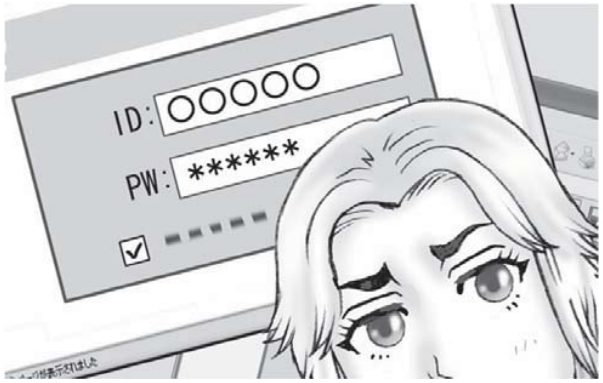
정보 윤리 소책자

악의성 웹 페이지



【 목표와 포인트】

1. 크로스 사이트 스크립팅의 원리와 문제점을 이해한다.
   - ○ 쿠키에 대해 이해한다.
   - ○ 크로스 사이트 스크립팅의 원리를 이해한다.
   - ○ 크로스 사이트 스크립팅의 원리를 이해하여 이 이야기의 다른 어떤 피해를 받을 가능성이 있는지를 인식한다.
2. 크로스 사이트 스크립팅 공격의 피해를 받지 않기 위해, 이용자로 어떤 주의가 필요한지를 이해한다.
3. 정보 보안과 관련된 다른 문제에 대해서도 조사하여 피해를 당하지 않기 위한 방책을 생각한다.


딩동~
앗.. 히로시씨 입장..
딩동
히로시> 유키링~ 안녕~ 찾고 있던 치마는 찾았어?
히로시씨 안녕하세요. 덕분에 가르쳐주신 사이트에서 싸고 이쁜 치마 샀어요. 감사해요^^
딩동~
히로시> 근데 있잖아 유키링~ 시부야@사이트 알아? 싸고 완전 질도 좋아~ 유키링이 좋아하는 옷도 있고 강추!!!
딩동~
요게 그 사이트 주소야~~
https://www.sibuya-net.....
일단 보자~
클릭!
와~~~!
SHIBUYA@NETLINE
정말 감사해요~
-----> 상상속의 히로시
히로시씨는 만난적도 없는 나한테 이렇게 친절하다니... 완전 좋은 사람인것 같당~

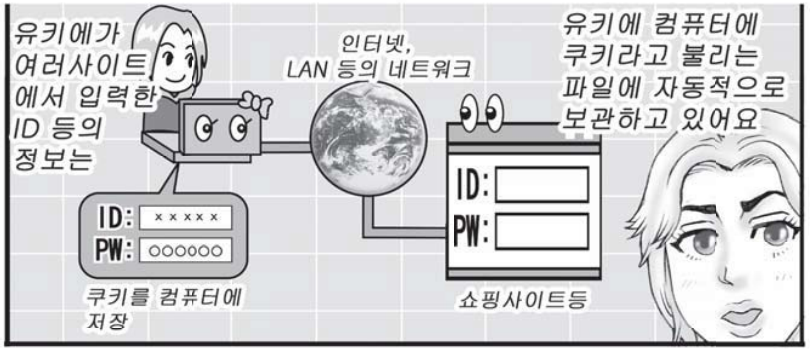

SHIBUYA@NE
즐겨찾기 추가하고~
어머~
지금 회원등록시 모든 고객에게 멋진 선물을~!
바로 회원등록하기
유키링> 지금 회원등록하려구요~
히로시> 그래~! 음악다운도 할 수 있고 포인트 모으면 만화나 DVD도 살 수 있어~! 일단 등록만으로도 좋지 않을까나?^^
유키링> 네~~!! 그럴께요^-^
히로시씨 추천이니까 문제 없겠지
주소 이름 카드번호 ...랑..
됐다~ 다썼다~!
클릭!!
전송
완료!!
히로시씨 아직 있어요?
일단 등록은 했어요~
딩동
히로시> 와~ 수고했어~! 그런데 나도 취미로 사이트 하나 운영하고 있어~ 시간있으면 와봐^^
http://www.teach-for
오~ 어떤 사이트 일까나?
클릭!

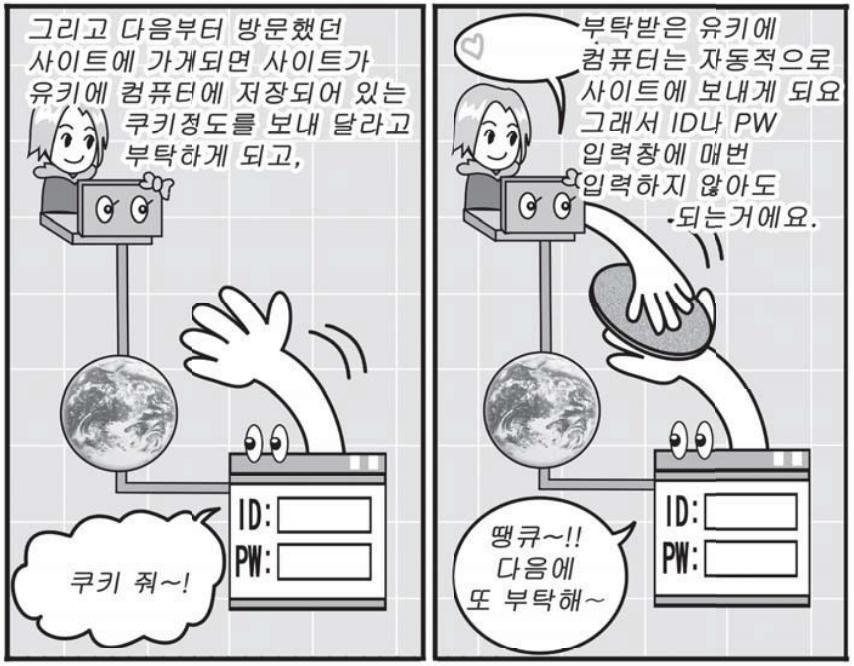

Pleasure room
링크가 많이 있는 사이트네~
BURNING T
SHIBUYA@NET
IKEBUKURO
아~ 시부야도 링크되어 있네~
유키링> 와~ 좋은 사이트네요~ 즐겨찾기 해둘께요~ (^▽^)♪
즐겨찾기야
히로시> 고마워~ 사실은 애드센스종류 같은건데 시부야 사이트들어갈때 내 사이트를 통해서 들어가면 나한테 많이 도움이 돼~
딩동~
뭐.. 그정도면 힘든일도 아니지... 도움도 주셨는데..
네~ 알겠습니다. 클릭 많이~ 할께요~^^
딩동~
히로시> 땡큐~~ 그럼 클릭 많이 부탁해요~ 난 그만 나갈게~~!!
딩동~
SyS> 히로시씨는 퇴장하셨습니다
그럼일단 히로시씨 사이트에서 ....
OUTLET K
BURNING T
SHIBUYA@NET
KEBUKURO
클릭! 하고...
SHIBUYA@NE


나도 애드센스 해볼까나?
앗~ 이 구두 예뻐~~
한달 후..
LOUNGE
뭐? 카드회사에서 청구서가 100만원 가까이 나왔다고??
목소리 좀 크다...
명세서에는 시부야@넷라인이라는 사이트에서 한도액까지 유료곡을 다운한걸로 나오는데?
근데.. 그게 하나도 짐작 가는게 없어... 난 회원등록만 했을 뿐이고~!! 쇼핑은 하지도 않았을 뿐이고~!!
잠깐만... 지금 좀 찾아보자..
시부야@넷라인
Google
클릭!
헉..


XSS취약성 있는
온라인 넷 쇼핑
아래의 사이트에서
쇼핑할때에는 꼭!
조심하세요!!
아시안e-net : http://....
시부야@넷라인.....
등....
XSS?
음..
잘은모르겠지만..
안정성에
문제가 있는
사이트인 것
같아
근데...
왜 이런 사이트에
가입을
해버린거야~!!
그게..
채팅룸에서
히로시씨가
추천했거든..
저번에
말했던
채팅친구?
그럼,
그 히로시란
사람한테
물어보면
뭔가 알 수
있지 않을까?
응.. 여러가지
가르쳐주기도 하고
너무 친절하고
좋은사람인데..
그게...
요즘 전혀..
모습이 안 보여서...
채팅방
친구들도
걱정하고
있는데..
뭔가..
수상한데.
그사람..?
하긴
..
아~~
어떻하면
좋지?
이 돈....
내가 내야
하는거야??

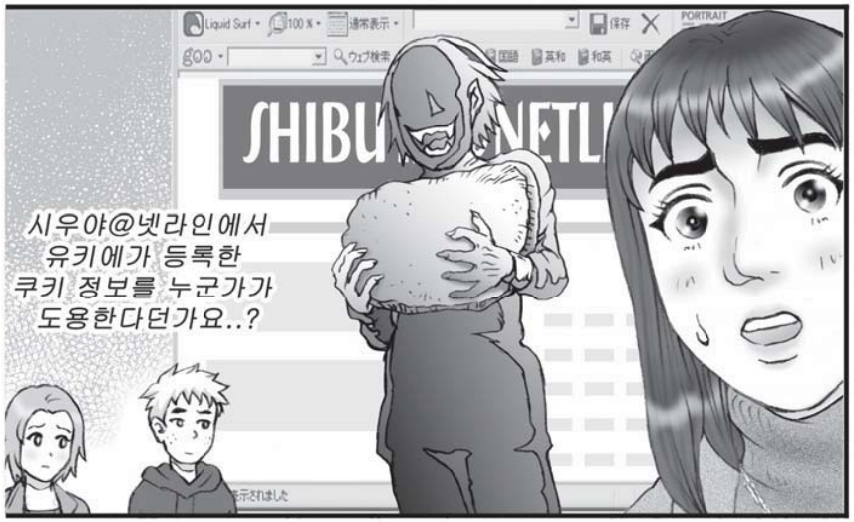

해결 편
자.
이건
곤란해요
지금 문제
되고 있는건
시부야
@넷라인의
XSS
크로스사이트
스크립트속임수
서버 xss
취약성
이에요.
그러니까
그..
크로스
뭐란게..
뭐죠?
그전
에..
유키에~
평소에
쿠키를
이용하는
사이트에
주의를
기울이고
있어요?
평소에
잘 만들어
먹긴해요~
이런.....
그러니까
온라인쇼핑 등에는
한번 입력한 ID정보를 다음부터는 일부러
입력안해도 될때가 있죠?
ID: OOOOO
PW: ******
그건 그 사이트가
쿠키를 사용하고 있기
때문이에요.
네.....?
....


유키에가 여러사이트에서 입력한 ID 등의 정보는
인터넷, LAN 등의 네트워크
유키에 컴퓨터에 쿠키라고 불리는 파일에 자동적으로 보관하고 있어요
ID: ××××
PW: ○○○○○○
ID:
PW:
쿠키를 컴퓨터에 저장
쇼핑사이트등

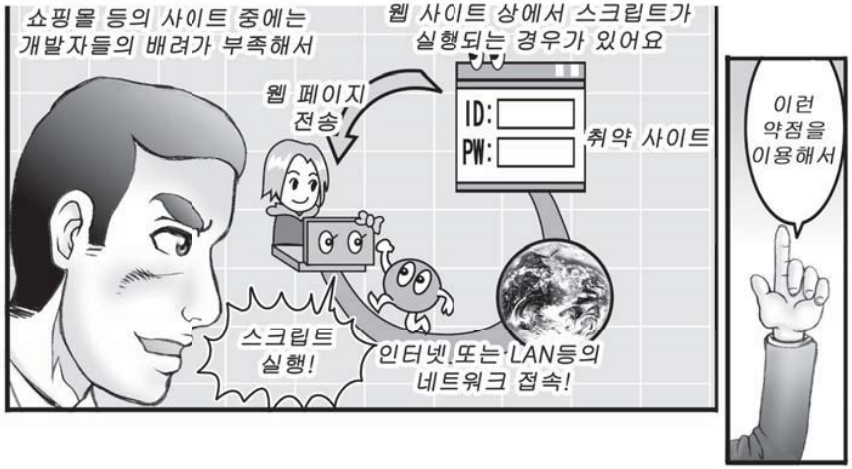

그리고 다음부터 방문했던 사이트에 가게되면 사이트가 유키에 컴퓨터에 저장되어 있는 쿠키정도를 보내 달라고 부탁하게 되고,
ID:
PW:
쿠키 줘~!
부탁받은 유키에 컴퓨터는 자동적으로 사이트에 보내게 되요 그래서 ID나 PW 입력창에 매번 입력하지 않아도 -되는거에요.
ID:
PW:
땡큐~!! 다음에 또 부탁해~


헉~ 유키에의 쿠키를 서버가 먹고 있네~ 배탈 안나야 할텐데?
야~~
흑시....


안전에 문제가 있는 서버에 ID나 PW를 입력하면..
어딘가 외부에서 그 정보를 훔쳐갈 수도 있는건가요?
예를 들면 ...


시우야@넷라인에서 유키에가 등록한 쿠키 정보를 누군가가 도용한다던가요..?

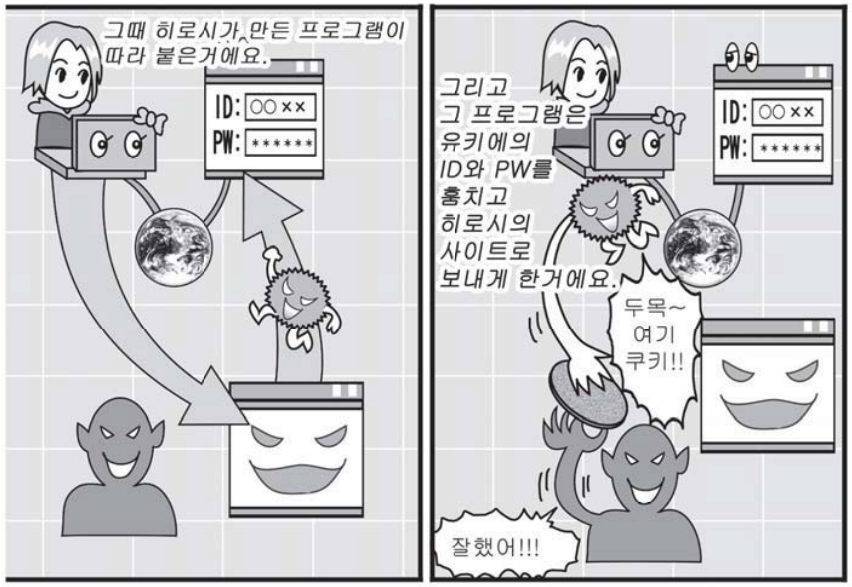

안타깝지만
가능할 수 있어요.
그럼 그건 죠~ 선생님께 물어 볼까요?
조 선생님!
자~ 설명해드리죠!!


쇼핑몰 등의 사이트 중에는
개발자들의 배려가 부족해서
웹 사이트 상에서 스크립트가
실행되는 경우가 있어요
웹 페이지
전송
ID:
PW:
취약 사이트
이런
약점을
이용해서
스크립트
실행!
인터넷 또는 LAN등의
네트워크 접속!

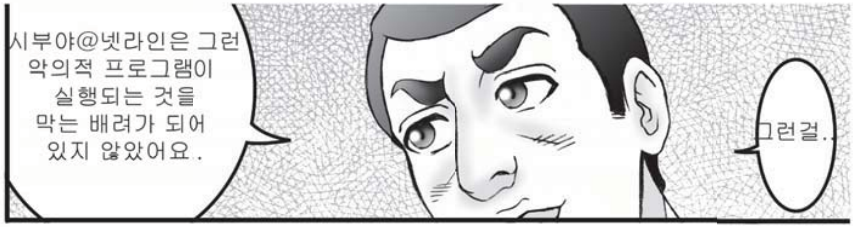

안 돼!!
사이트에 있는
링크를 클릭한
사람의 쿠키정보를
훔쳐오는
악의성 있는
웹 사이트를
만들 수 있는 거에요.
당사자가 생각하지도
못한 곳에서 정보를
가져간다는 것을
생각하면 일종의
범죄행위라고
볼 수 있죠~!


저
기
..
결국
제 쿠키를
도용한
것은...
친절하고 착한
착한 친구인
히로시 밖에
없는 거네요....
역시...


그는 한번 유키에에게 시부야@넷라인에서
ID나 PW를 등록 시켰지..
거기서 네 컴퓨터에
그런 정보가 쿠키로 보존 된거고..
그 후엔 자기 사이트로 경우
시켜 접속 시켰죠..
SHIBUYA@NET


그때 히로시가 만든 프로그램이
따라 붙은거에요.
ID: ○○××
PW: ******
그리고
그 프로그램은
유키에의
ID와 PW를
훔치고
히로시의
사이트로
보내게 한거에요.
두목~
여기
쿠키!!
잘했어!!!


그는 훔친 아이디와
비밀번호를 써서
유키에가 되어,
시부야@넷라인에서
유료 음반을
대량으로 다운받았다.
SHIBUYA@NETLIN
나?
유키
에
전부
사야
지..
무섭다..
그런것도
할 수
있구나...


시부야@넷라인은 그런 악의적 프로그램이 실행되는 것을 막는 배려가 되어 있지 않았어요.
그런걸..


크로스사이트 스크립트속임수 의 취약성 이 있다고 하는 겁니다.
XSS
즉, 히로시는 시부야@넷라인의 보안적 맹점을 이용한거죠~
어이쿠~
XSS


내 컴퓨터엔 보안 맹점 없는데...
시부야@넷라인도 그렇지만 안전인지 모르는 온라인숍을 이용하는 것은 엄청 위험해요
그렇죠, 특히~


온라인숍 같은 상용 사이트에서는 아주 중대한 문제가 되지만,
아직까지도 문제가 해결 안 된 사이트가 많이 있어요


온라인숍
상용사이트를 이용할때에는 쿠키를 자동적으로 보존하지 않도록 브라우저를 설정할것!


그리고 필요없는 쿠키 정보는 보존하지 않게 하는게 좋아요.
필요 없음 !!!!


이상! 이해됐어요?
네~!! 감사합니다!


음....


당분간... 인간불신과 쿠키를 못먹게 될것 같아요..
살 뺄 수 있어서 좋지않아?
ㅋㅋㅋ

용어

【자료】

어필리에이트

웹 등에 붙여진 기업의 웹 사이트로의 링크를 경유하여 그 기업의 상품의 구입 등이 행해지면, 그 기업에서 링크 건 사람에게 포인트나 보수가 지불된다 라고 하는 구조의 광고 수법의 하나. 인터넷 백서 2011(ISBN9784844330493)에 의하면, 어필리에이트 광고의 시청률은 PC로 약40%, 휴대전화로 약10%, 스마트 폰으로 약20% 정도이다.

보안 홀

보안 취약점 시스템의 보안상의 불량. 홀은 구멍(hole)으로, 「안전성의 구멍」이라는 의미. 홀은 큰방(hall)이란 뜻이 아니다. 새롭게 보안 취약점을 찾으면, 바로 바이러스 등의 악의 있는 프로그램이 작성되어 퍼지는 것이 있어 OS 및 웹 브라우저의 업데이트나 바이러스 백신 등의 보안 대책을 꼼꼼히 자주 해 줘야 한다.

쿠키

웹 사이트가 열람되었을 때, 웹 브라우저를 통해서 그 웹 사이트의 방문자의 컴퓨터 상에 방문자의 정보나 방문 일시 등을 전용의 작은 파일에 기록해서 보존하는 구조 또는 파일. 이것에 의해, 웹 사이트를 방문했을 때 ID나 신용카드 번호를 매회 입력하지 않아도 되거나, 열람한 페이지에 관계되는 웹 사이트를 소개 주는 등 편리하지만 취약하거나 악의가 있는 웹 사이트에 가게 되면 ID등이 도난 당할 위험성이 있다. 악의가 없을지라도 자신의 기호 등이 알려진다던가 멋대로 판단 되는 경우가 있으므로 주의해야 할 필요가 있다. 필요 없으면 쿠키를 삭제하길 바란다.

크로스 사이트·스크립팅

사이트를 거쳐(크로스하여), 스크립트를 실행하는 공격 수법에 따라 이 이름이 붙여졌다. 자세한 내용은 본 자료를 참조하길 바람. 웹 사이트에 이러한 취약성이 있을 경우 이용자 측 에서 피해를 피하는 것은 어렵다. ID등의 개인정보를 넣는 웹 사이트에는 잘 모르는 웹 사이트의 링크를 경유하지 않고 직접 액세스하도록 만든다. ID등의 개인정보를 넣을 때는 정말로 넣을 필요가 있는 것인가 침착하게 판단하길 바란다.

크로스 사이트·스크립팅의 위력과 피해

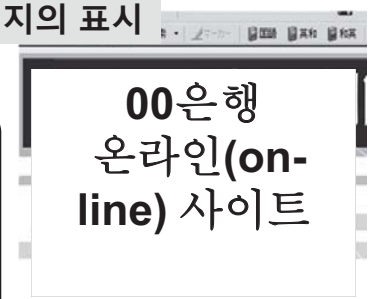
본 내용에서는「시부야@넷라인」과 같은 쇼핑 사이트에 크로스 사이트·스크립팅의 취약 성이 있었기 때문에 유키에(由紀惠)씨의 쿠키 정보가 도둑 맞아 피해를 받았습니다. 그러나 크로스 사이트·스크립팅에 의한 피해는 그 외에도 많습니다. 조금 정리해 봅시다.
크로스 사이트·스크립팅에 의해 생길 수 있는 피해에는 다음의 것 같습니다.

계기는, 악의가 있는 사이트를 열람하고, 악의가 있는 링크 등을 클릭하는 것 (유키에(由紀惠)씨의 예), 또는 그러한 장치의 링크를 포함하는 메일을 받고 그 링크를 클릭하는 것입니다. 그 때, 악의가 있는 사람이 작성한 스크립트가 취약한 웹 사이트로 보내집니다.

쿠키 정보의 취득

쿠키 정보누설

위조페이지의 표시

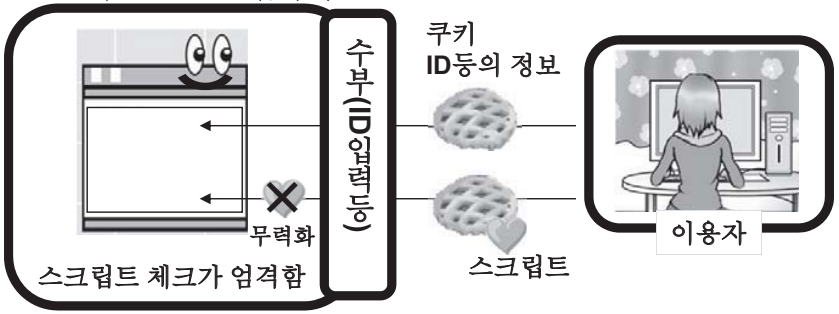


생길 수 있는 피해
·피싱 사기
·쿠키 정보누설 (본인행세, 개인정보의 누설 등. 쿠키와 스크립트에 의함)
・・・・

안심되는 사이트•위험한 사이트에서의 스크립트 처리의 차이

웹 사이트에서는 로그인 화면, 회원등록, 블로그나 게시판 등의 코멘트의 반영 등, 이용자의 입력 내용에 따른 처리가 발생합니다. 악의가 있는 사람이 작성한 스크립트가 웹 사이트에서 어떻게 처리될지 정리해 봅시다.

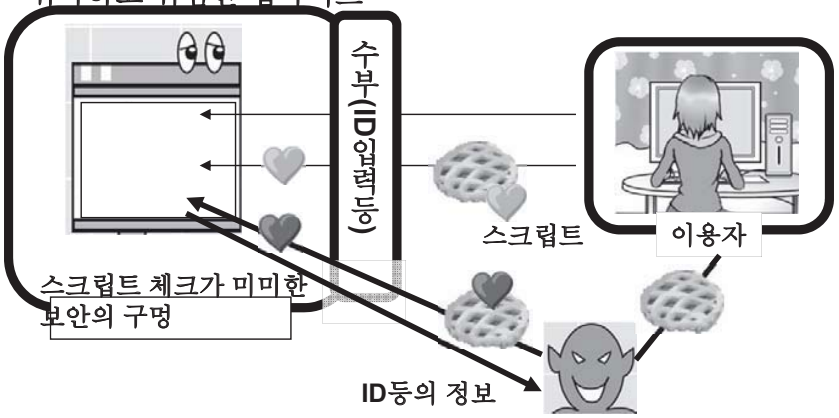
견고하고 안전한 웹사이트



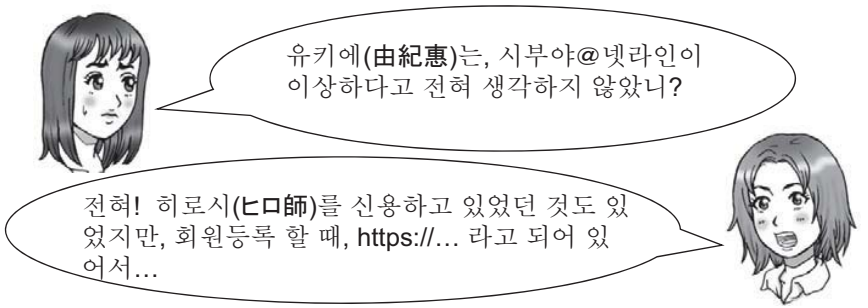
안심되는 온라인(on-line) 사이트에서는, 스크립트의 체크가 엄격하게, 가령 악의 있는 스크립트가 혼입하고 있어도 무력화되어 아무 일도 없습니다.

한편, 취약한 사이트에서는 스크립트의 체크가 미미하여 거기가 보안 홀(보안 취약점)이 되어 악의가 있는 스크립트가 실행되어버립니다.

취약하고 위험한 웹사이트



통신의 암호화와 크로스 사이트·스크립팅



https로부터 시작되는 웹 사이트는, 네트워크 상의 통신을 암호화하고 있음을 나타내고 있습니다. 비밀번호 등을 보낼 때 그것이 그대로 네트워크상에 흐르면 도중에 도난 당할 가능성이 있어 위험하므로 암호화해서 통신하는 것입니다. https로부터 시작되는 웹 사이트에서는 브라우저에 열쇠 마크가 붙고 있어 그 열쇠 마크를 클릭하는 것으로 그 웹 사이트의 증명서를 확인할 수 있습니다. 그런 의미에서 유키에(由紀恵)씨가 웹 사이트의 URL을 확인하고 https인 것을 체크한 것은 옳았네요.

그러나, 크로스 사이트·스크립팅의 취약성이 있는 웹 사이트가 비록 https에서 통신을 암호화하고 있어도 악의가 있는 프로그램(스크립트)은 들어가게 됩니다. https에서 통신의 암호화와 크로스사이트 스크립팅의 취약성은 별개의 이야기입니다.

어쨌던 신용카드 번호 등 중요한 정보를 입력할 때는 그것이 정말로 필요인가를 냉정히 생각합시다. 또 입력할 때는 다른 사이트의 링크를 경유할 일 없고 또한 상대편이 신뢰할 수 있는 사이트인 것을 확인한 뒤에 입력해야 합니다. 웹 사이트의 https의 증명서는 그 웹 사이트와의 암호통신의 신뢰성의 증명이며 그 웹 사이트 자체를 신뢰할 수 있다고 하는 증명은 아닙니다. 주의해 주십시오.

크로스 사이트•스크립팅의 취약성

독립 행정법인정보처리추진 기구의「취약성에 관한 신고서 상황 (http://www. ipa. go. jp/security/vuln/report/press. html)」에서는, 3개월 마다 (각 해의 제1사분기 (1Q)로부터 4사분기 (4Q)까지)에 소프트웨어 등의 취약성 관련 정보에 관한 신고 상황이 취합되고 있다.
2004년의 3사분기로부터 공표되고 있는 웹 사이트의 취약성에 관한 신고서는 2011년의 4사분기에 누계6025건이 되고 있으며 그 중에서 크로스 사이트·스크립팅의 신고 비율이 가장 높다. 크로스 사이트·스크립팅의 취약성의 원리는 널리 알려져 있지만 2011년도에는 급증하고 있어 전체의 91%을 차지하고 있다. 브라우저로부터 직접 문자열을 입력할 수 있는 칸에 취약성이 있는 것 이외로 숨김 요소 등 얼핏 보기에는 표시되지 않고 직접 입력할 수 없는 부분에 취약점이 있을 경우가 3분의 1을 차지하고 있는 것을 나타났다. 2011년도 4사분기까지의 상세한 결과는 다음 신고서 상황을 참조.

또한 소프트웨어의 취약성 관련 정보에서는 종류로서 웹 브라우저가 가장 많고 그 다음은 웹 어플리케이션 소프트, 라우터가 있다. 임의의 파일로의 액세스나 스크립트의 실행, 정보의 누설 등의 신고가 많고 또한 스마트폰 관계의 제품에 있어서의 신고가 증가하고 있다.

취약성에 관한 신고 상황
http://www. ipa. go. jp/security/vuln/report/documents/vuln2011q4.pdf

최근 공표된 크로스 사이트•스크립팅의 취약성

취약성 대책정보 포털 사이트 JVN(Japan Vulnerability Notes http://jvn. jp/)에서는, 신고가 있었던 취약성에 관한 정보가 공표되고 있습니다.

최근의 크로스 사이트·스크립팅의 취약성의 보고에 대해 아래에 일부 발췌해서 소개하고자 합니다.

Redmine 에 있어서의 크로스사이트스크립팅의 취약성
（2012/03/14 JJVNVU#428075）
Redmine 은 프로젝트 관리 소프트웨어입니다. Redmine 에는 크로스사이트스크립팅의 취약성이 존재합니다. (생각되는 영향: 사용자가 웹 브라우저상에서 임의의 스크립트를 실행될 가능성이 있습니다.)

SquirrelMail 용 플러그인 Autocomplete에 있어서의 크로스사이트스크립팅의 취약성 (2012/03/09 JVN#56653852)
Autocomplete 은, SquirrelMail 용의 플러그인입니다. Autocomplete 에는 크로스사이트스크립팅의 취약성이 존재합니다. (생각되는 영향은 위와 같다.)

Movable Type 에 있어서의 크로스사이트스크립팅의 취약성 (2012/02/23 JVN#49836527)
mt-wizard. cgi 및 Movable Type 에 동봉되어 있는 템플릿에는 크로스사이트스크립팅의 취약성이 존재합니다. (생각되는 영향은 위와 같음)

EProject Open 에 있어서의 크로스사이트스크립팅의 취약성 (2012/02/06 JVNVU#732115)
Project Open 에는, 입력 미터의 처리에 문제가 있어 크로스사이트스크립팅의 취약성이 존재합니다. (생각되는 영향은 위와 같음)

Oracle WebLogic Server 에 있어서의 크로스사이트스크립팅의 취약성（2012/01/20 JVN#54779201）
Oracle WebLogic Server 의 관리 콘솔에는 크로스사이트스크립팅의 취약성이 존재합니다. (생각되는 영향: 해당제품의 관리 콘솔에 로그인하고 있는 사용자의 웹브라우저 상에서, 임의의 스크립트를 실행될 가능성이 있습니다.)

WordPress 일본어판에 있어서의 크로스 사이트•스크립팅의 취약성（2011/12/26 JVN#44439553）
WordPress. Org 이 제공하는 WordPress 은 웹로그시스템입니다.
WordPress 일본어판에는, 크로스사이트스크립팅의 취약성이 존재합니다.
(생각되는 영향: 사용자의 웹 브라우저상에 임의의 스크립트를 실행될 가능성이 있습니다.)