IoTcube 보안취약점 자동분석 아이디어 공모전 A to Z

CSSA Center for Software Security and Assurance - SW보안국제공동연구센터

CONcert

제2회 보안취약점 자동분석 아이디어 공모전

with IoTcube Challenge 2017

챌린지와 공모전의 차이점은 무엇인가요?

	블랙박스	화이트박스	네트워크
챌린지	취약 패킷찾기	오픈소스SW 취약점 찾기	TLS Packet 분석 보고서
아이디어 공모전	취약 패킷을 이용 프로토콜 취약점 분석 보고서	1.CVE정보 이용한 PoC 검증 결과 2.컨트리뷰션 사례 3.코드 유사도 검사로 타 모델간 소스 분석	제시된 8개 외 SSL/TLS취약점 검출 추가 아이디어

챌린지에서 요구하는 문제는 IoTcube를 통하여 간단하고 직관적으로 문제만 해결한다면, 공모전은 챌린지 내용에서 더 들어가 관련된 내용을 더 분석하여 결과를 제언해주는 것 입니다.

IoTcube사용 시 어떤 지식이 필요한가요?

IoTcube는 자동 분석 프로그램으로 일반 개발자도 취약점의 전문적인 분석을 가능하게 만들어주는 프로그램입니다. 그렇기 때문에 주변에서 특별한 지식보다는 IoTcube를 개발 환경에서 적용하고 분석결과만 얻을 수 있는 지식이 필요합니다

참가자격에는 제한이 있나요?

아닙니다, 참가자격은 자유로우며, 동일인이 2가지(챌린지, 아이디어 공모전) 모두 참여 가능하십니다.

공모전 주관기관은 어디인가요?

국제공동연구센터(CSSA)는 고려대, 한국인터넷진흥원과 국제적으로 보안 분야의 활발한 연구실적을 보유한 미국 카네기멜론 대학교, 영국 옥스포드 대학교, 스위스 ETH대학교가 함께 참여하고 있습니다.

어떤 내용의 공모전인가요?

보안 취약점 자동분석 플랫폼(IoTcube)를 사용하면 소프트웨어 보안을 전혀 모르는 일반 사용자도 손쉽게 보안 취약점을 탐지하고, 분석해 볼 수 있어, 특별한 기술이나 비용 없이도 자신의 프로젝트의 보안성을 크게 향상 시킬 수 있는 장점이 있습니다.

응모자가 신경써야할 평가 기준은 무엇인가요?

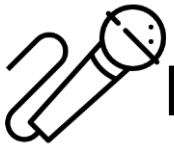
평가위원회를 통해 응모작의 전체적인 완성도를 심사합니다. (실현 구체성, 실질적 도움 여부)참고로 우수작 시상은 공모전 종료 후 개최되는 “IoTcube Conference 2018”에서 거행될 예정입니다.

챌린지는 정답이 있는 건가요?

챌린지의 경우 준비된 양식에 답안을 작성 후 결과물을 제출하시게 되며, 각 문제에 대한 답은 별도로 존재합니다. 이에 답안 양식에 맞춰 작성 후 제출해주시면 됩니다.

IoTcube를 활용해서 오픈소스, 상용 소프트웨어, 웹사이트 등을 대상으로 점검한 취약점 보고서도 응모작 대상이 되나요?

먼저 오픈 소스 프로젝트의 경우, 소스레벨에서 돌려볼 수 있을 것이므로 공모전의 방향성과 잘 맞습니다. 저작권법과 정보통신 관련 법령에 저촉되지 않는 범위 내 상용 소프트웨어와 웹사이트 점검도 마찬가지입니다.



마지막으로 응모자에게 한 말씀

소프트웨어 보안은 멀지도 그렇게 어렵지도 않습니다.
IoTcube를 통해 보안전문가에 도전해보세요~~~