Building the Protected Resource

Justin Boyer
OWNER, GREEN MACHINE SECURITY

https://justinboyerwriter.com

The Role of the Protected Resource

Verify the Token

Verify the token passed from the client

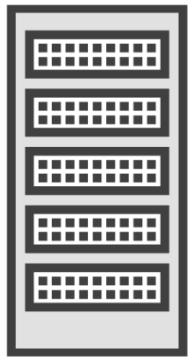
Allow Access to Data

Send the requested data according to client scopes

Where the Protected Resource Fits

Globomantics employee (resource owner)

Globomantics' HR system can now access the employees' workout data from the Carved Rock Fitness database



Carved Rock Fitness authorization server

Globomantics client

Carved Rock Fitness protected resource

Protected Resource Vulnerabilities

Cross-site Scripting (XSS)

Common web API vulnerability

Application places untrusted data into the HTML response

Fix: Validate all inputs and HTML encode where necessary

Token Replay

Token is stolen through another vulnerability and replayed to the protected resource

Fix: Tokens with short expiration dates

Fix: Use TLS with HSTS to enforce TLS on all connections

Web API Security Risks

Protected resources could be vulnerable to any common web API vulnerabilities

Fix: Follow security best practices for web APIs

Pluralsight's Web Application Security Learning Path

- https://app.pluralsight.com/paths/skills/web-application-security

What Have We Learned?

The protected resource is the web API the client is accessing

Implementing a protected resource in Node.js

Protected Resource Vulnerabilities

- XSS
- Token replay
- Web API vulnerabilities

You have the tools, now build your protected resource