AI Security: Applying AI to the OWASP Top Ten

Durée: 2 Jours   Réf de cours: GK840019   Méthodes d'apprentissage: Intra-entreprise & sur-mesure

Résumé:

Learn How to Boost your Cybersecurity Toolkit by Applying AI to Combat the OWASP Top Ten Vulnerabilities.
OWASP 2021 refers to the latest edition of the Open Web Application Security Project (OWASP) Top Ten list, which identifies the most critical web application security risks. It is a valuable resource as it provides organizations with insights into prevalent vulnerabilities, helping them prioritize their security efforts and fortify their applications against potential attacks.
Applying AI to the OWASP Top Ten is a two-day, expert led course geared for technical students eager to explore AI's potency in mitigating cybersecurity threats. This course unravels the intersection of AI, cybersecurity, and ethical considerations with a focus on the OWASP top ten. The curriculum provides a detailed exploration of OWASP's top ten security risks, illustrating how AI can be effectively applied to detect and mitigate these common threats, such as Injection and Broken Authentication.
Through engaging discussions, interactive activities, and case study reviews, attendees will delve into the practical application of sophisticated AI algorithms to counter prevalent OWASP risks. The course encompasses an array of OWASP-related topics including how to leverage AI to manage risks associated with Insufficient Logging & Monitoring and Using Components with Known Vulnerabilities, as well as how to prevent Cross-Site Scripting (XSS) and Insecure Deserialization through the power of AI. Emphasizing the importance of testing, validating, and fine-tuning AI models, the course provides a comprehensive understanding of these tools' robustness and effectiveness in addressing OWASP risks. Integrating technical skills with ethical considerations, attendees will learn about designing and implementing AI models that adhere to ethical standards while effectively detecting and mitigating OWASP risks.
You'll exit the course with a solid grasp of the crucial role AI plays in tackling OWASP's most prominent security risks, equipped to help bolster your organization's defense against cyber threats. You'll understand how to leverage AI for cybersecurity and how to create AI models to combat common vulnerabilities outlined by the OWASP Top Ten. Whether the goal is to strengthen an organization's security framework or to broaden personal understanding of AI and cybersecurity, this course offers the critical expertise needed to begin your journey into navigating the intricate realm of AI-enhanced cybersecurity.

Public visé:

This is an intermediate level course ideally suited for software developers, IT professionals, and cybersecurity enthusiasts who are keen to enhance their understanding of web application security. Roles might include:
- Cybersecurity Analysts
- IT Security Specialists
- Information Security Officers
- Risk Management Professionals
- IT Auditors or Compliance Managers
- Chief Information Security Officers (CISOs)
- Ethical Hackers
- Network Security Engineers
- Data Protection Officers
- Threat Intelligence Analysts
- Vulnerability Assessors
- Developers
- Project Managers

Objectifs pédagogiques:

- Throughout the course you'll learn to:

- Understand the Complexities of OWASP: Develop a firm grasp on the OWASP Top Ten, gaining insights into the most significant web application security risks and the mechanisms behind these vulnerabilities.

- Navigate the Intersection of AI and Cybersecurity: Gain a foundational understanding of how artificial intelligence can be utilized in the field of cybersecurity, specifically in the context of mitigating OWASP risks.

- Master Detection and Mitigation Techniques: Learn to leverage AI to detect and mitigate common security risks such as Injection

- Apply Advanced AI Algorithms: Harness the power of AI algorithms to address OWASP risks, seeing how to customize these algorithms for various security vulnerabilities.

- Tackle Real-World Security Challenges: Learn practical skills to manage risks associated with Insufficient Logging & Monitoring and Using Components with Known Vulnerabilities, while also learning methods to prevent Cross-Site Scripting (XSS) and Insecure Deserialization.

- Validate and Test AI Models: Learn the crucial process of validating and testing AI models, ensuring their robustness and effectiveness in detecting OWASP risks, while adhering to ethical standards in AI application.

and Broken Authentication, and apply these skills to design effective AI models.

Pré-requis:

This course is a seminar / workshop style event that combines engaging instructor-led presentations with demonstrations, use case exploration and engaging group activities. Even though this is not a programming class, it is helpful if you have:

- Basic Understanding of Web Applications
- Basic cybersecurity concepts
- Familiarity with OWASP Top Ten common vulnerabilities
- Familiarity with Basic AI Concepts

Contenu:

1. Introduction to AI, OWASP Top Ten, and AI Ethics

- Understand the intersection of AI, cybersecurity, and ethical considerations.
- Introduction to OWASP and the top ten security risks for web applications.
- Overview of AI and its applications in mitigating OWASP risks.
- Discussion on AI Ethics, including privacy concerns and biases in AI models.
- Exploring how AI can help mitigate these risks while ensuring ethical use.

2. AI for Injection and Broken Authentication Mitigation

- Learn how AI helps detect and mitigate Injection and Broken Authentication.
- Discussion on the nature of Injection and Broken Authentication attacks and their prevalence in OWASP.
- How AI can help in detecting these vulnerabilities in real time.
- Designing an AI model for mitigating these security risks. •
- Demo: Train a basic AI model to detect potential Injection and Broken Authentication attacks

3. Deep Dive into AI Algorithms and their application in mitigating OWASP Risks

- Comprehend the working mechanisms of key AI algorithms.
- Detailed analysis of AI algorithms used in mitigating OWASP security risks.
- Hands-on experience in choosing the right algorithm for a specific problem.
- Guided tutorial on customizing algorithms for different OWASP vulnerabilities.
- Demo: Selection and customization of AI algorithms for detecting Sensitive Data Exposure

4. AI for XML External Entity (XXE) and Security Misconfiguration Mitigation

- Gain skills to utilize AI for detecting and mitigating XXE and Security Misconfigurations.
- Introduction to XXE and Security Misconfigurations as significant OWASP risks.
- How AI can assist in real-time detection of these vulnerabilities.
- Designing an AI model for mitigating these OWASP threats.
- Demo: Train a basic AI model to detect potential XXE attacks and Security Misconfigurations

5. AI for Cross-Site Scripting (XSS) and Insecure Deserialization Mitigation

- Gain skills to utilize AI for detecting and mitigating XSS and Insecure Deserialization.
- Introduction to XSS and Insecure Deserialization as significant OWASP risks.
- How AI can assist in real-time detection of these vulnerabilities.
- Designing an AI model for mitigating these OWASP threats.
- Demo: Train a basic AI model to detect potential attacks

6. AI for Insufficient Logging ; Monitoring and Using Components with Known Vulnerabilities

- Gain skills to utilize AI for detecting and mitigating Insufficient Logging ; Monitoring and using components with known vulnerabilities.
- Introduction to these threats as significant OWASP risks.
- How AI can assist in real-time detection of these vulnerabilities.
- Designing an AI model for mitigating these OWASP threats.
- Demo: Train a basic AI model to detect potential risks associated with insufficient logging and known vulnerabilities

7. AI Model Validation, Testing, and Limitations

- Comprehend the importance of validation and testing in AI models.
- Learn methods for testing, validating, and fine-tuning AI models.
- Understanding the limitations of AI in the context of mitigating OWASP risks.
- Demo: Validate and test a basic AI model for detecting OWASP risks

8. Future of AI in Mitigating OWASP Threats

- Explore the future trends of AI in the context of cybersecurity and OWASP.
- Discuss research and future applications of AI in cybersecurity.
- Address advancements like adversarial AI, AI-powered intrusion detection systems etc.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s’auto-évaluer sur l’atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d’inscription :

• Vous pouvez vous inscrire sur l’une de nos sessions planifiées en inter-entreprises jusqu’à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form"""" signé. Vous recevrez ensuite la convocation et les modalités