디페이스 공격 및 워드프레스 취약점

202219934
it지능정보공학과
정보경

관련 기사

보안뉴스

#전체기사 | #시큐리티월드 | #사건사고 | #프리미엄리포트

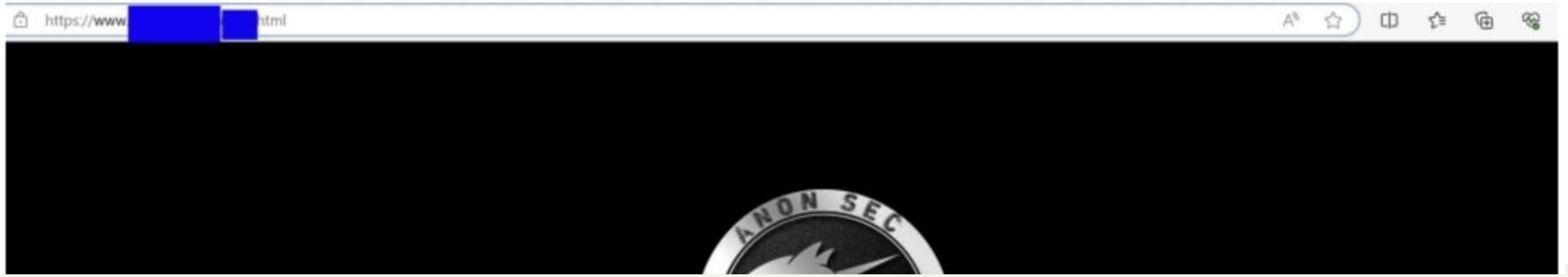
교육서비스 플랫폼 런피아, 웹사이트 해킹... 해커, 유튜브에 해킹 과정 공개

2024-01-22 15:13

국내 교육서비스 플랫폼 런피아, 웹사이트 위·변조 정황 포착

해커, 해킹 과정 유튜브 통해 공개...또 다른 해커, 디페이스 해킹 흔적 남겨

[보안뉴스 김경애 기자] 국내 교육서비스 플랫폼 런피아(learnpia)의 웹사이트가 위·변조(디페이스 해킹)된 정황이 포착됐다. 특히 이번 공격은 해당 웹사이트의 워드프레스 취약점을 악용한 공격으로 추정돼 취약점 조치의 중요성이 한층 부각되고 있다. 더욱이 해커가 해킹 과정을 유튜브로 공개하고 있어 이에 따른 추가 피해 가능성도 커지고 있다.



디페이스 공격 및
워드프레스 플러그인 취약점

디페이스 공격이란?

'Deface - 외관을 훼손하다'

- 웹 사이트의 첫 화면,즉 홈페이지를 해커가 마음대로 바꾸고 해킹을 성공했음을 알리는 공격형태

- 디페이스 공격은 주로 정치적 메시지를 전달하거나, 해킹을 성공했다는 실력 과시용으로 활용된다. 또한 공인이나 기업 혹은 기관의 이미지를 손상시키기 위한 공격 방식으로도 활용된다.

- 공격을 당했을 때 피해가 심각하지 않더라도, 웹사이트의 보안이 취약하다는 것이므로 위험을 인지하고 관련 조치를 취해야 함

디페이스 공격 및
워드프레스 플러그인 취약점

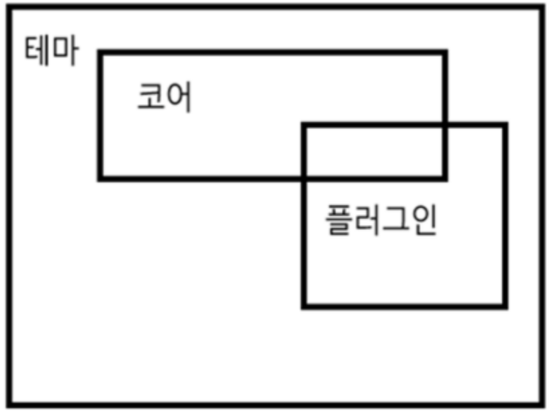
워드프레스 CVE 취약점이란?

워드프레스(WordPress) : 전 세계 모든 웹사이트의 40%가 사용 중인 웹사이트 제작 및 관리 시스템

- 사이버 공격자는 웹 서버를 공격 타깃으로 정할 때, 워드프레스 CVE 취약점 패치가 되지 않은 오래된 버전의 워드프레스 웹 서버를 탐색하기도 한다.
- 워드프레스로 제작된 웹페이지는 개인 블로그, 기업 블로그, 기업 공식 홈페이지까지 다양한 용도로 사용되기 때문에, 보안 패치가 되지 않은 취약한 워드프레스는 해커들의 주요 표적이 된다.
- MITRE Corporation의 CVE 통계 데이터 - 2004년부터 2022년 9월까지 발견된 워드프레스 CVE 취약점은 총 344개로, 그중 실제 공격자가 익스플로잇 가능한 CVE 취약점은 11개이다.

- 워드프레스 취약점은 크게 세 부분(**워드프레스 자체 취약점, 테마 취약점, 플러그인 취약점**)에서 발생하며, 이 중 플러그인에서 가장 많은 취약점이 발생한다.

- 워드프레스 플러그인은 누구든지 개발할 수 있는 장점이 있으나, 보안상 검증되지 않은 플러그인 사용으로 인해 취약점이 지속적으로 발생하고 있다.



디페이스 공격 및
워드프레스 플러그인 취약점

디페이스 공격과 워드프레스 CVE 취약점

- 디페이스 공격을 하기 위해서는 해커는 일단은 홈페이지 서버의 권한을 가져와야 한다.
- XSS(크로스 사이트 스크립팅), SQL 인젝션, 파일 업로드 취약점을 이용한 공격, 보통은 게시판에 웹쉘을 업로드하여 공격을 하게 된다.
- 웹쉘(Web Shell)은 해커가 악의적인 목적을 가지고 웹 서버에서 임의의 명령을 실행하도록 만든 악성코드이다.
- 취약점들을 이용해서 웹 서버의 권한을 얻게 되면 그 이후에 해커는 홈페이지 변조 혹은 추가로 다른 공격을 할 수 있는 선택지가 늘어나게 된다.

워드프레스 CVE 취약점 종류

- XSS(크로스 사이트 스크립팅)
- Http Response Splitting
- Execute Code
- Sql Injection
- Gain Information
- Denial of Service
- Directory Traversal
- Bypass Something
- CSRF
- Gain Privilege
- File Inclusion

디페이스 공격 및
워드프레스 플러그인 취약점

XSS(크로스 사이트 스크립팅) 취약점

: 웹사이트에 악성 스크립트를 주입하는 행위

공격자가 상대방의 브라우저에 스크립트가 실행되도록 해 사용자의 세션을 가로채거나,
웹사이트를 변조하거나, 악의적 콘텐츠를 삽입하거나, 피싱 공격을 진행하는 것

해커는 사람들이 친밀하고 안전하다고 생각하는 웹사이트에 악성 스크립트를 주입하고, 악성 스크립트가 포함된 게시글을 열람한 피해자들의 쿠키는 해커에게 전송됩니다.

- 공격대상 : 스크립트 언어와 취약한 코드

- 주요 목적 : 사용자의 정보 도용

- 로그인 입력란을 감염시켜 로그인 세부 정보와 쿠키를 탈취하는 방식으로 진행 -> 악성 소프트웨어는 사용자의 세부 정보를 기록해 해커에게 전송하고, 해커는 해당 정보를 사용해 피해자의 계정을 제어할 수 있게 된다.
- 악의적인 사용자가 C&C 서버로 리디렉션하기 위해 리디렉션 스크립트를 주입해 중간 경유지로 활용되기도 하며, 사용자의 쿠키를 탈취해 세션 하이재킹(Session Hijacking) 공격을 수행하는 역할을 하기도 한다.

디페이스 공격 및
워드프레스 플러그인 취약점

SQL Injection

SQL을 사용하는 이유:

웹 사이트를 운영하는데 있어 대용량의 데이터에 대한 관리 및 처리가 요구됨 -> 이런 데이터들을 단순히 텍스트 파일로 저장하거나, 파일로 간단하게만 관리한다면 양이 막대하기 때문에 원하는 데이터에 대한 조회,삭제,수정등의 처리가 곤란해지기 때문

SQL Injection : 악의적인 사용자가 보안상의 취약점을 이용하여, 임의의 SQL 문을 주입하고 실행되게 하여 데이터베이스가 비정상적인 동작을 하도록 조작하는 행위

우선 Injection 의 뜻은 "삽입한다" 는 뜻

즉, 개발자가 만들어놓은 SQL 쿼리 문에 서비스 사용자의 데이터 입력 값이 삽입된 후 악의적으로 활용되는 기법이다.

이때 서비스 사용자란 정상적인 사용자가 아닌, 해커들이 악의적으로 넣는 입력 데이터이다. 서비스 사용자의 입력값이 서버측에서 코드로 입력되어 실행되는 코드 인젝션 공격 기법 중 하나이다.

디페이스 공격 및
워드프레스 플러그인 취약점

더 공부하고 싶은 내용

- 대표 취약점의 방어 방법
- 세션하이재킹의 원리
- 취약점 진단, 대응방법

디페이스 공격 및
워드프레스 플러그인 취약점