LattePanda 웹서버 취약점 보고서(177)

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 |
| Lad page | http://192.168.137.2/index.html | D |  |

# 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

## SQL Injection



* 1','2','3')# 구문으로 게시판에서의 순서 확인
* 1',(select passwd from register where id = 'lad'),'3')# 구문으로 DB 내의 lad 계정 패스워드 탈취

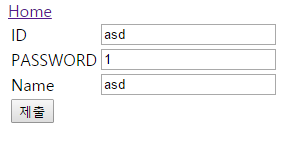


* 성공.
* **대응 방안**
* 입력 값 검증을 통해 구문이 DB서버로 전달되는 것을 방지함.
* 치환 함수를 이용해 특수문자를 일반 문자열로 전환함.
* Addslashe()

## Session management

* 오랜 시간이 지나도 세션이 유지되어 있다.
* 공격자가 사용자의 세션을 탈취할 수 있음.
* **대응 방안.**
* 세션 타임아웃을 설정하여 일정 시간이 지나면 세션이 종료되도록 설정함.

## 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

* sql인젝션 취약점이 발생하여 어렵지 않게 관리자 권한을 획득하는 것을 볼 수 있다. 또 사용자 계정 관리 부분에 대해서 암호화가 전혀 이루어 지고 있지 않다. 회원가입, 로그인 과정에서 암호화를 거치지 않고 평문으로 DB서버로 전송하게 되는데 DB칼럼 이름 까지 노출된다. 이는 중간의 공격자가 패킷을 스니핑하여 계정 탈취가 가능하므로 보완해야 할 것이다. 또한 파일 업로드에 대한 제한이 없어 공격자가 악성 스크립트를 업로드 할 경우 쉽게 서버 장악이 가능하다.