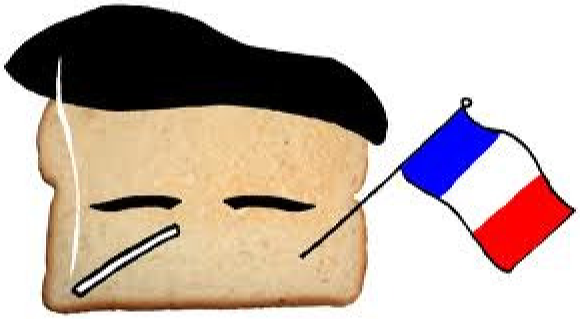
SecurusGlobal

Web Scanners FOR THE WIN…

<louis@securusglobal.com>

`id`



- French Security Consultant in Melbourne
- Did/do a lot a web pentests (from your e-banking website to your sex shop's website)
- Research focus on web stuff:
  - But no "Hello participants of Mailing List. Last month I wrote new article Anthology of attacks via captchas, for which I made English version yesterday"
  - Have try several times to write a web scanner…

The InterWeb…

- Your mum’s blog
- Public-facing websites
- Internal websites
- Internet Banking websites
- ... Not really the same risks/security needs

The InterWeb…

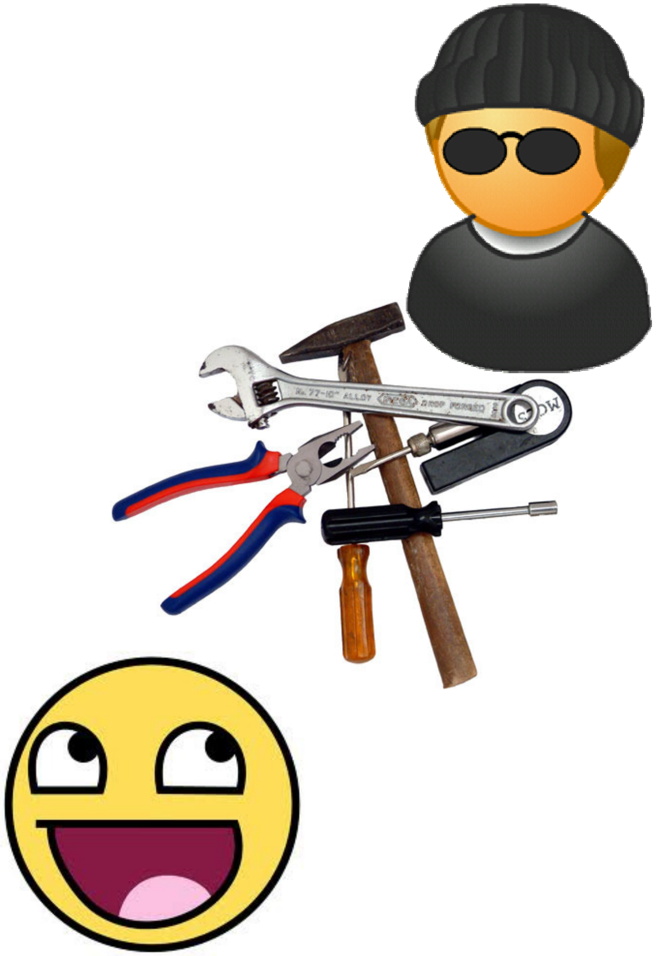
Spring
HIBERNATE
APACHE GERONIMO
JBoss
ORACLE
django
php
Microsoft .net
RAILS
CF

How can one tool solve the security problems associated with these technologies, and the countless number of other websites?

Automated testing

- Reduce costs
- Test more often
- Limited set of skills required
- You can browse Facebook/Twitter while the scanner is working for you ☺

Automated testing vs automated reporting?



Web scanners

- Open source: wapiti/sqlmap/skipfish/w3af/…
- Free: CAT
- Not Free but affordable: Burp
- “Others”: Appscan, NTO spider, Webinspect, Acunetix…

Web scanners are $$

- 30-day, single-app, single-client $2,500
- 30-day, multi-app, single-client: $5,000
- 1 year, 1 consultant (locked to a single machine) unlimited scans: $15,000

Writing a scanner…

- If you create a tool/product you’re not pentesting

- In my experience, I learn something new or discover a new idea during almost every pentest I carry out.

- A tool can only ever be as good as the person who wrote it…

What’s a Web Scanner…

- A “Browser”:
  - – understand and interpret HTML, JavaScript
  - – HTTP library
- A Spider
- A Scanner
- A Fancy Interface
- A Fancy Report Generator

Why is it so hard… Spider

- HTML-based web-app:
  - Form submission: even humans (at least I) have issues figuring out what a valid value is
  - Captcha

- Flash-application
- Web-services
- Thick-client
- …

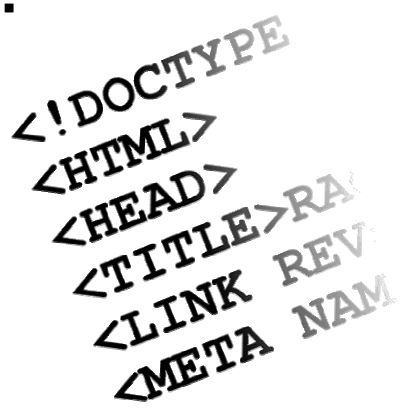
Why is it so hard… Spider

- URL format:
  - http://<server>/page_1.html
    rewrite -> http://<server>/page.php?id=1
  - http://<server>/page/1
- Malformed HTML
- What is a “page not found”? What is an “error”?
- Session issues:
  - Detection of logout
  - Detection of how to login

Why is it so hard… web pages

- 2 times the same request can provide 2 different pages:
  - Wizard-based applications
  - Date/time dependencies in the page
  - Adverts in the page

- 2 pages that were supposed to provide the same content (in case of vulnerabilities) can instead produce dissimilar results:
  - URL echoed in the page
  - Subpart of the page not vulnerable



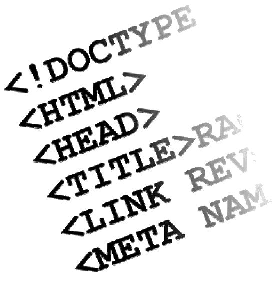
Why is it so hard… web pages

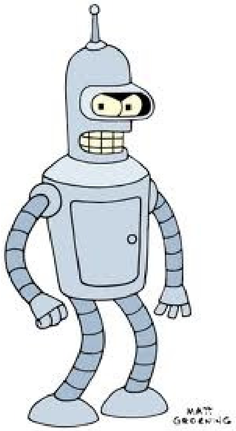
- A lot of information (HTML) is not useful (generic layout vs content)

  -> easy to spot for human eyes

  -> not so easy for a computer

- What is “this page shows X records” and “this page shows Y records” for a computer…





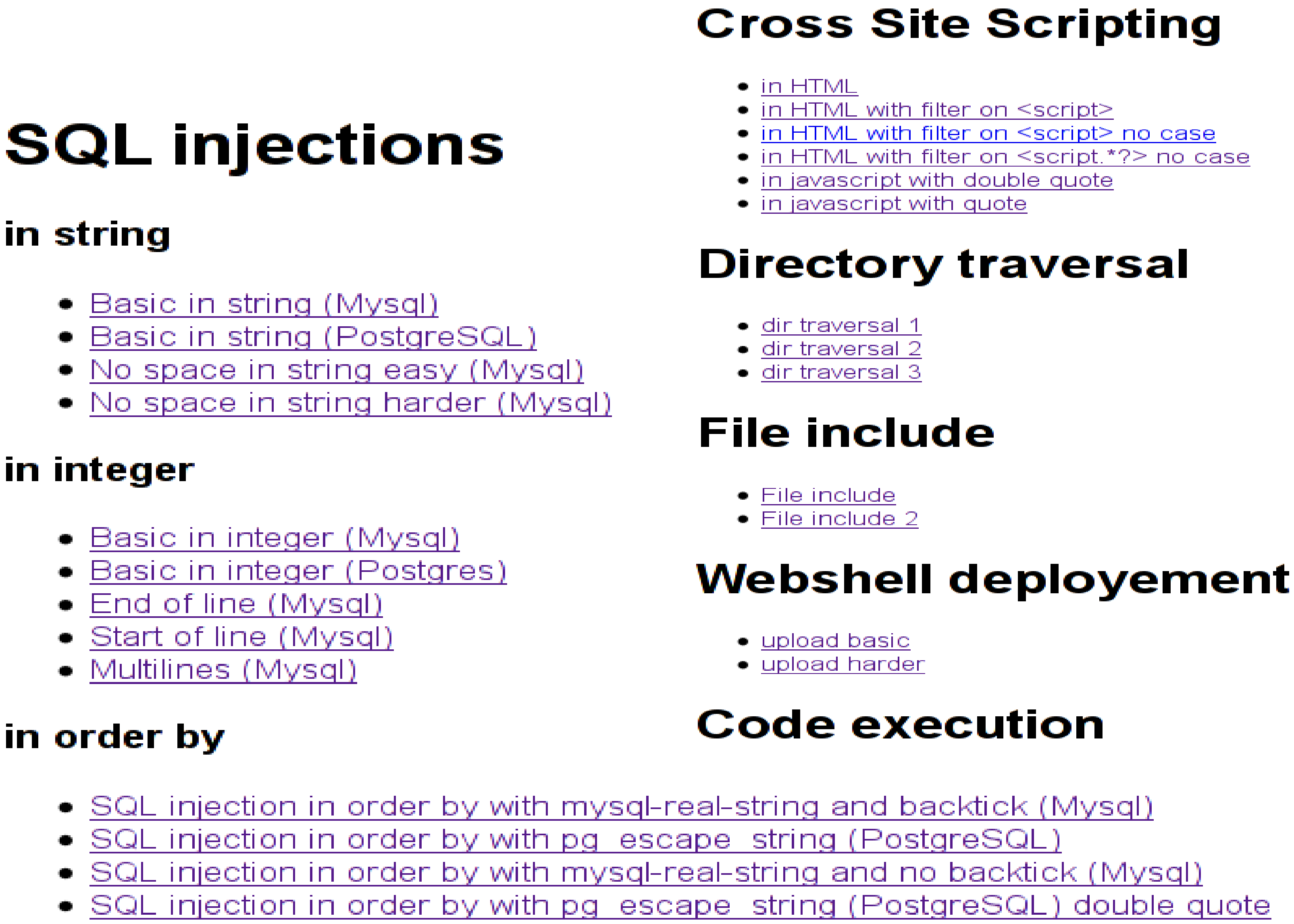
Automatic web scanner… limitations

- “They can't check for business logic...”
- But can they check for classic vulnerabilities…
- Often really good against webgoat/acme bank or their own demo site

Introducing obstacles

- Just a list of vulnerable webpages
- Good thing to learn detection/exploitation
- Good thing to test:
  - Web Scanners
  - WAF

Introducing obstacle



SQL injections

in string

- Basic in string (Mysql)
- Basic in string (PostgreSQL)
- No space in string easy (Mysql)
- No space in string harder (Mysql)

in integer

- Basic in integer (Mysql)
- Basic in integer (Postgres)
- End of line (Mysql)
- Start of line (Mysql)
- Multilines (Mysql)

in order by

- SQL injection in order by with mysql-real-string and backtick (Mysql)
- SQL injection in order by with pg_escape_string (PostgreSQL)
- SQL injection in order by with mysql-real-string and no backtick (Mysql)
- SQL injection in order by with pg_escape_string (PostgreSQL) double quote

Cross Site Scripting

- in HTML
- in HTML with filter on <script>
- in HTML with filter on <script> no case
- in HTML with filter on <script.*?> no case
- in javascript with double quote
- in javascript with quote

Directory traversal

- dir traversal 1
- dir traversal 2
- dir traversal 3

File include

- File include
- File include 2

Webshell deployement

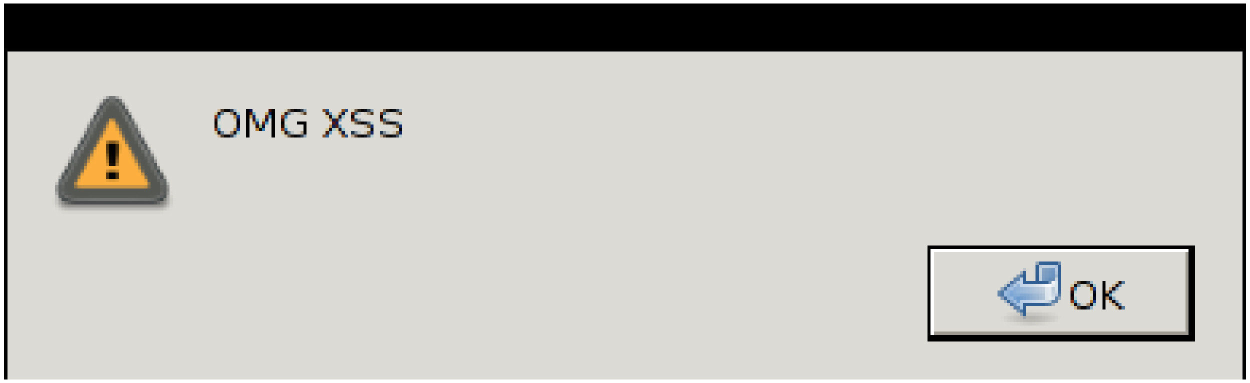
- upload basic
- upload harder

Code execution

How to test…

- Retrieve information:
  - HTTP Server logs
  - Tcpdump+urlsnarf
- Review of the results
- Review of the requests

Cross Site Scripting…



OMG XSS

Cross Site Scripting… background

XSS are mostly encoding issues not filtering issues !!!

Reflected XSS

- Easy to spot:
  - Send a request with a payload
  - Check if the payload is in the response

- Most scanners find most Reflected Cross Site Scripting:
  - This is probably what they are the best at

Stored XSS

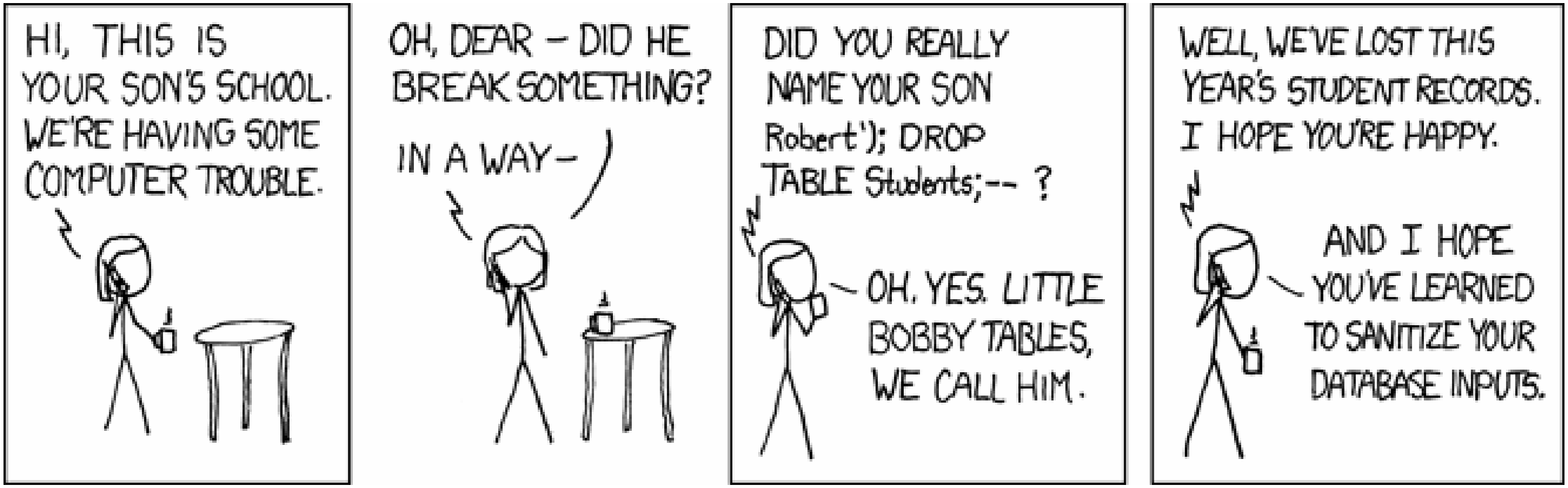
- Inject-payload/retrieve-response doesn’t work
- The response can be correctly encoded but another page can not do the encoding correctly
- Need to spider all the website again :/
  - Scanners don’t do that
  - I claim copyright on this technique and prohibit web application scanner developers from implementing it without my permission

Cross Site Scripting and filters

```
...
$n =  $_GET["name"];
$n=preg_replace("/<script.*>/i","", $n);
$n= preg_replace("/<\/script>/i","",$n);
echo $name;
...
```

All Scanners find this XSS except skipfish ☹

SQL injections


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

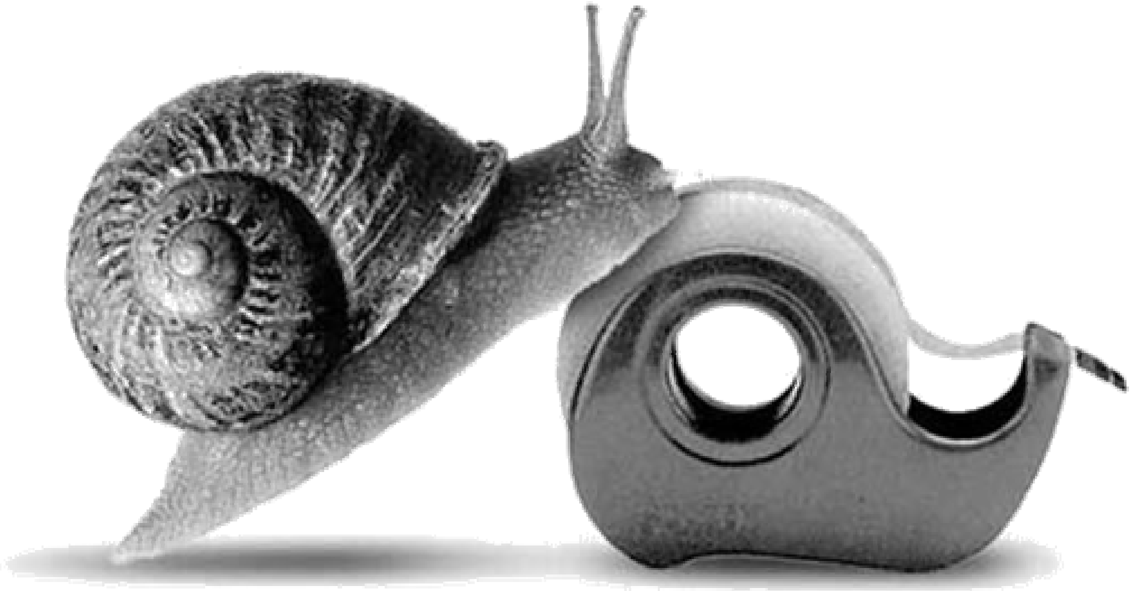
SQL injection in integer

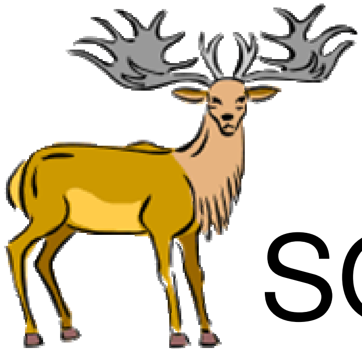
```
...
$id = $_GET["id"]
$sql="SELECT * FROM users where id=";
$sql.=mysql_real_escape_string($id);
...
```

Good news, all scanners find that one ☺

Only blind SQL injections…

- Most tools report all SQL injections as blind SQL injections…
  - Two much overhead to test union ?
  - Exploitability index ?





SQL injection in order by

```
...
$o = $_GET["order"];
$sql = "SELECT * FROM users ";
$sql.= "ORDER BY ";
$sql.= mysql_real_escape_string($o);
$result = mysql_query($sql);
...
```

Bad news, most scanners don’t find that one ☹

Results

SQLmap	X
Skipfish	X
Burp	X
Acunetix	X
Ntospider	X
Wapiti	V
Appscan	X

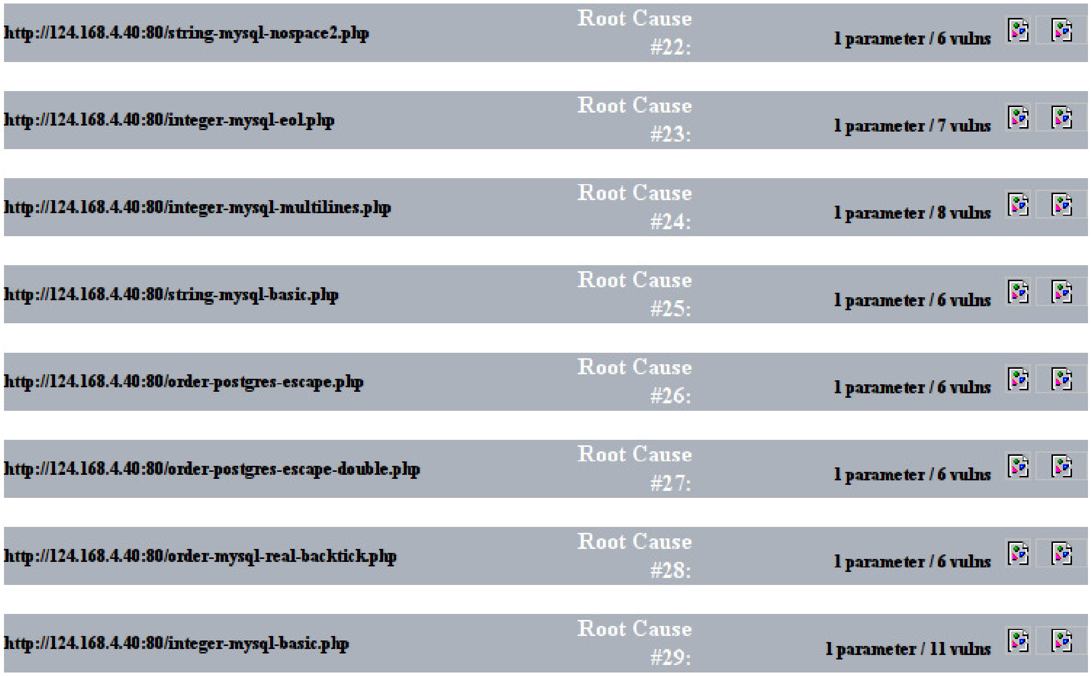
"Order by": probably
a good place
to search for
SQL injections
if you're doing
pentests

SQL injections in order by with ` for Mysql and any order by with PostgreSQL

SQLmap	X
Skipfish	X
Burp	X
Acunetix	X
Ntospider	X
Wapiti	X
Appscan	X

Order by + Ntospider + **display_errors=On**

"An invalid character submitted in a URL parameter causes an error in the database query or script execution. This indicates that the application has not fully validated user supplied input. These errors can lead to HTML injection, SQL injection, or arbitrary code execution."



http://124.168.4.40:80/string-mysql-nospace2.php	Root Cause #22:	1 parameter / 6 vulns
http://124.168.4.40:80/integer-mysql-eol.php	Root Cause #23:	1 parameter / 7 vulns
http://124.168.4.40:80/integer-mysql-multilines.php	Root Cause #24:	1 parameter / 8 vulns
http://124.168.4.40:80/string-mysql-basic.php	Root Cause #25:	1 parameter / 6 vulns
http://124.168.4.40:80/order-postgres-escape.php	Root Cause #26:	1 parameter / 6 vulns
http://124.168.4.40:80/order-postgres-escape-double.php	Root Cause #27:	1 parameter / 6 vulns
http://124.168.4.40:80/order-mysql-real-backtick.php	Root Cause #28:	1 parameter / 6 vulns
http://124.168.4.40:80/integer-mysql-basic.php	Root Cause #29:	1 parameter / 11 vulns

Scanners, filters and SQLi

- No bypass/encoding:
  - a simple filter on “space” or on “\s+” prevents detection for all scanners tested

- Burp Suite only tests for time based SQLi for SQLServer (only “waitfor…”)

Remote File Inclusion
/
Local File Inclusion

File include PHP

```
if ($_GET["page"]) {
    include($_GET["page"]);
}
```

Hard to test?

- Internal Network vs External Network:
  - Internal network:
    - Internet access for the server?
    - Different network access for the scanner and the web server scanned…
  - External network:
    - Do you really want your web scanner's provider to know that your website is vulnerable to RFI?

LFI/RFI

Remote File Inclusions are listed as directory traversals… by most tools :/

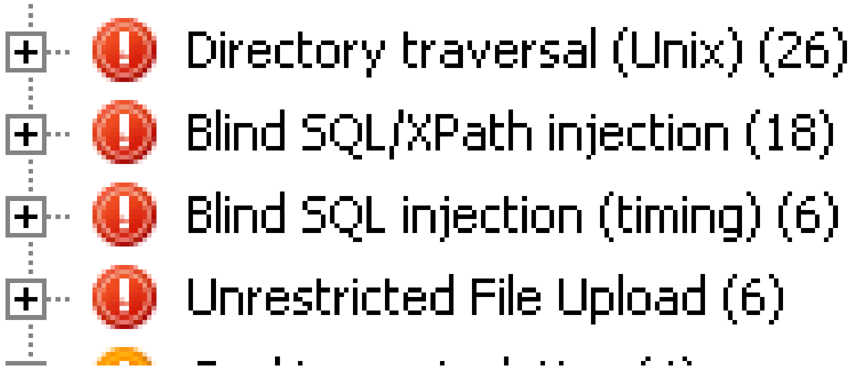
I can read a file

vs

I can execute code

Acunetix and display_errors

display_errors=**Off**



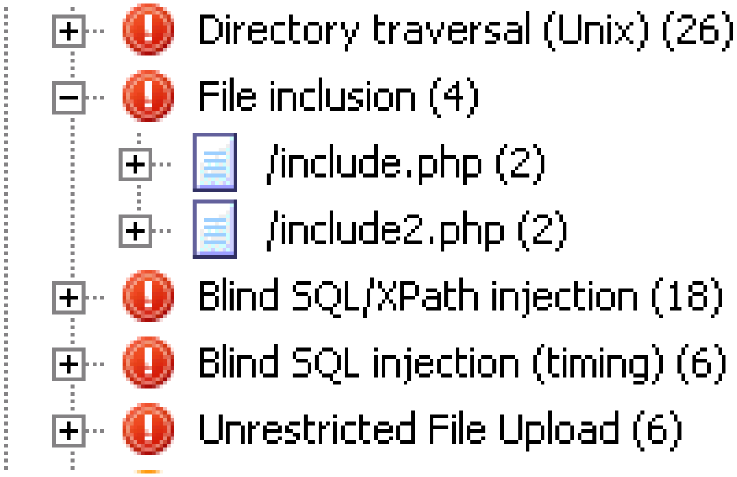
Directory traversal (Unix) (26)

Blind SQL/XPath injection (18)

Blind SQL injection (timing) (6)

Unrestricted File Upload (6)

display_errors=**On**



Directory traversal (Unix) (26)

File inclusion (4)

/include.php (2)

/include2.php (2)

Blind SQL/XPath injection (18)

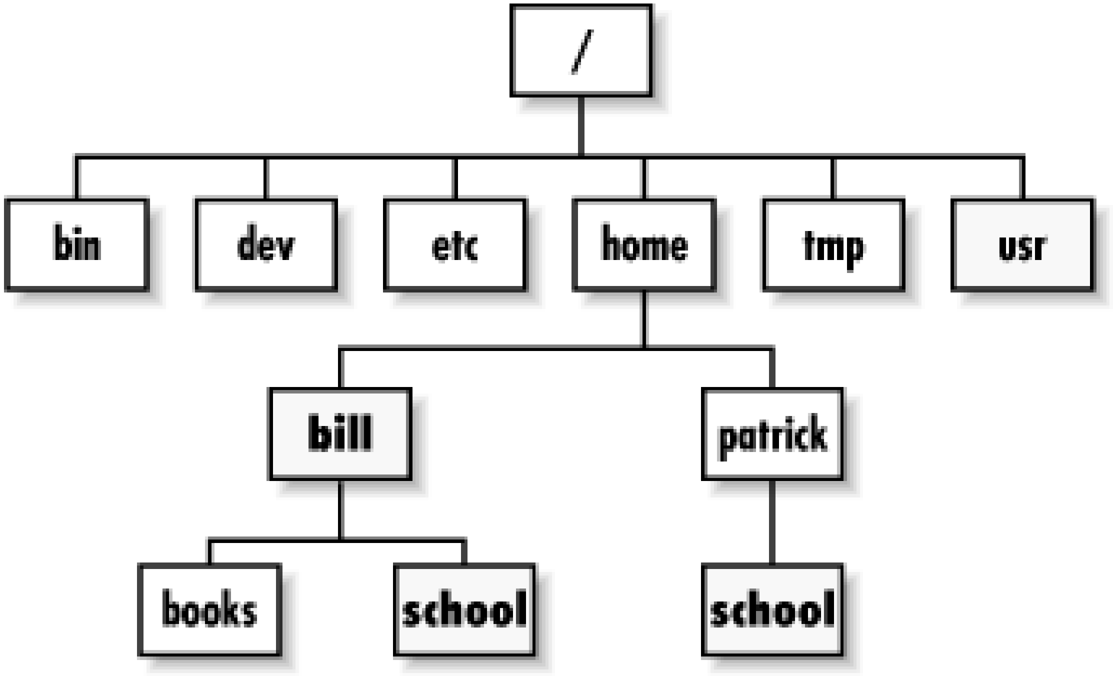
Blind SQL injection (timing) (6)

Unrestricted File Upload (6)

Results for error off

Tool	Seen as Directory traversal	Seen as Include
Skipfish	V	X
Burp	V	X
Acunetix	V	X
Ntospider	V	X
Wapiti	V/X	V/X (No distinction)
Appscan	V	X

Directory traversal/Arbitrary File Access



.net protection and boot.ini

- Quite easy to discover

- However (not found by any scanners…):

```
$file = $_GET['file'];

if (!(strstr($file,"/var/www/files/")))
  die();
```

File Upload

Webshell upload with basic filter

```
...
$f=basename($_FILES['image']['name']);
if (preg_match('/\.php$/',$file)) {
   DIE("NO PHP");
}
...
```

```
mojo% cat exec.php.test
<?php
   system($_GET["cmd"]);
?>
```

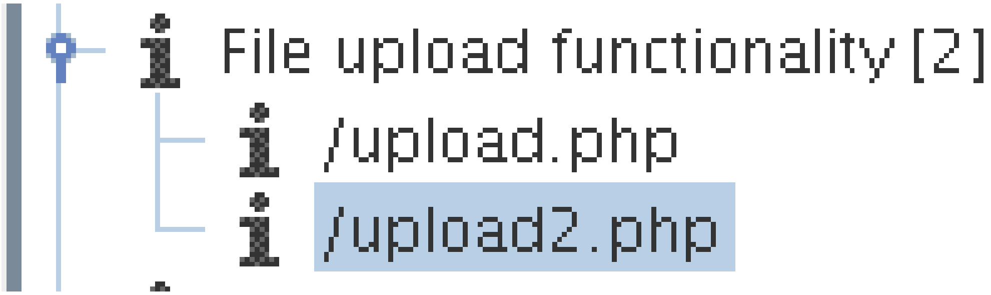
Results

- Skipfish uploaded files and informed you that there is upload form (green light) :/

- Wapiti told you that there is a upload form…

Burp and File upload

- Upload functionalities are listed as "Information"



File upload functionality [2]
/upload.php
/upload2.php

- For example "Information" can be:
  - HTML does not specify charset
  - Content-type incorrectly stated

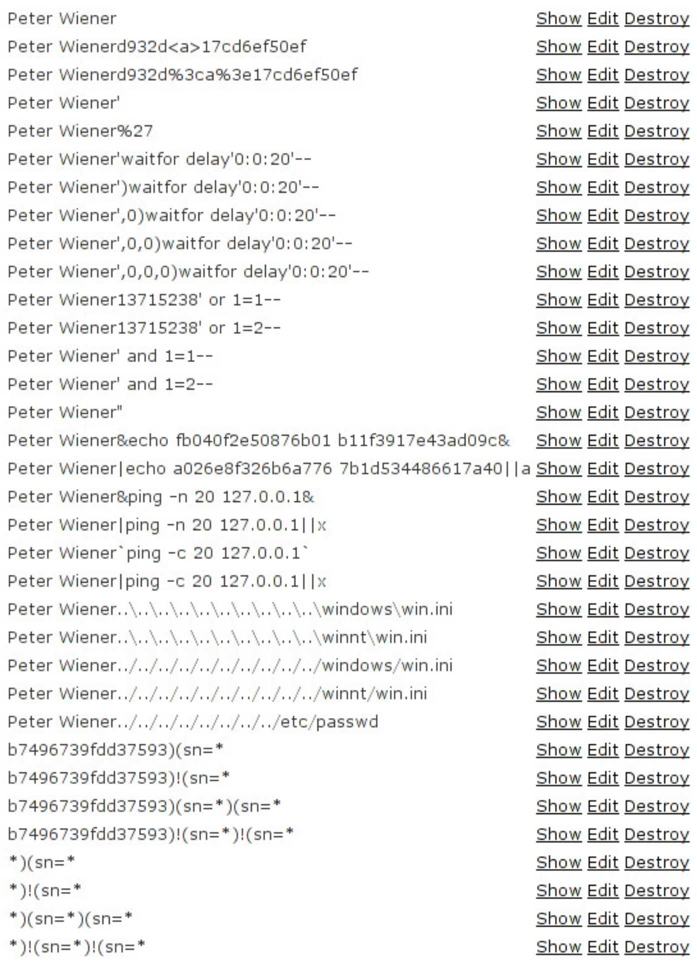
- Same thing for Appscan…

So I can get an easy shell and the scanner doesn’t test that…

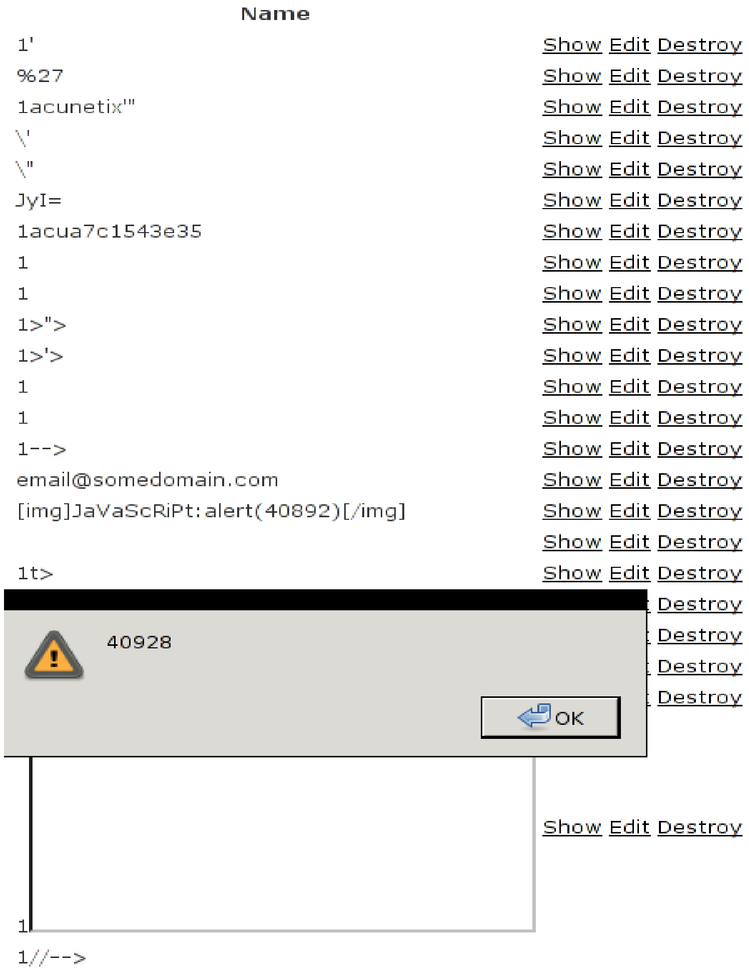
OK Thanks for the “information”

Scanners' fun…

Be prepared to clean up



Peter Wiener	Show	Edit	Destroy
Peter Wienerd932d<a>17cd6ef50ef	Show	Edit	Destroy
Peter Wienerd932d%3ca%3e17cd6ef50ef	Show	Edit	Destroy
Peter Wiener'	Show	Edit	Destroy
Peter Wiener%27	Show	Edit	Destroy
Peter Wiener'waitfor delay'0:0:20'--	Show	Edit	Destroy
Peter Wiener')waitfor delay'0:0:20'--	Show	Edit	Destroy
Peter Wiener',0)waitfor delay'0:0:20'--	Show	Edit	Destroy
Peter Wiener',0,0)waitfor delay'0:0:20'--	Show	Edit	Destroy
Peter Wiener',0,0,0)waitfor delay'0:0:20'--	Show	Edit	Destroy
Peter Wiener13715238' or 1=1--	Show	Edit	Destroy
Peter Wiener13715238' or 1=2--	Show	Edit	Destroy
Peter Wiener' and 1=1--	Show	Edit	Destroy
Peter Wiener' and 1=2--	Show	Edit	Destroy
Peter Wiener"	Show	Edit	Destroy
Peter Wiener&echo fb040f2e50876b01 b11f3917e43ad09c&	Show	Edit	Destroy
Peter Wiener|echo a026e8f326b6a776 7b1d534486617a40||a	Show	Edit	Destroy
Peter Wiener&ping -n 20 127.0.0.1&	Show	Edit	Destroy
Peter Wiener|ping -n 20 127.0.0.1||x	Show	Edit	Destroy
Peter Wiener`ping -c 20 127.0.0.1`	Show	Edit	Destroy
Peter Wiener|ping -c 20 127.0.0.1||x	Show	Edit	Destroy
Peter Wiener..\..\..\..\..\..\..\..\..\windows\win.ini	Show	Edit	Destroy
Peter Wiener..\..\..\..\..\..\..\..\..\winnt\win.ini	Show	Edit	Destroy
Peter Wiener../../../../../../../../../windows/win.ini	Show	Edit	Destroy
Peter Wiener../../../../../../../../../winnt/win.ini	Show	Edit	Destroy
Peter Wiener../../../../../../../etc/passwd	Show	Edit	Destroy
b7496739fdd37593)(sn=*	Show	Edit	Destroy
b7496739fdd37593)!(sn=*	Show	Edit	Destroy
b7496739fdd37593)(sn=*)(sn=*	Show	Edit	Destroy
b7496739fdd37593)!(sn=*)!(sn=*	Show	Edit	Destroy
)(sn=	Show	Edit	Destroy
)!(sn=	Show	Edit	Destroy
)(sn=)(sn=*	Show	Edit	Destroy
)!(sn=)!(sn=*	Show	Edit	Destroy



Name			
1'	Show	Edit	Destroy
%27	Show	Edit	Destroy
1acunetix'"	Show	Edit	Destroy
\'	Show	Edit	Destroy
\"	Show	Edit	Destroy
JyI=	Show	Edit	Destroy
1acua7c1543e35	Show	Edit	Destroy
1	Show	Edit	Destroy
1	Show	Edit	Destroy
1>">	Show	Edit	Destroy
1>'>	Show	Edit	Destroy
1	Show	Edit	Destroy
1	Show	Edit	Destroy
1-->	Show	Edit	Destroy
email@somedomain.com	Show	Edit	Destroy
[img]JaVaScRiPt:alert(40892)[/img]	Show	Edit	Destroy
	Show	Edit	Destroy
1t>	Show	Edit	Destroy
			Destroy
			Destroy
			Destroy
			Destroy
	Show	Edit	Destroy
1			
1//-->			

40928

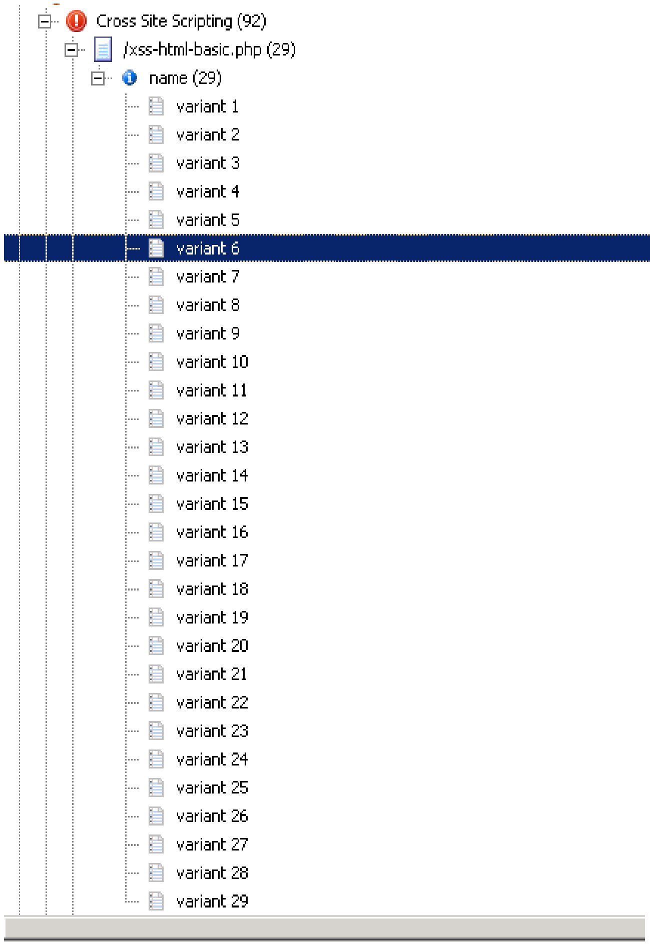
Web scanners are dangerous: or 1=1

- In a SELECT it’s OK:
  SELECT * FROM users where id=1 or 1=1 --

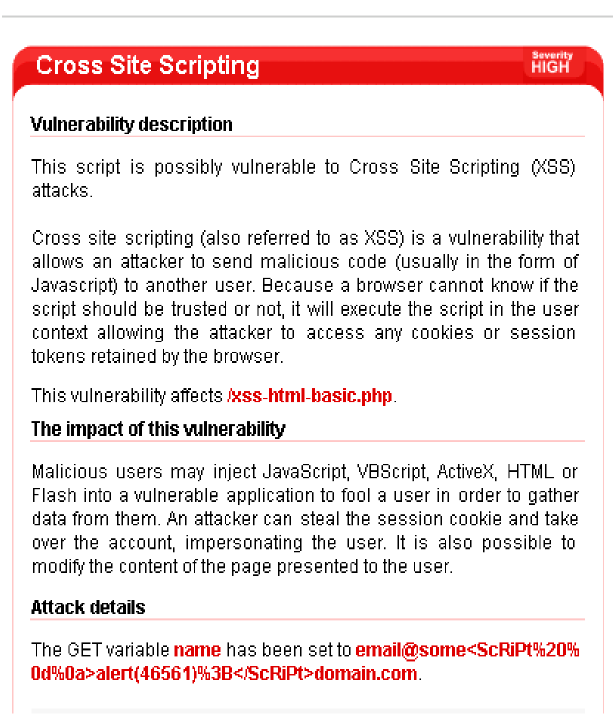
- In a DELETE…
  DELETE FROM users where id=1 or 1=1 --

- Most pentesters don’t use “or 1=1 – ” anymore … Most scanners do

Ergonomic?? …paid per bug??



- Cross Site Scripting (92)
  - /xss-html-basic.php (29)
    - name (29)
      - variant 1
      - variant 2
      - variant 3
      - variant 4
      - variant 5
      - variant 6
      - variant 7
      - variant 8
      - variant 9
      - variant 10
      - variant 11
      - variant 12
      - variant 13
      - variant 14
      - variant 15
      - variant 16
      - variant 17
      - variant 18
      - variant 19
      - variant 20
      - variant 21
      - variant 22
      - variant 23
      - variant 24
      - variant 25
      - variant 26
      - variant 27
      - variant 28
      - variant 29



Cross Site Scripting Severity HIGH

Vulnerability description

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

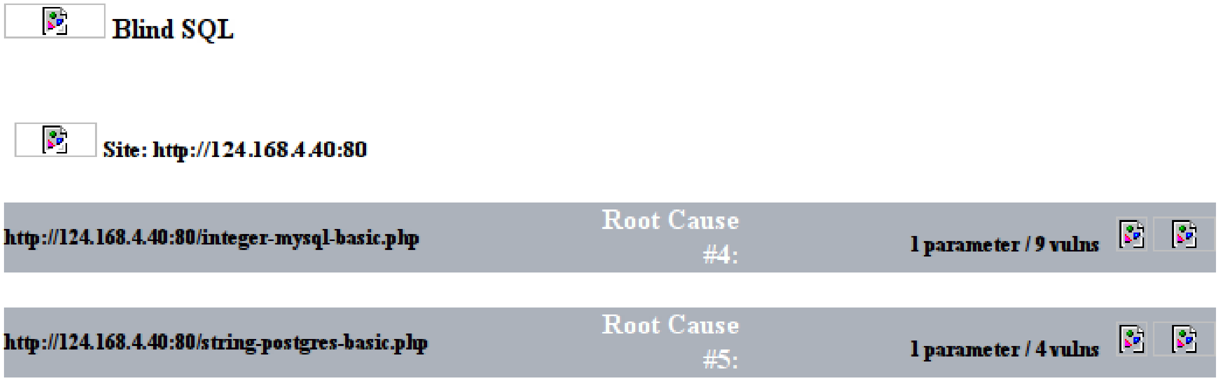
This vulnerability affects /xss-html-basic.php.

The impact of this vulnerability

Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to fool a user in order to gather data from them. An attacker can steal the session cookie and take over the account, impersonating the user. It is also possible to modify the content of the page presented to the user.

Attack details

The GET variable name has been set to email@some<ScRiPt%20%0d%0a>alert(46561)%3B</ScRiPt>domain.com.

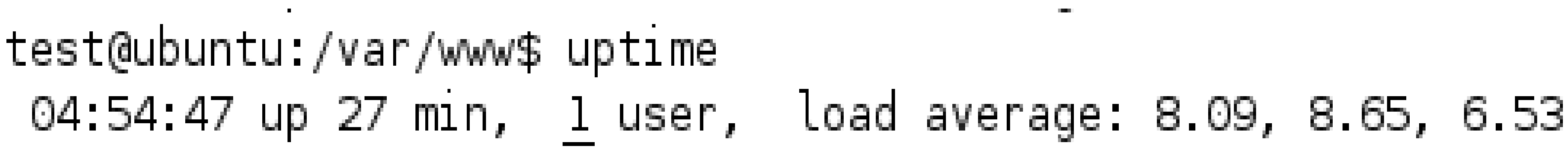


Blind SQL

Site: http://124.168.4.40:80

http://124.168.4.40:80/integer-mysql-basic.php	Root Cause #4:	1 parameter / 9 vulns
http://124.168.4.40:80/string-postgres-basic.php	Root Cause #5:	1 parameter / 4 vulns

Skipfish and Discretion…



```
test@ubuntu:/var/www$ uptime
 04:54:47 up 27 min,  1 user,  load average: 8.09, 8.65, 6.53
```

You probably want to limit the number of threads…

Recommendations

- Don’t use an automatic scanner in production
- Enable errors messages during scans and pentests
- Know your tools limits…

Web scanners are useful and should be used…

but point-and-click is a LIE…

However, web scanners are good for finding the low-hanging fruit

Thanks for review:
@securusglobal,
@lumc, Renaud
and @ddrazic

Play the CTF!!!

<louis@securusglobal.com>