The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 14, No. 4, pp.57-61, Aug. 31, 2014. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2014.14.4.57
JIIBC 2014-4-9

CSRF 공격기법에 대한 제로보드상의 취약점 방어

Vulnerability Defense of On-Zeroboard using CSRF Attack

김도원*, 배수연*, 안병구**

Do-Won Kim*, Su-Yeon Bae*, Beongku An**

요 약 제로보드는 PHP와 MySQL이 지원되는 공개용 게시판이다. 초보자들도 쉽게 사용할 수 있기 때문에 많이 사용되고 있으나 제로보드4를 마지막으로 더 이상의 업데이트는 없다고 알려져 있다. 때문에 취약점이 발생한다면 이를 사용하는 게시판 관리자들은 속수무책으로 당할 수밖에 없는 문제점이 존재한다. 본 논문에서는 XSS에서 확장하고 발전된 CSRF 공격에 대하여 알아보고, VM 웨어를 이용한 환경구축을 통해 대표적으로 게시판에서 이루어지는 CSRF의 공격방법과 그에 대한 대안방법을 제시한다. 제안된 방법(공격방법, 대안방법)의 주요한 특징 및 기여도는 다음과 같다. 첫째, VM 웨어를 비롯한 여러 tool들을 이용해 환경구축을 한다. 둘째, 프록시 서버를 사용해 취약점을 분석해 이에 대비한다. 성능평가는 고안한 대응방안을 적용시켜 그 성능을 평가한다.

Abstract Zeroboard is a public bulletin board that can support PHP and MySQL. It has been used by many people because it is easy to use, but there is no more updates after Zeroboard4. So, there is a problem that its administrator will have nothing to do about it if zeroboard has a vulnerability. In this paper, we will discuss about CSRF(Cross Site request Forgery) which is developed and expanded by XSS(Cross Site Scripting). Also, we will find CSRF attacks and suggest an alternative method using VM-ware. The main features and contributions of the proposed method are as follows. First, make an environment construction using VM-ware and other tools. Second, analyze and prepare vulnerabilities using Proxy server. Performance evaluation will be conducted by applying possible countermeasure.

Key Words : Zeroboard, CSRF, VM-ware

Ⅰ. 서 론

현대에 이르러 해킹공격 루트는 굉장히 한정적이다. 보안의식이 점차 성장함에 따라 일반 기업에서도 보안에 관심을 가지고 있고, 하드웨어나 소프트웨어에서도 기본적인 보안레벨이 강화됨에 따라 공격이 쉽게 성공하기가 어려워지고 있다. 그 중에서 웹서비스라는 항목은 더욱 확장되고 현재 대부분의 많은 사람들이 사용하고 있다. 웹 서비스는 어떤 서버에서 사용자에게 서비스를 제공해야만 하고, 권한이 있는 사람에게는 접근을 허용해야 한다. 그렇기 때문에 보안을 위해 모든 외부 접속 루트를 차단하여도 결국 웹은 차단 할 수 없다는 이야기다. 그만큼 웹 해킹에는 취약점이 많고 아직까지 발견하지 못한 보안방법이 많다.

그 방법 중 CSRF(Cross Site Request Forgery)는 인증 완료된 다른 사람의 권한으로 서버에 부적절한 요청

*준회원, 홍익대학교 컴퓨터정보통신공학과
**종신회원, 홍익대학교 컴퓨터정보통신공학과
접수일자 : 2014년 4월 4일, 수정완료 : 2014년 6월 24일
게재확정일자 : 2014년 8월 8일

Received: 4 April, 2014 / Revised: 24 June, 2014
Accepted: 8 August, 2014
**Corresponding Author: beongku@hongik.ac.kr
Dept. of Computer & Information Communications Engineering, Hongik University, Korea

을 하여 공격자의 공격이 사용자의 의도와는 관계없이 웹 브라우저 간의 상호 작용을 이루어지도록 한다.

본 논문에서는 VM 웨어(VM-ware)를 이용하여 서버를 설계하고 CSRF 기법이 많이 사용되는 제로보드를 설치해 제로보드에서 CSRF 공격을 수행하고 그 위험성을 확인한 후 그에 대한 대안 방안을 제시하는 것을 목표로 하고 있다.

본 논문은 II장에서 관련 기술 및 관련 연구를, III장에서는 환경 구축 및 CSRF를 이용한 공격을, IV장에서는 공격에 대한 대안방법으로 구성되며, 끝으로 V장에서는 결론을 맺도록 하겠다.

II. 관련연구

1. VM-ware

하나의 시스템에서 여러 가지 운영체제의 가상 실행 엔진을 사용하기 위해서 다수의 운영체제를 같이 사용할 수 있게 해주는 VM 웨어 프로그램을 사용하여 바이러스 테스트 시뮬레이션의 설계 및 구현을 할 수 있다. 한 운영체제에서 발생한 문제가 다른 운영체제에 영향을 미칠 수도 있다. 하지만 VM 웨어를 사용하면 재부팅을 하지 않고도 서로 다른 운영체제를 필요할 때마다 사용할 수 있을 뿐만 아니라 하드 디스크의 용량이 허용하는 범위 내에서는 수십 개의 운영체제를 실행 시킬 수 있다[1].

여러 플랫폼 상에서 개발한 웹 솔루션이나 바이러스 등을 테스트하는 것에 많은 도움이 된다. VM 웨어에서는 윈도우 창 없이도 윈도우 브라우저를 사용하여 프로그램 코드를 테스트 할 수 있으며 광범위 LAN으로 네트워크가 가능하므로 각각의 네트워크에서 솔루션을 테스트 할 수 있다[2].

VM 웨어는 실존하는 하드웨어 정보들을 공유하여 가상으로 하드웨어의 층을 만든다. 다시 말해 시스템의 하드웨어를 공유함으로 해서 현재 사용 중인 운영체제에 영향을 끼치지 않은 상태에서 다른 운영체제를 실행하는 것이다. 이러한 원리로 작동하기 때문에 다른 운영체제에 에러가 생기더라도 창 내에서만 멈추게 되므로 안전성도 뛰어나다[3]. 그림 1은 VM 웨어의 구동원리를 설명한다.

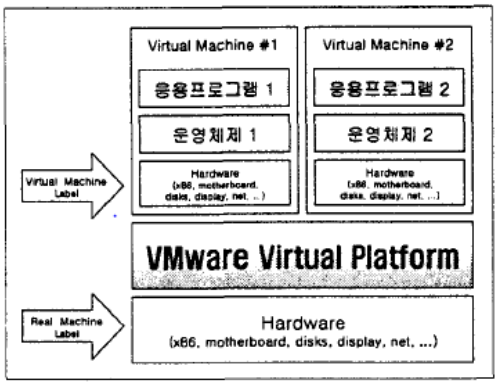


그림 1. VM-ware의 구동원리
Fig. 1. Operation of vm-ware

2. CSRF

웹페이지에 리소스 참조 태그를 삽입하여 사용자의 의도와 무관한 요청을 생성할 수 있다. 해커는 IMG 태그나 IFRAME 태그를 삽입하여 사용자의 자격으로 요청을 자동 생성한다. 조금 더 지능적인 방법으로 자바스크립트를 이용하여 DOM 객체를 동적으로 생산하거나 XTML, Http Request 객체의 setRequestHeader로 HTTP의 헤더까지 조작하여 요청을 생성할 수 있다. CSRF[4]는 웹사이트가 정상적으로 로그인한 사용자를 신뢰한다는 점을 이용하여, 로그인한 사용자의 인증정보를 악용하여 공격자가 변조된 HTTP 요청을 생성하며, 요청을 받은 취약한 웹어플리케이션이 해당 요청을 정당한 것으로 착각하여 공격자의 의도를 수행하게 만드는 공격이다. CSRF 공격[5-10]은 다음과 같은 시나리오로 동작한다.

- 클라이언트가 www.email.com 에 로그인(쿠키 값이 캐싱됨) 하고 e-mail을 열람한다.
- 클라이언트가 속임수, 숨겨진 이미지 링크를 통해 <SCRIPT src=http://www.email.com/index.html> 태그를 가진 evil.com을 방문
- 방문해서 받은 웹 페이지의 JavaScript가 실행, JavaScript 코드는 웹브라우저 캐시에 저장된 로그인 인증정보를 첨부하여 인증된 사용자로 가장, 웹 사이트 www.email.com에 위조된 요청을 보낸다[4]. 그림 2는 CSRF의 기본 원리를 설명한다.

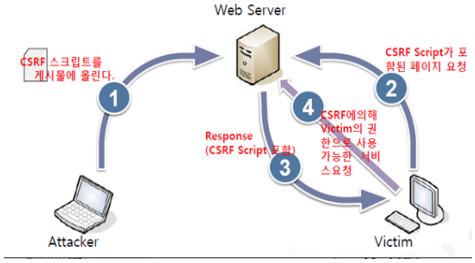


그림 2. CSRF의 원리
Fig. 2. Concepts of CSRF

3. 제로보드(Zero Board)

제로보드는 홈페이지용 전자게시판 프레임워크이다[10]. 이전에는 버그와 보안 취약점의 수정이 이루어 졌지만 현재 개발 및 유지가 포기 되었다. 그러나 컴퓨터에 대한 지식이 부족한 사람도 개인홈페이지나 인터넷 쇼핑몰 등으로 쉽게 사용가능 하여 많이 배포 되었으며 현재에도 많이 사용 되고 있다.

Ⅲ. CSRF를 이용한 공격

1. 환경 구축

환경 구축에 사용된 시스템 및 프로그램은 다음과 같다.

- VM-ware, Linux. Fedora7, httpd, mysql, php
- zb41pl2~zb41pl8
- 제로보드 xe 이하의 제로보드

2. 공격 방법

가. 프록시를 이용한 정보수집

공격에 앞서 중요한 것은 정보 수집이다. 먼저 게시판에서 패킷의 이동경로를 알아본다. 탈퇴 실행 시에 파라미터 값을 조작이 가능한지 알아봐야 한다. 탈퇴를 직접 해보면서 조사해보니 파라미터 값이 특별히 존재하지 않는다는 것을 알 수 있었다. 그림 3은 패킷의 이동경로를 설명한다.

```
GET /~          /bbs/member_out.php?id=&group_no=1 HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash,
application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Referer: http[redacted]          /bbs/member_modify.php?group_no=1
Accept-Language: ko
Proxy-Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; InfoPath.2)
Host: [redacted]
Cookie: PHPSESSID=98b60d57e3d64ee3c52e42771bf48dea
```

그림 3. 패킷의 이동경로
Fig. 3. Moving route of packets

그림 3을 참고하여 전송 페이지를 조사해 보면 member_out.php 로 전송되는 것을 확인한 뒤 바로 URL로 접근해 보면 아래와 같은 메시지가 출력된다. 그림 4는 출력된 메시지를 보여준다.

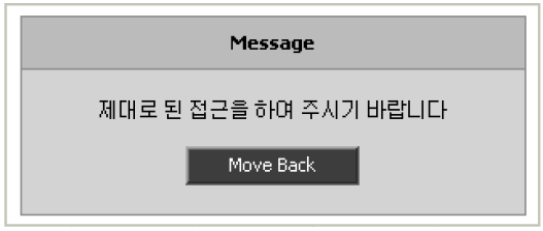


그림 4. 출력 된 메시지
Fig. 4. Output message

따라서 소스를 조사해 보면 아래와 같은 구문을 찾을 수 있다.

```
if(!eregi("member_modify.php",$HTTP_REFERER)) Error("제대로 된 접근을 하여 주시기 바랍니다");
```

위의 구문은 member_modify.php 라는 페이지에서 패킷을 전송하지 않으면 뒤의 에러문구를 출력하도록 한다는 뜻이다. 이를 거꾸로 생각하면 어떤 패킷이라도 일단 member_modify.php라는 이름이 있는 페이지에서 보낸 패킷이라면 위 문구에서는 패킷이 필터링 되지 않음을 알 수 있다.

그 다음으로 member_modify.php 파일을 열어 소스를 분석하여 탈퇴버튼을 눌렀을 때 보내어지는 파라미터 값을 확인한다.

```
<tr height=30 bgcolor=#ffffff>
  <td align=center>
  <? if($member[no]>1)
  {?><a href=member_out.php?id=<?=$id?>&group_no=<?=$group_no?> >
  <img src=images/button_out.gif border=0 alt="회원탈퇴"></a><?}?>
  </td>
  <td align=right ><img src=images/t.gif height=5><br>
  <input type=image border=0 src=images/button_modify.gif>  
```

여기에 회원 탈퇴 시 패킷을 보내는 페이지와 보내어지는 파라미터 값이 나와 있다. 이를 그래도 공격자의 서버에서 위 내용을 포함하는 페이지를 작성해 만들면 된다.

나. CSRF 공격 수행

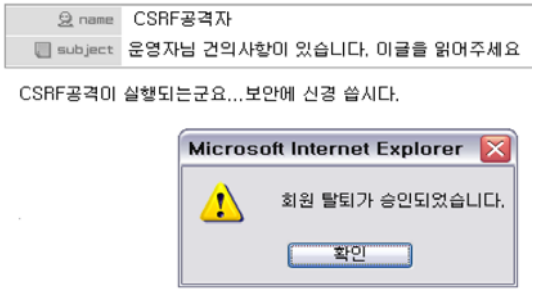
- 공격자는 자신의 서버에 페이지를 만들고 게시판에 그 페이지를 삽입할 것이다(XSS 기법사용). 아래와 같이 소스를 사용해 페이지를 만든다. 파일명은 경로 상관없이 member_modify.php로 한다. 그리고 나서 이 페이지를 게시판에 삽입한다.

```
<img height=0 width=0 src="[redacted].121/~LOUPOS
/bbs/member_out.php?id=<?=$id?>&group_no=<?=$group_no?>">
 <?php
      echo("
       <script>
       window.alert('회원 탈퇴가 승인되었습니다.')
        history.go(-1)
       </script>
       ");
   ?>
```

- 게시판에 아래내용을 삽입하면 이 게시글을 클릭하는 순간 위의 경로에 있는 페이지가 열린다. 따라서 공격자가 만든 페이지가 열리고 바로 탈퇴 페이지인 member_out.php로 파라미터 값이 전송되게 된다.

```
<boddy>
<iframe height=1 width=1 src="http:[redacted].116/csrf/member_modify.php?">
</iframe>
</body>
```

- 탈퇴가 성공적으로 이루어진다.



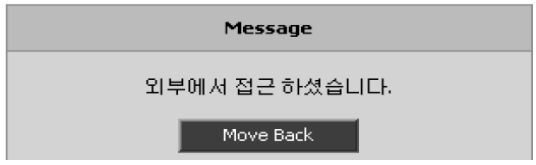
IV. 공격 대응방안

아래 구문을 새로 추가한다. 이 구문은 서버주소를 받아와서 이전페이지가 어떤 서버에 있었는지를 검사한다. 그래서 공격자가 자신의 서버(다른 서버)에 페이지를 올리고 중간에 페이지 삽입을 하였다면 이 때 나오는 패킷을 공격자 서버의 주소를 갖게 된다. 따라서 위 구문을 추가하면 페이지 명과 서버 주소값을 동시에 검사해 공격을 막을 수 있다.

```
if(!eregi("member_modify.php",$HTTP_REFERER))
    Error("제대로 된 접근을 하여 주시기 바랍니다");

if(!eregi($HTTP_HOST,$HTTP_REFERER))
    Error("외부에서 접근하셨습니다.");
```

위 구문을 추가한 뒤 접근하면 아래와 같은 화면이 출력된다.



V. 결 론

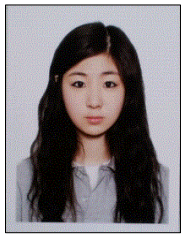
본 논문에서는 OWASP에 선정된 10대 웹 취약점 중 한가지로 뽑힌 CSRF(Cross Site Request Forgery)에 대한 분석과 실험을 통하여 그에 대한 위험성을 알아보고 대응 방안을 제시하였다. 공개용 소스인 제로보드의 취약점을 발견하고 그것을 이용하여 실험을 할 수 있었다. 이 공격방법은 외부서버(해커의 서버)에 페이지를 올려놓고 게시판에서 열게 되는데 이 때 탈퇴가 가능한 이유는 세션 값이 그대로 유지되기 때문이다. 이 탈퇴 방법이 일반사용자라면 큰 문제가 되지 않을 수도 있다. 그러나 관리자가 읽게 된다면 게시판 Admin 계정이 삭제되어 상당한 피해를 입게 될 것이다. 또한 복구 역시 굉장히 어려워 질 수 있다. 완성도가 높은 소스이기 때문에 제로보드를 사용하는 사용자가 많고, 개발이 중지된 현재로써 악의적으로 CSRF를 사용하여 피해를 입힐 수 있는 상황에서 이 보안방법은 적절한 대응이 이루어짐을 확인할 수 있다. 공격이 발견되고 나서 패치가 되기 직전까지 실제로 보안패치가 되지 않은 모든 동일 웹에서 공격이 성공할 수 있고, 이 실험뿐만 아니라 많은 공격이 응용가능하다. 그렇기 때문에 앞으로의 공격 기법들을 지속적으로 분석하여 보다 더 나은 대응 방안을 마련하는 것도 필요하다고 생각한다.

References

[1] http://www.vmware-com/support/ws3/doc/whatsnew_ws.html
[2] http://www.virusbtn.com/magazine/overview/index,xml
[3] ftp://ftp.cs.uta.fi/pub/vru/documents/test1997.zip
[4] Boyan Chen, Pavol Zavarsky, Ron Ruhl and Dale Lindskog, "A Study of the Effectiveness of CSRF Guard," IEEE Proc. of PASSAT/SocialCom 2011, October 2011.
[5] Xiaoli Lin, Pavol Zavarsky, Ron Ruhl, Dale Lindskog, "Threat Modeling for CSRF Attacks," IEEE Proc. of CSE2009, pp.486-491, August 2009.
[6] Hossein Saiedian, Dan S. Broyles, "Security Vulnerabilities in the Same-Origin Policy: Implications and Alternatives," Computer, vol.44, issue9, pp.29 -36, September 2011.
[7] Tatiana Alexenko, Mark Jenne, Suman Deb Roy, Wenjun Zeng, "Cross-Site Request Forgery: Attack and Defense," IEEE Proc. of CCNC2010, pp.1-2, January 2010.
[8] Yin-Chang Sung, Michael Cheng Yi Cho, Chi-Wei Wang, Chia-Wei Hsu, Shiuhpyng Winston Shieh, "Light-Weight CSRF Protection by Labeling User-Created Contents," IEEE Proc. of SERE 2013, pp.60-69, June 2013.
[9]Nenad Jovanovic, Engin Kirda, and Christopher Kruegel, "Preventing Cross Site Request Forgery Attacks," IEEE Proc. of Securecomm and Workshops 2006, pp.1-10, August 2006.
[10]Soeui Kim, Duri Choi, Beongku An, "Detection and Prevention Method by Analyzing Malignant Code of Malignant Bot," JIIBC, pp.199-207, vol.13, no.2, April 2013.

저자 소개

김 도 원(학생회원)



• 2014년 : 홍익대학교 컴퓨터정보통신공학과 졸업 (BS)
<주관심분야 : 네트워크보안, 데이터베이스 >

배 수 연(학생회원)

• 2014년 : 홍익대학교 컴퓨터정보통신공학과 졸업 (BS)
<주관심분야 : 네트워크보안, 컴퓨터보안>

안 병 구(종신회원)

• 1988년 : 경북대학교 전자공학과 (BS)
• 1996년 : (미)Polytechnic University, Dept. of Computer and Electrical Eng., USA (MS).
• 2002년 : (미)New Jersey Institute of Technology (NJIT), Dept. of Computer and Electrical Eng. USA.(Ph.D)
• 1989년 ~ 1994년 : 포항산업과학기술연구원(RIST), 선임연구원
• 2012년 : 대한전자공학회 컴퓨터소사이어티 회장
• 2003년 ~ 현재 : 홍익대학교 컴퓨터정보통신공학과 교수
• 2005년 ~ 2012년 : Marquis Who's Who in Science and Engineering was listed.(세계과학기술인명사전 등재)
• 2006년 ~ 2013년 : Marquis Who's Who in the World was listed.(세계인명사전 등재)
<주관심분야: Wireless Networks, Ad-hoc & Sensor Networks, Multicast Routing, QoS Routing, VLC, Cognitive Radio Networks, Cross-Layer Technology, Cooperative Communication, Network Coding, Bioinformatics>

※This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (MEST) (Grants No. 2013075605) and and by Business for Cooperative R&D between Industry, Academy, and Research Institute funded Korea Small and Medium Business Administration in 2013 (Grants No. C0150656).