

휘슬(WHISTL) 관련 FAQ

한국인터넷진흥원 해킹대응팀

○ 휘슬(WHISTL)이 무엇인가요?

공격자가 웹서버에 설치한 백도어 프로그램인 웹셸(Web Shell)을 찾는 프로그램입니다.

○ 휘슬(WHISTL)은 어떤 뜻인가요?

WHISTL은 **Web Hacking Inspection Security Tool**의 머리글자 모음입니다. 또한 발음으로는 Whistle와 동일하여 호루라기, 경적을 의미합니다. 이는 해당 프로그램이 웹셸을 탐지하는 경우 관리자에게 알려주어 대응을 하도록 한다는 의미로서 WHISTL을 명명하였습니다.

○ WHISTL은 어떻게 동작하나요?

반드시 웹 서버에 WHISTL을 설치 또는 복사하여 사용합니다. 또한 점검 대상 서버가 다수인 경우 개별 서버에 모두 프로그램을 복사해야 합니다. WHISTL은 웹서버가 운영중인 컴퓨터에서 웹문서 디렉토리에 존재하는 모든 웹문서 파일의 소스코드를 점검하는 방식으로 동작합니다.

○ 지원하는 웹 서버의 종류 및 개발 언어는 어떤것인가요?

현재 WHISTL은 ASP, JSP, PHP로 제작된 웹 셸을 탐지합니다. 그리고 웹 서버의 종류는 WHISTL의 구동과 관련이 없으므로 Apache, IIS 등 모든 웹서버에서 WHISTL을 이용하실 수 있습니다.

○ WHISTL은 어떤 운영체제를 지원하나요?

현재 Microsoft의 윈도우 서버 계열, 리눅스 커널 2.4/2.6을 지원합니다. 아직까지 유닉스(Solaris, HP-UX, IBM-AIX)는 지원하지 않고 있으며 조만간 지원할 계획입니다.

○ 윈도우, 리눅스 웹서버를 다수 운영중인데 버전마다 신청서를 따로 작성해야 하나요?

신청은 1 회만 신청하면 됩니다. 그리고 배포시 첨부하는 WHISTL 프로그램은 윈도우 버전 및 리눅스 2.4, 2.6 버전 모두를 포함하고 있으니 관리자가 선택하여 사용할 수 있습니다.

○ 웹 서버가 매우 많은 웹 호스팅 업체입니다. 모든 서버에 복사하기가 번거로운데 Client/Server 방식의 중앙집중 관리 프로그램 형식은 지원하지 않는가요?

WHISTL은 최초 설계부터 단일 프로그램을 염두에 두었습니다. 다만 향후 프로그램의 기능 개선에 대해서 대형 사이트를 염두에 둔 Client/Server 형식도 고려하고 있습니다.

○ WHISTL과 웹 방화벽의 차이는 무엇인가요?

WHISTL은 공격자가 설치한 웹셸을 찾는 프로그램입니다. 이에 반해 웹방화벽은 공격자의 공격을 실시간으로 차단하는 기능을 가지고 있습니다. WHISTL을 통해서 웹셸이 발견되는 경우 공격자의 공격 지점을 파악하고 홈페이지 소스코드 수정, 웹 방화벽의 보안정책 설정을 통해서 보안을 강화하셔야 합니다.

○ **WHISTL이 웹쉘을 찾아냈다면 홈페이지가 해킹되었다고 판단해야 하나요?**

꼭 그렇지는 않습니다. 일반적으로 모의해킹과 같은 취약점 점검시에도 시험적으로 웹쉘을 업로드하는 공격을 하기도 합니다. 그리고 공격자가 웹쉘 업로드는 성공하였지만 실행권한이 없어서 공격이 성공하지 못하는 경우도 있습니다. 그러므로 웹쉘이 발견되면 해당 서버가 공격을 당했는지 침해사고 분석을 진행하여 최종 판단을 해야 합니다.

○ **정보보호에 관심이 많은 개인 사용자입니다. 홈페이지 관리자가 아니라 개인 사용자도 WHISTL을 사용할 수 있나요?**

WHISTL의 개발은 홈페이지 관리자의 보안점검을 돕기 위함이 1차적인 목적입니다. 그러므로 현재 개인사용자에게는 보급되지 않고 있습니다. KISA는 향후 WHISTL의 배포 대상을 확대할 예정입니다.

○ **홈페이지에 iframe으로 포함된 악성 스크립트도 탐지할 수 있나요?**

현재 버전에서 iframe으로 삽입된 내역에 대해서는 탐지하지 않습니다. 이 기능은 차기 버전에서 구현될 예정입니다.

○ **최초 사용자 등록시 발급받은 아이디와 패스워드를 수정하고 싶습니다. 어디에서 수정할 수 있나요?**

기존에 발급된 아이디/패스워드를 사용자가 직접 수정은 지원하지 않습니다. 변경하고자 하시면 whistl@krcert.or.kr로 메일을 주시기 바랍니다.

○ **프로그램의 업데이트가 필요한 이유는 무엇인가요? 그리고 인터넷이 되지 않는 환경에서도 WHISTL을 사용할 수 있나요?**

WHISTL은 공격자의 웹쉘을 탐지하는 프로그램입니다. 만일 공격자가 WHISTL에 탐지되지 않도록 신규로 웹쉘을 생성하였다면 이를 탐지하지 못하는 경우가 발생합니다. 이는 신규 바이러스에 대해서 백신 프로그램이 탐지하지 못하는 것과 동일한 경우입니다.

이를 위해서 한국인터넷진흥원은 지속적으로 웹쉘을 수집하여 최신 패턴을 적용하고 업데이트를 하도록 개발하였습니다. 그러므로 최신의 패턴을 사용하기 위해서는 주기적으로 업데이트를 실행하셔야 합니다.

WHISTL은 인터넷이 되지 않는 환경에서도 프로그램 구동에는 전혀 문제가 되지 않습니다. 다만 실행시 최신 웹쉘 패턴이 업데이트가 되지 않으며, 이 경우 가장 최근에 업데이트한 웹쉘 패턴을 점검에 사용합니다.