Hacking Articles

Raj Chandel's Blog

CSRF Exploitation using XSS

posted in PENETRATION TESTING , WEBSITE HACKING on JUNE 24, 2017 by RAJ CHANDEL

SHARE

Hello friends! In our previous article we saw how an attacker can shoot web application against CSRF vulnerability with help of burp suite. Today again we are going to test CSRF attack with help of XSS vulnerability.AS we know taking the help of XSS attacker might be able to reads cookies from the same domain and if CSRF token are stored in cookies then attacker will able to read the CSRF token from CSRF protected post.

Let's have a look how an attacker can make CSRF attack for changing password of admin account when the web application is suffering from cross site scripting vulnerability. For this tutorial I had used **DVWA** and set its security level **low**.

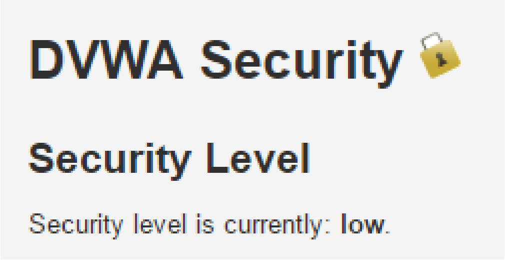
Search

ENTER KEYWORD

Subscribe to Blog via Email

Email Address

SUBSCRIBE

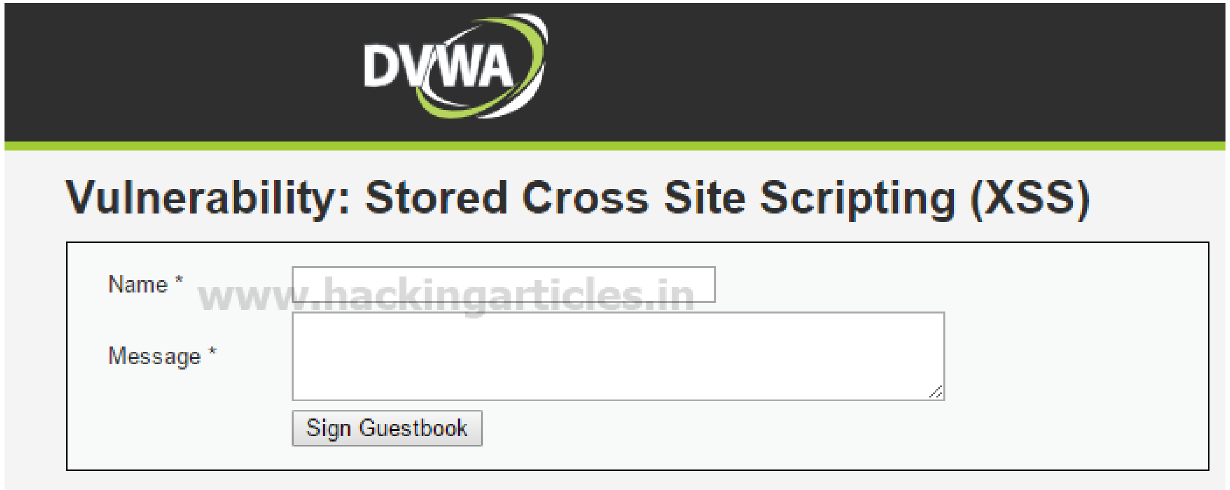


DVWA Security

Security Level

Security level is currently: low.

Suppose that you have found XSS vulnerability in any web application server. Here we are going to use java script or HTML script which will make CSRF attack for changing the password of admin account.



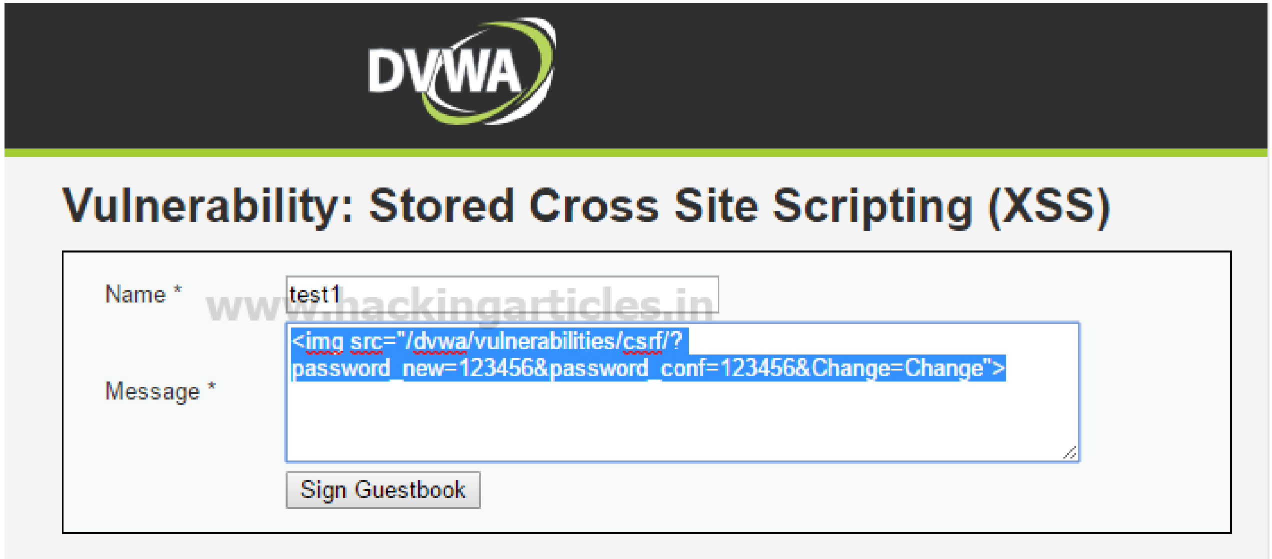
Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

An XSS attack can be used to read the cookies and get the valid tokens if it is stored in cookies which have to be inserted in the malicious script to make CSRF possible. Using image tag we will send a malicious script, inside script I had set **new password** as **123456**.

<img src=”/dvwa/vulnerabilities/csrf/?password_new=123456&password_conf=123456&Change=Change”>



Vulnerability: Stored Cross Site Scripting (XSS)

Name * test1

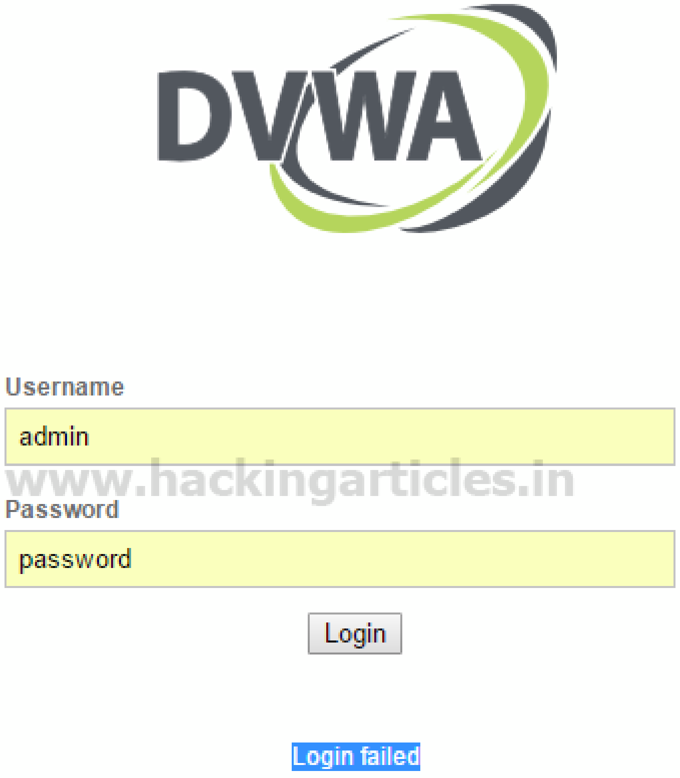
Message * `<img src="/dvwa/vulnerabilities/csrf/?password_new=123456&password_conf=123456&Change=Change">`

Now let's check whether the password for admin has been changed or not, previously credential was **admin: password**, if admin get failed to login inside web server using his previous credential then we had successfully made CSRF attack.

From given screenshot you can see using admin: password it confirms **login failed**. Now use your new password 123456 for login inside web server.

Categories

- BackTrack 5 Tutorials
- Best of Hacking
- Browser Hacking
- Cryptography & Stegnography
- CTF Challenges
- Cyber Forensics
- Database Hacking
- Domain Hacking
- Email Hacking
- Footprinting
- Hacking Tools
- Kali Linux
- Nmap
- Others
- Penetration Testing
- Social Engineering Toolkit
- Trojans & Backdoors
- Website Hacking
- Window Password Hacking
- Windows Hacking Tricks
- Wireless Hacking
- Youtube Hacking



Username

admin

Password

password

Login failed

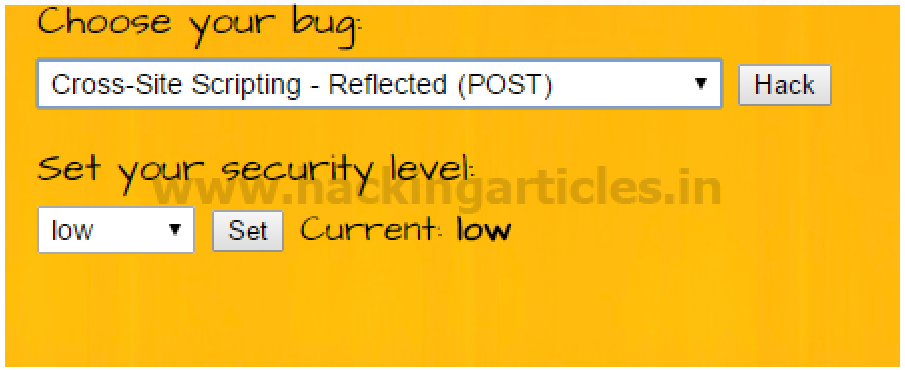
Articles

Select Month

Facebook Page

Ignite Technologies
5,288 likes
Like Page
www.ignitetechnologies.in
www.hackingarticles.in
Be the first of your friends to like this

Similarly there is another web application **bwapp** where we will demonstrate same attack using XSS vulnerability. First you need to chose your bug “**cross site scripting Reflected (post**)” and set security level **low**.



Choose your bug:

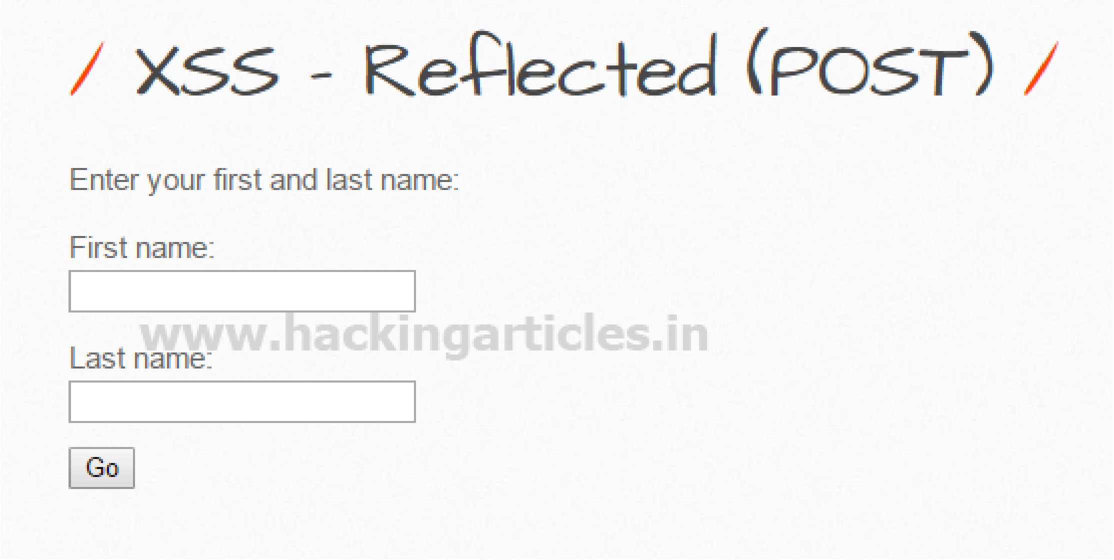
Cross-Site Scripting - Reflected (POST)

Set your security level:

low

Current: low

In given screenshot the form is suffering from XSS vulnerability now we are going to generate a script for making CSRF possible in order to change password for a user. Here we are login as **bee: bug** into web server now we will try to change its password with help of cross site scripting.



/ XSS - Reflected (POST) /

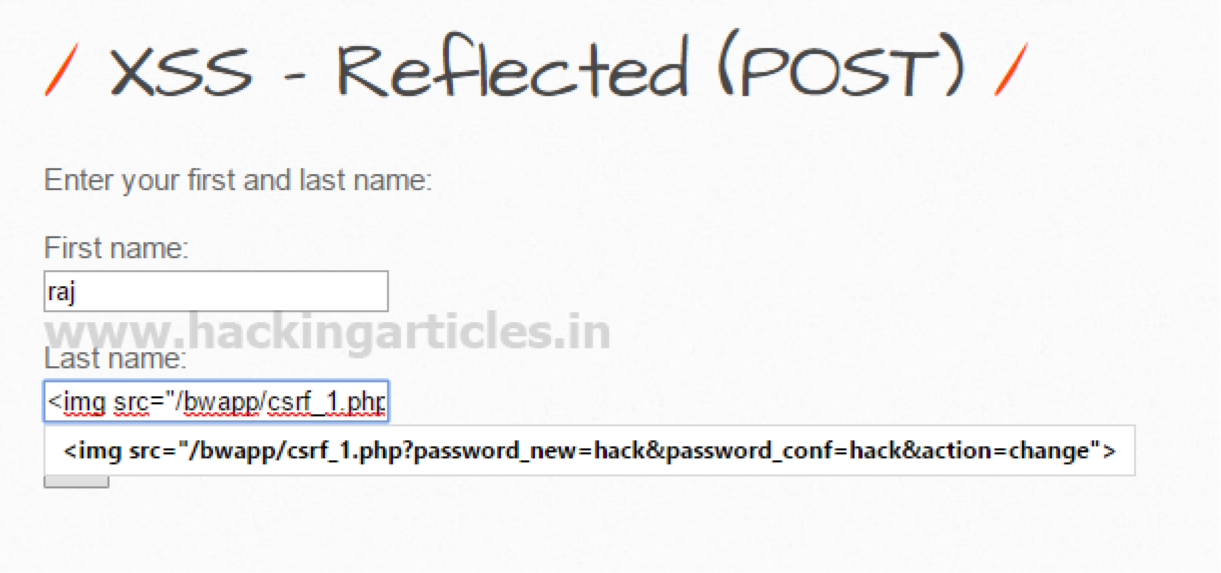
Enter your first and last name:

First name:

Last name:

Similarly using image tag we will send a malicious script, inside script I had set new password as **hack.**

<img src=”/bwapp/csrf_1.php?password_new=hack&password_conf=hack&action=change”>



/ XSS - Reflected (POST) /

Enter your first and last name:

First name:

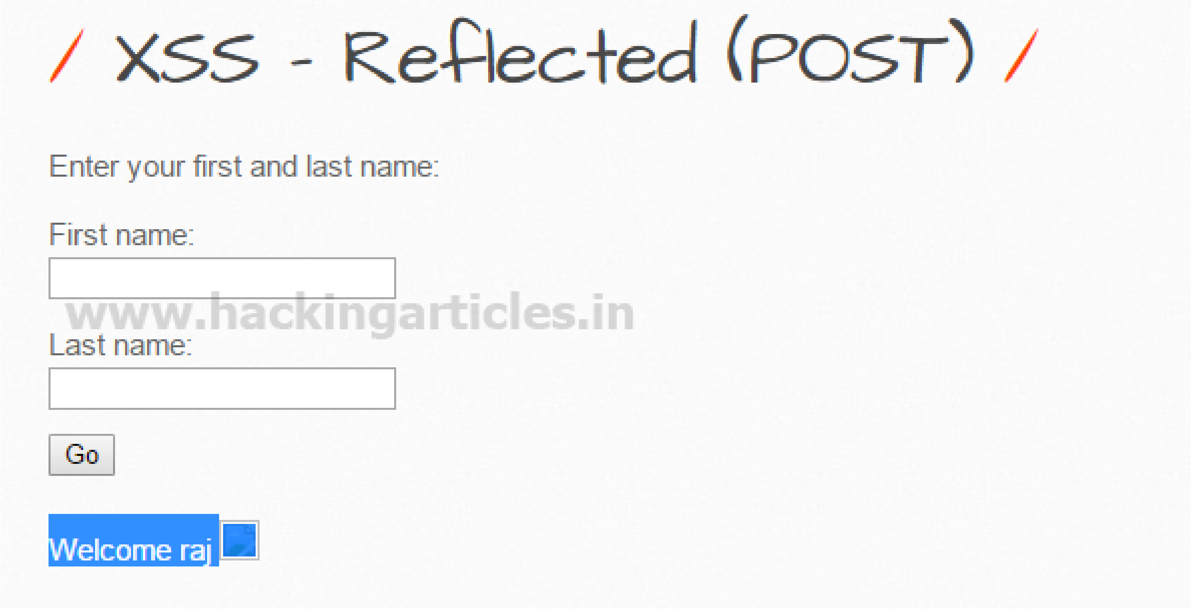
raj

Last name:

<img src="/bwapp/csrf_1.php

<img src="/bwapp/csrf_1.php?password_new=hack&password_conf=hack&action=change">

From screenshot you can see generated image icon which means this form has XSS flaws now let check whether the password has been modified or not for user bee.



/ XSS - Reflected (POST) /

Enter your first and last name:

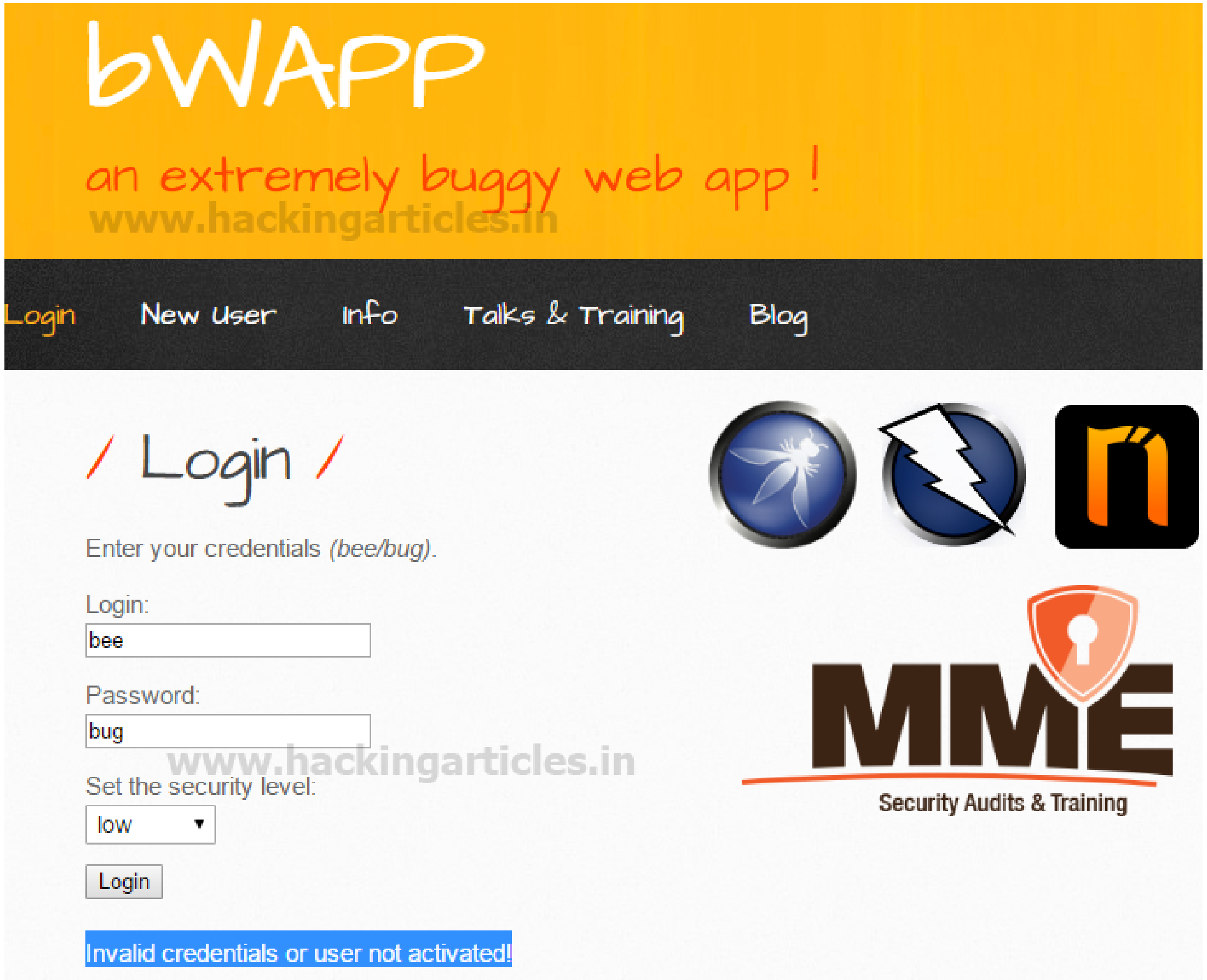
First name:

Last name:

Welcome raj

Now use previous credential bee: bug if login failed is confirmed it means we have successfully shoot the CSRF attack and from screenshot you can see "**invalid credential or user not activated**" message. Now use new password for login into web server.

Conclusion: XSS vulnerabilities exist anywhere in same domain it could lead to CSRF attack and allows attackers to remotely control the target's browser with full rights, making CSRF useless.



Enter your credentials *(bee/bug)*.

Login: bee

Password: bug

Set the security level: low

Invalid credentials or user not activated!

Author: AArti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact here

Share this:

Like this:

Loading...

ABOUT THE AUTHOR

RAJ CHANDEL

Raj Chandel is a Skilled and Passionate IT Professional especially in IT-Hacking Industry. At present other than his name he can also be called as An Ethical Hacker, A Cyber Security Expert, A Penetration Tester. With years of quality Experience in IT and software industry

PREVIOUS POST

← UNDERSTANDING ENCODING (BEGINNER'S GUIDE)

NEXT POST

DUMPING DATABASE USING OUTFILE →

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

□

Save my name, email, and website in this browser for the next time I comment.

POST COMMENT

□ Notify me of follow-up comments by email.

□ Notify me of new posts by email.