1 CSRF 공격의 개요

1 CSRF 공격의 개요

- 사이트 간 요청 위조(또는 크로스 사이트 요청 위조, 영어: Cross-site request forgery, CSRF, XSRF)는 웹사이트 취약점 공격의 하나로, 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록 등)를 특정 웹사이트에 요청하게 하는 공격을 말함(웹 브라우저)

- 유명 경매 사이트인 옥션에서 발생한 개인정보 유출 사건에서 사용된 공격 방식 중 하나 임

1 CSRF 공격의 개요

- 사이트 간 스크립팅(XSS)을 이용한 공격이 사용자가 특정 웹사이트를 신용하는 점을 노린 것이라면(웹 서버), 사이트간 요청 위조는 특정 웹사이트가 사용자의 웹 브라우저를 신용하는 상태를 노린 것(웹 브라우저)

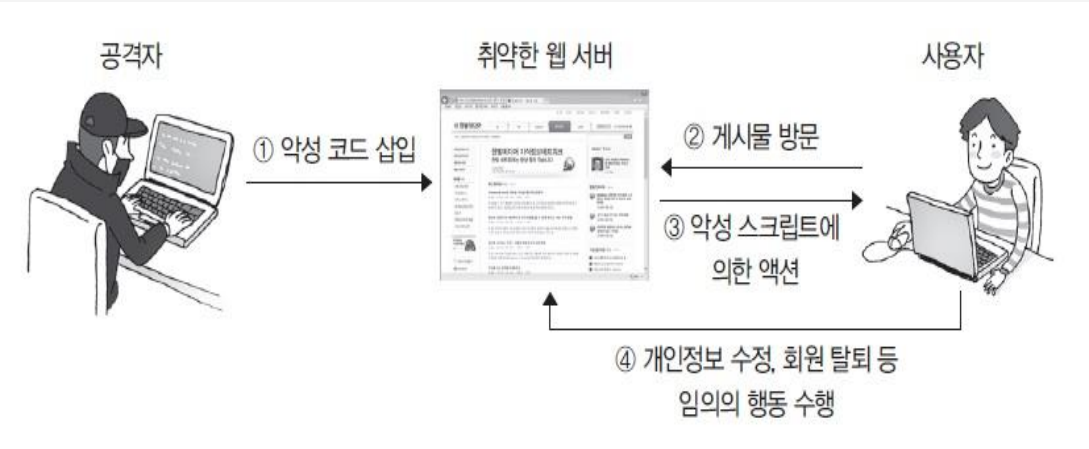
- 일단 사용자가 웹사이트에 로그인한 상태에서 사이트간 요청 위조 공격 코드가 삽입된 페이지를 열면, 공격 대상이 되는 웹사이트는 위조된 공격 명령이 믿을 수 있는 사용자로부터 발송된 것으로 판단하게 되어 공격에 노출 됨(믿는 도끼에 발등)

2 크로스 사이트 요청 변조(CSRF) 공격

- 기본적인 XSS 공격인 Stored XSS와 Reflected XSS 외의 XSS 공격
- 2001년 처음 발표
- 피해자가 인지하지 못하는 상태에서 피해자의 브라우저가 특정 사이트에 강제적으로 리퀘스트를 보내도록 하는 기법(현재 : 크립토재킹)

2 크로스 사이트 요청 변조(CSRF) 공격

[CSRF 공격의 원리]



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 CSRF 공격 구조

- 먼저 공격자가 취약한 웹 서버에 크로스 사이트 요청 변조 코드를 삽입 함
- 아무것도 모르는 사용자가 해당 사이트를 방문하면 악성 스크립트가 동작하는데, 이 악성 스크립트는 사용자로 하여금 개인정보 수정이나 회원 탈퇴 등 원치 않는 임의의 행동을 수행하게 만듦
- 이와 같이 사이트에 방문하는 사용자가 정상적인 요청이 아닌 임의의 요청을 하도록 위조하는 것이 CSRF 공격임(사용자의 의도완 무관)

3 CSRF 공격 구조

- CSRF(Cross Site Request Forgery)는 특정 사용자를 대상으로 하지 않고, 불특정 다수를 대상으로 로그인 된 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록, 송금 등)를 하게 만드는 공격임

3 CSRF 공격 구조

- CSRF는 기본적으로는 XSS 공격과 매우 유사하며 XSS 공격의 발전된 형태라고 보기도 함, 하지만 XSS 공격은 악성 스크립트가 클라이언트에서 실행되는데 반해, CSRF 공격은 사용자가 악성 스크립트를 서버에 요청 한다는 차이가 있음, XSS 취약점의 XSS 공격 구조와 비교해보길 바람(client-side script vs. server-side script)

3 CSRF 공격 구조

※ 출처 : 정보보안개론, 양대일, 한빛아카데미, 2018)

4 CSRF 공격

- CSRF 공격을 이용하면 공격자는 특정 물품을 구매하여 장바구니에 넣어두고, 해당 물품에 대한 결제를 다른 이를 통해 다음과 같은 형태로 수행할 수 있음(결제 속임)

```
<body onload = "document.csrf.submin()">
<form name="csrf" action="http://www.shop.co.kr/malladmin/order/order.jsp" method="POST">
<input type="hidden" name="uid" value="wishfree">
<input type="hidden" name="mode" value="pay_for_order">
<input type="hiddne" name="amount" value="10000">
</form>
```

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

5 CSRF 취약성 확인 방법

- 애플리케이션이 취약한지 확인하기 위해서, 링크 및 폼들이 예측할 수 없는 CSRF 토큰이 누락되었는지 봐야 함, 그러한 토큰이 없다면, 공격자들은 악의적인 요청들을 위조할 수 있음(CSRF 토큰)

- 대체 방어책은 사용자들에게 요청을 제출하는 의도를 증명하거나, 재인증 또는 진짜 사용자라는 일부 다른 증거(예를 들면 CAPTCHA)를 요구하는 것(재인증)

5 CSRF 취약성 확인 방법

- 상태를 변경하는 함수는 가장 중요한 CSRF 공격 목표가 되기 때문에 이러한 함수를 호출하는 링크나 폼에 집중해야 함, 그리고 다단계 처리기능은 기본적인 방어책이 없기 때문에 확인해야 함(상태 변경 함수)

- 공격자들은 다양한 기술 또는 아마도 자바스크립트를 사용하여 연속적으로 요청들을 쉽게 위조할 수 있음 (자바스크립트)

5 CSRF 취약성 확인 방법

- 브라우저에서 자동적으로 보내는 세션 쿠키, 출발지 IP 주소, 그리고 다른 정보들이 CSRF에 대한 방어책을 제공하지 않는지 확인해야 함, 왜냐하면 이러한 정보도 위조된 요청에 포함되어 있기 때문(위조 정보 요청)

6 CSRF 예방 방법

- CSRF를 예방하기 위해서는 각각의 HTTP 요청에서 예측 불가능한 토큰을 포함해 함, 최소한 이런 토큰들은 사용자 세션마다 고유해야 함(토큰 식별)
- 선호되는 옵션은 숨겨진 필드에 고유 토큰을 포함하는 것, 이렇게 하면 HTTP 리퀘스트 본문에 값이 보내지고, 노출될 위험이 큰 URL에 포함하는 것을 피할 수 있음 (토큰 식별)

6 CSRF 예방 방법

- 고유 토큰은 또한 URL 자체 또는 URL 매개변수에 포함될 수 있음, 그러나 토큰이 이런 곳에 있으면 공격자에게 URL이 노출되고 따라서 비밀 토큰이 해킹 당할 수 있음(토큰 해킹)

- 사용자에게 재 인증을 요구하거나, 또는 사용자 자신을 증명하도록 하는 것(예를 들어 CAPCHA를 통해)이 CSRF 보호책이 될 수 있음(재인증)

7 CSRF 공격 예

- 이용자는 웹사이트에 로그인하여 정상적인 쿠키를 발급 받음
- 공격자는 다음과 같은 링크를 이메일이나 게시판 등의 경로를 통해 이용자에게 전달 함(출발지와 도착지 등록)

```
http://www.geocities.com/attacker
```

7 CSRF 공격 예

- 공격용 HTML 페이지는 다음과 같은 이미지 태그를 가짐 (도착지 변조)

```
<img src=
"https://travel.service.com/travel_update?.src=Korea
&.dst=Hell">
```

- 해당 링크는 클릭 시 정상적인 경우 출발지와 도착지를 등록하기 위한 링크, 위의 경우 도착지를 변조하였음

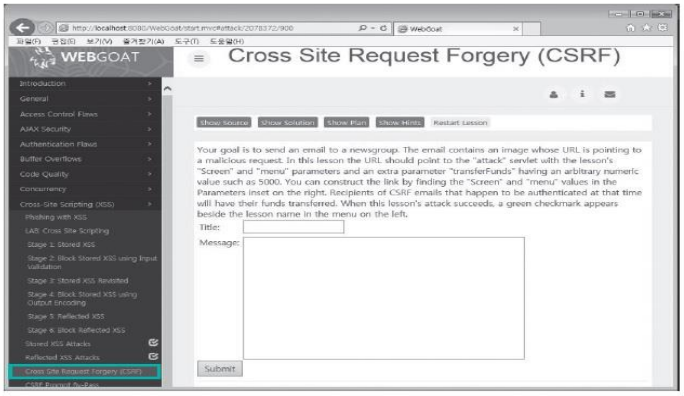
7 CSRF 공격 예

- 이용자가 공격용 페이지를 열면, 브라우저는 이미지 파일을 받아오기 위해 공격용 URL로 열림
- 이용자의 승인이나 인지 없이 출발지와 도착지가 등록됨으로써 공격이 완료됨, 해당 서비스 페이지는 등록 과정에 대해 단순히 쿠키를 통한 본인확인 밖에 하지 않으므로 공격자가 정상적인 이용자의 수정이 가능하게 됨(본인의 의도와 무관하게 도착지 변경)

2 CSRF 공격 방법

1 CSRT 공격 연습하기

1. [Cross Site Request Forgery(CSRF)] 클릭
   - WebGoat를 실행 후 메뉴에서 [Cross-Site Scripting(XSS)]-[Cross Site Request
   - Forgery(CSRF)]클릭



[CSRF 공격의 예제 화면]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

1 CSRT 공격 연습하기

2 [Cross Site Request Forgery(CSRF)] 클릭

- 이 예제는 뉴스그룹에 악의적인 요청이 담겨 있는 이미지 URL을 메일로 보내는 것, URL을 포함하여 1×1 픽셀의 이미지를 전달하고, URL에는 추가적인 변수인 'transferFunds=5000'을 포함 함
- 이 악의적인 요청이 담긴 메일을 클릭하는 사용자는 5000이라는 금액을 이체하게 됨

2 CSRT 공격 연습하기

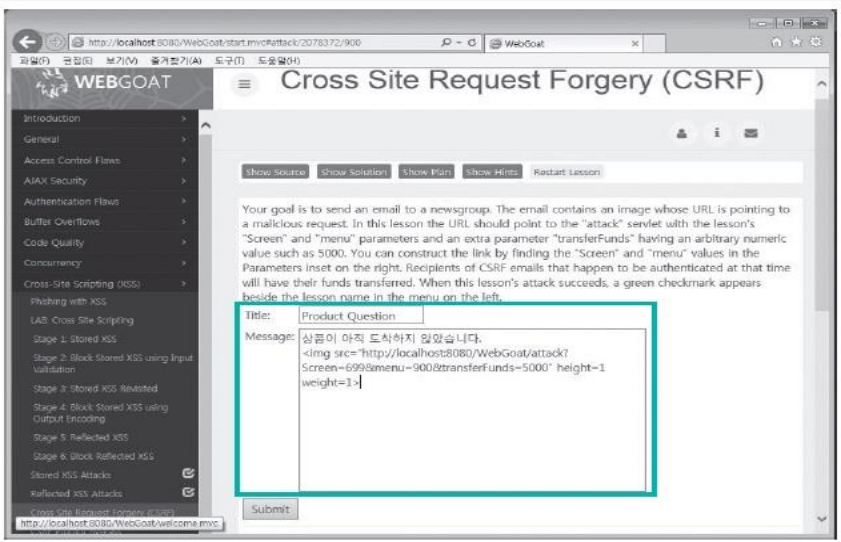
2 크로스 사이트 요청 변조 코드 작성

- Title : Product Question
- Message(악의적인 요청)
  : 상품이 아직 도착하지 않았습니다.
  <imgsrc="http://localhost:8080/WebGoat/attack?Screen=699&menu=900&transferFunds=5000" height=1 weight=1>

2 CSRT 공격 연습하기

2 크로스 사이트 요청 변조 코드 작성

[CSRF 공격 예제의 입력 코드 화면]



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 CSRT 공격 연습하기

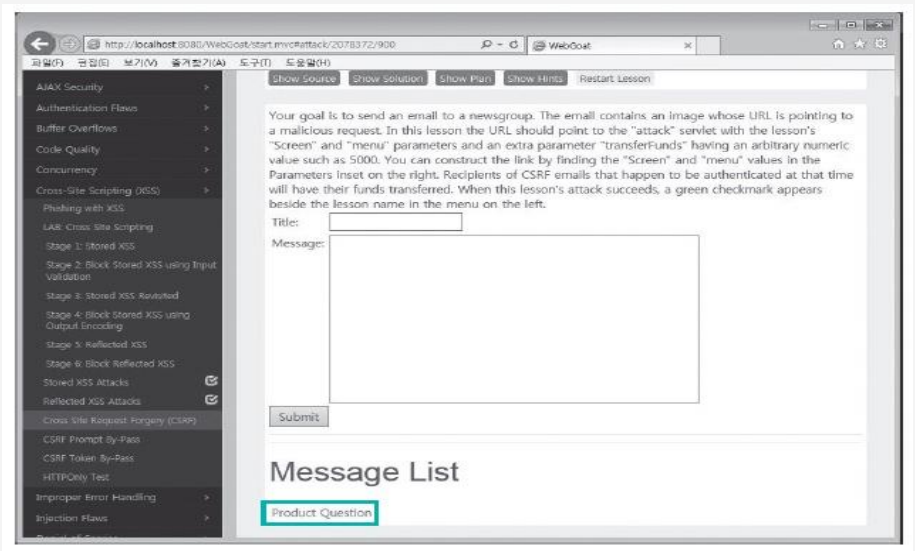
3 CSRF 공격 성공 확인

- 입력한 후 <Submit>를 클릭 후 전송하여 해당 게시물이 올라온 것 확인
- 해당 게시물을 클릭하면 공격자가 의도한 대로 5000이라는 금액이 이체될 것(악의적인 요청)

2 CSRT 공격 연습하기

3 CSRF 공격 성공 확인

[CSRF 공격 화면]



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017