Lab Report 8

1. Assessment Sheet
2. **Why is it critical to perform a penetration test on a Web application and a Web server prior to production implementation?**

Firstly, in web server and web application, it stores numerous of customer sensitive data such as the credit card number, expiration date, security code, personal identity etc. So, it is quite important for companies who keep all information of end user to protect these assets from being compromised or breach. In addition, the government mandates such companies to execute penetration test before the any web application or web server go to production.

1. **What is a cross-site scripting attack? Explain in your own words.**

The cross-site scripting attack refers to someone who takes advantages of the vulnerabilities existing within a form of a web application, which allows attackers to execute arbitrary scripts. These codes might cause serious information compromise or breach.

1. **What is a reflective cross-site scripting attack?**

As a reflective cross-site scripting, the attackers cannot be able to modify any data on the webserver and it can show its input/ output both on end user’s and attackers’ screen.

1. **Which Web application attack is more likely to extract privacy data elements out of a database?**

We can use SQL Injection to extract information from a database.

1. **What security countermeasures could be used to monitor your production SQL databases against injection attacks?**

In this case, we should set up a detailed review SQL log policy within the company. For instance, we should check the SQL log daily and try to find is there any abnormal SQL statements. Also, we can enable audit functions which provided by Database itself.

1. **What can you do to ensure that your organization incorporates penetration testing and Web application testing as part of its implementation procedures?**

In order to ensure organization have already incorporates the penetration testing, we should set up a policy and a specific procedure which contains detailed metrics in it. Then, we from the result of comparing metrics with actual environment, we can learn whether penetrating test are executed properly.

1. **Who is responsible for the CIA of production Web applications and Web servers?**

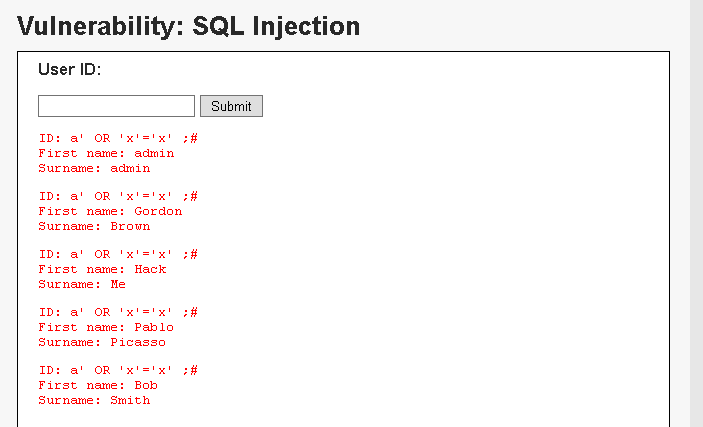
System engineer, network administrator and security professionals should be responsible for the CIA of production Web applications and Web servers.

1. Challenge Questions

**Description: Create a SQL injection attack to determine the field name that holds the user’s surname. Research best practices for preventing SQL injection attacks on the network. Identify at least three common practices and cite your sources**

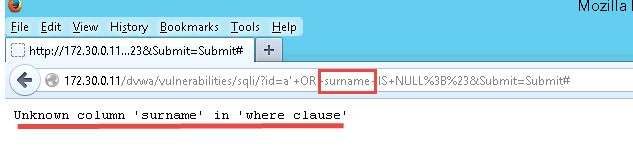
1. SQL injection attack to determine the field name that holds the user’s surname.
2. Test the existence of SQL Injection vulnerability

In this step, I entered a piece of string “a’ OR ‘x’ = ‘x’;#” and it returns all the data in this particular query of this textbox. The “OR ‘x’ = ‘x’ ” makes the filter statement in this SQL statement bulk not work because ‘x’= ‘x’ is always true. And, the result shows that we can exploit the web form vulnerability of SQL Injection.



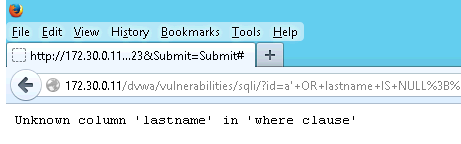
1. Test “ a’ OR surname IS NULL;#”

In this case, the web page shows an error that the surname is unknown column. It means that the column name must not be surname. So, we continue our test on other possibilities.



1. Test “a’ OR lastname;#”

It proves that lastname is not correct column name.



1. Test “a’ OR last\_name;#”

In this below picture, we find that when we type the above command, the web page doesn’t report an error. It proves that the column name of last\_name exists.



1. Test “a’ OR last\_name = ‘me’;#”

The below picture shows that we successfully find the correct columns’ name which contains users’ surname.

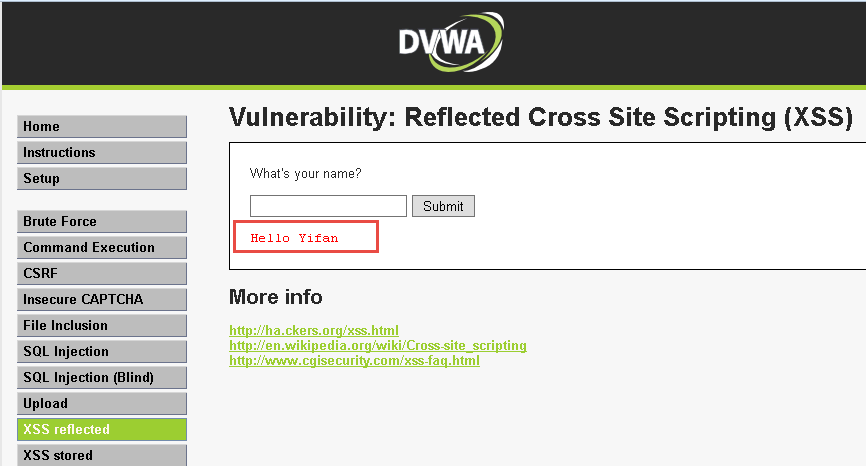


1. Three common practices and cite your sources

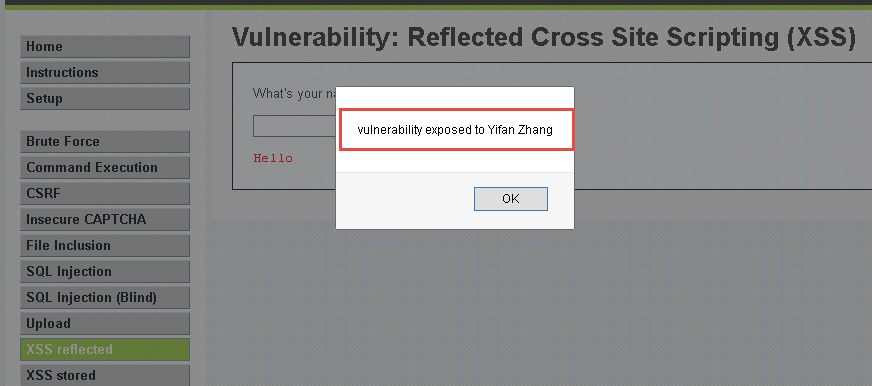
* Regularly updating and patching your web server and databases in order to prevent the SQL Injection
* Educate the programmers to develop a well written and well tested code which can minimize the possibility of SQL Injection attack
* Well define the access privilege and operational privilege of database.

References:

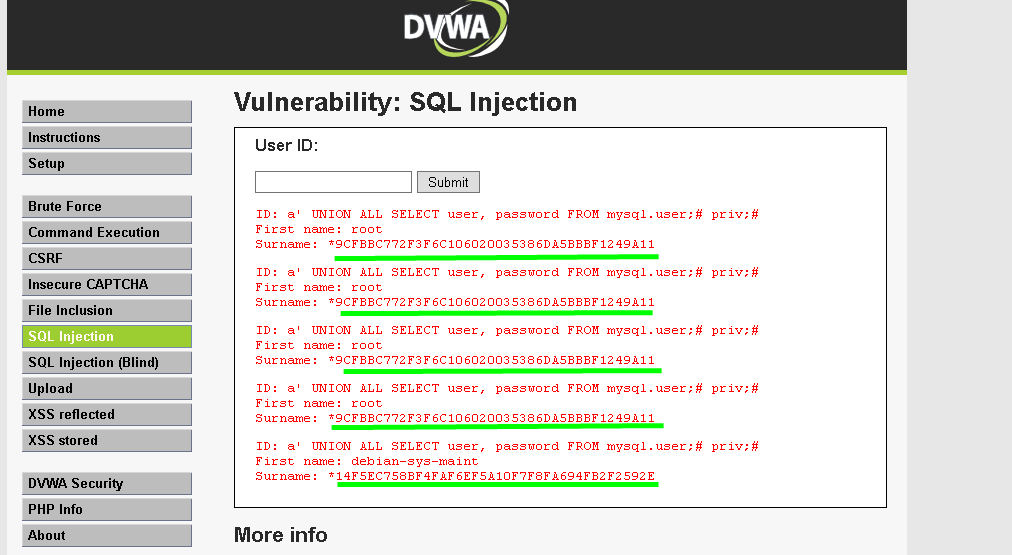
1. BEYOND security. (2015, 10 15). *SQL Injection*. Retrieved 10 18, 2015, from BEYOND security: http://www.beyondsecurity.com/about-sql-injection.html
2. Paul Rubens. (2010, 2 23). *10 Ways to Prevent or Mitigate SQL Injection Attacks*. Retrieved 10 18, 2015, from ENTERPRISE Networking Planet: http://www.enterprisenetworkingplanet.com/netsecur/article.php/3866756/10-Ways-to-Prevent-or-Mitigate-SQL-Injection-Attacks.htm
3. Report Screenshot
4. XSS – My name



1. XSS – exposed vulnerability



1. SQL Inject – user hash



1. Other additional supporting text/image content

Lab Report 15

1. Assessment Sheet
2. **Why is it critical to perform a penetration test on a Web application and a Web server prior to production implementation?**

Firstly, in web server and web application, it stores numerous of customer sensitive data such as the credit card number, expiration date, security code, personal identity etc. So, it is quite important for companies who keep all information of end user to protect these assets from being compromised or breach. In addition, the government mandates such companies to execute penetration test before the any web application or web server go to production.

1. **What is a cross-site scripting attack? Explain in your own words.**

The cross-site scripting attack refers to someone who takes advantages of the vulnerabilities existing within a form of a web application, which allows attackers to execute arbitrary scripts. These codes might cause serious information compromise or breach.

1. **What is a reflective cross-site scripting attack?**

As a reflective cross-site scripting, the attackers cannot be able to modify any data on the webserver and it can show its input/ output both on end user’s and attackers’ screen.

1. **Based on the tests you performed in this lab, which web application attack is more likely to extract privacy data elements out of a database.**

We can use SQL Injection to extract information from a database.

1. **If you can monitor when SQL injections are performed on a SQL database, what would you recommend as a security countermeasure to monitor your production SQL databases.**

In this case, we should set up a detailed review SQL log policy within the company. For instance, we should check the SQL log daily and try to find is there any abnormal SQL statements. Also, we can enable audit functions which provided by Database itself.

1. **Given that Apache and Internet Information Services(IIS) are the two most popular web application servers for Linux and Microsoft Windows platforms, what would you do to identify known software vulnerabilities and exploits?**

We can directly search the key words of Apache or IIS in National Vulnerability Database website and then it will show us more detailed information of all exposed vulnerabilities related to this key words. And, from the result we could find exploit method and mitigation solutions.

1. **What can you do to ensure that your organization incorporates penetration testing and Web application testing as part of its implementation procedures?**

In order to ensure organization have already incorporates the penetration testing, we should set up a policy and a specific procedure which contains detailed metrics in it. Then, we from the result of comparing metrics with actual environment, we can learn whether penetrating test are executed properly.

1. **What is the purpose of setting the DBWA security level to “low” before beginning the remaining lab steps?**

Set the security level to “low” because only in this setting the web application shows numerous vulnerabilities which are offered for us to do experiments. If we set the security level to “high”, we will not able to exploit the vulnerabilities in the web application.

1. **As an ethical hacker, once you’ve determined that a database is injectable, what should you do with that information?**

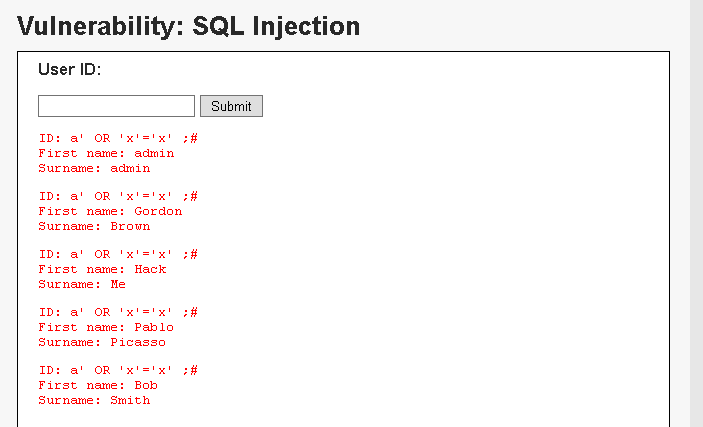
As an ethical hacker, once I detect a potential risk for SQL Injection, I will document this vulnerability with a harmless exploit and mitigation solutions. Then, I will send this document to my line manager and seeking permissions for further action.

1. Challenge Questions

**Description: Use SQL injection attack to determine the field name that holds the user’s surname. Document each test and the results of that test.**

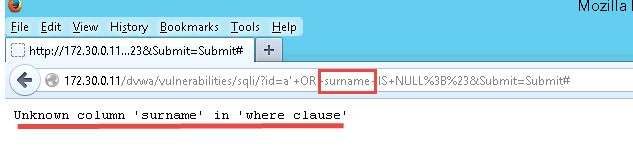
1. Test the existence of SQL Injection vulnerability

In this step, I entered a piece of string “a’ OR ‘x’ = ‘x’;#” and it returns all the data in this particular query of this textbox. The “OR ‘x’ = ‘x’ ” makes the filter statement in this SQL statement bulk not work because ‘x’= ‘x’ is always true. And, the result shows that we can exploit the web form vulnerability of SQL Injection.



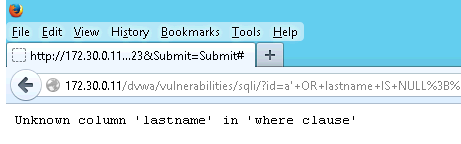
1. Test “ a’ OR surname IS NULL;#”

In this case, the web page shows an error that the surname is unknown column. It means that the column name must not be surname. So, we continue our test on other possibilities.



1. Test “a’ OR lastname;#”

It proves that lastname is not correct column name.



1. Test “a’ OR last\_name;#”

In this below picture, we find that when we type the above command, the web page doesn’t report an error. It proves that the column name of last\_name exists.



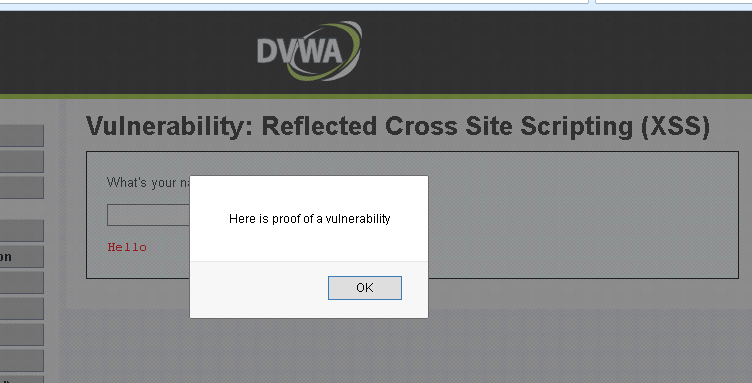
1. Test “a’ OR last\_name = ‘me’;#”

The below picture shows that we successfully find the correct columns’ name which contains users’ surname.

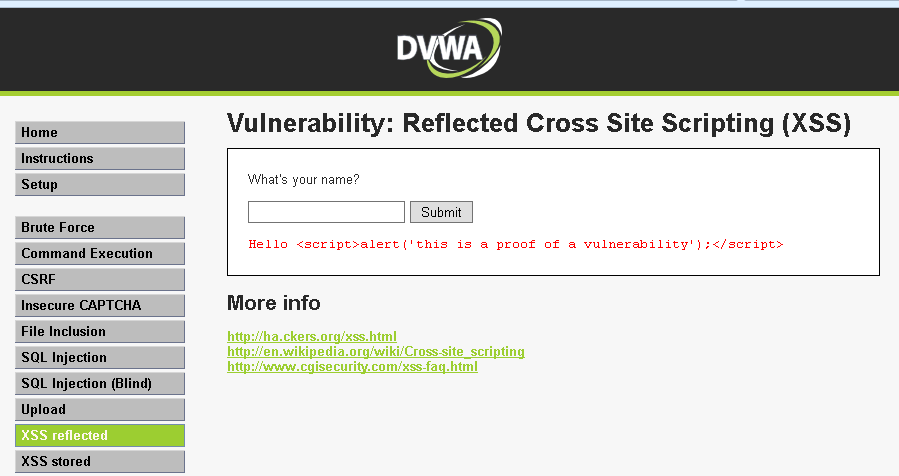


1. Report Screenshot
2. XSS attack – security level low

Run the script of “<script> alert(‘Here is proof of a vulnerability’);</script>” and we got the script executed successfully under security level as low.



1. XSS attack – Security level high



Explanation:

After we set the security level to high, we find that the script cannot be executed any more. Instead, it makes the script code become plain text and shows them on the screen.

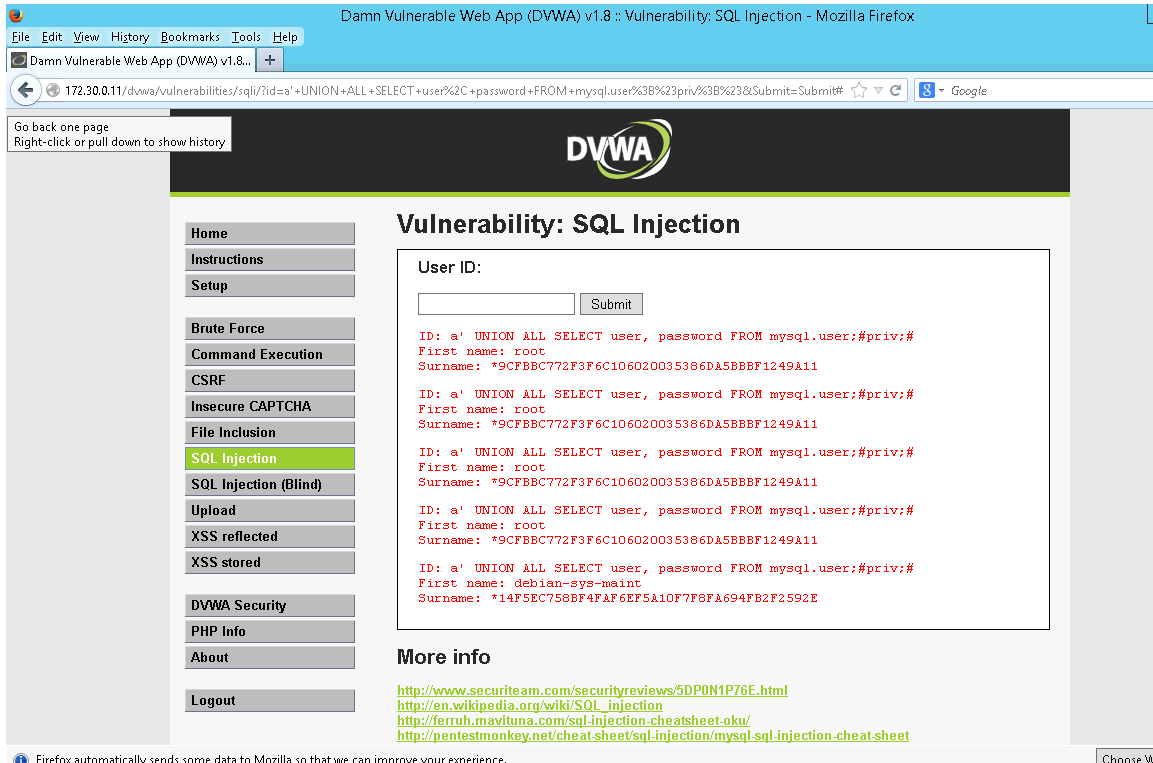
1. SQL injection – user information

In this case, we exploit the SQL injection vulnerability through typing the SQL statement “a’ UNION ALL SELECT system\_user(), user();#”. And we got the operation system’s user information from this vulnerability.



1. SQL injection – hash information

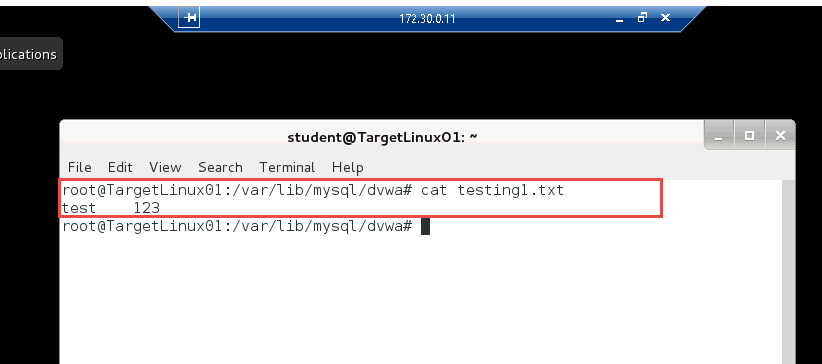
In this case, we exploit the SQL injection vulnerability through typing the SQL statement “a’ UNION ALL SELECT user, password FROM mysql.user;# priv;#”. And we got the operation system’s user information from this vulnerability.



1. The purpose of hashing in a database

Hash can be used anywhere in a database but in this case, the hash is the result of encrypted user password within mysql database.

1. Contents of the testing1.txt



Explanation:

In this case, we use SQL command to save some data to local drive.

1. Brief description of security countermeasures you recommend to mitigate the risk from compromise and exploitation

In order to prevent SQL Injection, first thing we need to do is to minimize the permissions to the user who could run such SQL statement. Secondly, we should educate programmers and teach them how to avoid SQL Injection while coding. For XSS, we can install anti-XSS component to prevent the happening of XSS attack. For both attacks, we need to perform penetration test frequently and try to identify them as early as possible.

References:

1. Microsoft. (2015, 10 15). *Mitigating Cross-Site Scripting(XSS) Attacks*. Retrieved 10 18, 2015, from Microsoft MSDN: https://msdn.microsoft.com/en-us/library/hh567599%28v=cs.95%29.aspx
2. Other additional supporting text/image content