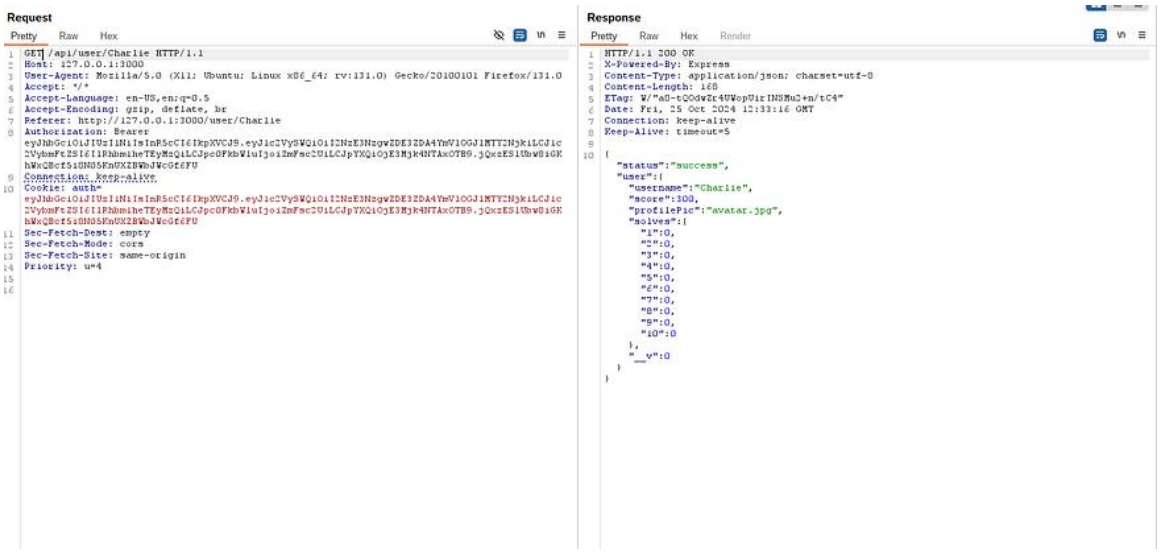
Las solicitudes a APIs consumen recursos como CPU, memoria, ancho de banda, almacenamiento e integraciones con otros servicios. Los atacantes pueden provocar un alto consumo de recursos enviando solicitudes excesivas, lo que puede dejar la API sin respuesta o aumentar los costes del negocio.

Creo la imagen grande

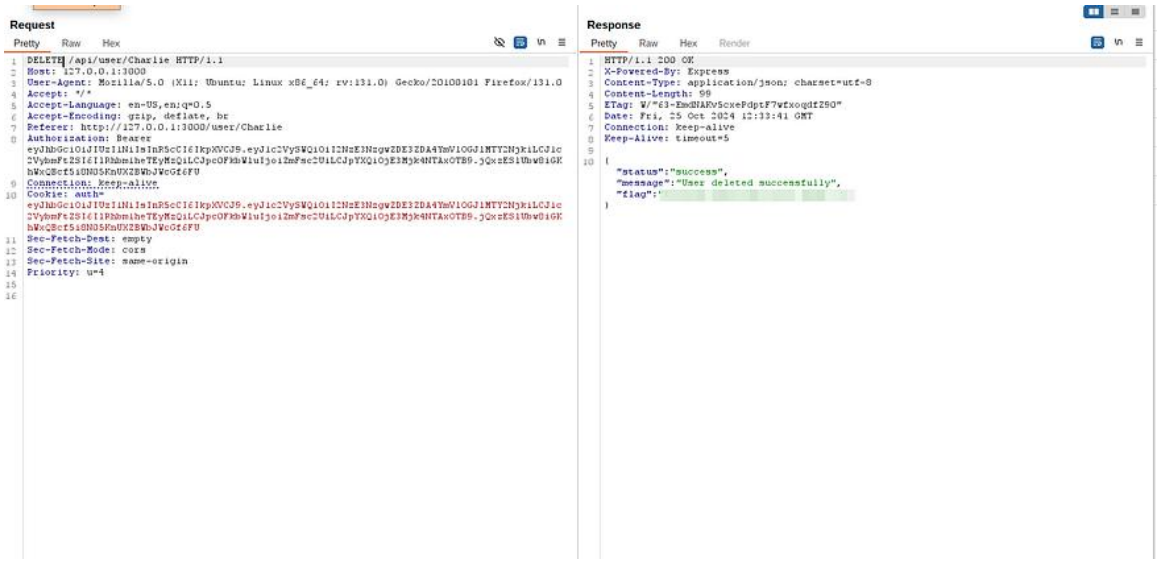
Subir a la foto de perfil

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

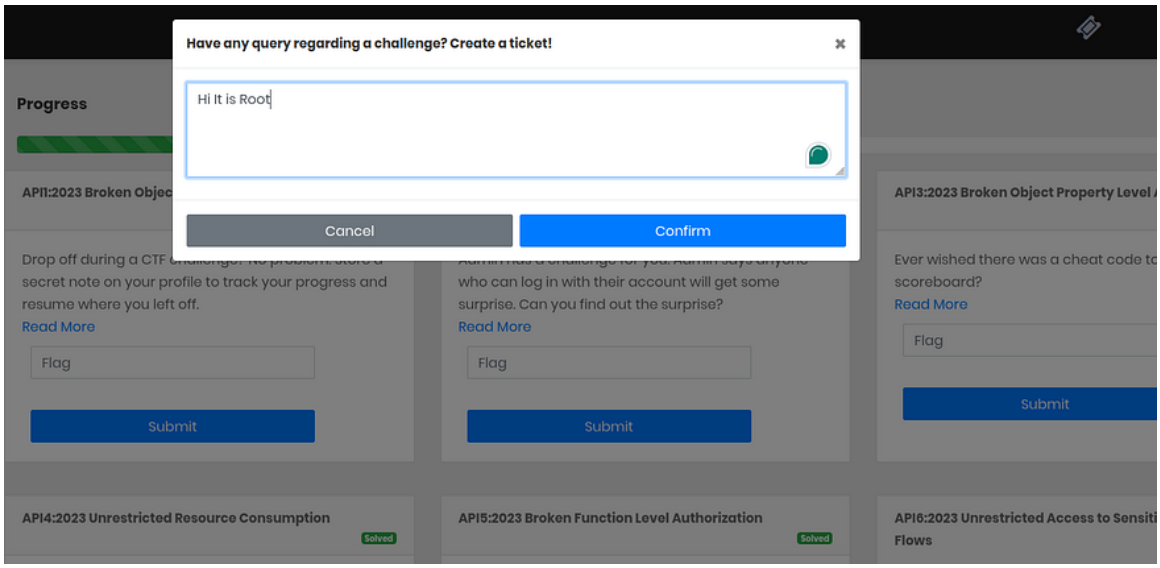


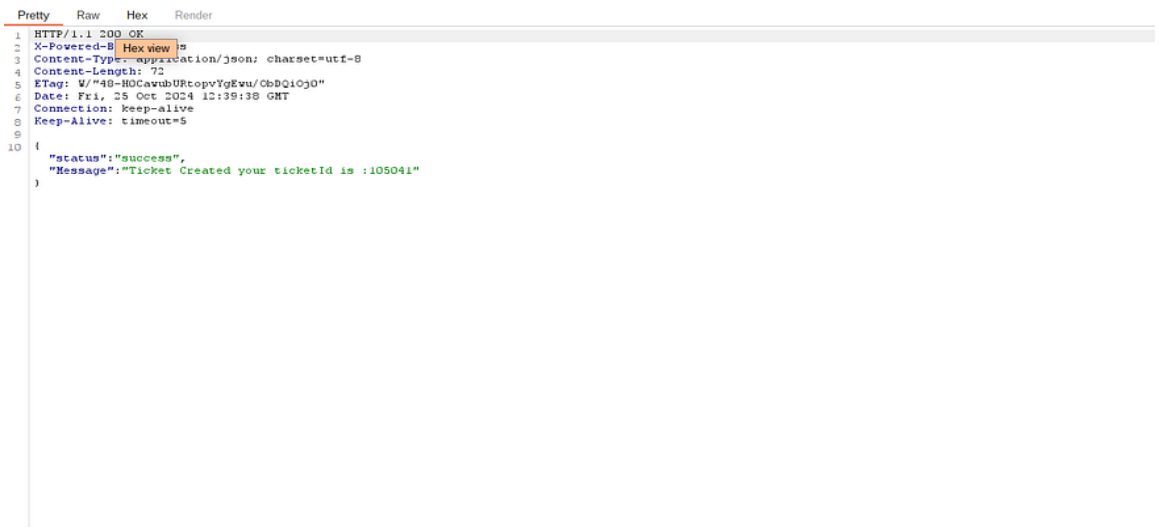
objetos.

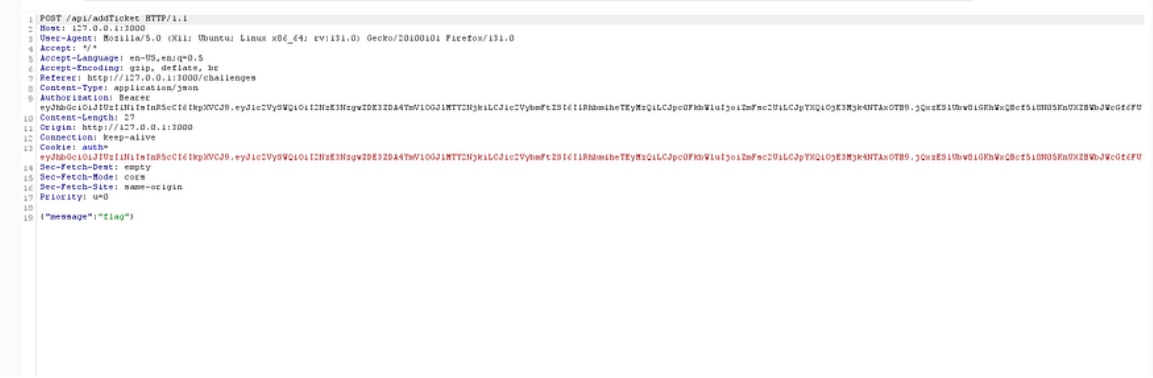


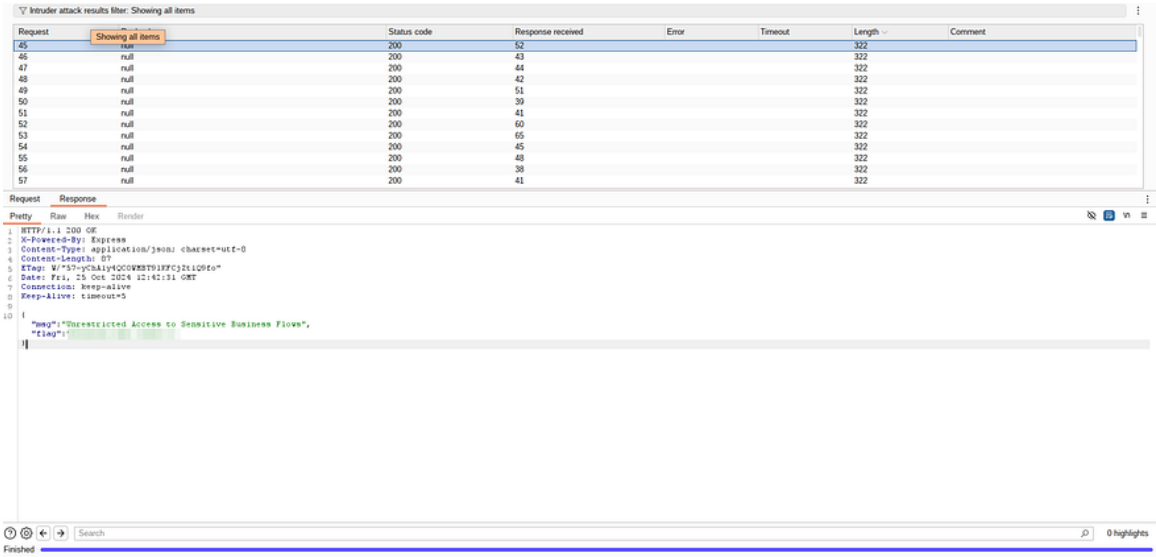
API6:2023 Unrestricted Access to Sensitive Business Flows

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.



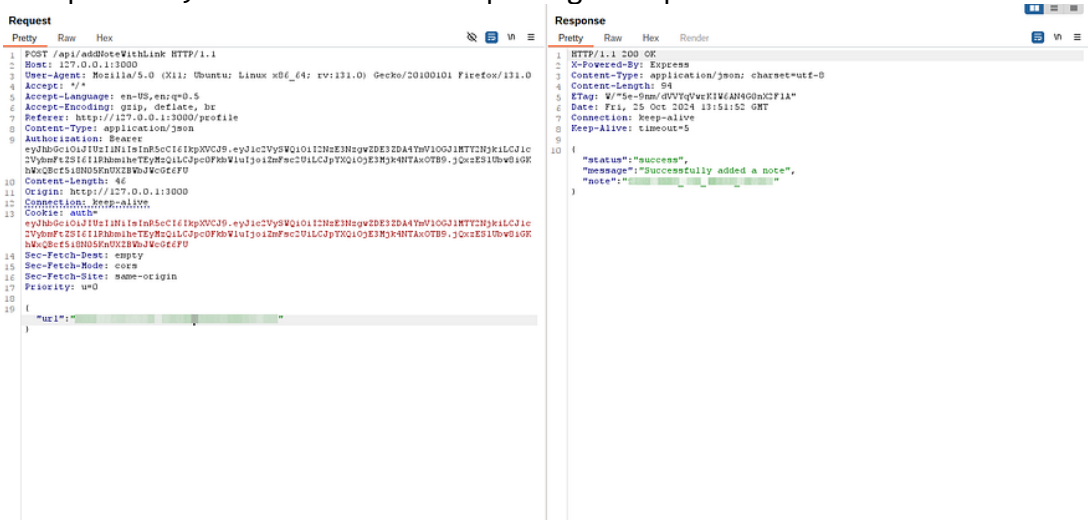






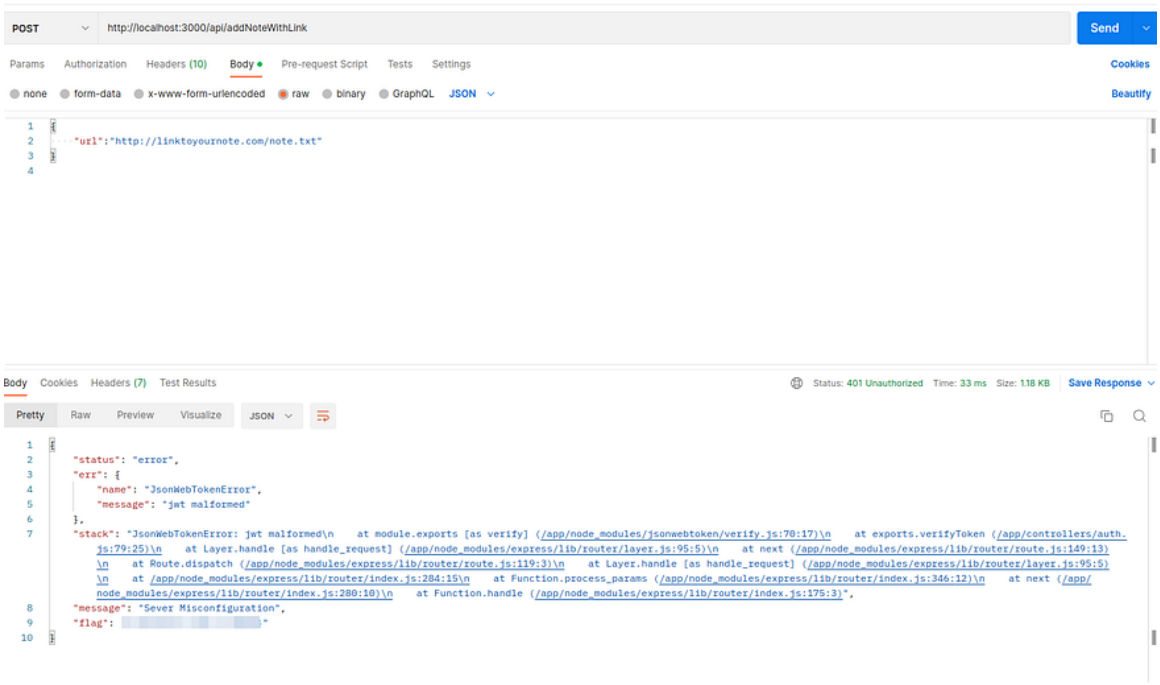
API7:2023 Server Side Request Forgery (SSRF)

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

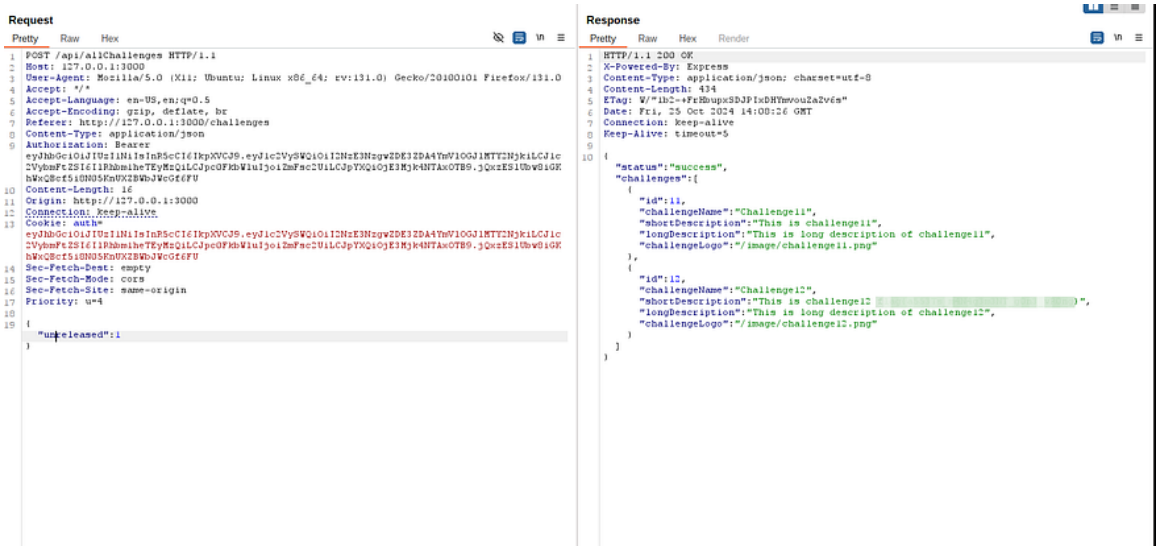
Una mala configuración de seguridad surge cuando ajustes de seguridad esenciales no se implementan o se implementan incorrectamente: por ejemplo, contraseñas por defecto, sistemas sin parchear, puertos abiertos innecesarios o mensajes de error con información sensible.



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.

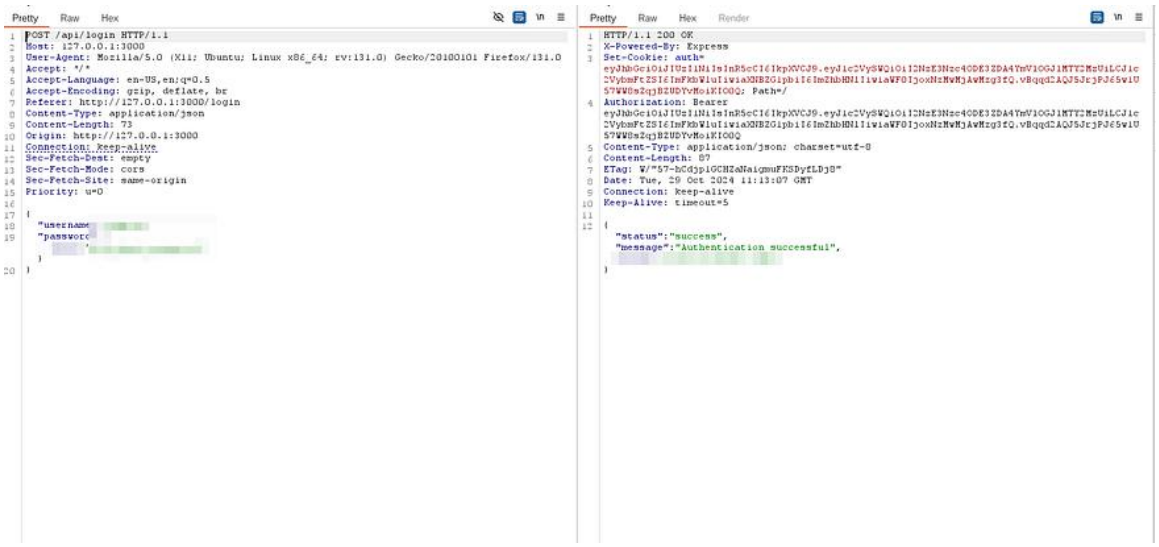
PROOF OF CONCEPT (POC): En el artículo original hay imágenes y capturas que documentan las pruebas de concepto del laboratorio DVAPI. Aquí se incluyen marcadores de posición que puedes reemplazar por las imágenes o capturas concretas.



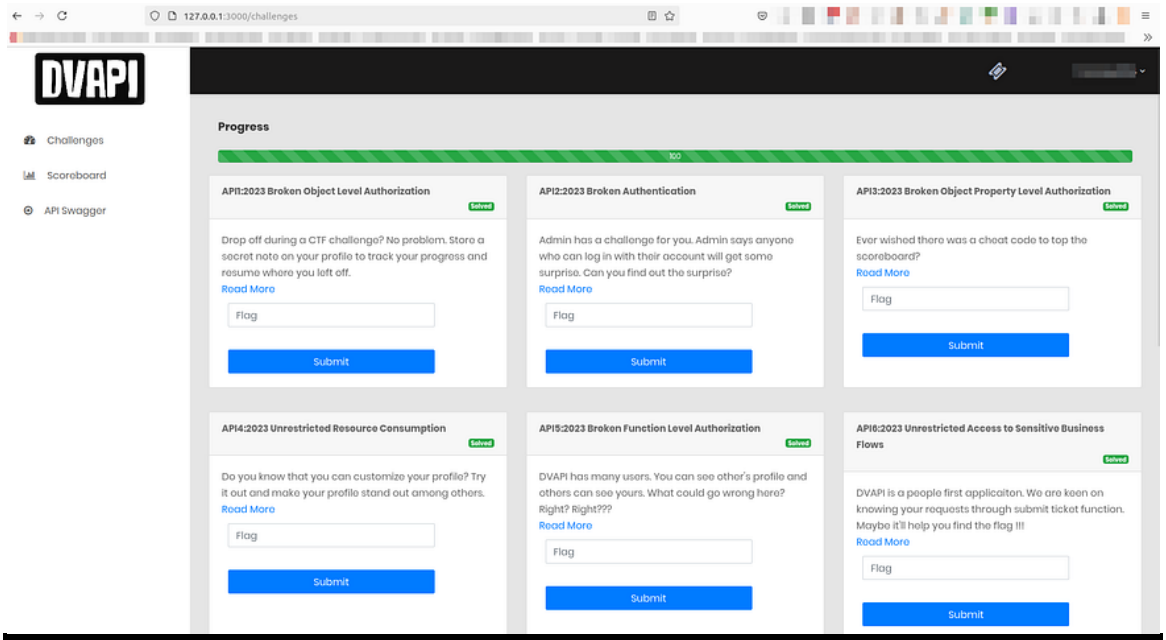
API10:2023 Unsafe Consumption of APIs

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.



Todas las banderas capturadas



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 proveniente 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