

# Trademark Strategy

Mike McCamon  
20-October-2020

# Goals of the Trademark Effort

- Protect the reputation and work of the Foundation
- Increase consistent use of marks
- Used consistently, brands increase trust
- Provide value to core and supporting members
- Monetize the value of marks

# Trademark Timeline

- Create a unique name or design for commerce
- Use the mark “unprotected” as a trademark
- File for registration following prior use within Classes (scope)
  - Our marks are generally in Classes 35 and 42
- **Determine what/if any Licensing Strategy**
- Trademark Enforcement and Litigation

# Status of Registered Trademarks

Mark	Status
OWASP	Registered in US and pending EU
Open Web Application Security Project	Registered in US and pending EU
Global AppSec	Registered in US and EU
AppSec Days	Pending US and registered EU

# Other Trademarks

OWASP, Open Web Application Security Project, and Global AppSec are registered trademarks and AppSec Days, AppSec California, AppSec Cali, SnowFROC, LASCON, and the OWASP logo are trademarks of the OWASP Foundation, Inc.

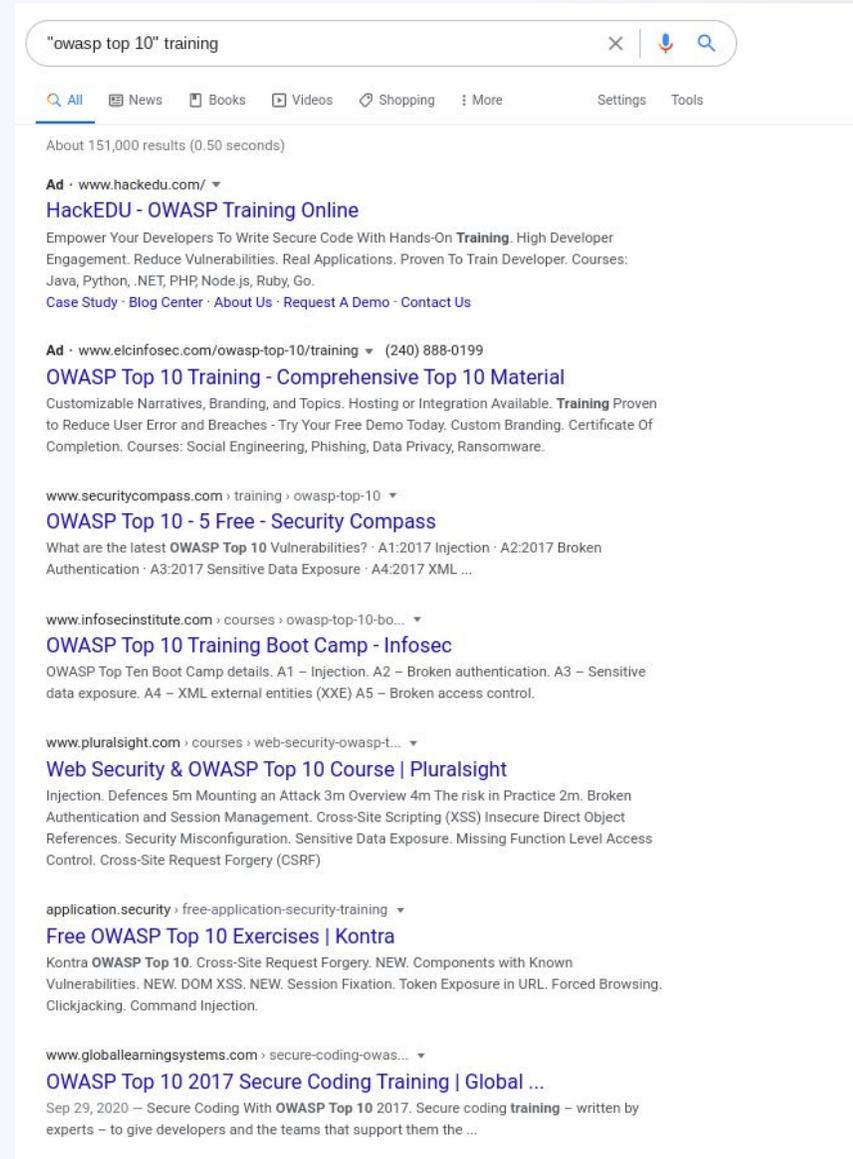
By declaring as trademarks, we protect “prior use” for the OWASP Foundation

# Proposed Licensing Strategy

- License OWASP tradename
  - Details following slides
- No licensing of Open Web Application Security Project
  - Not expecting any interest
- No licensing of Global AppSec
  - Used exclusively for OWASP Foundation major events
  - Append “location” following tradename
- Licensing of AppSec Days on case-by-case basis (if needed)
  - Migrate Regional events to AppSec Days appending “location”
  - Use for single and multiple day events; collectively “days” across OWASP

# Search of Marks

- Incognito search of...  
    "owasp top 10" training
- 151,000+ Results
- Only **two** links from the first results page are an OWASP Member
- These are not "fair use" instances, they are "commercial use"



The screenshot shows a search engine results page for the query "owasp top 10" training. The search bar at the top contains the query and shows "About 151,000 results (0.50 seconds)". Below the search bar, there are navigation links for "All", "News", "Books", "Videos", "Shopping", "More", "Settings", and "Tools". The results are listed as follows:

- Ad · www.hackedu.com/**  
**HackEDU - OWASP Training Online**  
Empower Your Developers To Write Secure Code With Hands-On **Training**. High Developer Engagement. Reduce Vulnerabilities. Real Applications. Proven To Train Developer. Courses: Java, Python, .NET, PHP, Node.js, Ruby, Go.  
[Case Study](#) · [Blog Center](#) · [About Us](#) · [Request A Demo](#) · [Contact Us](#)
- Ad · www.elcinfosec.com/owasp-top-10/training** (240) 888-0199  
**OWASP Top 10 Training - Comprehensive Top 10 Material**  
Customizable Narratives, Branding, and Topics. Hosting or Integration Available. **Training** Proven to Reduce User Error and Breaches - Try Your Free Demo Today. Custom Branding. Certificate Of Completion. Courses: Social Engineering, Phishing, Data Privacy, Ransomware.
- www.securitycompass.com** · training · owasp-top-10  
**OWASP Top 10 - 5 Free - Security Compass**  
What are the latest **OWASP Top 10** Vulnerabilities? · A1:2017 Injection · A2:2017 Broken Authentication · A3:2017 Sensitive Data Exposure · A4:2017 XML ...
- www.infosecinstitute.com** · courses · owasp-top-10-bo...  
**OWASP Top 10 Training Boot Camp - Infosec**  
OWASP Top Ten Boot Camp details. A1 – Injection. A2 – Broken authentication. A3 – Sensitive data exposure. A4 – XML external entities (XXE) A5 – Broken access control.
- www.pluralsight.com** · courses · web-security-owasp-t...  
**Web Security & OWASP Top 10 Course | Pluralsight**  
Injection. Defences 5m Mounting an Attack 3m Overview 4m The risk in Practice 2m. Broken Authentication and Session Management. Cross-Site Scripting (XSS) Insecure Direct Object References. Security Misconfiguration. Sensitive Data Exposure. Missing Function Level Access Control. Cross-Site Request Forgery (CSRF)
- application.security** · free-application-security-training  
**Free OWASP Top 10 Exercises | Kontra**  
Kontra **OWASP Top 10**. Cross-Site Request Forgery. NEW. Components with Known Vulnerabilities. NEW. DOM XSS. NEW. Session Fixation. Token Exposure in URL. Forced Browsing. Clickjacking. Command Injection.
- www.globallearningsystems.com** · secure-coding-owas...  
**OWASP Top 10 2017 Secure Coding Training | Global ...**  
Sep 29, 2020 – Secure Coding With **OWASP Top 10** 2017. Secure coding **training** – written by experts – to give developers and the teams that support them the ...

# Search of Marks

- Incognito search of...  
"owasp top 10" training
- 151,000+ Results
- Only **two** links from the first results page are an OWASP Member
- These are not "fair use" instances, they are "commercial use"

Search results for "owasp top 10" training:

- Ad · www.hackedu.com/ HackEDU - OWASP Training Online (NON-MEMBER)
- Ad · www.elcinfosec.com/owasp-top-10/training OWASP Top 10 Training - Comprehensive Top 10 Material (NON-MEMBER)
- www.securitycompass.com OWASP Top 10 - 5 Free - Security Compass (MEMBER)
- www.infosecinstitute.com OWASP Top 10 Training Boot Camp - Infosec (NON-MEMBER)
- www.pluralsight.com Web Security & OWASP Top 10 Course | Pluralsight (NON-MEMBER)
- application.security Free OWASP Top 10 Exercises | Kontra (NON-MEMBER)
- www.globallearningsystems.com OWASP Top 10 2017 Secure Coding Training | Global ... (NON-MEMBER)

"owasp top 10" training

Page 2 of about 151,000 results (0.39 seconds)

Ad · www.hackedu.com/

**HackEDU - OWASP Training Online**

Empower Your Developers To Write Secure Code With Hands-On **Training**. Reduce Vulnerability, Increase High Developer Engagement. Proven To Train Developer. Real Applications. Courses: Java, Python, .NET, PHP, Node.js, Ruby, Go.

About Us · Request A Demo · Contact Us · Case Study · Blog Center

NON-MEMBER

Ad · www.elcinfosec.com/owasp-top-10/training (240) 888-0199

**Online OWASP Training - Comprehensive Top 10 Material**

Interactive - Customizable Narratives, Branding and Graphics. **Training** Proven to Reduce User Error and Breaches - Get Your Free Demo Today. Certificate Of Completion. Custom Branding. Courses: Social Engineering, Phishing, Data Privacy, Ransomware, Social Media.

NON-MEMBER

www.youtube.com · watch

**Web Application Testing | OWASP Top 10 | Cyber Security ...**

Web Application Testing | OWASP Top 10 | Cyber Security Training | InfosecTrain. 4,023 views 4K views ... May 2, 2020 · Uploaded by Infosec Train

NON-MEMBER

owasp.org · www-project-top-ten

**OWASP Top Ten Web Application Security Risks | OWASP**

The OWASP Top 10 is the reference standard for the most critical web application security risks. Great keynotes, **training**, over 60 education sessions, and more.

OWASP

owasp.org · www-project-top-ten

**Table of Contents | OWASP**

Register now for Global AppSec 2020. Great keynotes, **training**, over 60 education sessions, and more. OWASP logo.

OWASP

www.lynda.com · Developer-Security-tutorials · Learn...

**Learning the OWASP Top 10 - Lynda.com**

Feb 22, 2018 — The OWASP Top 10 list describes the ten biggest vulnerabilities. In this course, application security expert Caroline Wong provides an overview ...

NON-MEMBER

www.synopsys.com · training · software-security-courses

**OWASP Top Ten (2017) - Application Security Course ...**

The OWASP Top Ten **training** course gives practical guidance for the most common ... While the OWASP Top 10 is a valuable document that raises awareness ...

MEMBER

www.protechtraining.com · overview-of-owasp-top-10...

**Overview of OWASP Top 10 Vulnerabilities - ProTech Training**

66,249.64.185. Your **Training** Location: Searching... No results found. Overview of OWASP Top 10 Vulnerabilities. Add Course To Watch List · View Full Course ...

NON-MEMBER

"owasp top 10" training

secureninja.com · Cybersecurity Courses

**OWASP Top 10 - Open Web Application Security Project**

In SecureNinja's OWASP Top 10 course, students will gain valuable insight ... These training courses are only delivered as an onsite format for groups of 5 or ...

NON-MEMBER

www.cybrary.it · course · owasp

**OWASP Certification Training Course - Online | Cybrary**

Take Cybrary's online OWASP certification **training** and earn a certification on your own time and schedule. ... This course will cover the OWASP Top 10 (2017).

NON-MEMBER

www.udemy.com · topic · owasp

**Top OWASP Courses Online - Updated [October 2020] | Udemy**

Complete guide to OWASP top 10 (2020). Guide to Web Security ... Web Security: OWASP Top 10 for APIs ... OWASP: Avoiding Hacker Tricks **Training**. OWASP: ...

NON-MEMBER

www.rangeforce.com · blog · get-a-head-start-on-owasp...

**Get a head start on OWASP Top 10 Vulnerabilities Training for ...**

Get a head start on OWASP Top 10 Vulnerabilities **Training** for 2020. Open Web Application Security Project (OWASP) provides an ongoing list of the Top 10 ...

NON-MEMBER

People also ask

- What are the Owasp top 10 vulnerabilities?
- What is Owasp certification?
- Why is Owasp top 10?
- What is the difference between Owasp 2013 and 2017?

Feedback

Videos

CYBER SECURITY ENGINEER  
Web Application Testing  
(DAY 2)  
4:27:41 INFOSEC TRAIN

Web Application Testing | OWASP Top 10 | Cyber Security

NON-MEMBER

Infosec Train  
YouTube · May 2, 2020

LASCON 2018 - OWASP Top-10 Training - Part 1  
2:30:43

LASCON  
YouTube · Oct 30, 2018

OWASP Training Course (Lesson 1 of 3) | Introduction | Open ...  
4:20

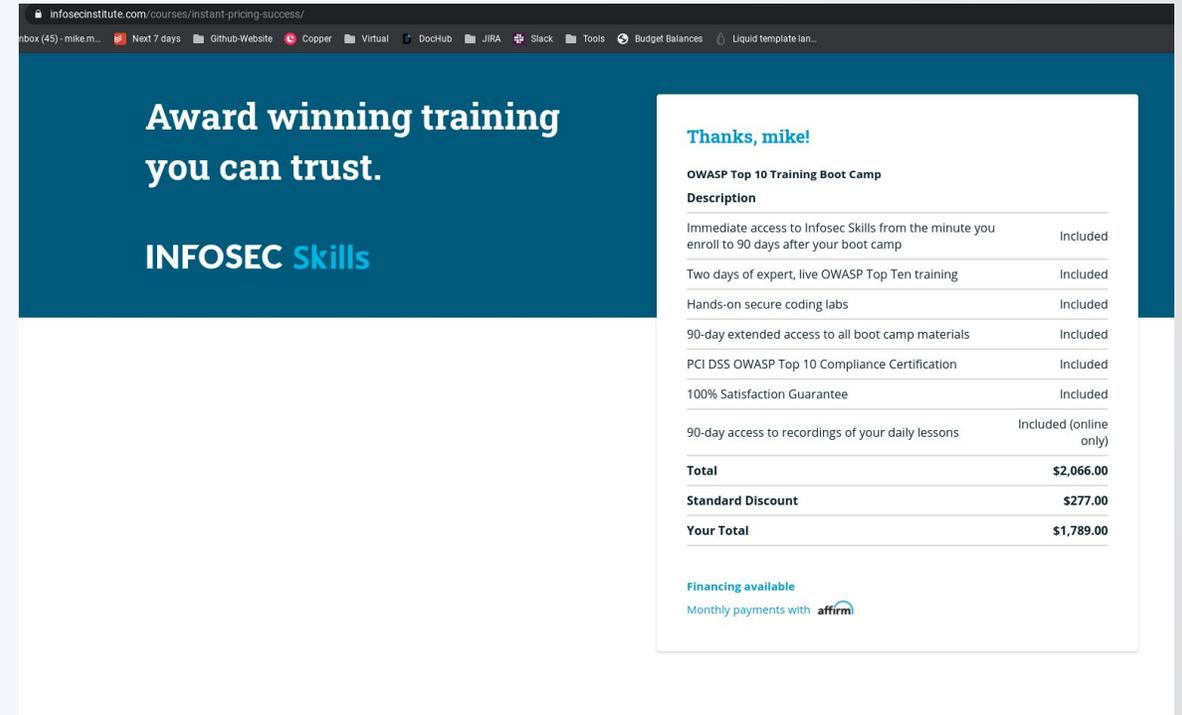
Cybrary  
YouTube · Aug 18, 2020

NON-MEMBER

View all

# Example Training Class Costs

- Not inherently wrong to charge for training on OWASP projects
- In fact, the content is open source in nearly all cases
- HOWEVER, when soliciting for students, the OWASP trade name helps improve the perceived value of the training.



The screenshot shows a webpage for the 'OWASP Top 10 Training Boot Camp' on the Infosec Institute website. The page features a dark blue header with the text 'Award winning training you can trust.' and the 'INFOSEC Skills' logo. Below the header, there is a table listing the components of the boot camp and their associated costs. The total cost is \$2,066.00, with a standard discount of \$277.00, resulting in a final price of \$1,789.00. The page also includes a 'Thanks, mike!' message and a note about financing options available through Affirm.

Description	
Immediate access to Infosec Skills from the minute you enroll to 90 days after your boot camp	Included
Two days of expert, live OWASP Top Ten training	Included
Hands-on secure coding labs	Included
90-day extended access to all boot camp materials	Included
PCI DSS OWASP Top 10 Compliance Certification	Included
100% Satisfaction Guarantee	Included
90-day access to recordings of your daily lessons	Included (online only)
<b>Total</b>	<b>\$2,066.00</b>
<b>Standard Discount</b>	<b>\$277.00</b>
<b>Your Total</b>	<b>\$1,789.00</b>

Financing available  
Monthly payments with 

# Example #2 - Training Class

Log In   Join   Contact Us   SANS Sites ▾   Search 🔍

**SANS**   Train and Certify   Manage Your Team   Programs   Resources   Vendor   About

Home > Courses > SEC522: Defending Web Applications Security Essentials

## SEC522: Defending Web Applications Security Essentials

 GIAC Certified Web Application Defender (GWEB)

[Register Now](#)   [Course Demo](#)

 Online   36 CPEs

This is the course to take if you have to defend web applications! The quantity and importance of data entrusted to web applications is increasing, and defenders need to learn how to secure these critical data. Traditional network defenses such as firewalls fail to secure web applications. In covering the OWASP Top 10 Risks and beyond, SEC522 will help you better understand web application vulnerabilities, thus enabling you to properly defend your organization's web assets.

**Course Authors:**

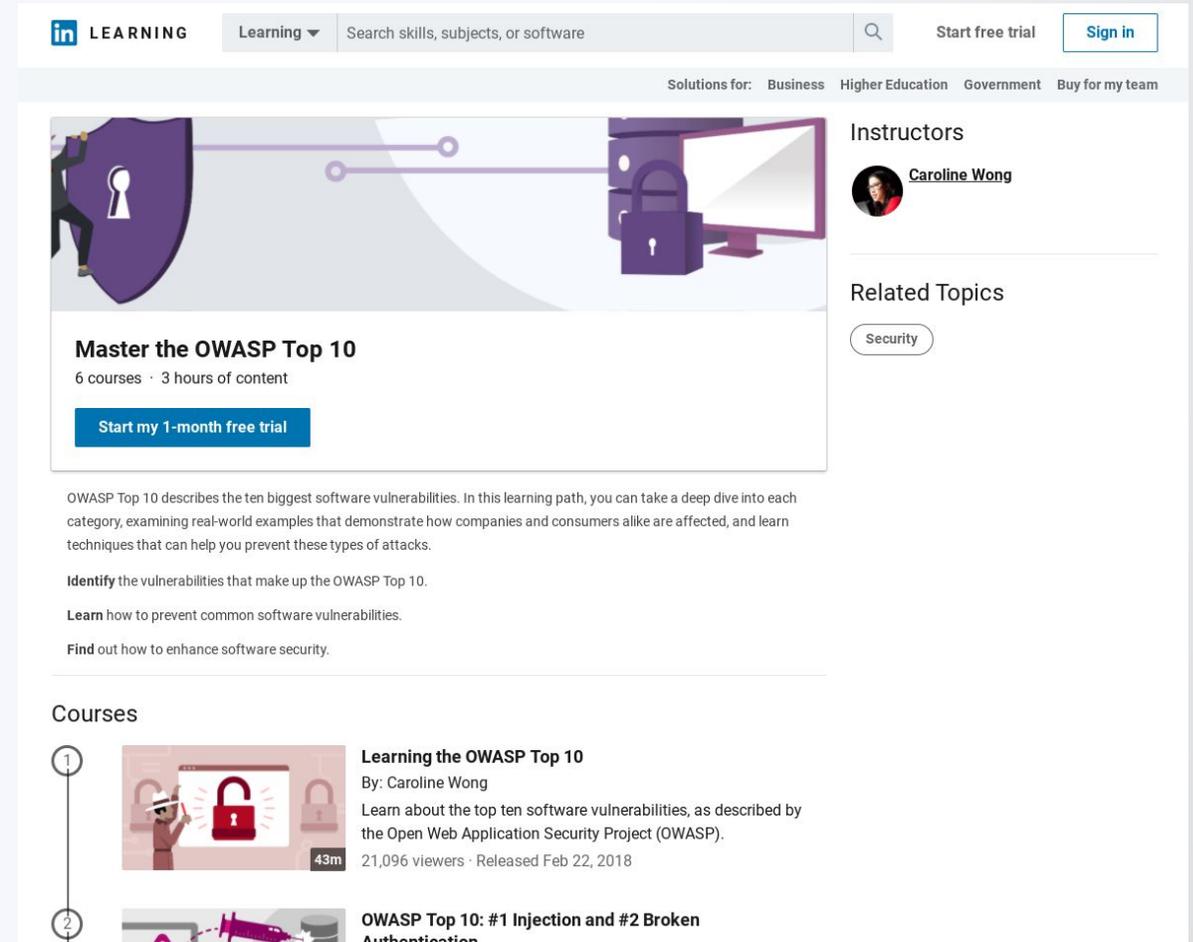
 **Jason Lam**  
Certified Instructor

 **Dr. Johannes Ullrich**  
Fellow

[What You Will Learn](#)   [Syllabus](#)   [Certification](#)   [Prerequisites](#)   [Laptop Requirements](#)   [Author Statement](#)   [Reviews](#)

# Example #3

- Platforms also allowing OWASP as part of monetization strategy
- LinkedIn Premium users get In-Learning included
- Instructors get royalty when users take classes
- This use case is currently out of scope of current strategy



The screenshot shows the LinkedIn Learning interface for the course "Master the OWASP Top 10". The page features a header with the LinkedIn Learning logo, a search bar, and navigation links for "Start free trial" and "Sign in". Below the header, there are tabs for "Solutions for: Business, Higher Education, Government, Buy for my team". The main content area includes a large banner image with a shield and a padlock, followed by the course title "Master the OWASP Top 10", the duration "6 courses · 3 hours of content", and a "Start my 1-month free trial" button. A descriptive paragraph explains that the course covers the ten biggest software vulnerabilities. Below this, there are three bullet points: "Identify the vulnerabilities that make up the OWASP Top 10.", "Learn how to prevent common software vulnerabilities.", and "Find out how to enhance software security." The "Courses" section lists two items: "Learning the OWASP Top 10" by Caroline Wong (43m, 21,096 viewers, released Feb 22, 2018) and "OWASP Top 10: #1 Injection and #2 Broken Authentication". On the right side, there is an "Instructors" section for Caroline Wong and a "Related Topics" section for Security.

# License for “OWASP” Training/Publications

- Fee is waived for OWASP Corporate Members
  - Individual Membership does not apply
- Annual flat fee per annual revenue (aligns with Membership pricing)
  - Up to \$50M, \$2,500
  - Between \$50M and \$100M, \$7,500
  - Over \$100M, \$12,500
- Requires License Agreement for Member or Non-Members
  - Not an endorsement of quality
  - Not a certification; only a license to use the OWASP Mark

# License for “OWASP” in Event Name

- No waiver for Corporate Members
- Unlikely, but want to define program name
- OWASP Foundation can discriminate; not under obligation to license marks as part of an event name
- Flat fee per event date based on gross revenue
  - Up to \$100,000, \$1,000
  - Between \$100,000 and \$250,000, \$10,000
  - Between \$250,000 and \$1,000,000, \$25,000
  - Over \$1,000,000, Negotiated on case-by-case event

# Following Adoption, Next Steps...

- Develop website content
  - Explains “Commercial Use”
  - Outlines Registered Marks
  - Provides Rationale for Licensing
- Collect list of Licensee Opportunities starting in US
- Approach Licensee Opportunities with standard “choice” email
  - Grace period until 1-January 2021
  - On or around 1-April, 2021 identify potential violators
  - Take high-profile actions with violator who is well known to community
- Approach Platforms for custom arrangements

# Board Resolution

Resolved that the Executive Director or their designatee develop, implement, and manage a trademark licensing effort with organizations that provide training on OWASP projects, publishers, and event organizers as outlined by staff at the October 2020 Board Meeting.