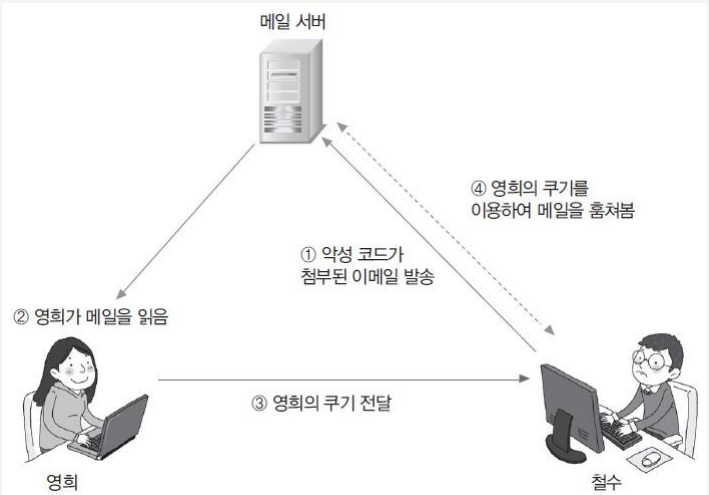
1 XSS 공격의 개요

1 XSS 공격의 기본 원리

- 간단하지만 파괴력이 있음
  (웹 애플리케이션 사용자를 공격하는 기법 중 최고)



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 웹 애플리케이션이 사용자를 인증하는 방법

- 가장 먼저 아이디와 패스워드를 기반으로 사용자의 신원 확인
- 신원 확인 후 웹 애플리케이션이 사용자에게 고유한 값을 전달(쿠키)
- 그 이후부터 사용자는 웹 애플리케이션으로부터 받은 고유한 값을 가지고 사이트 이용(쿠키)

2 웹 애플리케이션이 사용자를 인증하는 방법

- 사이트 간 스크립팅(또는 크로스 사이트 스크립팅, 영문 명칭 cross-site scripting, 영문 약어 XSS)은 웹 애플리케이션에서 많이 나타나는 취약점의 하나로 웹사이트 관리자가 아닌 이가 웹 페이지에 악성 스크립트를 삽입할 수 있는 취약점임(CSS)
- 주로 여러 사용자가 보게 되는 전자 게시판에 악성 스크립트가 담긴 글을 올리는 형태로 이루어 짐, 이 취약점은 웹 애플리케이션이 사용자로부터 입력 받은 값을 제대로 검사하지 않고 사용할 경우 나타남

2 웹 애플리케이션이 사용자를 인증하는 방법

- 이 취약점으로 해커가 사용자의 정보(쿠키, 세션 등)를 탈취하거나 자동으로 비정상적인 기능을 수행하게 할 수 있음, 주로 다른 웹사이트와 정보를 교환하는 식으로 작동하므로 사이트 간 스크립팅이라고 함(쿠키)

- 크로스 사이트 스크립팅(XSS)의 공격 유형은 표준화로 정해져 있지 않지만, 전문가들은 크로스 사이트 스크립팅의 유형을 구분함. 비 지속적인 공격(Non-persistent XSS)과 지속적인 공격(persistent XSS), 소스 코드 추가로 발생되는 DOM 기반 XSS 등 유형으로 구분함(DOM)

2 웹 애플리케이션이 사용자를 인증하는 방법

- 비 지속적(Non-persistent) 크로스 사이트 스크립팅 취약점은 반사(Reflected) XSS라고도 불리며 가장 일반적인 유형임, 웹 클라이언트가 제공하는 HTTP 쿼리 매개 변수(예 : HTML 양식 제출)에서 적절하지 않고 구문 분석 및 해당 사용자에 대한 결과의 페이지를 표시하는 공격 기법임(URL 이용)

2 웹 애플리케이션이 사용자를 인증하는 방법

- 검증 되지 않은 사용자가 URL 파라미터나 HTTP 요청 헤더 정보를 수정하여 공격할 수 있음, 잠재적인 취약점이 존재하는 대상은 검색 엔진임 (검색 엔진의 검색창에서 하나의 문자열을 검색하는 경우, 검색 문자열은 일반적으로 결과 페이지에 그대로 다시 표시되며, 삽입 된 문자열을 다시 표시하면서 문자열이 가지고 있는 스크립트가 동작된다면 취약점이 존재하는 것)(악성 스크립트 실행)

2 웹 애플리케이션이 사용자를 인증하는 방법

- 지속적(Persistent) 크로스 사이트 스크립팅
  취약점은 더 치명적인 기법임
  : 공격자가 제공 한 데이터가 서버에 저장 한 다음 지속적으로 서비스를 제공하는 "정상"페이지에서 다른 사용자에게 노출됨, 해당 취약점이 대표적인 발생하는 위치는 사용자가 읽을 수 있고, HTML 형식의 메시지를 게시 할 수 있는 온라인 게시판이 해당 됨(정상 페이지에 악성 코드 -> 계속 노출)

3 쿠키(Cookie)

- 사용자가 인터넷 웹 사이트에 방문할 때 생기는 4KB 이하의 파일
- 1994년 넷스케이프에서 처음 사용
- 쿠키 내용을 이용하여 클라이언트의 신분을 알 수 있음
- 많은 웹 사이트는 쿠키를 이용하여 사용자 정보를 수집 (현재는 쿠키를 사용할지 물어봄)

3 쿠키(Cookie)

쿠키(Cookie) 생성

- 웹 사이트에서 쿠키를 만들기 위한 코드의 예

```
Set-Cookie: Name = Value; expires=Date;
domain = DOMAIN_NAME; Path = Path;
Secure
```

3 쿠키(Cookie)

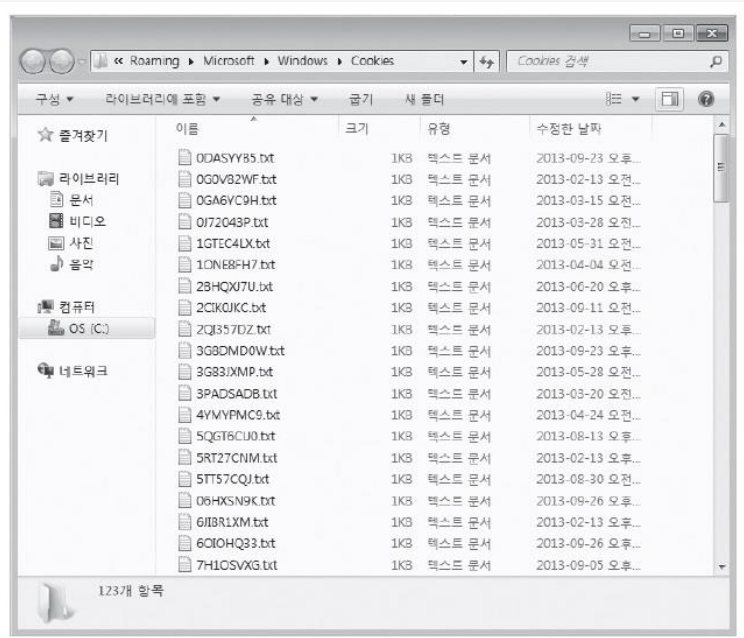
쿠키(Cookie)의 사용

- 사용자 컴퓨터에 쿠키 생성
  - 사용자가 사이트를 방문하면 사이트가 사용자의 컴퓨터에 쿠키 만듦
  - 윈도우 7 이후 버전에서는 'C:₩Users₩사용자이름₩AppData₩Roaming₩Microsoft₩Windows₩Cookies'에서 확인 가능
  - 쿠키를 만든 사이트의 도메인 이름, 그 사이트를 구분하는 숫자, 쿠키 만기일등의 정보가 공통적으로 들어있음

3 쿠키(Cookie)

쿠키(Cookie)의 사용

- 사용자 컴퓨터의 쿠키를 웹 서버로 전송
  - 방문했던 사이트에 다시 접속하면 이미 저장된 쿠키를 통해 개인 정보를 알 수 있음(공격 포인트)



[사용자 컴퓨터에 저장된 쿠키 파일]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 쿠키(Cookie)

쿠키의 용도('Cookie Central'에서 발췌)

- 사이트 개인화
  - 쿠키를 이용하면 아이디와 비밀번호 외에도 사용자의 '성향'까지 파악 가능
  - 사용자의 성향을 고려한 개인 맞춤 서비스를 마련한다면 다른 사이트와 중요한 차별 점(광고)
- 장바구니 시스템
  - 사용자가 고른 물건을 쿠키에 저장 (수정할 수 있다면?)

3 쿠키(Cookie)

쿠키의 용도('Cookie Central'에서 발췌)

- 웹 사이트 이용 방식 추적
  - 사용자들의 사이트 방문 유형을 파악하여 마케팅 정보로 활용(광고)

3 쿠키(Cookie)

쿠키의 용도('Cookie Central'에서 발췌)

- 타깃 마케팅
  - 광고주가 대형 포털 사이트의 광고 공간을 사들여 자회사의 광고를 사용자에게 보여주는 것 (더블클릭 대표적)
  - 광고를 낸 업체들이 광고 효과가 궁금해하기 때문에 광고 대행업체는 제3의 업체의 쿠키를 사용자 컴퓨터에 저장해 사용자 이용 정보를 수집 (불법접속 차단)

3 쿠키(Cookie)

쿠키에 관한 오해

- 쿠키가 바이러스를 전파한다?
  - 쿠키는 텍스트 파일이기 때문에 '실행'되지 않아 바이러스를 전파할 수 없음(실행 파일 아님)
  - 예전 인터넷 익스플로러 3.0 브라우저에서 실행 가능한 쿠키에 바이러스를 심은 적이 있으나 지금은 위험성이 없음

3 쿠키(Cookie)

쿠키에 관한 오해

- 쿠키가 사용자 컴퓨터에 피해를 입힌다?
  - 사이트에서 만든 특정 데이터만 있을 뿐
    어떠한 정보도 담겨 있지 않음
  - 스스로 디렉터리를 읽거나 파일을 지우는 작업도
    절대 수행 불가능(실행 파일 아님)

4 XSS

- 다른 사용자의 정보를 추출하는 공격 기법으로,
  입력을 받아들이는 부분의 스크립트 코드를 필터링 하지
  않음으로써 공격자가 스크립트 코드를 실행할 수 있음

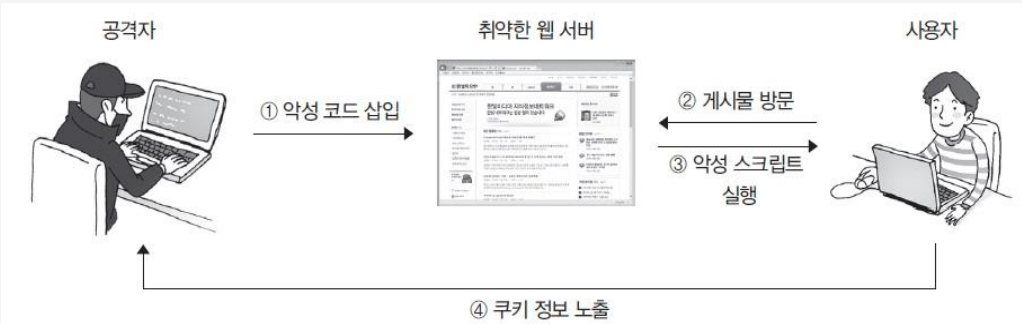
[정상적인 문자열을 입력한 경우]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 XSS

- 다른 사용자의 정보를 추출하는 공격 기법으로,
  입력을 받아들이는 부분의 스크립트 코드를 필터링 하지
  않음으로써 공격자가 스크립트 코드를 실행할 수 있음
  (악성 스크립트 저장)

[스크립트 코드 문자열을 입력한 경우]



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

5 Stored XSS

- 가장 일반적인 XSS 공격 유형
- 사용자가 글을 저장하는 부분에 정상적인 평문이 아닌 스트립트 코드를 입력(악성 스크립트 저장)
- 다른 사용자가 게시물을 열람하면 공격자가 입력해둔 악성 스크립트가 실행되어 사용자의 쿠키 정보가 유출되거나 악성 스크립트가 기획한 공격에 속수무책으로 당하게 됨

6 Reflected XSS

- URL의 변수 부분처럼 스크립트 코드를 입력하는 동시에 결과가 바로 전해지는 공격 기법(URL vs. URI)

7 XSS(Cross Site Scripting) - 상세 설명

- XSS는 'Cross Site Scripting'의 약자로 줄여서 CSS라고도 부르나 웹에서 레이아웃과 스타일을 정의할 때의 사용되는 캐스케이딩 스타일 시트(Cascading Style Sheets)와 혼동되어 일반적으로 XSS라고 하게 됨

  XSS는 과부하를 일으켜 서버를 다운시키거나 피싱(Phishing) 공격의 일환으로 사용되기도 하지만, 가장 일반적인 목적은 웹 사용자의 정보 추출임(쿠키)

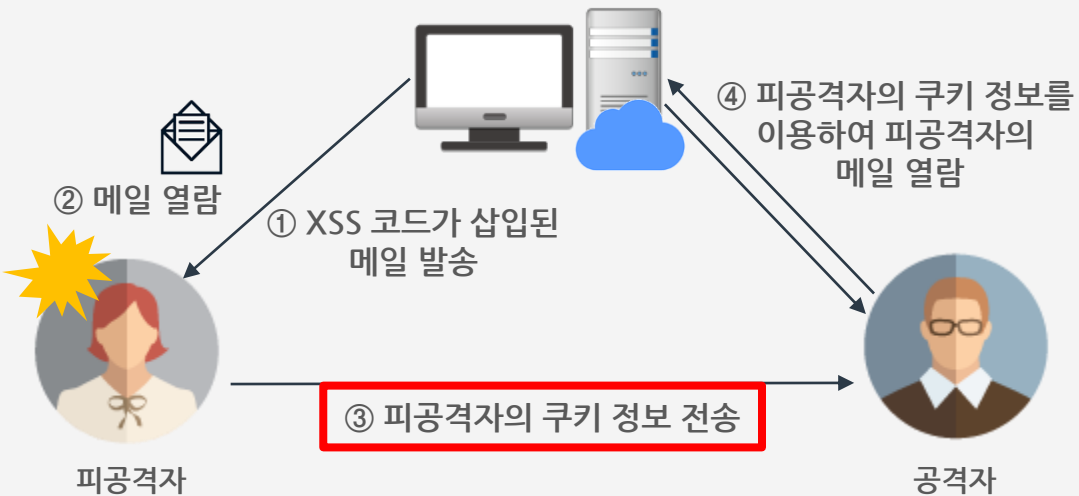
7 XSS(Cross Site Scripting) - 상세 설명

- XSS 공격은 브라우저로 전달되는 데이터에 악성 스크립트(script)가 포함되어 개인의 브라우저에서 실행되면서 해킹을 하는 것임

  이 공격용 악성 스크립트는 공격자가 웹 서버에 구현된 웹 어플리케이션의 XSS 취약점을 이용하여 서버 측 또는 URL에 미리 삽입해놓은 것임(저장, 반사 XSS)

7 XSS(Cross Site Scripting) - 상세 설명

[메일 서비스를 이용한 XSS 공격 개요도]



※ 출처 : 정보보호총론, 장상수, 생능출판사

8 XSS(Cross Site Scripting) 공격 - 상세 설명

- XSS 취약점을 이용한 공격 방법은 3가지로 분류됨

  하나는 접속자가 많은 웹 사이트를 대상으로 공격자가 XSS 취약점이 있는 웹 서버에 공격용 스크립트(script)를 입력시켜 놓으면, 방문자가 악성 스크립트가 삽입되어 있는 페이지를 읽는 순간 방문자의 브라우저를 공격하는 방식(저장 XSS 공격), 또 하나는 반사 XSS 공격으로 악성 스크립트가 포함된 URL을 사용자가 클릭하도록 유도하여 URL을 클릭하면 클라이언트를 공격하는 것이고(반사 XSS 공격), 마지막으로 DOM(Document Object Model) 환경에서 악성 URL을 통해 사용자의 브라우저를 공격하는 것임(DOM 기반 XSS 공격)

8 XSS(Cross Site Scripting) 공격 - 상세 설명

- DOM : 그래픽, 텍스트, 헤드라인, 스타일 등
  웹의 모든 요소가 스크립트 언어에 의해 조정

- XSS 취약점은 쉽게 악용될 수 있으며,
  공격 효과도 커 공격자들이 자주 이용하는 기술(현재)

- 많은 조직에서 XSS 공격을 대응하기 위해 웹 방화벽
  (Web Application Firewall, 방화벽 기능이 웹에 특화)
  을 도입하여 방어를 하고 있으나, 대부분의 웹 방화벽은
  시그너쳐(signature) 기반의 XSS 공격만을 탐지

8 XSS(Cross Site Scripting) 공격 - 상세 설명

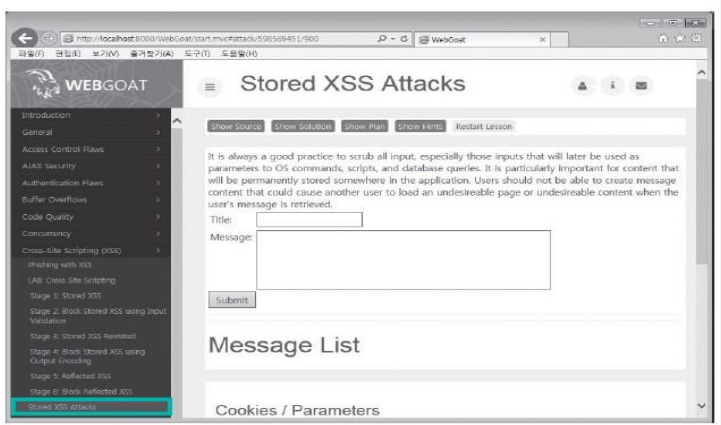
- 특정 문자열을 탐지하는 기술은 쉽게 우회(bypass)가 가능하여 방어가 효과적이지는 못함, 또한 웹 어플리케이션 개발자는 <script> 태그 등 브라우저에서 실행되는 위험한 문자를 중성화(Neutralization)하여 XSS 취약점을 예방하고 있음

2 XSS 공격 방법

1 Stored XSS 공격 연습하기

1. [Stored XSS Attacks] 클릭
   - WegGoat를 실행 후 [Cross-Site Scripting(XSS)]-[Stored XSS Attacks] 클릭

[Stored XSS 공격의 예제 화면]



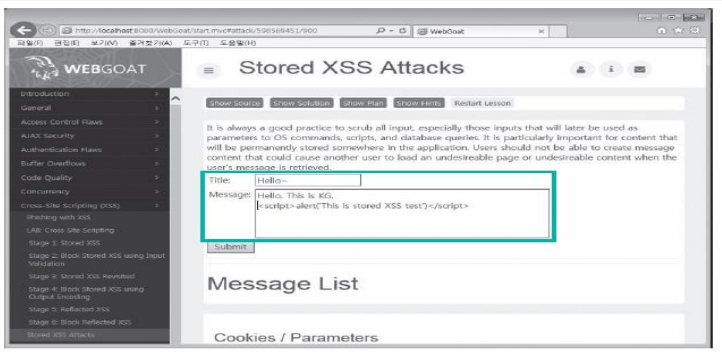
※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

1 Stored XSS 공격 연습하기

2 Title과 Message 입력(악성 스크립트 저장)

- Title : Hello~
- Message : Hello. This is KG.
  <script>alert(' This is stored XSS test')</script>

[Stored XSS 공격 시도 화면]



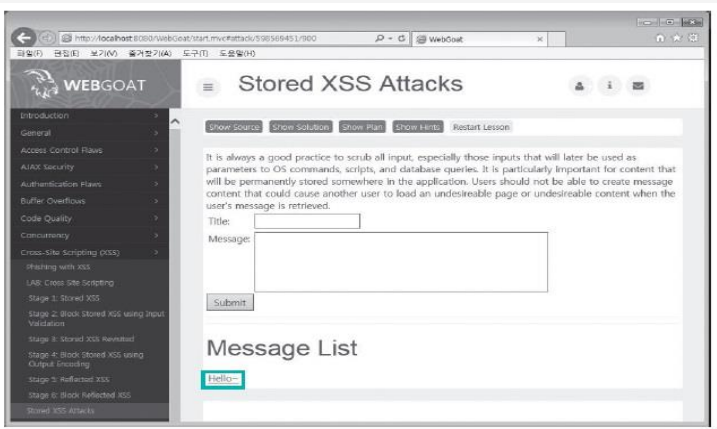
※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

1 Stored XSS 공격 연습하기

3 게시물 확인

- 입력한 후 <Submit>를 클릭하여 게시물을 저장하면 Message List에서 저장된 게시물 확인 가능

[Stored XSS의 게시물 목록 화면]



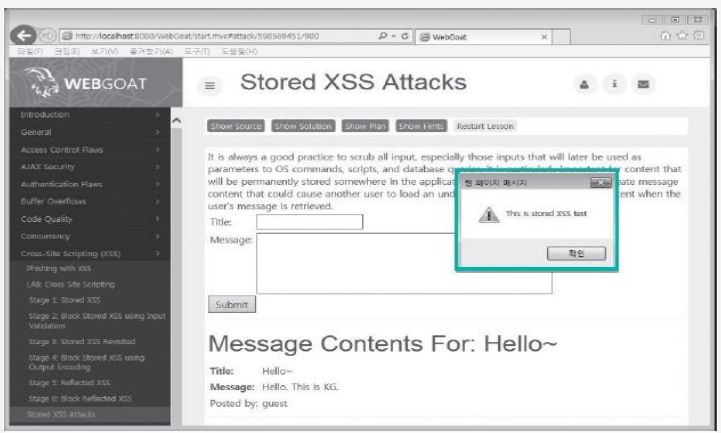
※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

1 Stored XSS 공격 연습하기

4 스크립트 공격 코드 실행 확인

- 게시물 ‘ Hello~’를 클릭하면 스크립트 공격 코드가 실행됨(저장 악성 스크립트 실행)

[Stored XSS의 공격 성공 화면]

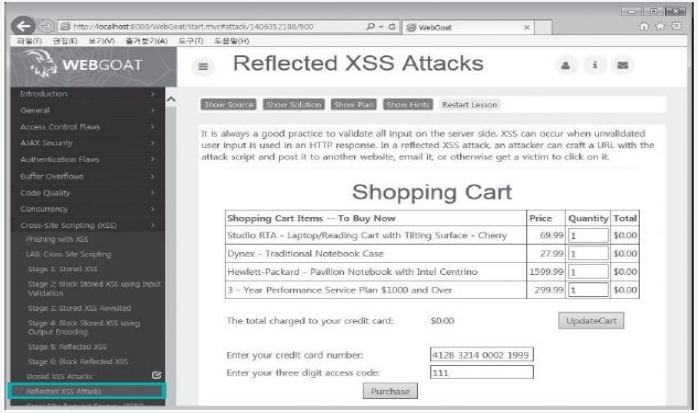


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 Reflected XSS 공격 연습하기

1. [Reflected XSS Attacks]
   - WebGoat를 실행 후 왼쪽 메뉴에서 [Cross-Site Scripting(XSS)]-[Reflected XSSAttacks] 클릭

[Reflected XSS 공격의 예제 화면]



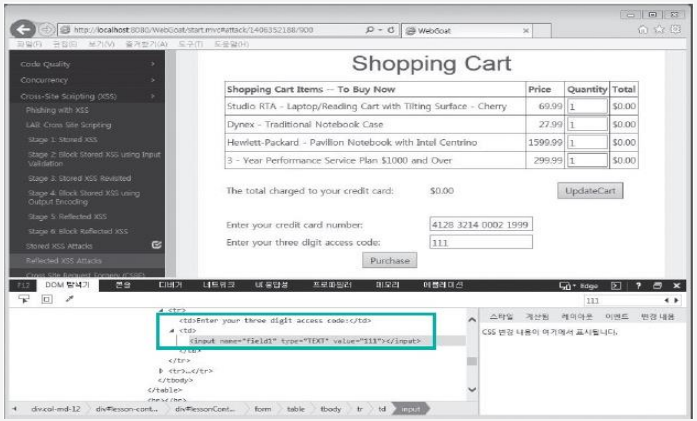
※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 Reflected XSS 공격 연습하기

2 페이지의 소스코드 확인

- 화면에서 '111' 값이 있는 부분을 클릭한 후 마우스 오른쪽 버튼을 누르고 [요소 검사] 선택

[Reflected XSS 예제의 소스코드 화면]



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 Reflected XSS 공격 연습하기

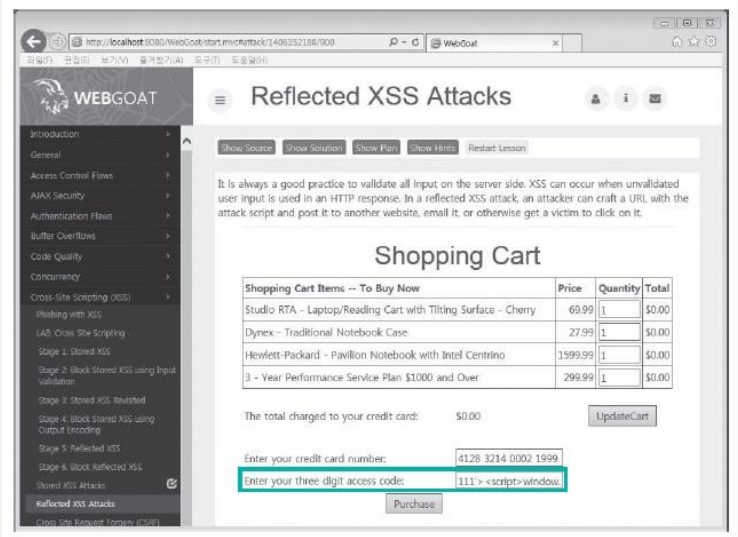
3 공격 스크립트 작성

- 자바스크립트로 특정 사이트를 강제로 띄우기 위한 공격 스크립트 만들기
- 다음 스크립트 코드를 Enter your three digit access code의 값으로 입력(악성 스크립트)
- 111'><script>window.open ('http://www.naver.com')</script><font size='4

2 Reflected XSS 공격 연습하기

3 공격 스크립트 작성

[Reflected XSS 공격의 스크립트 입력 화면]



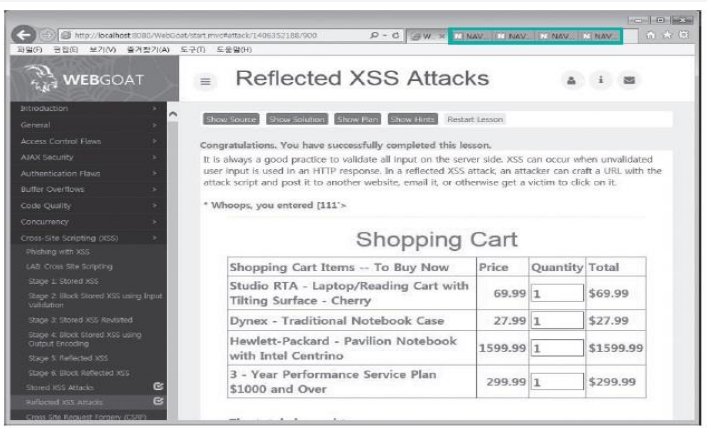
※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 Reflected XSS 공격 연습하기

4 Reflected XSS 공격 결과 확인

- 〈Purchase〉를 클릭하면 성공했다는 문구와 함께 네이버 창이 강제로 뜸

[Reflected XSS 공격의 결과 화면]



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 XSS 취약점 찾는 방법

- 표준 스크립트 문자열을 입력해보기

```
<script>alert(document.cookie)</script>
```

4 스크립트 검증 예시로 사용되는 코드

```
"><script>alert(document.cookie)</script>
"><ScRiPt>alert(document.cookie)</ScRiPt>
"%3e%3cscript%3ealert(document.cookie)%3c/script%3e
"><scr<script>ipt>alert(document.cookie)</scr</script>ipt>
%00"><script>alert(document.cookie)</script>
```