웹 서비스 보안성 강화를 위한 Blackbox Pen testing

보안 컨설팅 진행

적용대상

로톡 웹 서비스 2EA

배경

(주)로앤컴퍼니의 '로톡'은 변호사 법률 상담 서비스로, 일반 사용자가 웹 서비스를 통해 예약 후 대면 및 전화를 통해 변호사와 상담을 진행합니다. 최근 다양한 광고/마케팅을 통해 인지도가 올라가고, 서비스를 이용하는 고객이 늘어남에 따라 블랙 해커의 공격 시도에 대비할 필요성이 증가하였습니다. 또한 점차 규모가 확장되는 서비스를 보다 안전하고 안정적으로 운영하기 위해 보안 컨설팅 프로젝트를 진행하였습니다.

적용

프로젝트에는 국내외 해킹대회 우승 및 입상, 한국인터넷진흥원 SW 취약점 신고제 명예의 전당 등재 등 다양한 경력을 보유한 인력이 참여했습니다. 모의해킹은 Blackbox 형태를 시작으로 Whitebox 형태로 전환할 수 있도록 추진하였습니다. 로톡 서비스의 특징을 파악하여 웹을 기준으로 각각 XSS, LFi, SQLi 등의 취약점을 찾았습니다. 발견된 취약점의 상호 연계로 인해 서비스 구조에 영향을 미칠 수 있는 시나리오를 구성하여 대응 방안을 마련하였습니다.

효과

보안 컨설팅을 통해 발견한 다수의 취약점을 보완하는 과정에서 서비스의 보안성을 향상시킬 수 있었습니다. 또한, 정상적으로 패치되었는지 이중으로 확인하는 이행점검 절차를 통해 안정성을 다시 한번 검증할 수 있었습니다. 그러나 새로운 공격 기법이 시시각각 나타나 보안 위협은 여전히 만연하여 주기적인 모의해킹 프로젝트의 도입을 검토하게 되었습니다. 이에 2021 년도에도 추가적인 연간 모의해킹 프로젝트를 진행할 예정입니다.

STEALIEN