

CASTLE 관련 FAQ

한국정보보호진흥원 해킹대응팀

○ CASTLE은 무엇인가요?

CASTLE은 홈페이지에 적용하여 사용할 수 있는 홈페이지 해킹 방지 프로그램입니다.

○ CASTLE은 어떤 뜻인가요?

CASTLE은 "홈페이지를 보호하는 성벽"을 의미합니다. 이는 최근에 성행하고 있는 홈페이지 해킹을 방어할 수 있는 튼튼한 성벽이라는 의미로 CASTLE이라고 명명하였습니다.

○ CASTLE은 어떻게 적용하고, 동작하나요?

홈페이지 관리자는 반드시 CASTLE의 설치 페이지를 통해 설치 과정을 거쳐야 하며, 이후에 모든 어플리케이션에서 공통으로 참조하는 헤더파일에 CASTLE 을 적용(헤더로 선언)해주어야만 합니다. 홈페이지에 적용 하면, 사용자가 전달하는 GET, POST, COOKIE, FILES 데이터를 CASTLE이 먼저 처리하여 공격 문자열들을 사전에 차단하는 방식으로 동작합니다.

○ 지원하는 웹 서버의 종류 및 개발 언어는 어떤 것인가요?

현재 CASTLE은 ASP, JSP, PHP로 제작하여 보급하고 있습니다. 그리고 웹 서버의 종류는 CASTLE의 구동과 관련이 없으므로 Apache, IIS 등 모든 웹서버에서 CASTLE을 이용하실 수 있습니다.

○ CASTLE은 어떤 운영체제를 지원하나요?

CASTLE은 운영체제와 상관없이, ASP, PHP, JSP 어플리케이션으로 운영하는 홈페이지의 경우, 모두 지원 가능합니다.

○ ASP .NET 은 지원하나요?

현재는 ASP 버전만 지원 가능하며, ASP .NET 버전은 지원하지 않고 있습니다.

○ CASTLE과 웹 방화벽 차이는 무엇인가요?

CASTLE은 홈페이지에 설치하여 적용하는 프로그램이므로, 각 홈페이지별로 보안 정책을 다르게 적용할 수 있습니다. CASTLE은 개발 단계에서 적용할 수 있고, 개발자들이 통합적으로 정책을 관리할 수 있는 프로그램입니다. 홈페이지 관리자 또한 소스의 몇 줄을 수정하여 공격 방어능력을 향상시켜 홈페이지의 보안성을 높일 수 있습니다.

○ CASTLE을 설치했는데, 홈페이지에 iframe 같은 악성스크립트가 삽입되었습니다. 어떤 이유인가요?

이미 피해를 입은 홈페이지에 CASTLE을 적용한 경우, 공격자가 설치한 웹셸을 통해 iframe 재 삽입 될 수 있습니다. CASTLE을 설치하기 전 웹셸 검사를 위해 KISA에서 보급하는 웹셸탐지프로그램, WHISTL을 신청하여 점검하시기 바랍니다.

○ CASTLE의 관리자 아이디/패스워드를 분실했습니다. 확인할 수 있는 방법은 없나요?

현재 CASTLE의 경우, 관리자 아이디/패스워드 찾는 기능을 제공하지 않기 때문에 설치 과정 및 패스워드 관리 기능에서 설정하셨던 관리자 아이디/패스워드를 반드시 기억하셔야 합니다. 만약 분실 시에는 정책 파일인 castle_policy.(asp, php, jsp)를 삭제하셔야 하므로, 주의 하셔야 합니다.

○ **RESIN 환경에서도 CASTLE JSP 버전, 운영 가능한가요?**

CASTLE JSP 버전은 주로 Tomcat 환경에서 개발 및 실험을 했지만, RESIN 환경에서도 문제없이 운영할 수 있다는 것을 확인했습니다. RESIN 환경이 Tomcat 환경과 거의 유사하므로, CASTLE을 적용하시는데 크게 문제가 없을 것입니다.

○ **웹방화벽과 함께 사용했을 경우 문제는 없나요?**

웹방화벽과 함께 사용해도 전혀 문제가 없습니다. 하지만 탐지 룰이 중복될 경우는, 웹방화벽이 먼저 차단하므로 착오 없으시길 바랍니다.

○ **저희 홈페이지에는 모든 어플리케이션 파일에서 공통으로 참조하는 헤더파일이 없습니다. 어떻게 CASTLE을 적용 해야 하나요?**

공통으로 참조하는 헤더파일이 없는 경우는, 다소 불편하시더라도 모든 파일에 CASTLE을 적용해 주셔야 합니다. 이러한 경우를 대비한 스크립트 및 대응 방법에 대해 계속해서 연구하고, 대비하도록 하겠습니다.

○ **CASTLE 을 적용할 경우 홈페이지 응답시간이 느려지지 않나요?**

자체적으로 점검을 한 결과, 일반적인 홈페이지 운영환경에서는 느려지는 문제는 없었습니다. 하지만, 상당히 많은 동시 접속자들이 일정 시간 접속하는, 심한 스트레스를 받는 경우는 일부 성능이 떨어지는 현상이 있을 수 있습니다.