「제1회 「i-Keeper 웹 취약점 경진대회」 대회 공지」

[준수사항 안내]

1. 본 대회는 “대구가톨릭대학교 i-Keeper 정보보안 학술 동아리(이하 ‘동아리’)”에서 주최하며, 대구가톨릭대학교 재학생만 참여 가능합니다.
2. 대회 주최자가 허용한 범위 외 공격 및 침투행위를 금지하여 주십시오.
3. 과도한 스캐닝 및 DDoS 공격을 통해 정상적인 서비스를 방해하는 행위를 금지하여 주십시오.
4. 자동화된 웹 취약점 점검 및 서버 취약점 점검 툴 등 사용은 금지하여 주십시오.
5. 본 대회를 통해 발견한 취약점 및 내부정보를 귀 동아리의 허가 없이 판매 및 발표 등 외부 공개를 금지하여 주십시오.
6. 상기사항 미준수로 인해 주최자의 손해가 발생하지 않도록 주의하여 주십시오.
7. 본 동아리는 대회기간 중 정상적인 보안활동을 유지하고 있기 때문에 사전 공지 및 동의 없이 접속이 차단될 수 있음을 알려드립니다.

※ 본 대회는 해당 동아리에서 개최 하지만 대회 내용은 보안전문가 2명(17학번 윤성호, 18학번 이정우) 및 김기성 교수님께서 주관함으로 대회 진행 및 심사 간의 투명함을 약속드립니다.

※ 상기사항은 “제1회 i-Keeper 웹 취약점 경진대회”참여자가 지켜야 할 준수사항임을 알려드립니다. 이를 위반할 경우 정보통신망법, 형법, 민법 등에 의거하여 처벌 대상이 될 수 있습니다.

저촉 받는 법조항	처벌 내용
- 정보통신망법 제48조, 제49조, 제71조 - 정보통신망법 제48조 제2항	- 5년 이하 징역 또는 5천만 원 이하의 벌금 - 7년 이하 징역 또는 7천만 원 이하의 벌금
- 정보통신망법 제48조 제3항	- 5년 이하 징역 또는 5천만 원 이하의 벌금
- 형법 제307조 제1항의 명예훼손	- 2년 이하의 징역이나 금고 또는 500만 원 이하의 벌금
- (정보통신망을 통하여 행하였을 경우) 정보통신망법 제44조의7 제1항 제2호	- 3년 이하 징역 또는 3천만 원 이하 벌금
- (판매하였을 경우) 부정경쟁방지법 제18조 위반	- (국내) 5년 이하의 징역 또는 5천만 원 이하의 벌금 - (국외) 10년 이하의 징역 또는 1억 원 이하의 벌금
- 민법 제705조 불법행위 규정	- 손해액을 입증하여 해당자에게 손해 상당 금액을 청구가능

[대회 진행 안내]

1. 참가 신청은 Google Form(이하 “구글 폼”)을 통해 참가신청서를 제출하면 완료됩니다.
2. 참가 신청 기간은 2024년 11월 18일(월) 09:00:00부터 2024년 12월 5일(목) 17:59:59까지입니다.
3. 참가 신청서 작성 시 IP대역은 **공인 IP주소**를 명기합니다.
4. 참가 신청 확인 메일과 SMS는 각 개인에게 2024년 12월 6일(금) 18:00:00까지 통보됩니다.(미통보 시 전자우편(whitecrow0413@gmail.com)으로 연락 확인 바랍니다.)
5. 대회 기간은 2024년 12월 7일(토) 10:00:00 ~ 16:59:59 까지입니다.
6. 대회 개시 30분 전(2024년 12월 7일(토) 09:30)까지 각 개인에게 메일과 SMS로 대상 웹서비스의 도메

인이 통보됩니다.

7. 대회 기간 중 발견된 취약점은 취약점 신고서(첨부된 서식 파일 활용)를 작성하여 전자우편(whitecrow0413@gmail.com)로 제출하시면 됩니다.

   * 취약점 심사 시 지정된 시간(2024년 12월 7일(토) 10:00:00 ~ 16:59:59) 이후 접수된 보고서는 심사에서 제외됩니다.

   (※ 취약점 심사 시 동점자가 발생하지 않을 경우 제출 우선순위 가중치는 부여하지 않음.
   동점자 발생 시 보고서 완성도 순으로 가중치 부여 심사)

[취약점 심사 안내]

1. 취약점 심사의 공정성 확보를 위해 i-Keeper 동아리 임원진은 관여하지 않으며 현직 보안전문가 2명(17학번 윤성호, 18학번 이정우)으로 심사위원회를 구성하여 평가 후 담당 교수님(김기성 교수)의 최종 보고로 심사를 진행합니다.
2. 취약점 심사기준은 문서 하단의 **[붙임] 경진대회 취약점 평가 항목**이 기준이 됩니다.
   하기 계산식에 따라 각 취약점 점수가 산정되고 합산 점수가 시상 기준이 됩니다.
   - 총 점수 = 각 취약점 점수의 합
   - 각 취약점 점수 = 위험도 * 평가단계
   - 위험도: 상 3점, 중 2점, 하 1점

   ※ 중복체크: URL 기준으로 체크(동일 URL에서 발생한 종류가 다른 취약점은 인정하나 같은 취약점은 중복으로 처리되어 인정 불가)
   - www.test.com/dashboard URL에서 XSS 취약점과 SQL Injection 취약점 발견 시 두 취약점 모두 보고서 작성 시 점수 획득 가능
   - www.test.com/dashboard URL에서 XSS 취약점을 두 개 이상의 파라미터에서 발견 시 하나만 취약점으로 인정

   ※ 점수 중복 시 보고서의 완성도로 추가 점수 부여(보고서 작성이 미흡할 경우 감점 존재)
3. 취약점 심사 일정과 장소는 공정성 확보를 위해 공개하지 않습니다.
4. 취약점 심사 결과 발표는 2024년 12월 13일(금) 18:00에 각 개인에게 메일과 SMS로 통보됩니다(단, 심사 결과가 빨리 나온 경우는 즉시 통보됨).

[경진대회 시상]

구 분	수 량	상금/상품
대상	1	150,000원
최우수상	1	100,000원
우 수 상	1	50,000원
장려상	2	약 2만원(상당의 기프티콘)
합 계	5	총 340,000원

붙임 경진대회 취약점 평가 항목(1/2)

취약점 명	위험도	평가 단계	취약점 기준
개인정보 유출	상	3	「개인정보 보호법」에 명시된 다수의 "고유식별정보" 유출을 확인한 경우
		2	「개인정보 보호법」에 명시된 다수의 "개인정보" 유출을 확인한 경우
		1	「개인정보 보호법」에 명시된 개인의 "개인정보" 유출을 확인한 경우
파일 업로드	상	3	악성 스크립트 파일 업로드 후 업로드한 악성 파일이 정상 동작한 경우
		2	악성 스크립트 파일 업로드 후 업로드한 악성 파일이 정상 동작하지 않은 경우
		1	악성 스크립트 파일을 업로드하였으나 업로드 파일의 경로를 찾지 못한 경우
파일 다운로드	상	3	애플리케이션 중요정보를 탈취한 경우 (DBMS Connection 정보 등)
		2	시스템 내부 파일을 탈취한 경우 (/etc/passwd 등)
		1	단순 권한 우회로 인한 파일 다운로드를 성공한 경우
인젝션	상	3	DB 내부 중요정보 탈취 및 관리자 권한을 획득하거나 시스템 명령어를 정상적으로 실행한 경우
		2	SQL 쿼리를 이용한 DBMS 버전정보 및 DB명 정도 조회한 경우
		1	단순 참, 거짓 증상 확인 및 DBMS 에러메세지를 확인한 경우
인증 및 세션 관리 취약점	중	3	인증 우회하여 관리자 권한으로 권한 상승한 경우
		2	인증 우회하여 다른 사용자 권한으로 접속하거나 실명 인증우회하여 회원가입 및 로그인한 경우
		1	쿠키 및 세션 재사용 및 중복 로그인을 확인한 경우

붙임 경진대회 취약점 평가 항목(2/2)

취약점 명	위험도	평가 단계	취약점 기준
관리자 페이지 노출	중	3	홈페이지 관리자 페이지 및 Editor, WAS 페이지 접근 후 관리자 계정 절취
		2	홈페이지 관리자 페이지를 확인한 경우
		1	Editor 등 관리 페이지를 확인 한 경우
매개변수 변조	중	3	매개변수 변조로 권한 상승이 이루어진 경우
		2	매개변수 변조로 중요정보를 절취한 경우(중요 문서, 기밀 문서 절취 등)
		1	매개변수 변조로 다른 사용자의 권한을 획득한 경우(게시글 변조 등)
XSS	중	3	XSS 취약점을 이용하여 다른 사용자의 세션을 탈취한 경우
		2	문자열 인코딩 등으로 문자열 필터링을 우회하여 XSS 취약점을 발견한 경우
		1	Reflected, Stored XSS 등 취약점을 발견한 경우
중요정보 노출	중	3	소스코드 내 마스킹 및 암호화된 중요정보 및 개인정보를 복호화한 경우
		2	소스코드 내 하드코딩된 중요정보 및 개인정보를 확인한 경우
		1	서버 및 애플리케이션 등의 버전정보 등을 확인한 경우
암호화 전송 미흡	하	3	전송 구간에서 다른 사용자의 중요정보 및 개인정보를 복호화한 경우
		2	전송 구간에서 다른 사용자의 중요정보 및 개인정보 노출 확인의 경우
		1	전송 구간에서 자신의 정보 평문 노출 확인의 경우
기타 취약점	하	3	알려진 CVE 취약점을 도출한 경우
		2	디렉터리 리스팅 취약점 및 URL 리다이렉트 취약점을 확인한 경우
		1	불필요한 파일 노출(임시 및 테스트 페이지, 백업 파일 등)