**CROSS SITE SCRIPTING (XSS)**

**PROJECT - 5**

**DEME SAI KIRAN**

**AZURE SKYNET**

**ADGAONKER SHASHANK**



**Table of contents:**

* **Introduction to the XSS**
* **HTML usage**
* **Non Persistent Scripts**
* **Persistent Scripts**
* **Malicious Attacks**
* **Avoiding Basic Filters**
* **Avoiding Advanced Filters**
* **Analyzing Twitters Tweet Deck XSS Script**

**XSS – CROSS SITE SCRIPTING :**

* Cross Site Scripting, otherwise known as XSS is a code injection attack allowing the injection of malicious code into a website.
* XSS is currently one of the most common website attacks, with almost every website requiring the user to have JavaScript turned on.
* Rather than being an attack on the website itself, it uses the website as a means to attack the users of that website.
* When you can get your XSS permanently on a website all those who visit that page will have the JavaScript executed by their browser.
* The victim's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site.

**WHAT IT CAN DO ?**

* Malicious JavaScript can be used to do all sorts of malicious tasks.
* It can be used to steal users cookies, allowing for someone to use the website pretending to be that user.
* JavaScript can modify the page to make it look different or behave differently.
* It can even send you to another website taking data with you.

**HTML USAGE :**

* Let’s first look at how HTML works.
* HTML is a tag based language, so when we open a tag such as <b> for bold, all text after that tag becomes bold until a matching </b> closing tag is found.
* happen if we were to only put a <b> tag in a search box that doesn’t strip the tag…….
  + Then everything in the rest of this slide would be bold until a closing bold was found.
  + The scary part of XSS comes when we use the <script> tag, informing the browser anything between the script tags is JavaScript.

**NON PERSISTENT SCRIPTS :**

* A Non Persistent Script is as the name describes. The attack only affect’s the user running the script.
* It may indicate that the Website’s creator may have forgot to protect other input fields.
* It’s not very useful to attack yourself, so we need to be a little crafty.
* A Non persistent script can also be referred to as Reflected XSS.

**REFLECTED XSS :**

* I like to split Reflected Attacks as their own little sub field.
* Reflected XSS is harnessed by attaching the malicious script to the end of a URL/Link.
* Though it may be obvious to see code on the end of a URL, techniques of hiding it are possible.
* Also with the service of link shortening services this can be very deadly.

**WORKING OF REFLECTED XSS:**

* Reflected XSS is very common cross site scripting method currently.
* The malicious code possibilities are endless. But for examples sake we could:

- Redirect to a phishing

- Steal Cookie information

- Force the user to make an action.

* Then created website can be sent in any of the social media or else even we can mail too.

**PERSISTENT SCRIPT :**

* A persistent script is as you can probably guess by now a script that persists on a website.
* Usually having the malicious code stored in the websites database.
* This would be your ultimate goal, to get your code permanently on the target site.

**FINDING INJECTION LOCATIONS:**

* It needs to be something that interacts with either a database or file storage.
* Think, comments, submission forms, contact forms, posts, uploads, etc.
* Imagine if you we conducting a Pentest and you manage to inject a script into a ticket system that didn’t sanitize. You could get cookies for an employee/admin account.
* (**CODE STORED** )The script tag allows you to link to a javascript file. (Good for limited character fields) Eg   
  <script src=“http://asite.com/myxss.js”></script>

**MALICIOUS ATTACKS :**

* Here we will start with stealing cookies
* Then we will move onto making forced actions on a site with a Reflected Attack.
* With these skills, you can perform many other attacks.
* ***COOKIES ARE ABUNDANT :***
* Most, if not all website you log into have a remember me function meaning they give you a cookie with a session/auth code.
* Meaning if we use a cookie attack on a website where the user needs to be logged on to see the page. We will have a cookie with their auth code, that we can use to login as them .
* ***A BASIC COOKIE STEALER:***
* Using the code we learned in the previous two tutorials we can easily set up a cookie stealing system.
* You can download the new modified 2 php files. Index.php and cookiemonster.php
* Let’s Steal some cookies!
* ***POWER OF REFLECTED XSS:***
* No doubt you have heard a story of someone clicking a link and having something scammed from their online account.
* Chances are that was done with some sort of reflected attack.
* We can force a person’s hand quite a fair bit with JavaScript/jQuery.

**BY PASSING BASIC FILTERS :**

***MAGIC\_QUOTES\_GPC :***

* Versions of PHP < 5.3.0 used a configuration variable called magic\_quotes\_gpc which would change all:  
  *'* (single-quote)  
  *"* (double quote)  
  *\* (backslash)   
  \0 (*NULL)*Into an escaped form of those characters.
* The resulting alert would look possibly like   
  alert(\”xss\”) or  
  alert(\xss\)
* This php variable has since been removed as it was not a plausible solution to many attacks and as many people were learning about SQL injection. More database specific functions were designed to be used instead. Eg.  
  *mysql\_real\_escape\_string( $astring);*
* Many websites still use old   
  versions of PHP! This means many sites still use this magic\_quotes\_gpc as their only line of defense.
* Some websites may only add in a simple filter to convert the magic\_quote values into their html entity equivalent.

**Using fromCharCode:**

* Let’s try out bypassing this type of filter with a little trick to generate a string at runtime. Avoiding all use of quotes!
* The new index.php file will simulate the now removed magic\_quotes\_gpc.

**ANOTHER TYPE OF ATTACK :**

* Up until now we have used the <script> tag to run all of our cross site scripts.
* However if you know much about javascript, we can also run scripts from the browser’s address bar. (Address Bar Scripts)
* Try typing: javascript:alert(“Hello”) while on a webpage.

COMING TO THE ***DVWA*** (Damn vulnerable web application) :

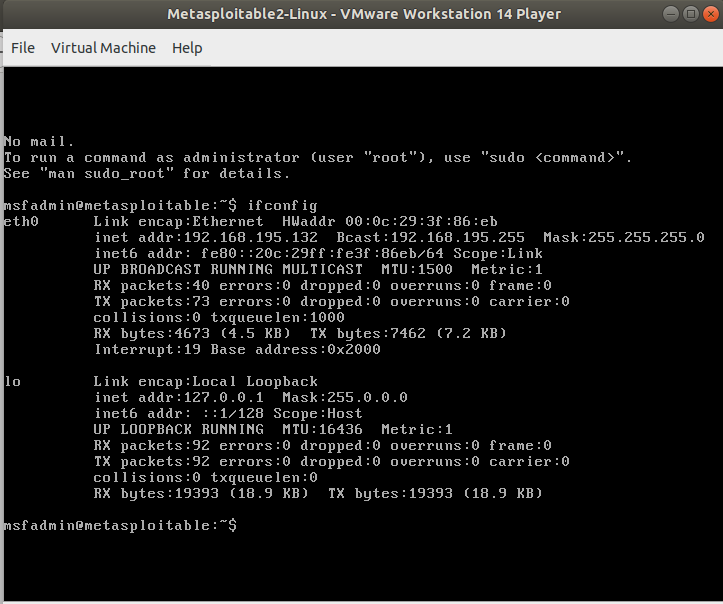
**🡪 D V W A :**

***WHAT IS DAMN VULNERABLE WEB APP ?***

* Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable.
* Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment and help web developers better understand the processes of securing web applications.

**Lets begin the story with this DVWA ☺ ……………**

* Initially open the metasploitable operating system and capture the ipaddress of the corresponding metasploitable operating system.
* By the main techiques we know i.e, by **netdiscover** in terminal or by using the inbuilt application “**ETTERCAP”.**



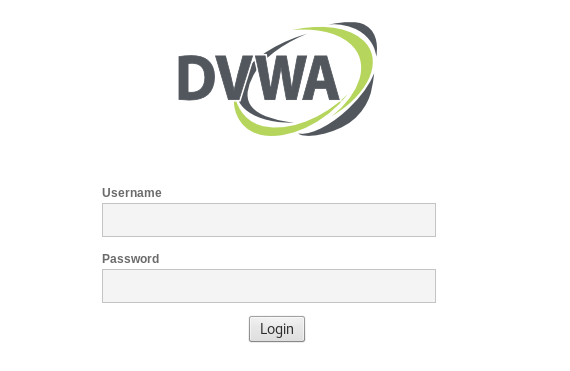
* This is the sceen of the metasploitable OS
* Here we can find the ip address of the meta OS
* Copy the metasploitable OS.
* Opening the browser in the kali linux and paste the copied ip address of the metasploiatable OS to select the DVWA option.

websearch.png

* Then we will get the screen like this……



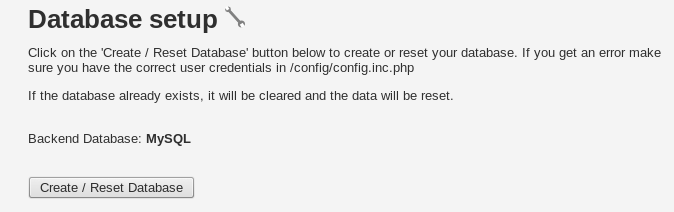
* Then selecting the DVWA option we get the login screen of the DVWA as shown below…..



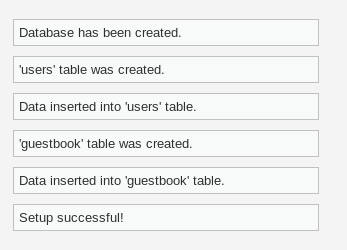
* Here username is **admin** and the password is **password** after login we will the screen like this…..



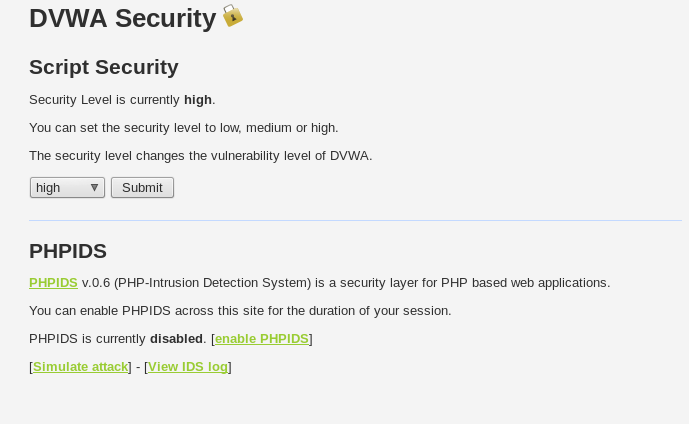
* Here we can observe the set of options on your left hand side.
* We need to setup the XSS database (create/reset)



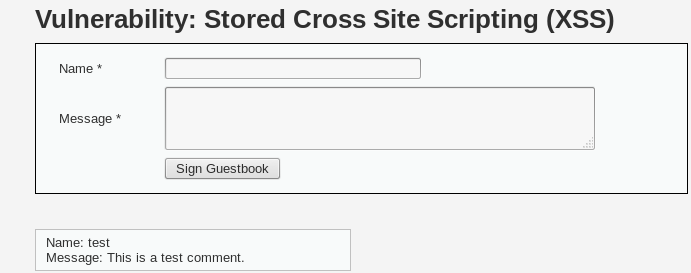
* Then it shows the following set of lines as shown below that indicates the setup has been done (Data base was ready to modify)



* Now we need to set the security level to send alert message and lots more…
* We can see the DVWA security option was mentioned in the left hand side of the screen.
* Then follow the required steps as shown below…..



* Here in this picture we can notice that the script security level was mentioned as high change it into the low mode and submit it .
* After that get into the XSS stored optipon which was present in the options on your left hand side…. ☺…..
* Then we can see the screen that contains empty test box and the message box.
* Here message box is to mention the dialogue that will appear on the oponents system…



* Enterning some required details in it as shown below it will appear on the oponents system….



* Here is all bout the XSS (Cross site scripting )……………………
* Learn php , java script to do more lots of things with this DVWA app.

☺ THANK YOU…………………………………….<DEME SAI KIRAN>………………