웹사이트 보안 취약점 개선

"세.다.책"
[대학생들을 위한 중고책 쇼핑몰]

KOREATECH

2022-2학기

컴퓨터보안

2019136151 이상영

Contents.

Part 1,

웹사이트 소개

Part 1,

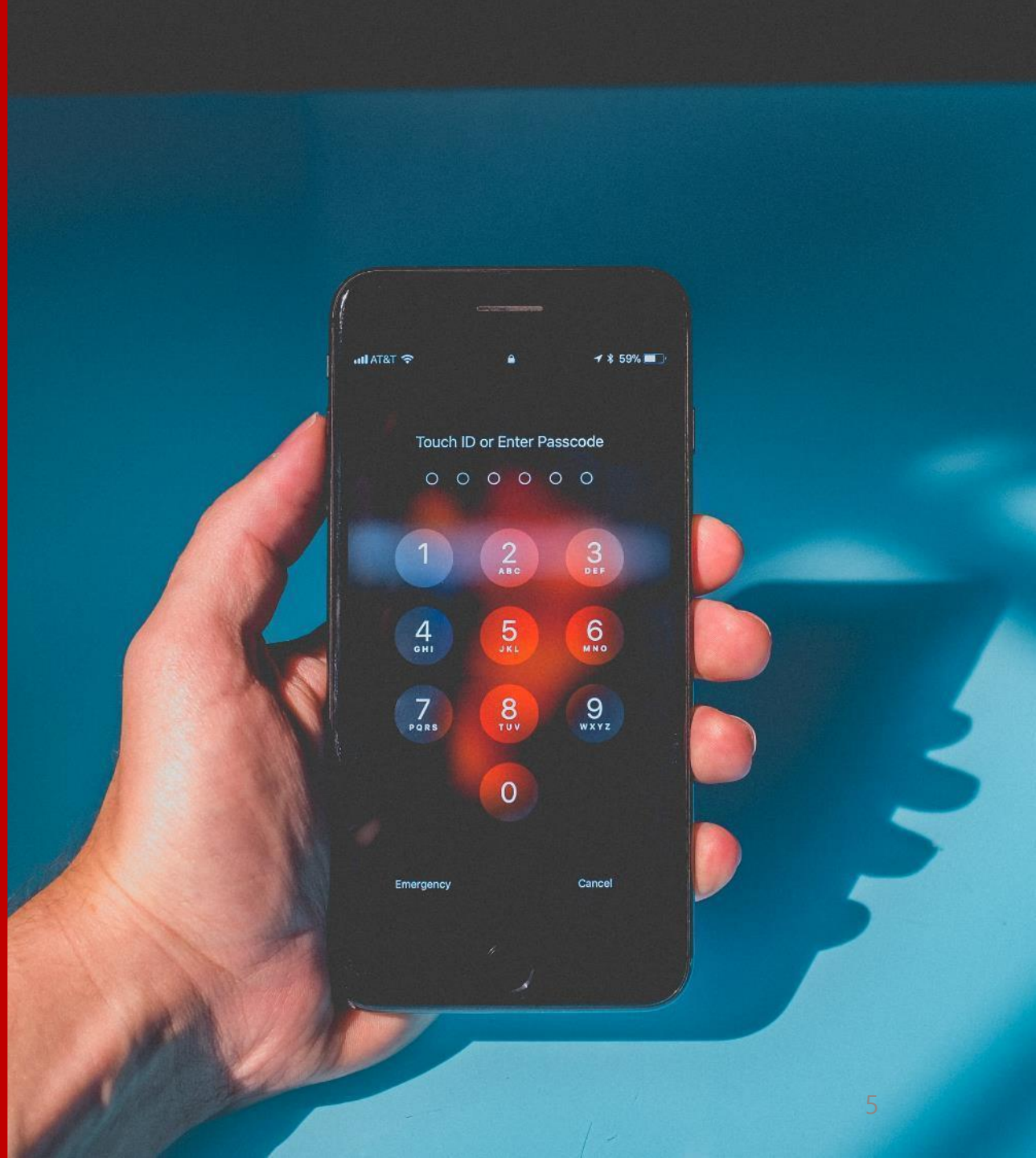
웹사이트 소개

What is “세.다.책”?

사이트명	세.다.책(세상에 다 쓴 책은 없다)
주제	중고책 쇼핑몰
개발기간	2022.03 ~ 2022. 06(3개월)
개발목적	대학생들이 조금 더 편하게 중고 책을 거래할 수 있는 환경 구축
주요기능	▪ 로그인 ▪ 회원정보 수정 ▪ 중고책 판매 등록 ▪ 상품 검색 ▪ 공지사항 게시판 ▪ 홍보(구매/판매) 게시판 ▪ …
개발언어	HTML, CSS, JavaScript, PHP, MySQL

Part 2,

보안 취약점


AT&T
59%
Touch ID or Enter Passcode
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0
Emergency
Cancel

Part 2,

보안 취약점

Security Vulnerability

비밀번호 노출

개선 전 웹사이트는 **비밀번호가 암호화 과정**을 거치지 않고, DB에 저장되어 DB가 노출될 경우 비밀번호 유출 위험이 존재함

SQL Injection

쇼핑몰의 특성 상 입력창(INPUT) 이 많은데, 이곳에 잘못된 값을 입력 시 SQL 에러문장이 출력되면서 DB를 유추할 수 있음

비정상 접근

사용자(비회원, 회원, 관리자)별로 접근이 가능한 사이트가 설정되어 있지 않아, 비정상적인 접근이 가능함

보안 취약점

Security Vulnerability

비밀번호 노출

개선 전 웹사이트는 **비밀번호가 암호화 과정**을 거치지 않고, DB에 저장되어 DB가 노출될 경우 비밀번호 유출 위험이 존재함

num	userid	pass	username	tel	email	gender	school_id	user
1	chumji	1234	김첨지	01012348568	chumji1940@naver.com	0	한국공과대학교	
2	admin	1234	세다책	01012345798	admin@babook.com	0	한국기술교육대학교	
3	sodud39	hansy5590!	한소영	01073783028	sodud39@babook.com	1	한국기술교육대학교	
4	sangho	sangho!@	이상호	01085413564	sangho@gmail.com	0	충남대학교	
5	samsun	samsun!@	김삼순	01085771325	samsun@gmail.com	0	경기대학교	
6	test	1234	가나다	01098854772	test@naver.com	0	충남대학교	

암호화되지 않은 비밀번호

보안 취약점

Security Vulnerability

SQL Injection

쇼핑몰의 특성 상 입력창(INPUT) 이 많은데, 이곳에 잘못된 값을 입력 시 SQL 에러문장이 출력되면서 DB를 유추할 수 있음

SQL 에러 문장 노출
(DB 유추 가능)

보안 취약점

Security Vulnerability

비정상 접근

사용자(비회원, 회원, 관리자)별로 접근이 가능한 사이트가 설정되어 있지 않아, 비정상적인 접근이 가능함

비회원 마이페이지 접근

Part 3,

개선사항

Part 3,

개선사항

Improvement Contents

비밀번호 암호화

회원가입 시 입력된 비밀번호를 bcrypt 해시 알고리즘을 통해 암호화 한 뒤 DB에 저장하여 로그인 시 해당 값을 비교함

```php
<?php
    $id = $_POST["id"];
    $pass = $_POST["pswd1"];
    // 비밀번호 암호화
    $pass = password_hash($pass, PASSWORD_DEFAULT);
    $name = $_POST["Name"];
```

num	userid	pass	username
1	chumji	$2y$10$T80Y.BRpttJyY/c0eh6kG.a6JcjWgudzo0uM9FoMsTL...	김첨지
2	admin	$2y$10$zr1Tty9LpAGj9/8prgXo0.pNS.HxDS4qJh1/Nd8k/fb...	세다책
3	sodud39	$2y$10$Ly4Zc9E5tN.Mjl/3yjWvk.ATGbIpAABkU6DwVviCo4O...	한반도
4	sangho	$2y$10$Vp3NMbzNFnbMkoN7AI96/.lTsD6a1WJZMS2QrcYn1xt...	이상호
5	samsun	$2y$10$gn3Y96V6dL6/DQbmSz0jB.X/QeFTEvjUT0wn/RVz6cr...	김삼순
6	test	$2y$10$mBrWhEz2yWuooWgxxEi9YOJNXxPAM8lDkE.ghVmTu3Y...	테스터
7	sans	$2y$10$aAOCB7baWmvR2PAgSTd5xu8ZES3EpfhP8ejK4Ao8Jsb...	이상영

```php
    $row = mysqli_fetch_array($result);
    $db_pass = $row["pass"];
    mysqli_close($con);
    // [개선 전 비밀번호 비교]
    // if ($pass != $db_pass)
    // [개선 후 비밀번호 비교]
    if(!password_verify($pass, $db_pass))
    {
    echo("
    <script>
        window.alert('비밀번호가 틀렸습니다')
```

① 비밀번호 암호화

(password_hash, bycrpt 해시 알고리즘 사용)

② 암호화 비밀번호 저장

③ 비밀번호 비교

(password_verify)

개선사항

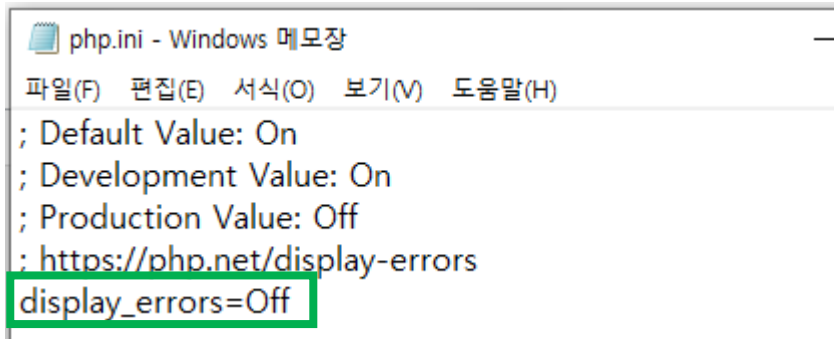
Improvement Contents

SQL Injection 방지

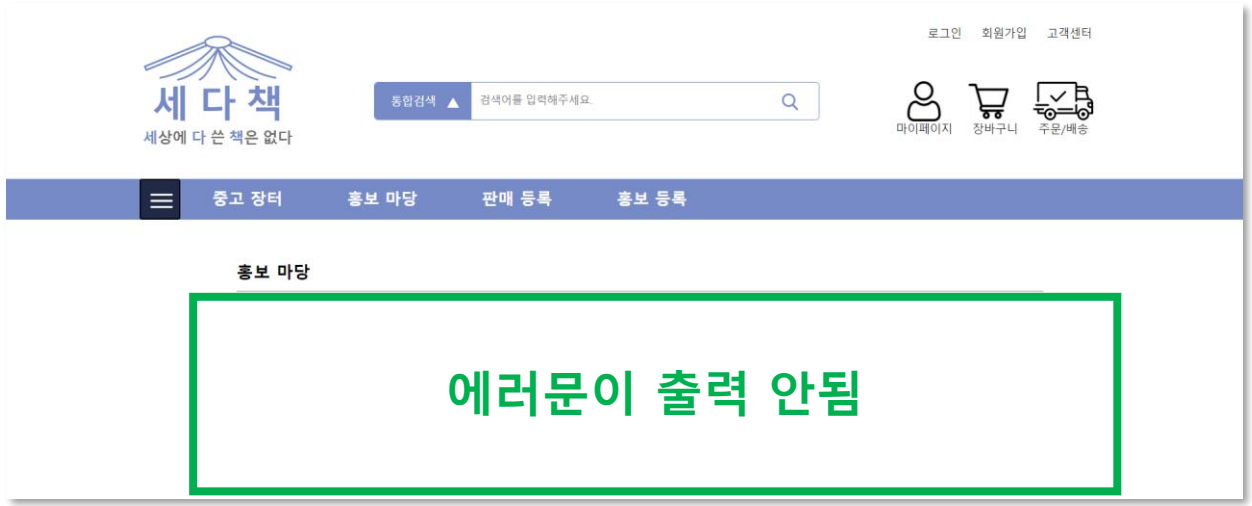
공격자가 SQL Injection을 수행하기 위해서는 DB의 정보(테이블명, 컬럼 명 등)이 필요하다. 따라서, 에러 발생시 에러문이 보이지 않도록 처리하여 사전에 위험 요소를 제거함

```php
<?php
    // Mysql 에러 출력 제거
    ini_set( 'display_errors', '0' );
?>
```

방법 1.
페이지별 코드 삽입
(ini_set('display_errors', '0'); 설정)



방법 2.
php.ini 파일 수정
(display_errors=Off로 변경)



Part 3,

개선사항

Improvement Contents

비정상 접근 불가

사용자(비회원, 회원, 관리자)별로 level을 나누고, session을 통해 검사하여 일치하지 않는 경우
해당 페이지에 접근이 불가하도록 함

num	userid	pass		gender	school_id	userlevel
1	chumji	$2y$10$T	r.com	0	한국공과대학교	9
2	admin	$2y$10$z	om	0	한국기술교육대학교	1
3	sodud39	$2y$10$L	.com	1	한국기술교육대학교	9
4	sangho	$2y$10$V	m	0	충남대학교	9
5	samsun	$2y$10$g	m	0	경기대학교	9
6	test	$2y$10$m		0	충남대학교	9
7	sans	$2y$10$a	m	0	KOREATECH	9

① 사용자 level 설정

```php
<?php
  <div id="gnb">
      <ul id="gnb_menu">
          <?php
              if(!$userid){
          ?>
          <li><a href="/BABOOK_Project/login_form.php">로그인</a></li>
          <li><a href="/BABOOK_Project/signUp/verification.php">회원가입</a></li
          <?php
              }else{
                  $logged = "<a href='/BABOOK_Project/member/modify_form.php'>"
          ?>
          <li><?=$logged?></li>
          <li><a href="/BABOOK_Project/logout.php">로그아웃</a></li>
          <?php
              }
              if($userlevel == 1){
          ?>
          <li><a href="/BABOOK_Project/admin/dashboard.php">관리자 모드</a></li>
          <?php
              }
?>        ?>
```

② 페이지별 session 검사

(level에 일치하는 경우 or 로그인한 경우, 관리자인 경우 접속 가능)

Q & A

웹사이트 보안 취약점 개선

"세.다.책"
[대학생들을 위한 중고책 쇼핑몰]

KOREATECH

2022-2학기

컴퓨터보안

2019136151 이상영

「 감사합니다. 」