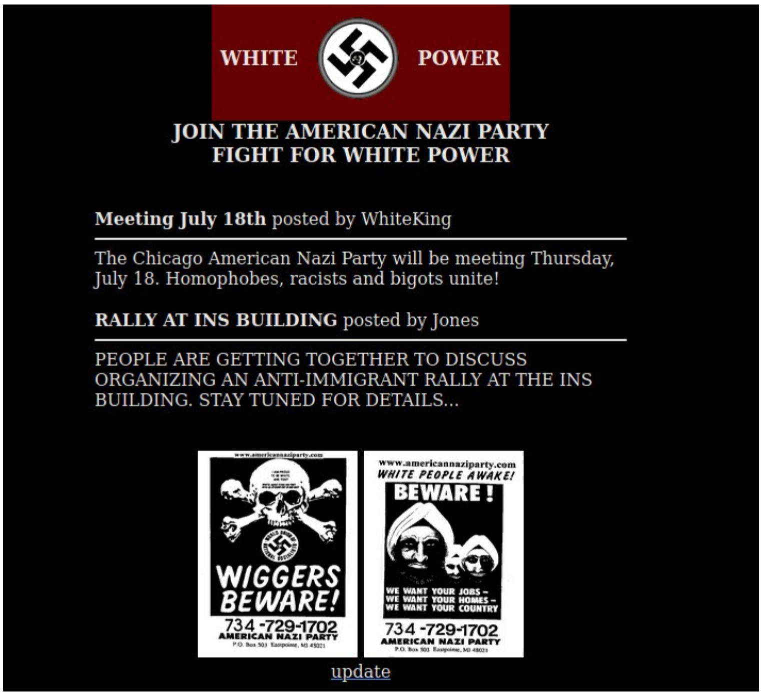
Hack this site realistic mission 02

This document is written by Twemlow and is intended for further understanding of the realistic challenges on HackThisSite. The idea behind this document and the ones that follow is that I am explaining what you will need to do, look for and execute. I will also explain why you need to do what I do in these tutorials to create a better understanding of the vulnerabilities, scenario and exploits used.

Vulnarability: SQLi (Sequeal Injection) Injection Attack.

Link: https://www.hackthissite.org/missions/realistic/2/



WHITE POWER

JOIN THE AMERICAN NAZI PARTY
FIGHT FOR WHITE POWER

Meeting July 18th posted by WhiteKing

The Chicago American Nazi Party will be meeting Thursday, July 18. Homophobes, racists and bigots unite!

RALLY AT INS BUILDING posted by Jones

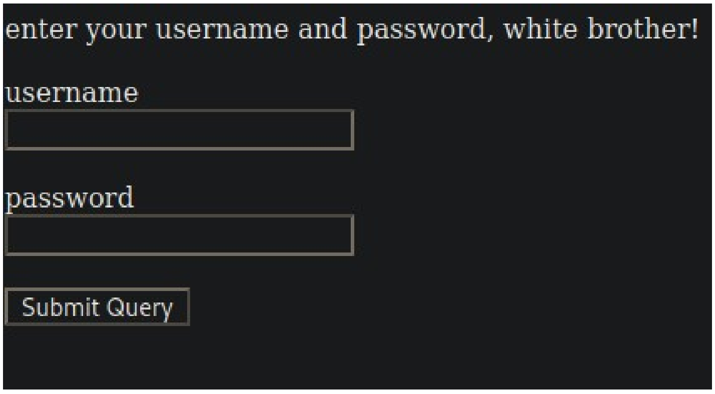
PEOPLE ARE GETTING TOGETHER TO DISCUSS ORGANIZING AN ANTI-IMMIGRANT RALLY AT THE INS BUILDING. STAY TUNED FOR DETAILS...

update

First, analyse the webpage, look at the HTML source (crtl U) and look for any comments in the code that could provide any useful information.

Next step would be to analyse any possible links (remember to always read the link before clicking), in this case, the link you will want to follow is the “update” link. This link may not always be visible to you so zoom in and out of the webpage to see if there are any hidden links, also `CRTL A` to see if any links are high lighted, some links may be hidden in plane sight.

After you have fully analysed the webpage the next step would be to click the link “update”.



enter your username and password, white brother!

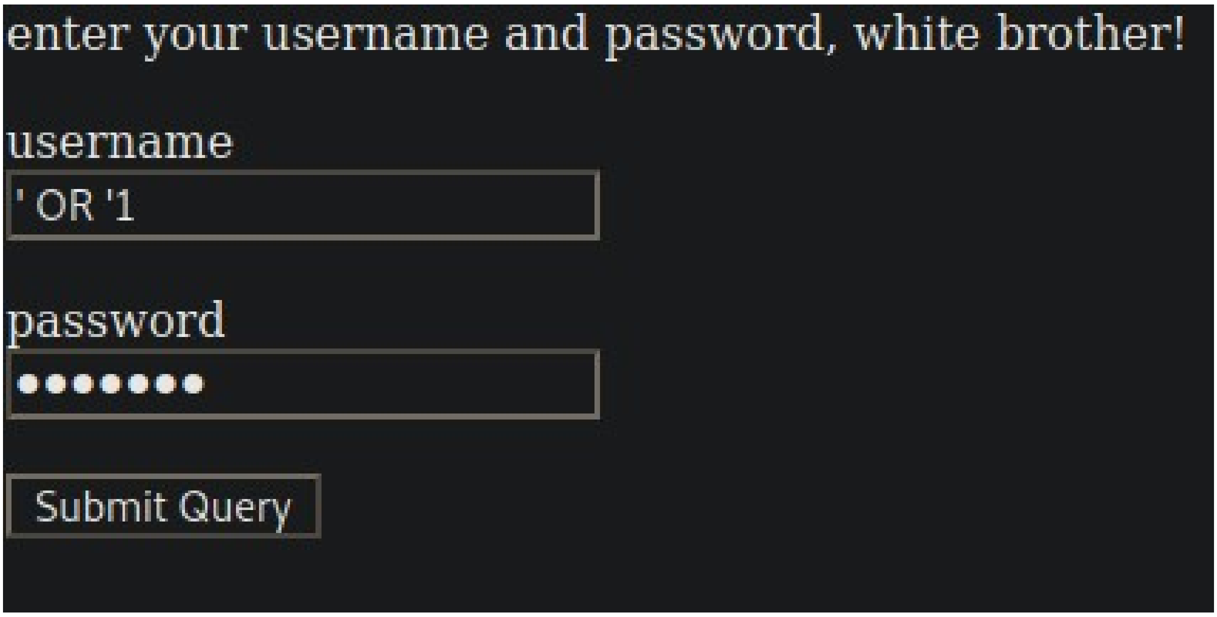
username

password

You will be taken to a second web page which is a login page, however, you do not have any login credentials of any kind so at this point you would be stuck, however remembering that this website has an SQL database we can inject SQL queries into the username and password fields until the correct query is injected and therefore bypassing the login phase with legitimate credentials. SQLi allows the hacker to log into the login field without the correct login credentials, therefore bypassing the login phase.

In this instance, the correct query is >' OR '1<. Other queries >' or '1'='1< basically meaning that if 1 = 1 then the answer is true and the correct condition is returned. SQLi injections are just queries to get a result back from the SQL database.

Result:



enter your username and password, white brother!

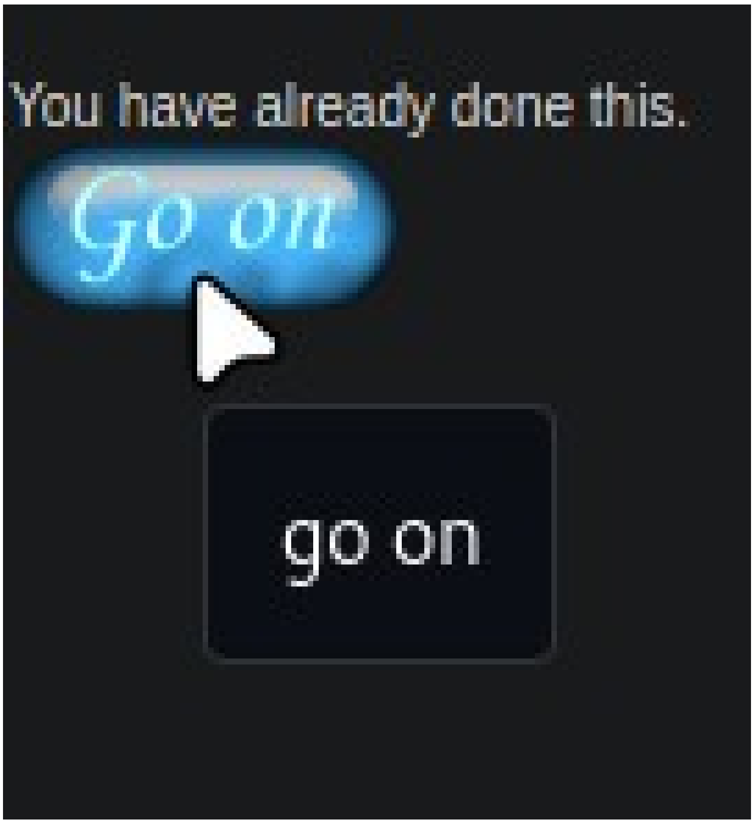
username

' OR '1

password

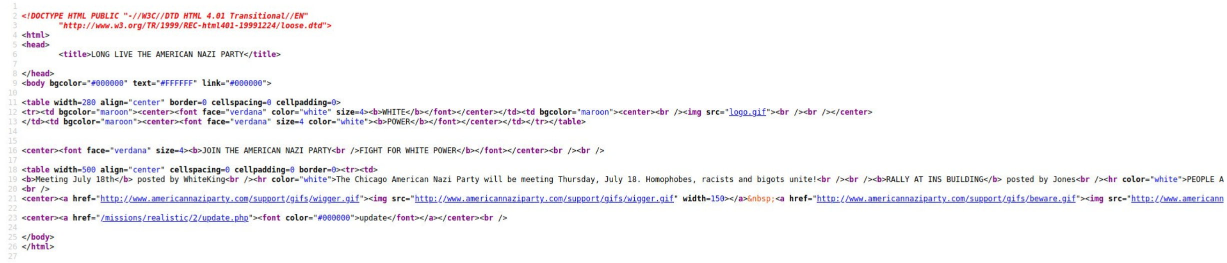
●●●●●●●●

Correct!



You have already done this.

It’s good practise to analyse HTML and Java code.



```

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
        "http://www.w3.org/TR/1999/REC-html401-19991224/loose.dtd">
<html>
<head>
        <title>LONG LIVE THE AMERICAN NAZI PARTY</title>

</head>
<body bgcolor="#000000" text="#FFFFFF" link="#000000">

<table width=280 align="center" border=0 cellspacing=0 cellpadding=0>
<tr><td bgcolor="maroon"><center><font face="verdana" color="white" size=4><b>WHITE</b></font></center></td><td bgcolor="maroon"><center><br /><img src="logo.gif"><br /><br /></center>
</td><td bgcolor="maroon"><center><font face="verdana" size=4 color="white"><b>POWER</b></font></center></td></tr></table>


<center><font face="verdana" size=4><b>JOIN THE AMERICAN NAZI PARTY<br />FIGHT FOR WHITE POWER</b></font></center><br /><br />

<table width=500 align="center" cellspacing=0 cellpadding=0 border=0><tr><td>
<b>Meeting July 18th</b> posted by WhiteKing<br /><hr color="white">The Chicago American Nazi Party will be meeting Thursday, July 18. Homophobes, racists and bigots unite!<br /><br /><b>RALLY AT INS BUILDING</b> posted by Jones<br /><hr color="white">PEOPLE A
<br />
<center><a href="http://www.americannaziparty.com/support/gifs/wigger.gif"><img src="http://www.americannaziparty.com/support/gifs/wigger.gif" width=150></a>&nbsp;<a href="http://www.americannaziparty.com/support/gifs/beware.gif"><img src="http://www.americann

<center><a href="/missions/realistic/2/update.php"><font color="#000000">update</font></a></center><br />

</body>
</html>

```