LattePanda 웹서버 취약점 보고서(164)

정보보안과 황태호

내용

개요  [1](#_Toc330396898)

[결과 요약 2](#_Toc330396899)

[분석 결과 3](#_Toc330396900)

[대응 방안 4](#_Toc330396901)

총평  [5](#_Toc330396902)

# 개요

본 취약점 보고서는 개인 웹 서버의 취약점을 분석하고 대응 방안 제시 및 취약점 보완을 목적으로 함.

## 점검 항목

1. SQL Injection
2. XSS
3. Session Management
4. Directory Listing
5. Information leakage
6. File upload exploit
7. 안전하지 않은 암호 저장
8. 불충분한 전송 계층 보호

# 결과 요약

현재 시점에서 취약점 분석을 통해 결과로 나타난 대상 시스템에 대한 수준 평가입니다.

아래의 기준에 따라 평가 등급을 나누게 됩니다.

A - 안전

취약한 보안 문제점 발견되지 않음

B - 양호

비교적 위험도가 낮은 취약점 존재

서버 환경 설정 미비로 인한 단순 정보 유출 가능성 존재

C - 취약

비교적 위험도가 높은 취약점 존재 / 서버 주요 정보 유출 가능

개인 정보 유출 가능

D - 매우 취약

관리자 권한 획득 가능

서버 시스템 접근 및 웹 소스 파일 접근 / 수정 가능

|  |  |  |  |
| --- | --- | --- | --- |
| 사이트 | 도메인 | 등급 | 비고 |
| - | http://10.156.146.164/index.php | C |  |

# 분석 결과

## 항목별 취약점 발생 여부

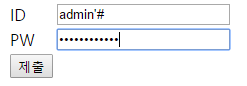
|  |  |
| --- | --- |
| 1. SQL Injection | O |
| 1. XSS | X |
| 1. Session Management | O |
| 1. Directory Listing | X |
| 1. Information leakage | X |
| 1. File upload exploit | X |
| 1. 안전하지 않은 암호 저장 | O |
| 1. 불충분한 전송 계층 보호 | O |

# 세부 사항 및 대응 방안

## Session Management

* 오랜 시간이 지나도 세션이 유지됨.
* **대응 방안**
* 세션 타임아웃을 설정하여 일정 시간이 지나면 세션을 종료하도록 함.

**-SQL Injection**





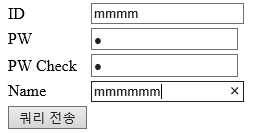
- 간단한 인젝션으로 관리자 계정 탈취가 가능하다.

**- 대응 방안**

**-** 입력 값 검증을 통해 구문이 DB서버로 전달되는 것을 방지함.

**-** 치환 함수를 통해 특수문자를 일반 문자열로 전환 EX) addslashe()

## 안전하지 않은 암호 저장



* 비밀 번호가 한 글자임에도 로그인 및 회원가입이 가능함.
* **대응 방안**
* 암호의 최소 길이 제한을 설정한다.
* 민감한 정보의 경우 DB에 암호화 하여 저장한다.

## 불충분한 전송 계층 보호





* 로그인, 회원가입, 글쓰기 할 때 정보가 그대로 노출되어있음.
* **대응 방안**
* 로그인 또는 회원가입시에 값을 전달할 때에 암호화 하여 값을 전달하도록 함.
* SSL을 적용하여 스니핑에 의한 정보유출을 방지함.

# 총평

* XSS 취약점은 발생하지 않았으나 로그인과 회원가입 과정에서 값을 넘겨주는데 평문으로 넘겨주는 취약점이 발견되었다. 암호화 하여 값을 넘겨주는 과정이 필요해 보이며 암호의 길이를 검증하여 취약한 암호는 사용하지 않도록 하는 것이 좋겠다.