http://dx.doi.org/10.14400/JDPM.2013.11.12.327

XSS 공격과 대응방안

홍성혁*
백석대학교, 정보통신학부 정보보호 전공

XSS Attack and Countermeasure: Survey

Sunghyuck Hong*
Baekseok University, Division of Information and Communication

요 약 XSS는 공격자가 상대방의 브라우저에 Script를 실행할 수 있게 하여 사용자의 Session을 가로채거나 웹 사이트 변조, 악의적 컨텐츠 삽입, 피싱 공격을 할 수 있다. XSS공격은 저장(Stored)XSS와 반사(Reflected)XSS 이렇게 크게 두 가지 공격이 있다. XSS 공격의 형태는 Cookie Sniffing, 스크립트 암호화 및 우회, 악성코드 유포, Key Logger, Mouse Sniffer, 거짓정보 추가가 있다. XSS 공격은 스크립트 언어 그리고 취약한 코드들이 공격 대상이 된다. XSS 공격의 대응 방법에는 관리자의 대응과 사용자의 대응 두 가지를 제한 하였다.

주제어 : XSS 공격, Script 공격, 정보보호, Web 보안, URL 보안

Abstract XSS is an attacker on the other party of the browser that is allowed to run the script. It is seized session of the users, or web site modulation, malicious content insertion, and phishing attack which is available. XSS attacks are stored XSS and reflected XSS. In that, two branch attacks. The form of XSS attacks are cookie sniffing, script encryption, bypass, the malignant cord diffusion, Key Logger, Mouse Sniffer, and addition of lie information addition. XSS attacks are target of attack by script language. Therefore, the countermeasure of XSS is presented and proposed to improve web security.

Key Words : XSS, Script, information Security, Web, URL

1. 서론

웹의 확대와 더불어 각종 사용자 정보 침해사건도 증가하고 있다. 다양한 서비스에 발맞춰 이를 노리는 각종 공격들이 새로 등장하고 있기 때문이다.[1]

OWASP(The Open Web Application Security Project) Foundation은 OWASP Top 10-2013을 발표 했는데 이에 포함된 10대 취약점을 보면 Injection, XSS(Cross-site Scripting), 인증과 세션 관리 취약점, 취약한 직접 객체 참조, CSRF(Cross-site request forgery), 보안 설정 오류, 민감 데이터 노출, 기능 수준의 접근 통제 누락, 알려진 취약점이 있는 컴포넌트 사용, 검증되지 않은 리다이엑트 포워드로 나누었다. XSS는 가장 심각한 웹 애플리케이션 보안 위협 리스트에서 2위에 있

* This research was partially supported by Baekseok University.
Received 15 October 2013, Revised 7 November 2013
Accepted 20 December 2013
Corresponding Author: Hong, Seong Hyuk(Baekseok University)
Email: shong@bu.ac.kr

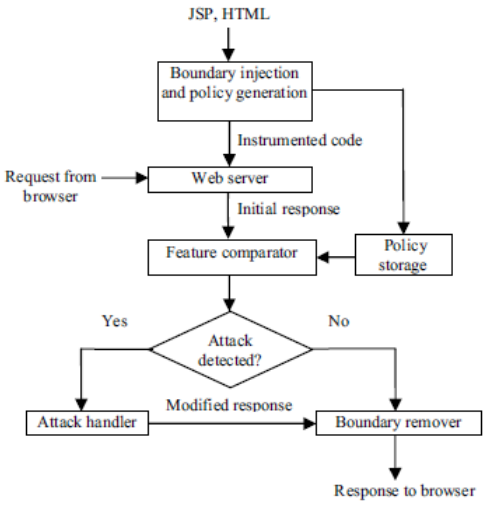
ISSN: 1738-1916

다.[2] 이 Web해킹 중에서도 XSS공격과 SQL-Injection 취약점은 Web 해킹의대표적 기법이라고 할 수 있다. XSS 공격은 현실적으로 방어하기 상당히 어렵다. 그렇기 때문에 많은 웹사이트에서 XSS의 취약점이 존재하고 악용되고 있다. 본 연구의 구성은 다음과 같다. 2장에서는 XSS와 XSS의 공격 방법, 형태를 기술 하였고, 3장에서는 XSS공격의 대응방안을 가술 하였다. 마지막으로 4장에서는 본 연구를 마무리하는 결론을 맺는다.

2. XSS

2.1 XSS

XSS란 Cross Site Scripting의 약자이다. 공격자가 상대방의 브라우저에 Script를 실행할 수 있게 하여 사용자 Session을 가로채거나 웹 사이트 변조, 악의적 컨텐츠 삽입, 피싱 공격을 할 수 있다. 웹이 발전함에 따라 XSS 또한 지능화 되고 있으며, 현재도, 앞으로도 가장 위협적인 Web 취약점이 될 것이다. 이 취약점이 위협적인 이유는 공격 기법 자체가 HTML과 Script를 사용하여 쉽게 공격 코드를 제작할 수 있다는 것과, 이렇게 제작된 간단한 공격 코드를 대부분의 홈페이지에 손쉽게 올릴 수 있다는 것이다.



[Fig. 1] XSS attack framework

[Fig. 1]은 XSS 공격의 예다. 실행 가능한 악성 코드를 웹페이지에 삽입한 뒤 다른 사용자가 악성 코드가 심어진 웹페이지를 보게 하여 사용자의 컨텍스트에서 코드를 실행 시키는 기법이다.[3]

2.2 XSS공격 방법

XSS공격은 저장(Stored)XSS와 반사(Reflected)XSS 이렇게 크게 두 가지 공격이 있다.

저장(Stored)XSS는 공격자가 XSS 취약점 공격을 위해 가장 많이 살펴보는 곳이 같은 사이트를 방문하는 다른 사용자들에게 보이는 데이터를 입력하는 부분이다.

Stored XSS의 기본 방식은 공격자가 게시물에 악성 Script를 삽입한다. 사용자는 게시물을 클릭하고. 공격자의 JavaScript가 포함된 응답이 전송된다. 브라우저에서 스크립트가 실행이 되고 공격자는 사용자의 쿠키, 세션 등 원하는 정보를 획득 하게 된다.

반사(Reflected)XSS는 URL의 CGI 인자에 Script Code를 삽입하는 것이다. 공격자가 이메일을 이용해 어떤 웹 페이지 링크를 보내고 사용자가 링크를 클릭하면 그 링크에 대한 웹 페이지가 화면에 나오게 된다. 그때 웹페이지에 대한 링크 URL에 삽입된 스크립트 코드가 실행되면서 웹 페이지의 내용이 변경된다. Reflected 방식의 기본적인 방식이다.[4]

이 공격은 스크립트를 저장하기 위한 웹 사이트는 필요하지 않으며 사용자가 조작된 링크 주소를 클릭하면 링크에 대한 웹페이지가 로드 되면서 그 스크립트 코드가 실행되기 때문이다.

위에서 보듯이 XSS는 프로그래밍 기술 측면과 복잡성을 고려할 때 공격자에게 최상의 공격 방법이다.

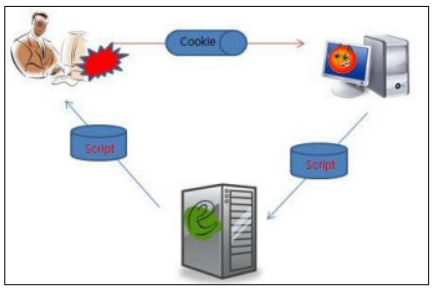
2.3 XSS공격의 다양한 형태

먼저 Cookie Sniffing 기법이 있다. Cooke는 사용자 인증에서 봤을 때 사용자의 인증 데이터를 가지고 있는 값이다. 이 Cookie는 클라이언트에 저장 되면, 파기 되기 전까지 서버에 데이터를 요청할 때 항상 서버로 보내지게 된다. 특정 웹에서 id/password를 입력하면 서버가 "id=guest"데이터를 Cookie를 통해 전송한다. 이 데이터는 요청할 때 마다 전송되기 때문에 로그인 한 상태로 웹을 탐색 할 수 있게 된다.

위의 경우 “id=guest” 라는 값을 클라이언트가 저장하고 있기 때문에 공격자가 조작을 할 수 있다. "id=admin"

값으로 공격자가 조작하여 서버로 전송하면, 서버는 guest 사용자가 아닌 admin이라는 사용자로 인식하여 동작한다. 이를 방어하기 위해 서버는 Session을 사용한다. Session은 기존 공격의 문제점인 Cookie 값의 변조를 막기 위해, Cookie에 사용자 정보를 바로 전송하지 않고 서버에 사용자 정보를 저장해두고 그 저장해준 데이터를 찾을 수 있는 Key 값을 Cookie로 전송한다. 사용자의 정보가 서버에 잠기 때문에 데이터 조작이 불가능하다.

이러한 방어 기법을 무너트리기 위해 공격자는 XSS를 사용한다.



[Fig. 2] Cookie Sniffing

Cookie Sniffing 방식의 기본 적인 형식은 Fig. 2와 같다. 예를 들어 공격자는 악성 Script를 정상 홈페이지에 올린다. 사용자들은 아무것도 모르고 공격자가 올린 게시물을 열어 악성Script를 실행하게 된다. 자신의 Cookie 값을 공격자에게 자동으로 전송한다. 공격자는 사용자의 Cookie값을 이용하여 개인정보와 데이터를 유출, 삭제 가능하게 된다.[5]

두 번째 공격 방법으로는 악성코드 유포가 있다. 악성코드는 사람들이 많이 찾는 사이트, 카페를 통해 ActiveX를 설치하게 하는 경우와 SQL injection공격을 이용하여 사이트에 공격 코드를 심어놓는다.

세 번째 스크립트 암호화 및 우회가 있다. 업체에서는 XSS 공격으로 피해가 많아 Script를 계속 필터링 하고 있다. 고객들의 편의를 위해 모두 필터링 못하고 문자열만 필터링 함으로써 XSS공격에 대비 한다. 그러나 공격자들은 이런 필터링들을 우회 하는 방법을 가지고 이어 필터링은 XSS공격에 대한 대안법이 되지 못한다. <Table 1>은 우회하는 대표적인 예이다.

〈Table 1〉 XSS via Method

<script SRC=http://www.sss.com/xss.js></script>	Bypass filtering using the new line character
<IMG SRC=JaVaSCiPt:alert('XSS')>	Bypass filtering in mixed capital and small letter
<IMG SRC=javac&#114 ipt:le&#11 6;('SS')>	Bypass filtering using the Unicode encoding scheme
<IMG SRC="javasc ript:alert('XSS');">	Bypass filtering using word space

네 번째 공격 방법은 Key Logger이 있다. 사용자 키보드 이벤트를 했을 때 입력된 키 값을 공격자에게 계속 전송하여 입력되는 키를 가로채는 것을 말한다. 이는 웹페이지에 들어가 로그인 할 때부터 가로채므로 주의 해야 한다.

다섯 번째 공격 방법은 Mouse Sniffer다. Mouse Sniffer는 공격자가 사용자의 마우스 위치를 추적하는 것이다. 이것은 사용자가 마우스 클릭 시 X, Y 좌표를 공격자가 획득하여 사용자가 마우스를 이동한 곳을 알 수 있다.

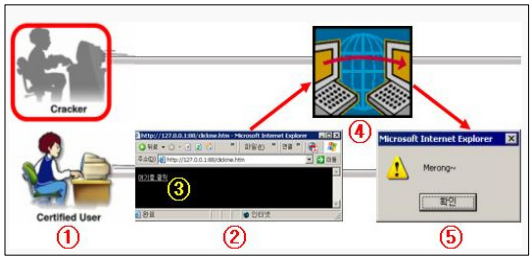
여섯 번째는 거짓 정보 추가하기다. 공격자는 사용자가 이용하고 있는 웹 화면을 수정할 수 있다. 현재 보이는 페이지를 공격자가 원하는 것으로 바뀔 수 있다. 예로 은행이나 개인정보 페이지가 바뀔 수 있다.

2.4 XSS공격 대상

XSS공격은 스크립트 언어 그리고 취약한 코드들이 공격 대상이 된다. 스크립트나 언어는 JavaScript, VBScript, ActiveX, HTML, Flash가 있고 취약한 코드들은 interactive bulletin boards, custom error pages, search engines CGI scripts 들이 있다.

2.5 XSS공격 순서

1. 해커가 사전에 만든 웹페이지에 사용자가 브라우저로 엑세스를 시도한다.
2. XSS공격 link가 포함된 웹페이지가 브라우저에 표시된다.
3. 사용자가 link를 클릭한다.
4. 사용자가 느끼지 못하는 사이 취약한 사이트에 있는 해커의 스크립트에 엑세스 된다.



[Fig. 3] Attack Procedure

5. 사용자의 웹브라우저 상에서 해커의 스크립트가 실행된다. [6]

이것이 기본적인 XSS공격 순서다. 이 외에도 다양한 응용이 있다. [Fig. 3]의 5단계 순서에서 재미있는 부분은 1단계에서 3단계로 이 것는 사용자가 조작을 선택하게 하는 부분이다. 하지만 해커는 웹페이지를 위장하여 사용자가 인식하기 전에 3단계까지 가게 만들었다.

예를 들면 인터넷을 돌아다니다 보면 사용자들은 이런 massage를 본적이 있을 것이다.

"이 페이지는 www.@@@.co.kr으로 변경되었습니다. *초후 자동으로 이동합니다."

이 메세지는 사이트가 자동으로 이동한다는 것을 설명하고 있다. 같은 원리로 사용자가 직접 링크를 클릭 하는 것을 기다리지 않고 메시지 없이 자동으로 특정page로 이동하게 만들어 사용자가 인식 하기 전에 3단계를 실행할 수 있다.

2.6 XSS공격 TEST

HTML코드에 <script>태그를 삽입하여 공격하는 방식이다. HTML 태그 중 IMG 라는 이미지 삽입 태그를 공격을 하였다 Fig. 4 참조.

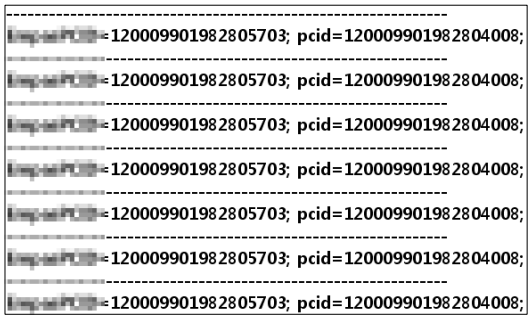
```
<IMGSRC=javascript:document.location='http://MyWeb/Getcookie.asp?cookie='+document.cookie;>
```

[Fig. 4] Tage Insert

[Fig.5]에 나와 있는 것처럼 희생자가 메일을 읽으면 다음과 같은 화면이 나타날 것이고 이 화면 보게 되면 사용자의 쿠키 값은 공격자의 웹 서버에 남는다.

[Fig. 5] Mail Shot

그림 6처럼 공격자의 C: \xss \xss.txt 파일에 쿠키 값이 저장 된다.



[Fig. 6] Attacker's xss.txt

공격자는 훔친 쿠키로 로그인을 해서 사용자의 개인정보를 알 수 있다.

2.6 XSS공격 피해 사례

1. 트위터 XSS공격 당해…백악관 대변인도 피해

미국서 트위터가 사이버 공격에 당하면서 음란물 유포 사이트로 변신하는 소동이 벌어졌다. 씨넷 등 미 외신들은 현지시간 21일 새벽 5시경부터 '트위터닷컴'에서 단문 메시지가 담긴 '트위트'에 클릭없이 마우스만 올려도 음란물이 뜨는 새 페이지로 연결된다고 이날 보도했다. 영국계 보안회사 소포스에 따르면 트위터는 전형적인 'XSS(Cross-site scripting)' 공격에 당한 것으로 보인다. 소포스는 이번 공격의 영향을 받은 사람을 최소 10만명 이상으로 추정했다.[8]

2. 단돈 700달러에 야후 메일계정 훔칠 수 있다니!

새로운 XSS(Cross-Site Scripting) 취약점을 이용한 익스플로잇이 시장가격의 절반 이하인 700달러에 한 언더그라운드 마켓에서 독점으로 유통되고 있는 것으로 나

타났다. 이는 해커들이 쿠키를 훔친 후 야후(Yahoo) 이메일 계정에 접근할 수 있도록 해준다. 미국 보안전문가인 브라이언 크렙스(Brian Krebs)는 블로그를 통해 이번 공격은 야후 이메일에 사용되는 세션 쿠키를 빼낸 후 해커들이 계정에 접속해 메시지를 읽거나 전송할 수 있는 기능을 제공한다고 밝혔다. 해당 익스플로잇을 판매하는 해커는 이번 공격이 XSS 취약점을 이용한 공격이라 설명했는데, 저장된 XSS 공격들이 크롬과 인터넷 익스플로러 등의 브라우저에 내장된 XSS 필터를 우회할 수 있다며 이러한 공격의 일반적인 가격대는 1,500달러선이라고 설명했다. (2012.11.28 보안뉴스) [9]

3. XSS공격 대응방법

XSS 취약점은 웹 개발자가 사용자가 입력을 하는 부분에서 사용자에 대한 입력을 검증을 하지 않았기 때문에 이런 공격에 취약하다. 개발자나 관리자는 XSS공격에 대응하는 방법을 나열해보겠다.

첫 번째로 중요한 정보를 쿠키에 저장을 안하는 것이다. 관리자는 사용자를 식별해야 하기 때문에 쿠키에 사용자의 정보를 저장하는 데 이를 쿠키에 넣지 않아야 한다. 두 번째로 Script code에 사용 되는 특수문자에 대해 정확히 필터링을 해야 한다. 예로 사용자가 입력 할 수 있는 문자만 빼고 필터링을 하는 것이다. 이 방법은 XSS 공격에 필요한 특수문자<Table 2>들을 막을 수 있다.

〈Table 2〉 XSS Attack Special Characters

Special Characters	Meaning
< , >	Start of tags, end of tags
&	Parameters of the discriminator
“ , ‘	Property Value
tab, new line	End of URL
%	HTTP escape sequence
″ in !	Server Side Script

세 번째로 게시판에서 HTML 포맷의 입력을 할 수 없도록 해야 한다. 최근 게시판들은 효과를 위해 사용자가 HTML 태그를 사용할 수 있게 하지만 XSS 공격에 대비하기 위해서는 HTML 포맷의 입력을 할 수 없도록 해야 한다.

마지막으로 관리자나 개발자가 주기적으로 점검을 해야 한다. 일반 사용자들도 XSS 공격에 노출 되어 있다. 메일이나 카페 그리고 게시판 같은 곳에 들어가서 자신도 모르게 악성 Script코드가 자신의 컴퓨터에 들어갔는지 모르기 때문이다. 그럼 및에 사용자가 할 수 있는 대처법에 대하여 설명하면 다음과 같다.

첫 번째로 자신이 받은 이메일에 링크 같은 것이 걸려 있으면 바로 클릭하지 말고 주소창에 URL을 직접 입력하여 들어가는 것이다. 이 방법은 URL 스푸닝이나 XSS 공격에 가장 기본적으로 대비하는 방법이다.

두 번째는 자신의 인터넷의 패치를 가장 최신의 것으로 업데이트 하는 것이다. 업데이트를 함으로써 자신의 인터넷 취약점을 보완할 수 있다.

세 번째로 인터넷 옵션에 개인 정보 등급을 높이는 것이다. 이 방법은 불필요한 Cookie값을 보내지 않는 것으로 많은 도움이 된다.

네 번째로 사용자들이 할 수 있는 XSS 대응 방안으로는 웹 메일 옵션에서 ‘JavaScript 허용여부’등을 선택할 수 있다면 허용하지 않는 것으로 설정하는 것이다. 그러나 사용자가 자바 스크립트를 해제시키더라도 이 기능을 해제하지 않은 다른 사용자가 e-mail을 받을 경우에는 JavaScript의 악성 행위의 효력을 발휘한다.[10]

4. 결론

XSS는 공격자가 상대방의 브라우저에 Script를 실행할 수 있게 하여 사용자의 Session을 가로채거나 웹 사이트 변조, 악의적 컨텐츠 삽입, 피싱 공격 등을 할 수 있다. 이런 XSS의 공격방법은 대표적으로 Stored XSS, Reflected XSS가 있다. 공격 형태로는 Cookie Sniffing, 악성코드 유포, 스크립트 암호화 및 우회 등 많은 공격 형태들이 존재 한다. 공격들이 다양하여 각각의 대응법도 존재 한다. 개발자들은 관리와 제품의 업데이트, 그리고 점검을 자주 해야 하며 사용자들은 자신의 컴퓨터에 대한 지식을 쌓고 자신의 인터넷의 업데이트를 통한 취약점을 보안함으로써 보안을 높일 수 있다.

REFERENCES

[1] Shaikh, F.B.; Haider, S., "Security threats in cloud computing," Internet Technology and Secured Transactions (ICITST), 2011 International Conference for , vol., no., pp.214-219, Dec. 11-14, 2011

[2] Open Web Application Security Project(OWASP). "OWASP Top 10 for 2013". 12 June, 2013.

[3] Shahriar, H.; Zulkernine, M., "S2XS2: A Server Side Approach to Automatically Detect XSS Attacks," Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on, vol., no., pp.7,14, Dec. 2011.

[4] Yi Wang; Zhoujun Li; Tao Guo, "Program Slicing Stored XSS Bugs in Web Application," Theoretical Aspects of Software Engineering (TASE), 2011 Fifth International Symposium on, vol., no., pp.191-194, Aug. 2011

[5] Chomsiri, T., "Sniffing Packets on LAN without ARP Spoofing," Convergence and Hybrid Information Technology, 2008. ICCIT '08. Third International Conference on , vol.2, no., pp. 472-477, Nov. 2008

[6] Hui Zhao; Wen Chen, "A Web Page Malicious Script Detection Method Inspired by the Process of Immunoglobulin Secretion," Intelligence Information Processing and Trusted Computing (IPTC), 2010 International Symposium on , vol., no., pp.241-245, Oct. 2010

[7] Mirtalebi, A.; Khayyambashi, M.R., "Enhancing security of Web service against WSDL threats," Emergency Management and Management Sciences (ICEMMS), 2011 2nd IEEE International Conference on , vol., no., pp. 920-923, Aug. 2011

[8] Bozic, J.; Wotawa, F., "XSS pattern for attack modeling in testing," Automation of Software Test (AST), 2013 8th International Workshop on , vol., no., pp.71-74, May, 2013

[9] Ross, P.E., "Microsoft to spammers: go phish [e-mail security]," Spectrum, IEEE , vol.43, no.1, pp. 48-49, Jan. 2006

[10] Matsuda, T.; Koizumi, D.; Sonoda, M., "Cross site scripting attacks detection algorithm based on the appearance position of characters," Communications, Computers and Applications (MIC-CCA), 2012 Mosharaka International Conference on , vol., no., pp. 65-70, Oct. 2012.

홍 성 혁(Hong, Sunghyuck)

・1995년 2월 : 명지대학교 컴퓨터공학과 (공학사)
・2007년 8월 : Texas Tech University, Computer Science (공학박사)
・2012년 3월 ~ 현재 : 백석대학교 정보통신학부 교수
・관심분야 : 네트워코 보안, 해킹, 센서네트워크 보안
・E-Mail : shong@bu.ac.kr