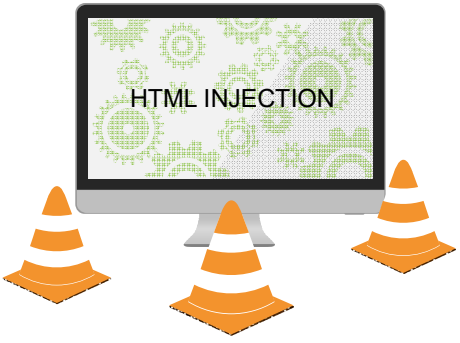
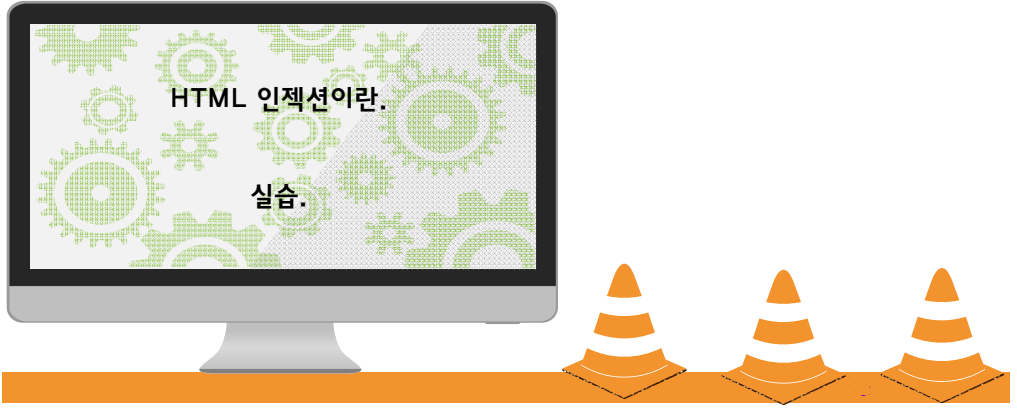


2주차 스터디 발표

정보보호학전공 1학년 정재성

목차



HTML

HyperText Markup Language

우리가 보는 웹페이지가

어떻게 구조화되어 있는지

브라우저로 하여금

알수 있도록 하는

마크업 언어

Injection

사전적 의미는 주사

공격자에 의해 신뢰할 수 없는

입력을 프로그램에

주입하도록 하는 공격

악용 범위가 무궁무진한
공격이다.

HTML INJECTION

일종의 코드 인젝션 공격의 하위 개념, 취약한 매개변수에 악의적인 HTML코드를 삽입하는 공격이다.

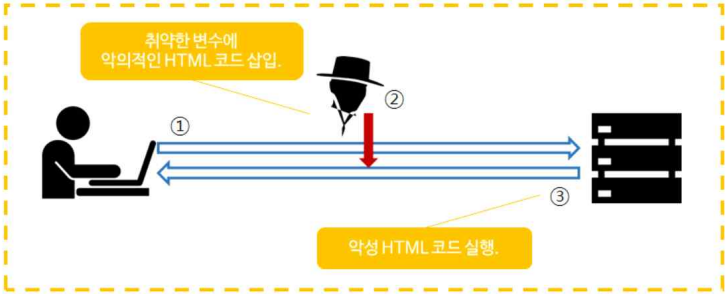
공격자는 사용자가 연결을 요청한 페이지에 HTML 태그를 삽입하여 의도하지 않은 내용을 보게 하거나 악의적인 사이트에 연결 시킬 수 있다.

#XSS or CSRF공격을 이해하는데 좋은 수단

HTML Injection 기법 종류

1. 반사기법(Reflected)

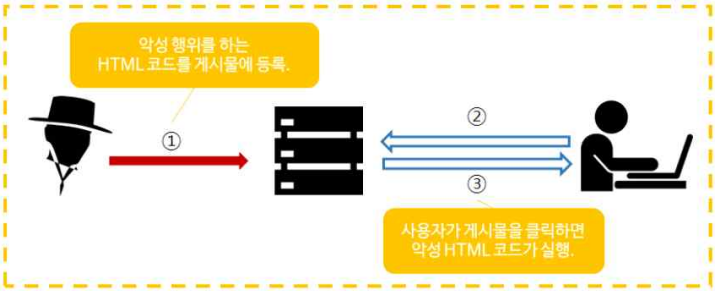
Get방식 - URL뒤에 붙어서 전송된다. #데이터 전송 양 제한적 특정 페이지를 다른 사람에게 접속하게 한다. 사용자가 입력한 값을 바탕으로 정보를 가져오는 역할	Post방식 - 값을 body 안에 숨겨서 전송한다. Get방식과는 달리 많은 양의 데이터 전송 가능 사용자가 입력한 값을 바탕으로 작업을 수행하는 역할



HTML Injection 기법 종류

2. 저장기법(Stored)

악의적인 HTML태그를 데이터베이스에 저장하여 저장된 태그 내용을 확인한 사용자의 PC에 HTML태그가 실행되게 하는 공격기법	Ex) 공개된 게시판에 악의적인 HTML 태그를 올리면 많은 사용자를 대상으로 공격 가능



실습

```php
<?php
$name = $_REQUEST['name'];
?>
<html>
<h1>Welcome to the Internet!</h1>
<br>
<body>
Hello, <?php echo $name;?>!
<p>We are so glad you are here!</p>
</body>
</html>
```

vul.php 소스코드

```php
<?php
$ip_address;
$ip_address = $_SERVER['REMOTE_ADDR'];
$port = $_SERVER['SERVER_PORT'];
$agent = $_SERVER['HTTP_USER_AGENT'];
$time = time();

$log = $ip_address." , ".$port." , ".$agent." , ".$time;
$file = './log.txt';
file_put_contents($file, $log.PHP_EOL, FILE_APPEND);
?>
```

ip.php 소스코드

클라이언트의 IP주소를 로그로 기록하는 파일

실습

취약점 공격 과정 : 사용자PC에서 이름입력(주소창) -> 변수전달(vul.php) ->

공격자전송(<iframe>태그) -> 사용자 정보수집(ip.php) -> 공격자PC로 IP, Port, 브라우저, 접속시간 탈취

Thank You