42crunch

Pragmatic Web Security
Security for developers

NEW YEAR'S
FITNESS RESOLUTION

OWASP API SECURITY TOP 10

Find, Fix and Secure your APIs

JAN 25, FEB 17 & MAR 24
3-PART WEBINAR SERIES

Dr. Philippe de Ryck
Web Security Expert
Pragmatic Web Security

Colin Domoney
Security Researcher
& Developer Advocate
42Crunch

Introduction

About our Speakers

Colin Domoney

API Security Research Specialist & Developer Advocate

Editor of APISecurity.io

42Crunch

Dr. Philippe De Ryck

Web Security Expert

Pragmatic Web Security

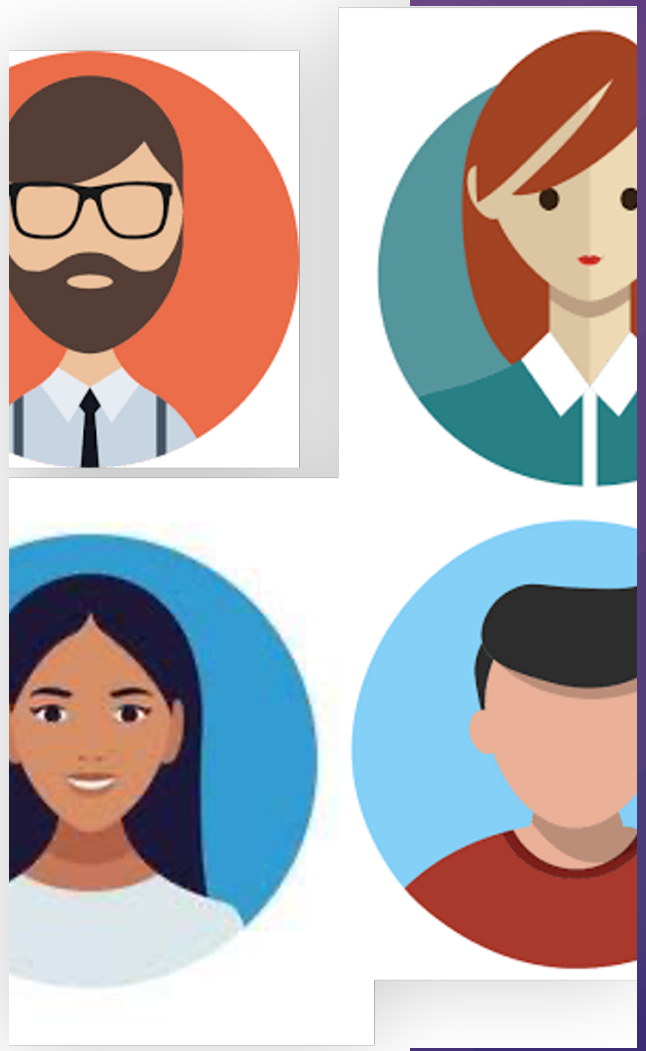
Housekeeping Rules

- All attendees muted
- Questions via chat window
- Recording will be shared on-demand
- Polling questions

Polling Question 1:

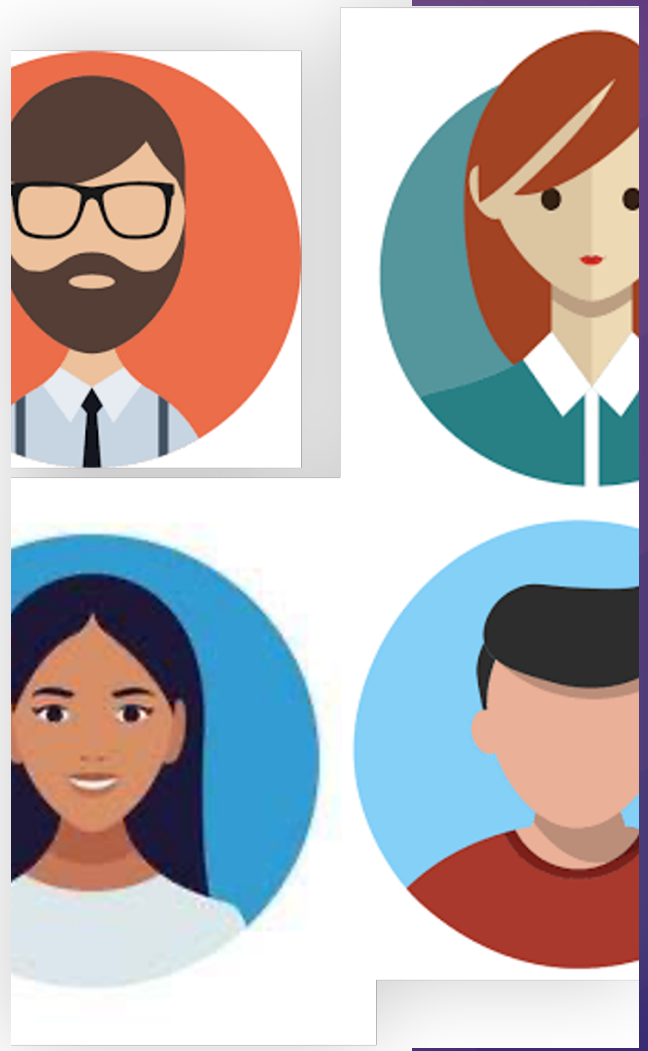
What is the closest description of your current job title?

1. API Developer
2. Security Engineer
3. Enterprise Architect
4. Head of Security
5. Front or Back End Developer
6. Other



1. Q1. What is the closest description of your current job title? (Single Choice) *

API Developer	(6/108) 6%
Security Engineer	(40/108) 37%
Enterprise Architect	(20/108) 19%
Head of Security	(4/108) 4%
Front/Back-end Developer	(14/108) 13%
Other	(24/108) 22%



1	Broken object level authorization
2	Broken user authentication
3	Excessive data exposure
4	Lack of resources & rate limiting
5	Broken function level authorization
6	Mass assignment
7	Security misconfiguration
8	Injection
9	Improper assets management
10	Insufficient logging & monitoring

1	Broken access control
2	Cryptographic failures
3	Injection
4	Insecure design
5	Security misconfiguration
6	Vulnerable and outdated components
7	Identification and authentication failures
8	Software and data integrity failures
9	Security logging and monitoring failures
10	Server-Side Request Forgery (SSRF)

1	Broken object level authorization	1	Broken access control
2	Broken user authentication	7	Identification and authentication failures
3	Excessive data exposure		
4	Lack of resources & rate limiting		
5	Broken function level authorization	1	Broken access control
6	Mass assignment		
7	Security misconfiguration	5	Security misconfiguration
8	Injection	3	Injection
9	Improper assets management		
10	Insufficient logging & monitoring	9	Security logging and monitoring failures

Polling Question 2:

Which OWASP API security vulnerability has impacted you the most?

1. Authentication issues
2. Data issues (mass assignment, leakage)
3. Authorization issues
4. Broken object-level authorization (BOLA)

2. Q2. Which OWASP API security vulnerability has impacted you the most? (Single Choice) *

Authentication issues	(42/108) 39%
Data issues (mass assignment, leakage)	(26/108) 24%
Authorization issues	(28/108) 26%
Broken object-level authorization (BOLA)	(12/108) 11%

Attendee Question:

Do you think that the security tools that we have traditionally been using for web application testing, so the likes of SAST and DAST, are applicable and suited for API testing?

1	Broken object level authorization
2	Broken user authentication
3	Excessive data exposure
4	Lack of resources & rate limiting
5	Broken function level authorization
6	Mass assignment
7	Security misconfiguration
8	Injection
9	Improper assets management
10	Insufficient logging & monitoring

Attendee Question:

“…Does a tool designed to find web security vulnerabilities (ex Burp, ZAP) can/should be used to find vulnerabilities in APIs also or should go to more "specialized" tools…”

Attendee Question:

“Can you share where we can learn more about contract security testing?”

Attendee Question:

“What contract spec do you advise (e.g. OAS/Swagger)?”

Business

Mobile Health Apps Systematically Expose PII and PHI Through APIs, New Findings from Knight Ink and Approov Show

9 February 2021, 12:00 CET

https://www.bloomberg.com/press-releases/2021-02-09/mobile-health-apps-systematically-expose-pii-and-phi-through-apis-new-findings-from-knight-ink-and-approov-show

“Of the 30 popular apps Knight Ink tested, 77 percent contained hardcoded API keys, some which don’t expire, and seven percent contained hardcoded usernames and passwords.”

Business

Mobile Health Apps Systematically Expose PII and PHI Through APIs, New Findings from Knight Ink and Approov Show

9 February 2021, 12:00 CET

https://www.bloomberg.com/press-releases/2021-02-09/mobile-health-apps-systematically-expose-pii-and-phi-through-apis-new-findings-from-knight-ink-and-approov-show

“100 percent of API endpoints tested were vulnerable to BOLA attacks that allowed the researcher to view the PII and PHI for patients that were not assigned to the researcher’s clinician account.”

Reverse Engineering Bumble's API

When you have too much time on your hands and want to dump out Bumble's entire user base and bypass paying for premium Bumble Boost features.

Sanjana Sarda Follow

Nov 14, 2020 · 8 min read

https://blog.securityevaluators.com/reverse-engineering-bumbles-api-a2a0d39b3a87

7

#962604

Revoked User can still view the Merge Request created by him via API

Share:

TIMELINE

muthu_prakash submitted a report to **GitLab**. Aug 19th (about 1 year ago)

Summary

In Gitlab when a user is demoted to Guest role, the Guest user will not be able to view and edit the Merge requests in a project even if the merge request is created by him. But this check is not implemented in API so the Guest user will be able to the following actions for the Merge request which he don't have a permission.

The Show Must Go On: Securing Netflix Studios At Scale

Netflix Technology Blog Follow

Sep 13, 2021 · 11 min read

Written by Jose Fernandez, Arthur Gonigberg, Julia Knecht, and Patrick Thomas

https://netflixtechblog.com/the-show-must-go-on-securing-netflix-studios-at-scale-19b801c86479

Attendee Question:

“In the spirit of shift left security (do as much as possible as leftward as possible) what are best practices/ tools/<add here anything else> that a developer should use to check that the API (they are) developing is safe.?”

Attendee Question:

“For an enterprise with hundreds of APIs (internal and external), are there any recommendations for API discovery, catalog and risk rating.”

Attendee Question:

“Everyone is talking about DevSecOps. Why are we not able to fix the security issues?”

Extra Reading

Further Information

Webinar 2: Address the OWASP API Authentication and Authorization Challenges.
11am EST / 4pm GMT - February 17, 2022

Webinar 3: Remediating the outstanding OWASP API Security Top 10 Issues.
11am EST / 4pm GMT - March 24, 2022

APIsecurity.io Weekly Newsletter
https://apisecurity.io/

#1 OpenAPI Editor - 400k+ users
https://42crunch.com/resources-free-tools/

Developer-First API Security Platform
https://42crunch.com/request-demo

42crunch

Pragmatic Web Security
Security for developers

NEW YEAR'S
FITNESS RESOLUTION

OWASP API SECURITY TOP 10

Find, Fix and Secure your APIs

JAN 25, FEB 17 & MAR 24
3-PART WEBINAR SERIES

Dr. Philippe de Ryck
Web Security Expert
Pragmatic Web Security

Colin Domoney
Security Researcher
& Developer Advocate
42Crunch