

CMPE-279
Assignment-3

Team Members:

Shanmukha Yaswanth Reddy Kallam	015998840
Purna Sai Mahesh Goud Palagani	015999308

1.

Describe the SQLi attack you used, how did you cause the user table to be dumped? What was the input string you used?

DVWA Security

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code. Prior to DVWA v1.9, this level was known as 'high'.

Low

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications. PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [\[Enable PHPIDS\]](#)

[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Username: admin
Security Level: low
PHPIDS: disabled

Firstly, We setup the security level of DVWA (Damn Vulnerable Web App) to "low" .

Vulnerability: SQL Injection

User ID:

ID: 1' or 1=1#
First name: admin
Surname: admin
ID: 1' or 1=1#
First name: Gordon
Surname: Brown
ID: 1' or 1=1#
First name: Hack
Surname: Me
ID: 1' or 1=1#
First name: Pablo
Surname: Picasso
ID: 1' or 1=1#
First name: Bob
Surname: Smith

More Information

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://terrub.mavifuna.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
- <http://bobby-tables.com/>

[View Source](#) [View Help](#)

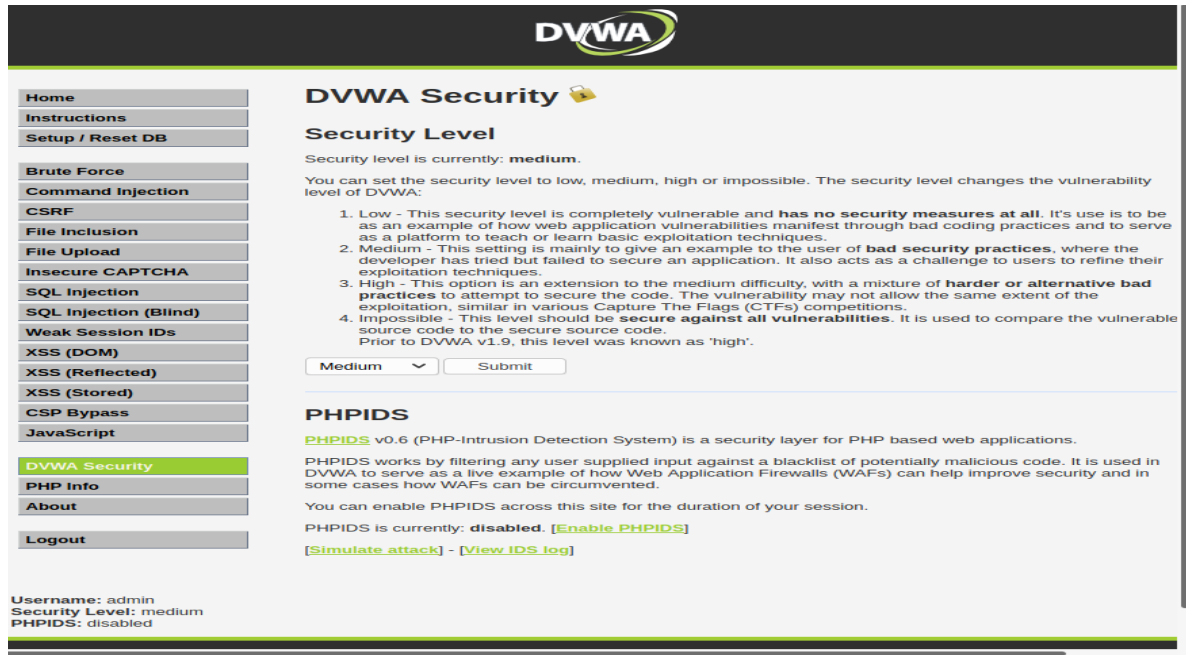
Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.10.5 Development

Now we pass 1' or 1=1# to satisfy the queries and display the list of users in the database. It then displayed the "FIRST NAME" and "SURNAME" of all the users in the database.


2.

If you switch the security level in DVWA to “medium”, does the SQLi attack still works?



The screenshot shows the DVWA Security page. The left sidebar contains a list of links: 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), CSP Bypass, JavaScript, DVWA Security (highlighted), PHP Info, About, and Logout. The main content area is titled "DVWA Security" with a lock icon. Below the title is the "Security Level" section, which states the current level is "medium". It explains that the security level can be set to low, medium, high, or impossible, and that it changes the vulnerability level of DVWA. A list of four levels is provided: 1. Low (completely vulnerable), 2. Medium (basic exploitation techniques), 3. High (harder or alternative bad practices), and 4. Impossible (secure against all vulnerabilities). At the bottom of this section is a dropdown menu set to "Medium" and a "Submit" button. Below this is the "PHPIDS" section, which describes the PHP-Intrusion Detection System and provides links to enable it and simulate an attack. The footer shows the username "admin", security level "medium", and PHPIDS status "disabled".

Now, if we check the same query after changing the security level of DVWA to “medium” then the SQL injection attack didn’t work.

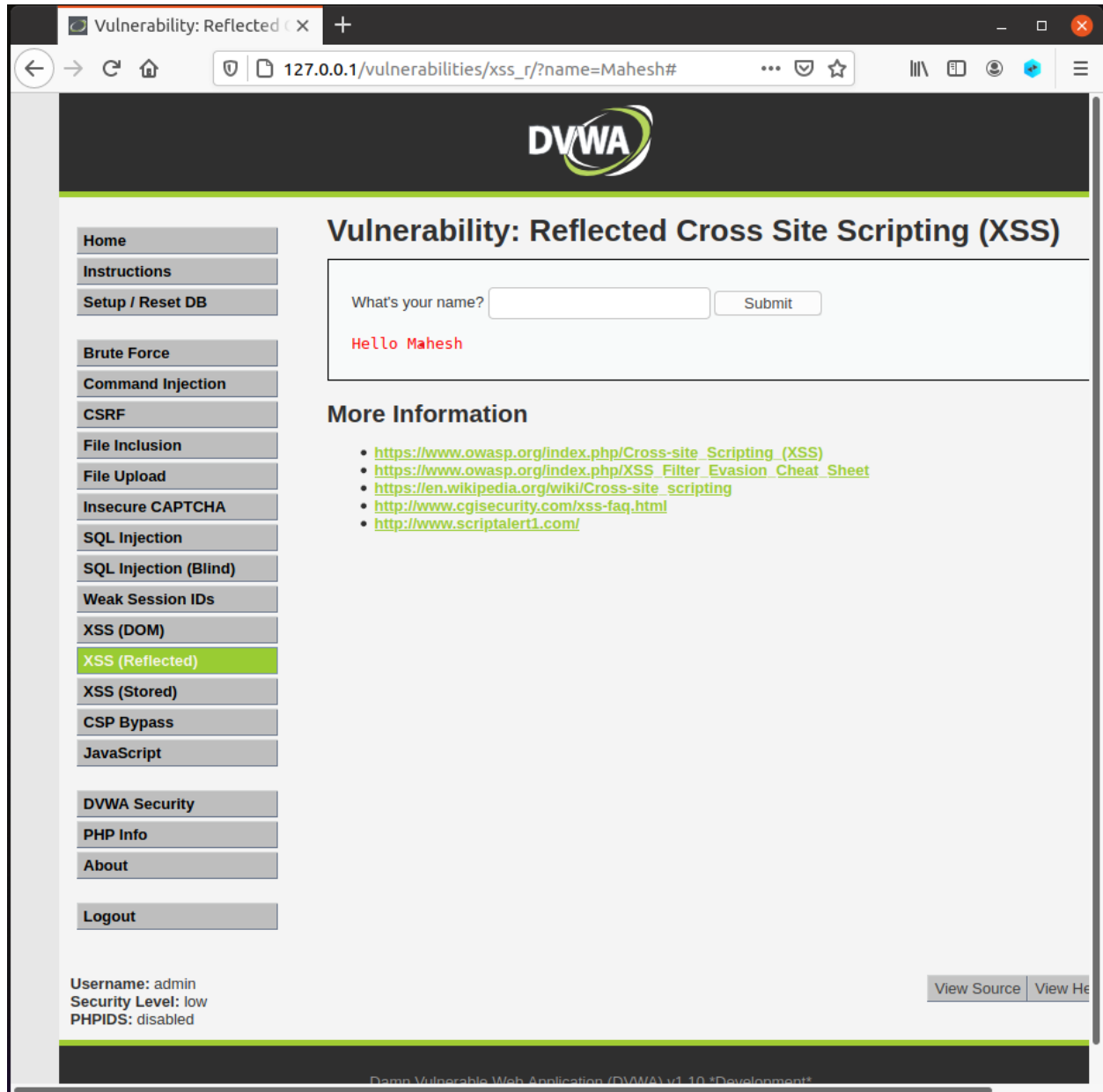


The screenshot shows the DVWA Vulnerability: SQL Injection page. The left sidebar is identical to the previous screenshot, with "SQL Injection" highlighted. The main content area is titled "Vulnerability: SQL Injection". Below the title is a form with a "User ID:" label, a dropdown menu set to "1", and a "Submit" button. Below this is the "More Information" section, which contains a list of links to external resources about SQL injection. The footer shows the username "admin", security level "medium", and PHPIDS status "disabled".

3.

Describe the reflected XSS attack you used, how did it work?

Now, set the security level to low and select XSS(Reflected) from the available options and enter input name here (eg: Mahesh) .



A message saying "Hello Mahesh" pops on the screen.

4.

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The top header displays the DVWA logo. The left sidebar contains a list of navigation links: 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) (highlighted), XSS (Stored), CSP Bypass, JavaScript, DVWA Security, PHP Info, About, and Logout. The main content area is titled 'Vulnerability: Reflected Cross Site Scripting (XSS)'. It contains a form with the label 'What's your name?' and a 'Submit' button. Below the form, the output shows 'Hello alert("Hello From Input")' in red text. Under the heading 'More Information', there is a list of links: [https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)), https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet, https://en.wikipedia.org/wiki/Cross-site_scripting, <http://www.sqlsecurity.com/xss-faq.html>, and <http://www.scriptalert1.com/>. The footer shows 'Username: admin', 'Security Level: medium', and 'PHPIDS: disabled'. There are also links for 'View Source' and 'View Help'. At the bottom, a small text line reads 'Copyright © 2012-2013 by the DVWA Development Team. All rights reserved. This is a security tool and should not be used for illegal or unauthorized activities.'

If we change the security level to medium and give input `<script>("Hello From Input")</script>` . XSS attack doesn't work the input was processed as characters but not as code/program.