과제!

http://175.198.224.248:8888/gm/

-쇼핑몰 회원가입 우회

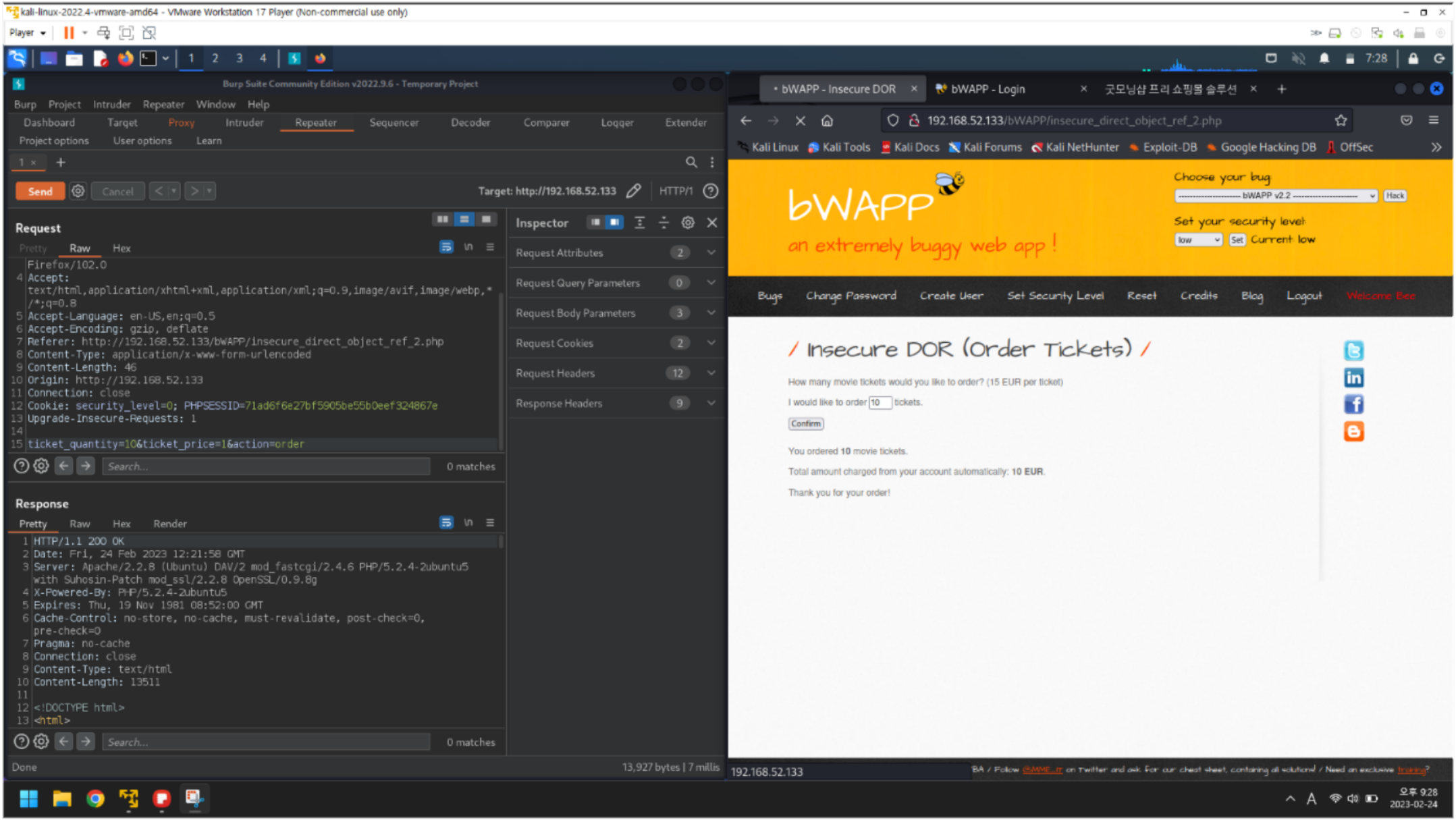
-물품구매시 금액변경

-게시판 (타인작성)비밀글 확인&수정

부적절한 인증 및 인가

beebug

-order tiket 금액바꾸기


kali-linux-2022.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender
Project options User options Learn
Send Cancel
Target: http://192.168.52.133
HTTP/1
Request
Pretty Raw Hex
Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.52.133/bWAPP/insecure_direct_object_ref_2.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 46
Origin: http://192.168.52.133
Connection: close
Cookie: security_level=0; PHPSESSID=71ad6f6e27bf5905be55b0eef324867e
Upgrade-Insecure-Requests: 1
ticket_quantity=10&ticket_price=1&action=order
Search...
0 matches
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Date: Fri, 24 Feb 2023 12:21:58 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Connection: close
Content-Type: text/html
Content-Length: 13511
<!DOCTYPE html>
<html>
Search...
0 matches
Done
13,927 bytes | 7 millis
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 3
Request Cookies 2
Request Headers 12
Response Headers 9
bWAPP - Insecure DOR
bWAPP - Login
192.168.52.133/bWAPP/insecure_direct_object_ref_2.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
bWAPP
an extremely buggy web app !
Choose your bug
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: low
Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee
/ Insecure DOR (Order Tickets) /
How many movie tickets would you like to order? (15 EUR per ticket)
I would like to order 10 tickets.
Confirm
You ordered 10 movie tickets.
Total amount charged from your account automatically: 10 EUR.
Thank you for your order!
192.168.52.133
오후 9:28
2023-02-24

http only
sessid 접근자 확인용 ID
secure
https는 암호화가 걸려서 http와 달리 네트워크감청이 불가

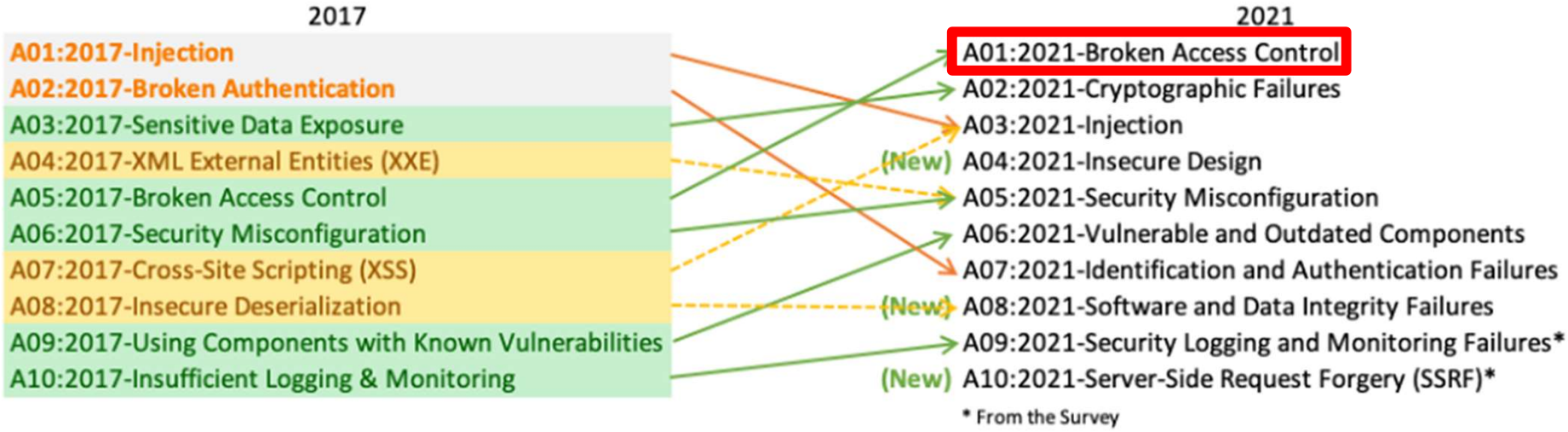
부적절한 인증 및 인가

부적절한 인증 및 인가

부적절한 인증 및 인가

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



부적절한 인증 및 인가

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
버퍼 오버플로우		
포맷스트링		
LDAP 인젝션		
운영체제 명령 실행		
SQL 인젝션		
SSI 인젝션		
XPath 인젝션		
디렉터리 인덱싱		
정보 누출		
악성 콘텐츠		
크로스사이트 스크립팅		
약한 문자열 강도		
불충분한 인증		
취약한 패스워드 복구		
크로스사이트 리퀘스트 변조(CSRF)	상	CF
세션 예측	상	SE
불충분한 인가	상	IN
불충분한 세션 만료	상	SC
세션 고정	상	SF
자동화 공격	상	AU
프로세스 검증 누락	상	PV
파일 업로드	상	FU
파일 다운로드	상	FD
관리자 페이지 노출	상	AE
경로 추적	상	PT
위치 공개	상	PL
데이터 평문 전송	상	SN
쿠키 변조	상	CC

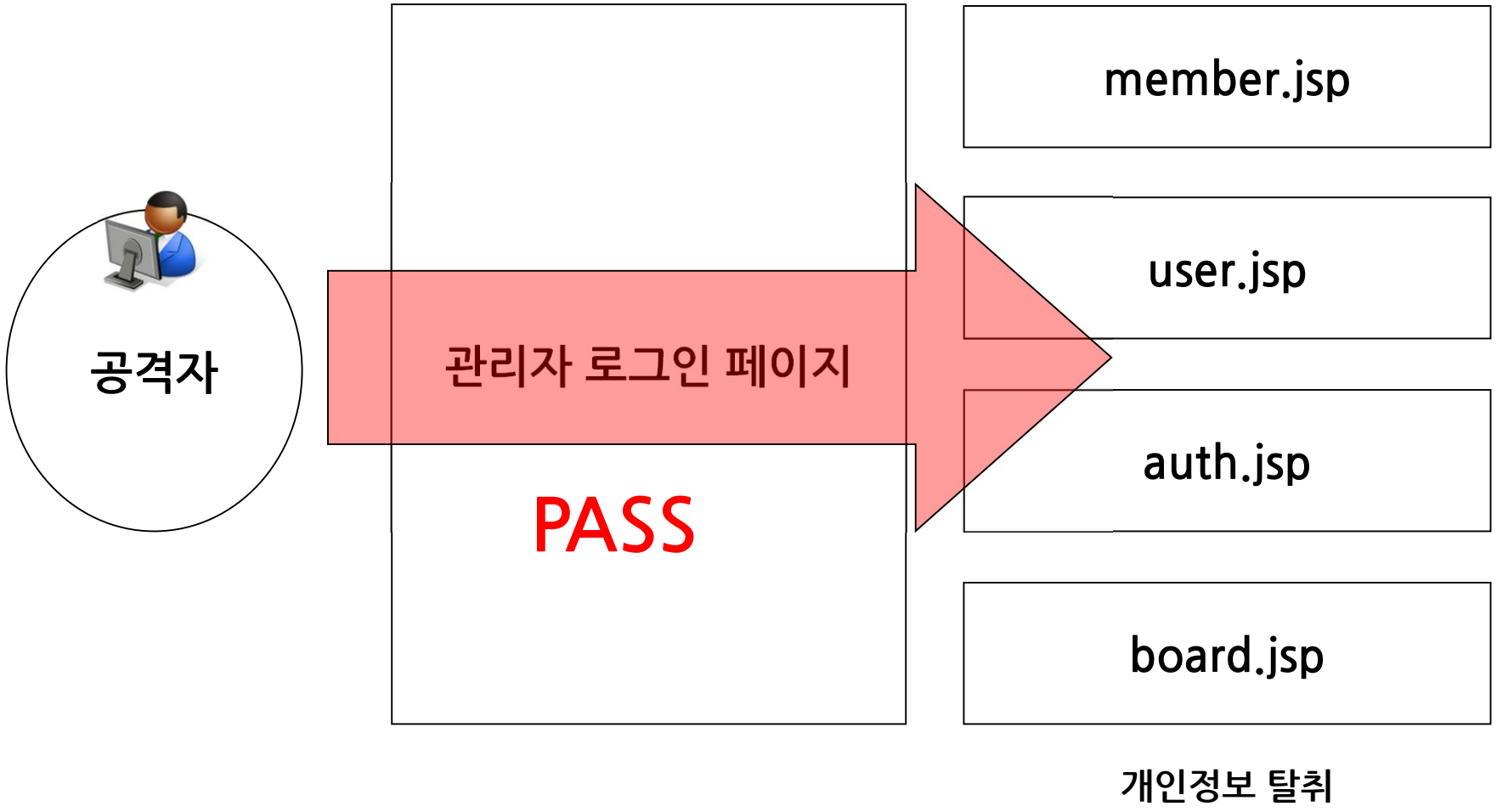
부적절한 인증 및 인가

부적절한 인증 및 인가

- 관리자 페이지 접근
- 다른 사용자 게시글 수정 / 삭제
- 다른 사용자 개인정보 수정
- 비밀글 조회 (1:1 상담글, 비밀글 체크)
- 결제 금액 조작
- 유료 컨텐츠 접근
- 쿠키 세션 조작으로 권한 상승
- 회원가입 우회
- …

부적절한 인증 및 인가

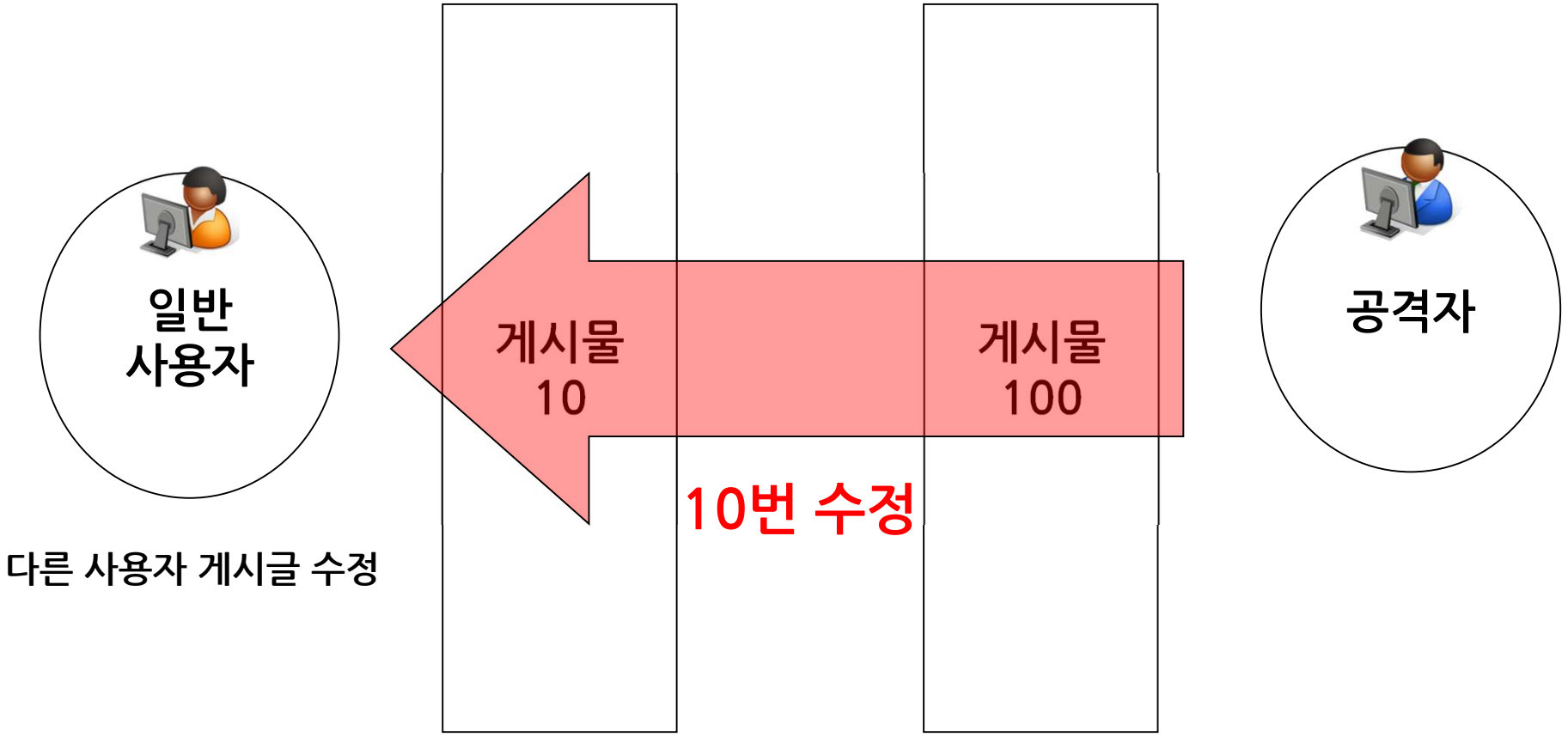
부적절한 인증 및 인가 - 관리자 페이지 접근



부적절한 인증 및 인가

부적절한 인증 및 인가 - 파라미터 값 변조

- 게시물 형태의 모든 곳에서 발생: 자료실, Q&A, 비밀글, 이력서 등



부적절한 인증 및 인가

부적절한 인증 및 인가

- 시나리오를 한번 생각해봅시다.

1) 다른 사용자 게시물 수정 및 삭제 여부가 가능한가? 해당 페이지에는 개인정보들이 포함되어 있는가?
2) 다른 사용자 개인정보 수정 페이지에 접근 가능한가? 개인정보가 제일 많이 포함된 부분이다. - 이력서 서비스, Q&A 상담글, 1:1 문의 게시물 등도 동일한 프로세스
3) 비밀글(상담글 등) 접근 가능 여부 가능한가? 사용자가 비밀글을 체크한 이유는 분명히 있다.
4) 상품 결제 금액 조작 여부 가능한가? 가격금액/할인율/쿠폰/카드할인률/배송비 등 조작할 부분은 너무 많다. 금액 조작뿐만 아니라 배송프로세스까지의 관리적인 문제까지 도출해낼 수 있는 부분이다.
5) 쿠키세션정보를 이용하여 권한 상승 여부 가능한가? 획득한 세션정보로 접근하지 못한 관리자 페이지에 접근이 가능하다. 회원관리/게시판관리 등 관리자별로 구분이 있을 경우 다양한 접근 시나리오를 구상할 수 있다.
6) 공인인증서 우회를 통한 권한 획득 여부 가능한가? 공인인증서 로그인 과정에서 타인의 정보를 이용하여 권한 우회가 가능하다.
7) 다른 사용자의 온라인 증명서 발급이 가능한가? 발급페이지 솔루션에 대한 인증 처리를 우회하여 다른 사용자의 개인정보가 포함된 증명서 발급이 가능하다.
8) 유료 컨텐츠에 대한 접근이 가능한가? 유료 서비스를 신청한 사용자에 대한 체크 권한을 우회하여 유료 컨텐츠에 마음대로 접근 및 다운로드 가능하다.

부적절한 인증 및 인가

대응 방안

- 접근제어가 필요한 중요한 페이지는 세션을 통한 인증 등 통제수단 구현 필요
- 페이지별 권한을 지정하여 접근제어가 모든 페이지에서 권한 체크가 이뤄지도록 구현 필요
- 결제 상품과 금액에 대한 서버 측에서 무결성 검증 필요
- 클라이언트 측에서 검증하는 경우 동일한 역할을 하는 검증 로직이 서버 측에서도 필요

```
// JSP
String userID = request.getParameter("userid");
HttpSession session = request.getSession(true);
String sessionID = session.getAttribute("userID");

// 사용자 검증 : 세션 정보와 사용자ID 파라미터 값 비교
if ( !sessionID.equals(userID) ) {
    ...
    //  인증  실패
}
```

부적절한 인증 및 인가

대응방안 - Insecure DOR (Change Secret)

- 토큰 검증

```
else
{
    // If the security level is MEDIUM or HIGH
    if(!isset($_REQUEST["token"]) or !isset($_SESSION["token"]) or $_REQUEST["token"] != $_SESSION["token"])
    {

        $message = "<font color=\"red\">Invalid token!</font>";

    }

    else
    {

        $secret = mysqli_real_escape_string($link, $secret);
        $secret = htmlspecialchars($secret, ENT_QUOTES, "UTF-8");

        $sql = "UPDATE users SET secret = '" . $secret . "' WHERE login = '" . $login . "'";

        // Debugging
        // echo $sql;

        $recordset = $link->query($sql);

        if(!$recordset)
        {

            die("Connect Error: " . $link->error);
```

부적절한 인증 및 인가

대응 방안 - Insecure DOR (Order Tickets)

- 티켓 가격을 하드 코딩하여 사용

```
include("security.php");
include("security_level_check.php");
include("functions_external.php");
include("selections.php");

$ticket_price = 15;

?>
```

```
    $ticket_quantity = abs($_REQUEST["ticket_quantity"]);
    $total_amount = $ticket_quantity * $ticket_price;

    echo "<p>You ordered <b>" . $ticket_quantity . "</b> movie tickets.</p>";
    echo "<p>Total amount charged from your account automatically: <b>" . $total_amount . " EUR</b>.</p>";
    echo "<p>Thank you for your order!</p>";

    $_SESSION["amount"] = $_SESSION["amount"] - $total_amount;

}
```

부적절한 인증 및 인가

대응 방안 - (Session Mgmt. - Administrative Portals)

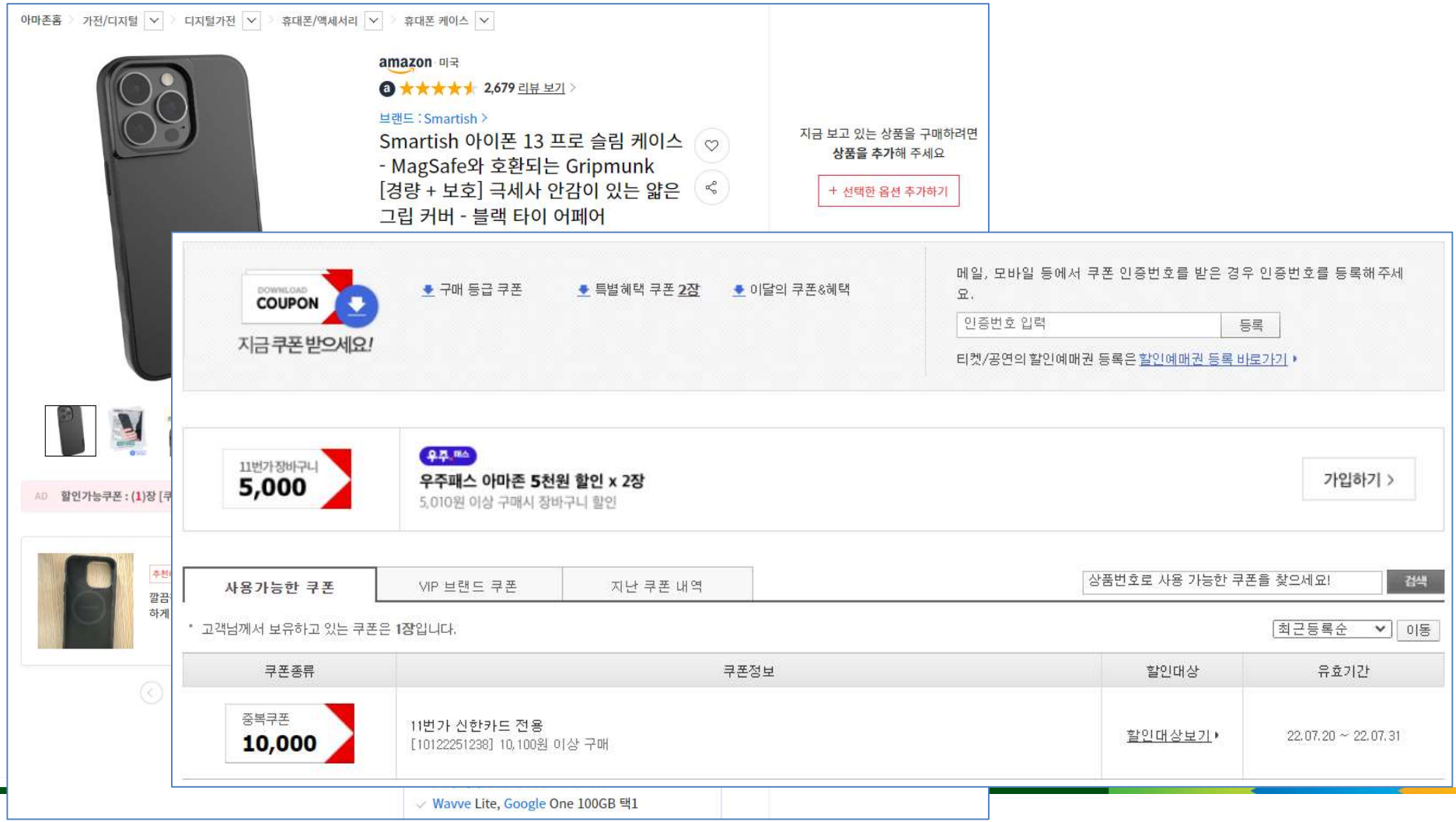
- 사용자 입력 값이 아닌 서버 세션으로 검증

```
case "2" :

    // Debugging
    // print_r($_SESSION);

    if(isset($_SESSION["admin"]) && $_SESSION["admin"] == 1)
    {

        $message = "Cowabunga...<p><font color=\"green\">You unlocked this page with a little help from the dba :)</font></p>";

    }

    else
    {

        $message="<font color=\"red\">This page is locked.</font><p>HINT: contact your dba...</p>";

    }

    break;
```

부적절한 인증 및 인가

쇼핑을 잘하면, 모의해킹도 잘한다

- 금액만 수정할 것인가? 옵션, 쿠폰, 회원등급, 무료배송 등



부적절한 인증 및 인가

쇼핑몰 해킹 사건

쇼핑몰 해킹해 사이버머니 44억 챙긴 일당 기소

연합뉴스 | 2013.12.13 오전 10:00
최종수정 | 2013.12.13 오전 10:02

(서울=연합뉴스) 김계연 기자 = 서울중앙지검 첨단범죄수사2부(조재연 부장검사)는 인터넷 쇼핑몰의 보안상 허점을 이용해 수십억원어치의 사이버머니를 챙긴 혐의(컴퓨터등사용사기 등)로 김모(39)씨 등 2명을 구속기소하고 유모(28)씨 등 3명을 불구속 기소했다고 13일 밝혔다.

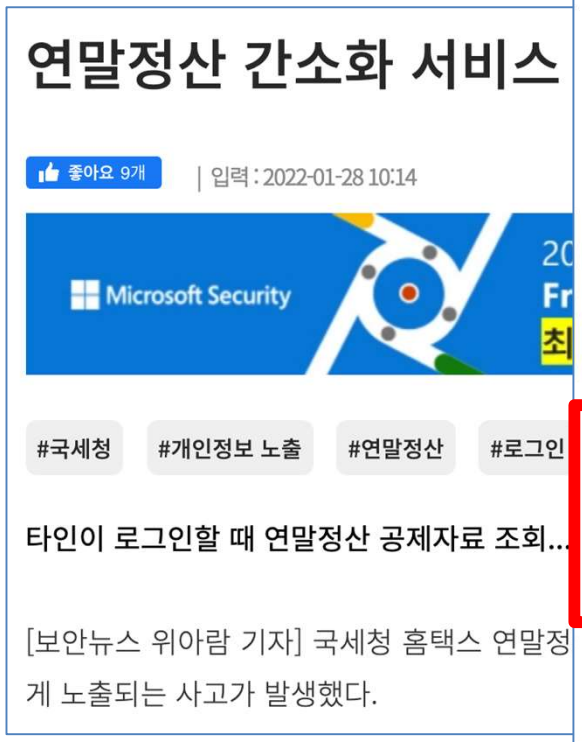
검찰에 따르면 김씨 등은 10월 말부터 지난달까지 '11번가'와 '아이템베이' 등 인터넷 쇼핑몰 홈페이지를 해킹해 서버에 전송되는 사이버머니 관련 데이터를 조작하는 수법으로 자신들의 계정에 43억8천여만원 상당의 사이버머니를 늘린 혐의를 받고 있다.

이들은 쇼핑몰 마일리지를 상품권으로 바꾸면서 서버에 전송되는 데이터를 변조했다. 실제 갖고 있는 마일리지보다 5~10배 늘리는 조작을 6천번 넘게 반복해 상품권처럼 쓸 수 있는 3억8천여만원 상당의 핀(PIN) 번호를 전송받았다.

한 쇼핑몰은 사이버머니를 인출할 때 요청 금액 데이터를 마이너스로 조작하면 잔액이 오히려 늘어나는 허점을 드러냈다. 김씨 등은 이를 이용해 40억원어치의 사이버머니를 공짜로 얻었고 상품권이나 금을 사는 데 일부를 쓴 것으로 조사됐다.

부적절한 인증 및 인가

개인정보 노출



국세청은 가족관계, 의료비, 카드사용금액 등 민감한 개인정보가 타인에게 노출됐다고 밝혔다. 국세청은 개인정보가 노출된 피해자들에게 사과문을 개별 통지할 예정이다. 또 외부 전문가가 참여하는 테스크포스를 구성해 재발방지 대책을 세울 계획이다.

연말정산 간소화 서비스에 오류가 생긴 것은 지난 15일 오전 6시 개통과 함께 민간인증서를 통한 간편 인증 과정에 문제가 생겼기 때문으로 알려졌다. 간소화 서비스는 카카오톡, 통신3사 PASS, 삼성패스, KB국민은행, 네이버, 신한은행 민간인증서를 통해 로그인할 수 있다. 그런데 새롭게 네이버와 신한은행 2종의 인증을 추가하는 과정에서 인증기관 연결용 프로그램에 오류가 발생했다.

로그인 절차는 이용자 성명과 주민등록번호를 입력하면 인증 요청 및 회신 등 간편 인증을 거쳐 이용자 인적사항과 인증 시 인적사항 일치 여부 검증의 단계로 진행되는데, 이 일치 여부를 검증하는 단계가 빠진 것이다. 이 때문에 다른 사람의 이름과 주민등록번호만 알면 로그인해 가족관계, 의료비 지출, 카드 사용금액 등 연말 정산 자료를 모두 조회할 수 있게 됐다.

국세청은 오류가 발생한 지 3일 뒤인 18일 이를 인지했다. 당일 오후 8시부터 3시간 정도 민간인증서 로그인을 차단한 후 오류를 수정했지만 이미 개인정보 노출 피해는 발생한 뒤였다.

국세청은 로그인 기록을 분석한 결과 다른 사람의 이름과 주민등록번호를 적어넣고 자신의 인증서로 로그인해 자료를 조회한 사람이 821명으로 나타났다고 밝혔다. 국세청은 시스템 개통 이전에 유사한 사례가 있었는지 추가 분석 중이며, 이번 유출 사례는 가족이나 지인에 의한 조회일 것으로 추정했다.

https://m.boannews.com/html/detail.html?mtype=1&idx=104496