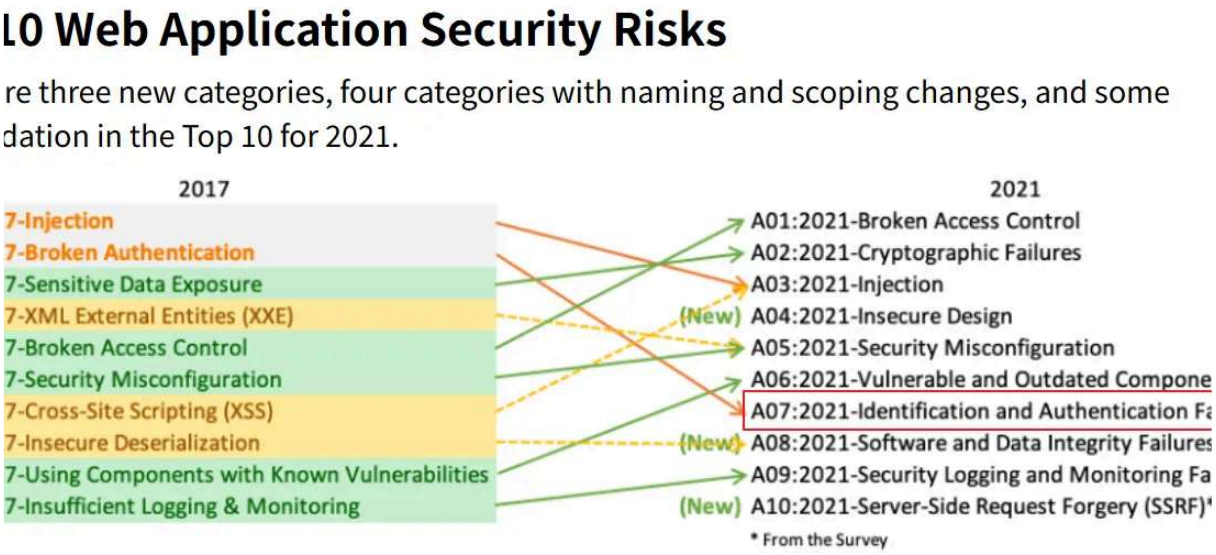
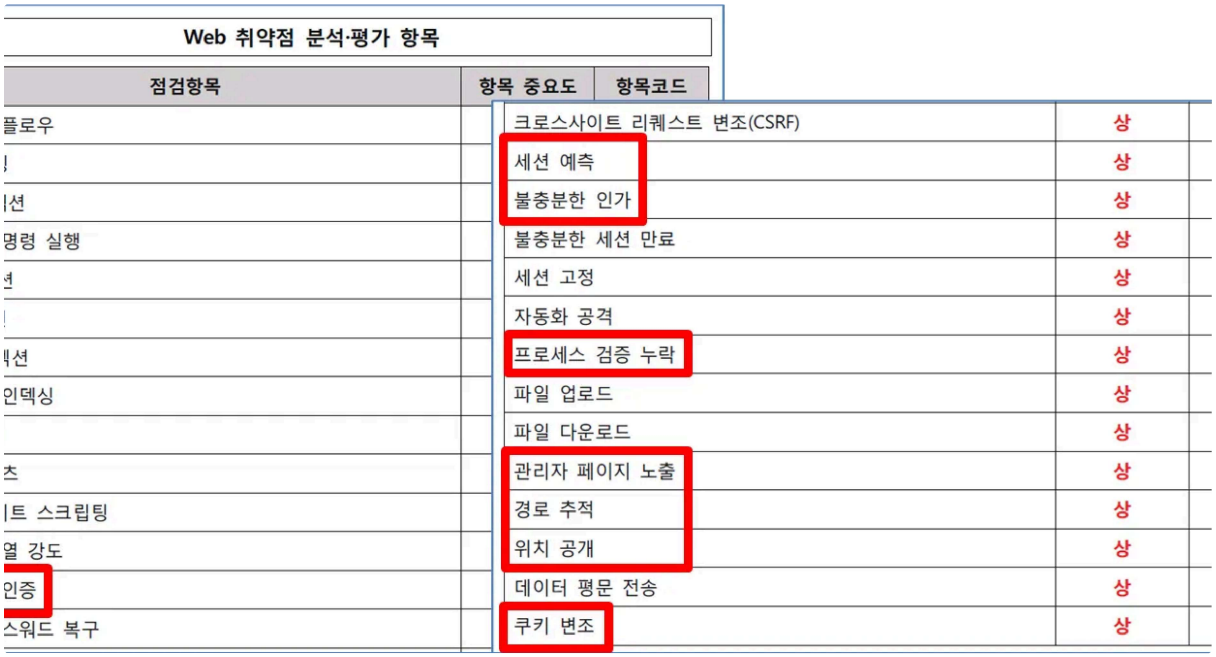
인증 및 인가 취약점

부적절한 인증 및 인가

- 인증 및 인가에 대한 검증 로직이 잘못 구현되었을 때 발생
- 다른 사용자 게시글 수정/삭제, 관리자 페이지 접근, 다른 사용자 비밀번호 변경, 2단계 인증 우회, 결제 로직 우회 등





Web 취약점 분석·평가 항목

점검항목	항목 중요도	항목코드		
플로우		크로스사이트 리퀘스트 변조(CSRF)	상	
		세션 예측	상	
션		불충분한 인가	상	
명령 실행		불충분한 세션 만료	상	
션		세션 고정	상	
		자동화 공격	상	
션		프로세스 검증 누락	상	
인덱싱		파일 업로드	상	
		파일 다운로드	상	
츠		관리자 페이지 노출	상	
트 스크립팅		경로 추적	상	
열 강도		위치 공개	상	
인증		데이터 평문 전송	상	
스워드 복구		쿠키 변조	상	

- 649 페이지

한국인터넷진흥원

https://www.kisa.or.kr/2060204/form?postSeq=12&lang_type=KO&page=1

다양한 시나리오

1. 다른 사용자 게시물 수정 및 삭제 여부
   - 다른 사용자의 게시물을 수정하거나 삭제할 수 있는지 여부.
   - 해당 페이지에 개인정보가 포함되어 있는지 여부.
2. 다른 사용자 개인정보 수정 페이지 접근 가능 여부
   - 다른 사용자의 개인정보 수정 페이지에 접근할 수 있는지 여부.
   - 이력서 서비스, Q&A 상담글, 1:1 문의 게시물 등도 동일한 프로세스.
3. 비밀글 접근 가능 여부
   - 비밀글(상담글 등)에 접근할 수 있는지 여부.
   - 사용자가 비밀글을 체크한 이유를 고려한 접근 가능성.
4. 상품 결제 금액 조작 여부
   - 상품 결제 금액, 할인율, 쿠폰, 카드 할인율, 배송비 등을 조작할 수 있는지 여부.
   - 금액 조작뿐만 아니라 배송 프로세스까지의 관리적인 문제 도출 가능성.

5. 쿠키 세션 정보를 이용한 권한 상승 여부
    - 쿠키 세션 정보를 이용해 권한 상승이 가능한지 여부.
    - 획득한 세션 정보로 접근할 수 없던 관리자 페이지에 접근 가능 여부.
    - 회원 관리, 게시판 관리 등 다양한 접근 시나리오 구상 가능성.
6. 공인인증서 우회를 통한 권한 획득 여부
    - 공인인증서 로그인 과정에서 타인의 정보를 이용해 권한 우회가 가능한지 여부.
7. 다른 사용자의 온라인 증명서 발급 가능 여부
    - 발급 페이지 솔루션의 인증 처리를 우회하여 다른 사용자의 개인정보가 포함된 증명서 발급 가능 여부.
8. 유료 콘텐츠 접근 가능 여부
    - 유료 서비스를 신청한 사용자에 대한 체크 권한을 우회하여 유료 콘텐츠에 마음대로 접근 및 다운로드 가능한지 여부.
9. **회원 가입 과정에서 자바스크립트 우회**

우선 쇼핑물 설치 (복습용)

gm.zip 16431.8KB

```
bee@bee-box:~$ sudo su - [sudo] password for bee: root@bee-box:~#
root@bee-box:~# root@bee-box:~# mkdir /var/www/gm root@bee-box:~# cp
/home/bee/gm.zip /var/www/gm/ root@bee-box:~# cd /var/www/gm/ root@bee-
box:/var/www/gm# ls gm.zip root@bee-box:/var/www/gm#
```

```
root@bee-box:/var/www/gm# mysql -u root -p Enter password: bug (입력)
Welcome to the MySQL monitor. Commands end with ; or \g. Your MySQL
connection id is 39 Server version: 5.0.96-0ubuntu3 (Ubuntu) Copyright (c)
2000, 2011, Oracle and/or its affiliates. All rights reserved. Oracle is a
registered trademark of Oracle Corporation and/or its affiliates. Other
names may be trademarks of their respective owners. Type 'help;' or '\h'
for help. Type '\c' to clear the current input statement. mysql> show
databases; +--------------------+ | Database | +--------------------+ |
information_schema | | bWAPP | | drupageddon | | mysql | +----------------
----+ 4 rows in set (0.00 sec) mysql> create database gmshop; Query OK, 1
row affected (0.00 sec) mysql> show databases; +--------------------+ |
Database | +--------------------+ | information_schema | | bWAPP | |
drupageddon | | gmshop | | mysql | +--------------------+ 5 rows in set
(0.00 sec) mysql> exit
```

- **윈도우에서** http://비박스_아이피주소/gm/ **접속**

```
cd lib mysql -uroot -pbug gmshop < solution.sql
```

```
cat db_info.php cat solution.sql Ctrl+C
```

다른 사용자의 게시물 관련된 취약점 사례
1:1 문의 게시판 → 다른 사용자가 접근 (취약점), 다른 사용자가 수정 or 삭제(취약점)
자유게시판 → 다른 사용자가 접근(취약점O), 다른 사용자가 수정 or 삭제 (취약점)
상품평 / 상품질문 사이트 삭제 여부 확인!!!

실무에서 주의할 점!!!!

- 절대!!! 절대로 일반 사용자(컨설턴트 이외) 게시물을 함부로 수정/삭제 안됨!!!
- 2명이 투입될 때는 서로 글 올리고, 서로 삭제하고!!
- 1명이 투입될 때는 다른 브라우저를 두개를 사용해서, 계정을 두개를 만들어요.

- 시큐어 코딩 적용

```
<? include "head.php"; $dataArr = Decode64($data); $view_row = $MySQL-
>fetch_array("select *from bbs_data where idx=$dataArr[idx] limit 1"); ?>
```

표 1-7 GM Shop 질문과답변 페이지 board_view.php 소스 코드 수정 전

질문과답변 게시판 페이지인 board_view.php는 사용자별 세션 인증과 사용자에게 전달받은 파라미터 값이 원래 파라미터값과 맞는지 확인하지 않아 게시판의 파라미터값을 조작 가능한다