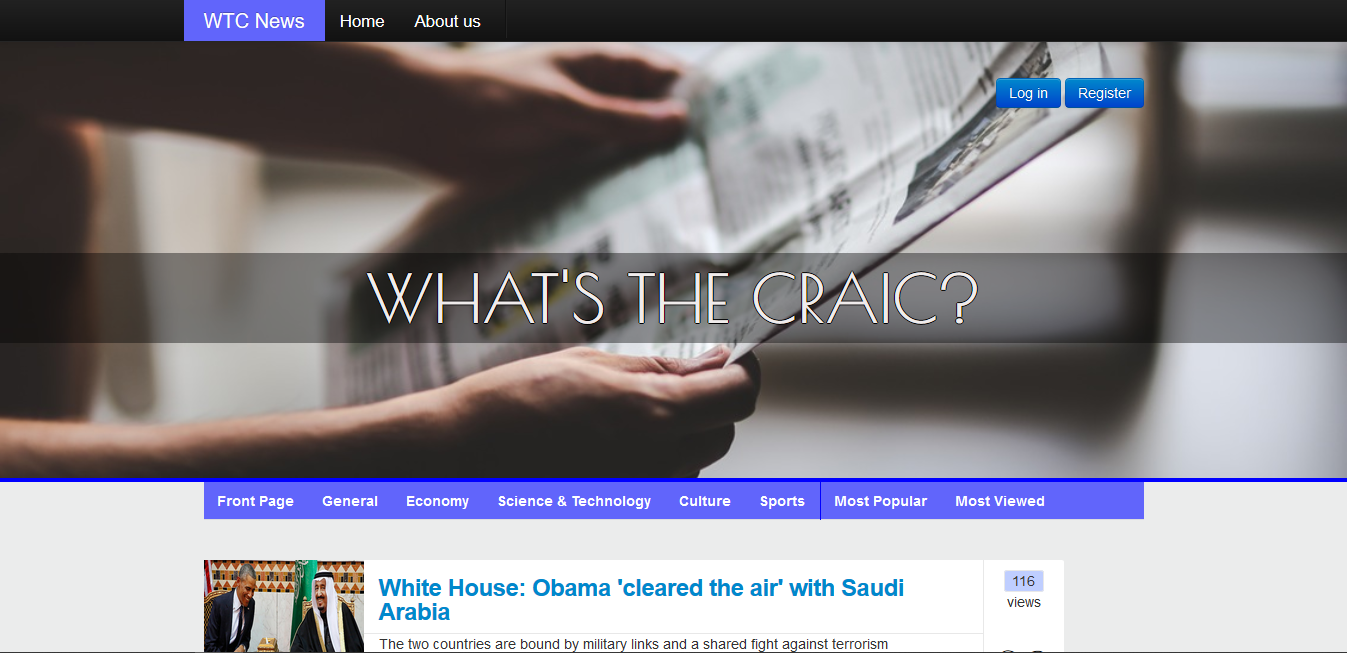
**Application Security CA1**

**Rob Stewart (D00210089) Application Security CA1**

1. The News Article Website as an unregistered visitor is very functional, all tabs and articles are very responsive.

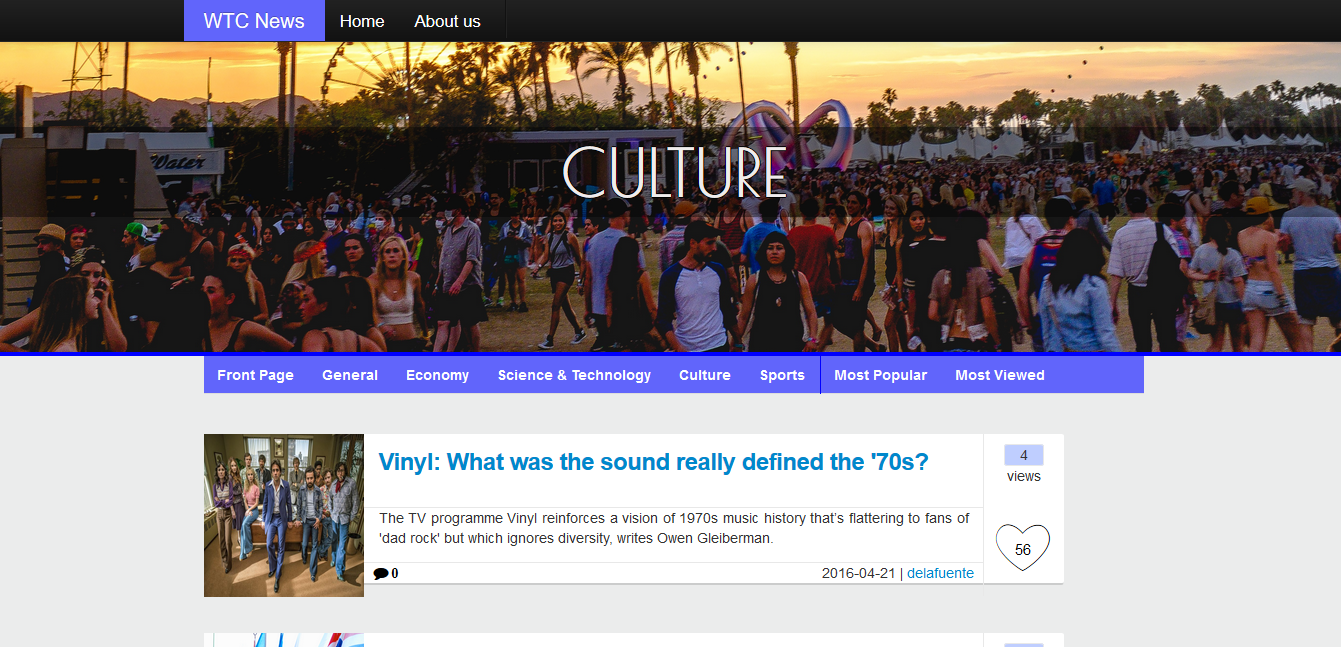
Home Page

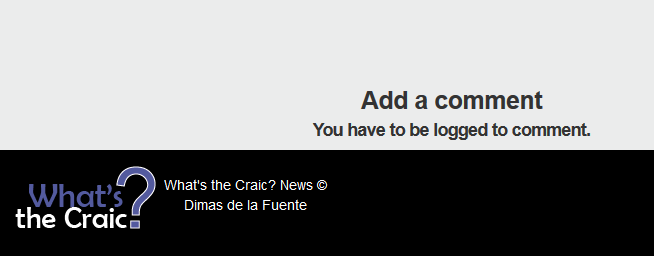


News Article

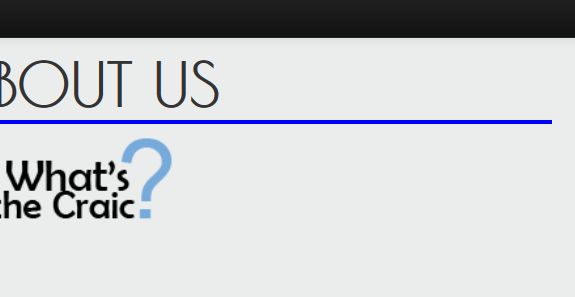
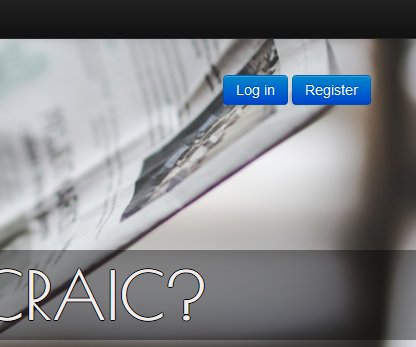


Culture Category

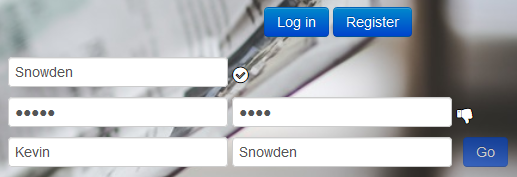


Without registration users are unable to comment. 

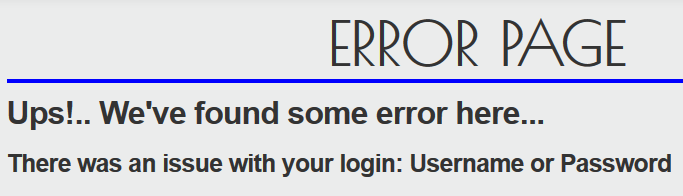
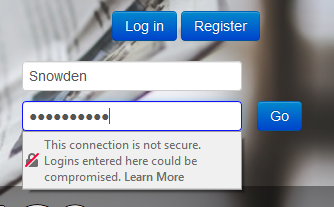
You can only login or register from the home page or one of the links on the navigation bar, the option is unavailable in articles or within the About Us tab.



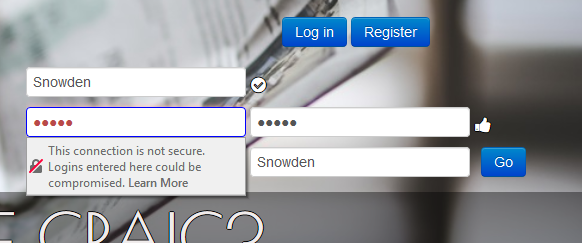
1. When registering the user must make sure both password entries match otherwise the thumbs up will turn upside down. The name fields need to be filled out too.



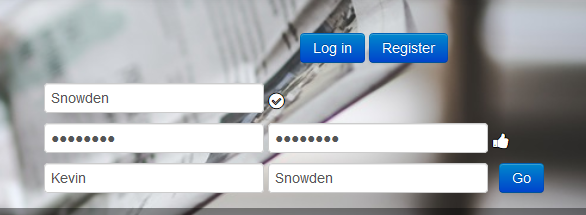
Trying to log in without registering throws this error to the user, it doesn’t reveal if the problem lies with either the username or password, it should never reveal if it’s one or the other, you can easily return home by clicking the home button.



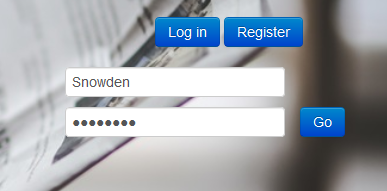
The message cannot be seen because a Firefox error is blocking it, but a message box appears stating that the password must be at least eight characters long, with one uppercase letter and one number.



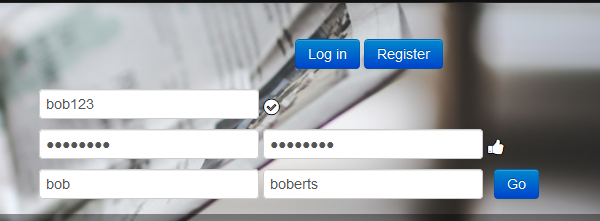
When all requirements are met click on go.



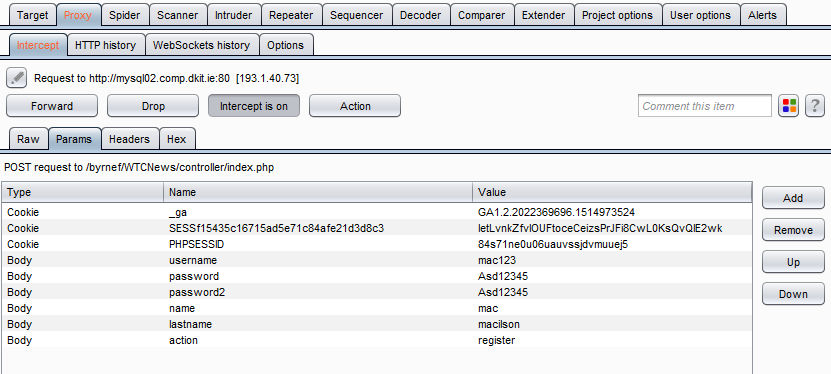
Once registered logging in is very straight forward, make sure to type Username and Password correctly.



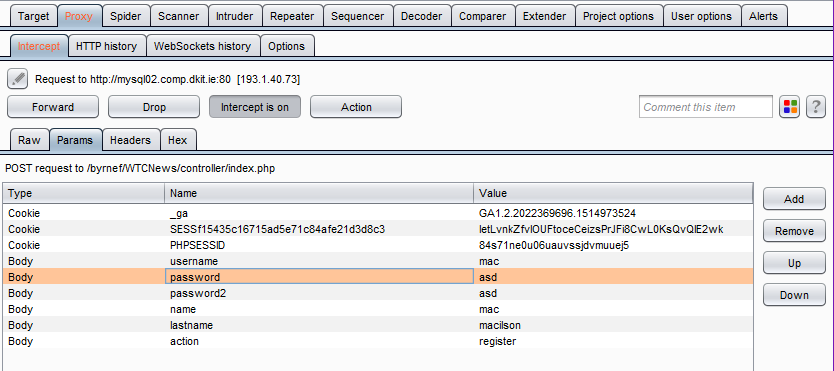
Here I am going to attempt to intercept the registration process and manipulate the registration credentials.



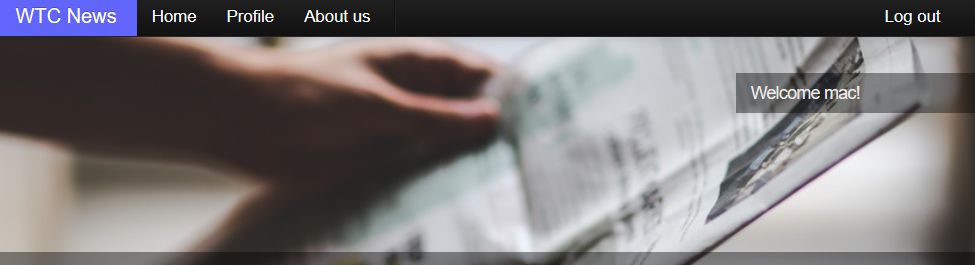
In burp have intercept turned on so the application can takeover for the client machine, with this in effect burp takes the necessary credentials needed from the server side. You can see all the client-side information entered by the user within burp now.



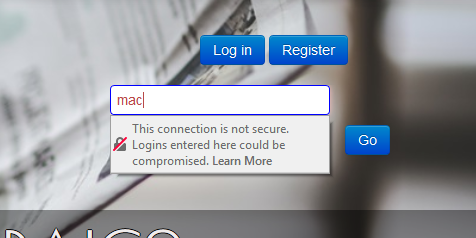
Here with the credentials changed to states that do not match client-side requirements, I am going to force forward it to the server within Burp.



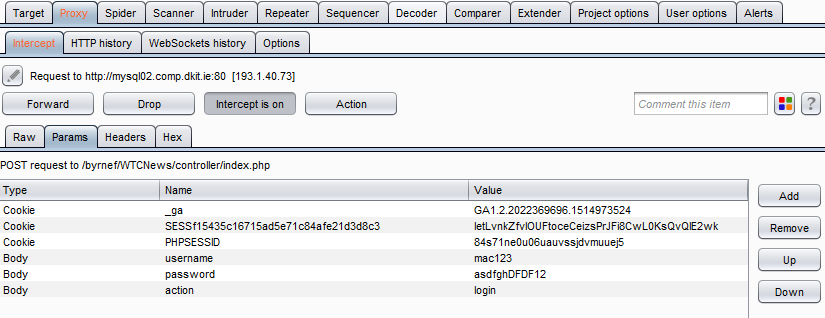
After clicking forward my user account was registered with credentials that do not match what’s required from the client.



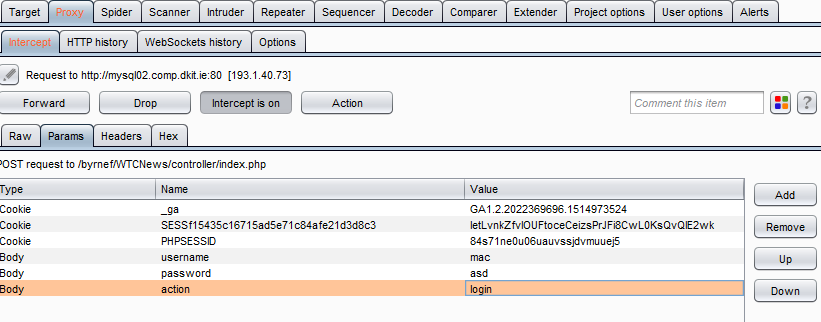
Once logged out the client will not accept the new name and password because the credentials are wrong, the first name and password are no longer valid because they no longer exist.



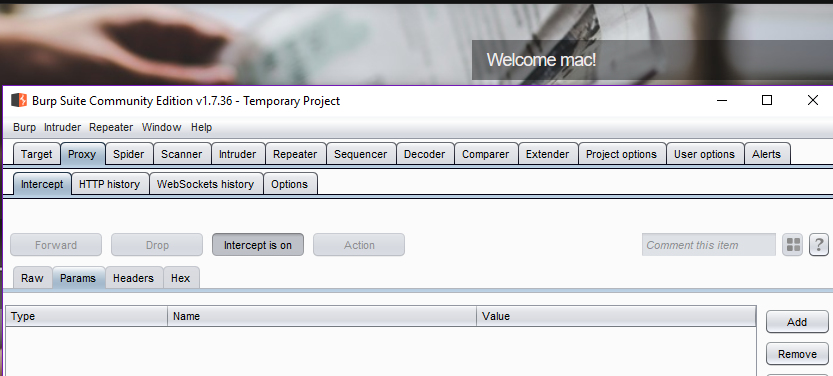
Type in any name and password with the correct credentials.



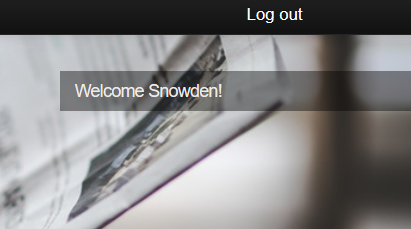
Change the name and password to what they were changed to in Burp previously and click Forward.



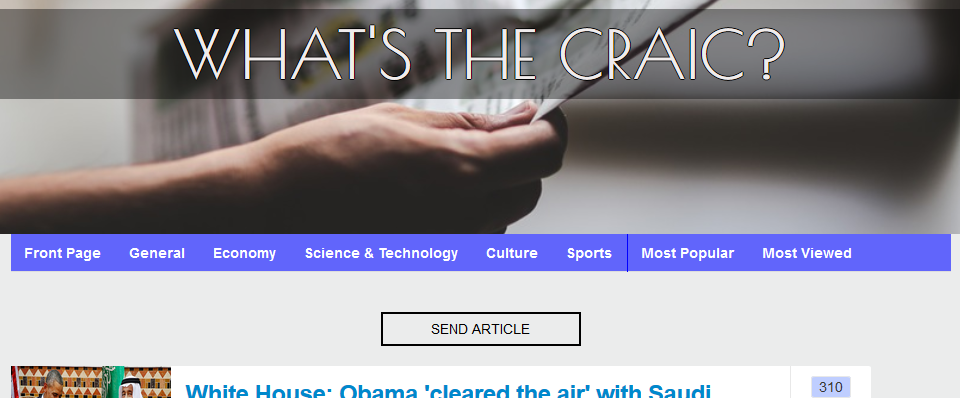
Here I have successfully signed in with the account through Burp with the incorrect credentials.



Once logged in you will receive a welcome message and be given the option to log out in the top of page link bar.



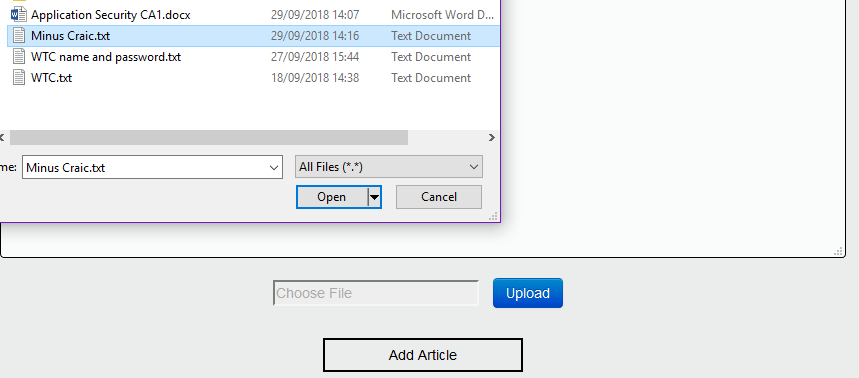
I noticed that there was a send article button that I figure only the administrator should have access to.



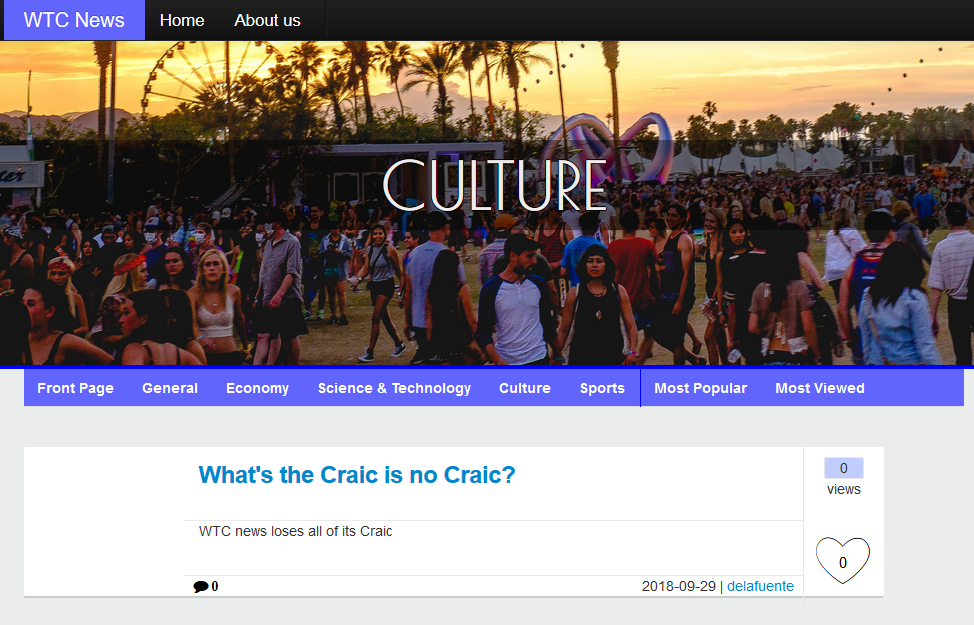
I attempted to add my own article here, bashing the website and putting down its otherwise good name through its own forums.



I tried uploading text files and images with the upload button but it would not allow me to do so, I then clicked the add Article.



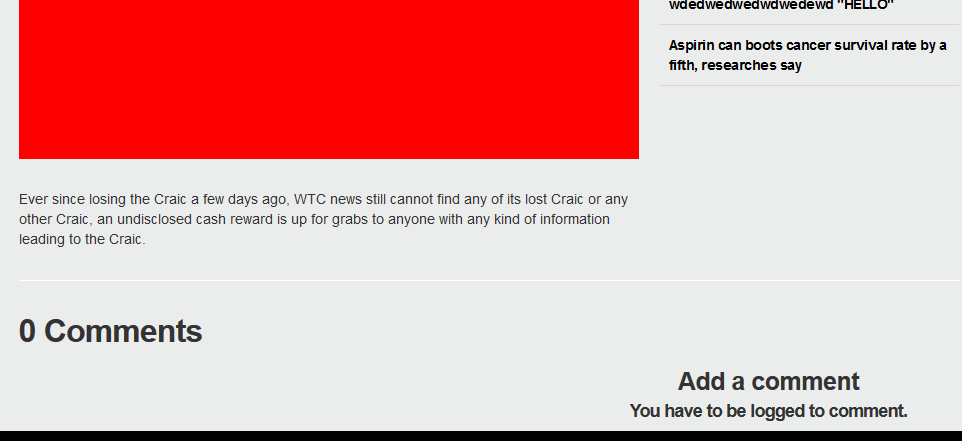
As a user I was allowed to add my own article, I was also automatically logged out once I published it.



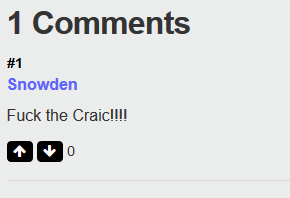
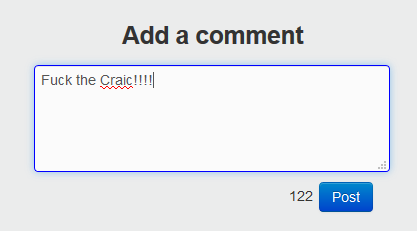
To further test this I added an article to General, it again auto logged me out once I published the article, the only thing I seem to not be allowed to do is publish to the front page and to upload images.



These articles are viewable to unregistered and members who are not logged in. The auto logout once something is published makes sense to a degree, an admin should be able to check that a newly published article is viewable to a site visitor, but its still not very practical as that kind of functionality is assumed these days.

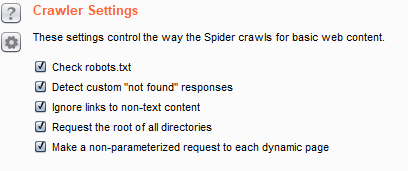


Logged in users can write comments, assuming as a news website that while not aimed at younger viewers it should be assumed that they will visit, as you can see there is no content filter for the use of foul or offensive language.

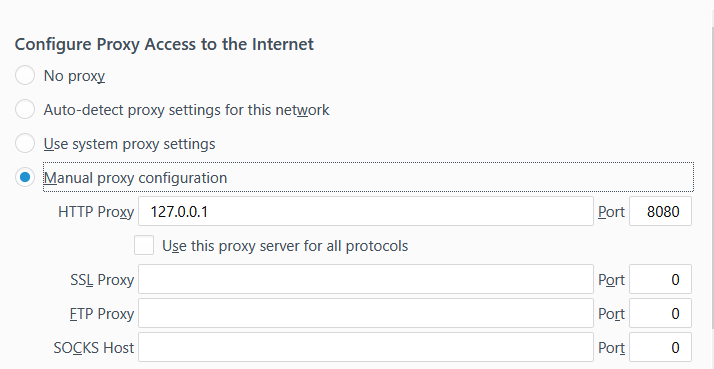


1. The technologies used are HTML, CSS, PHP, Javascript, Jquery and Ajax.
2. The Robots.txt file is a text file that is place on a web server, which specifies parts of a web application that you don’t want search engine crawlers like Googles Googlebot to access. Having this can negatively impact security because it shows hackers which part of an application you don’t want accessed, they also have malware bots that ignore the robots.txt. Robots.txt should not be used to hide information.

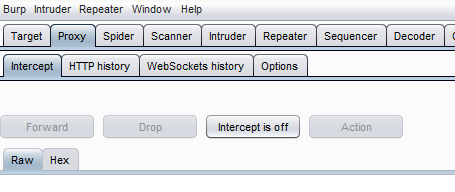
WTC news does not have a robots.txt file in the web root.



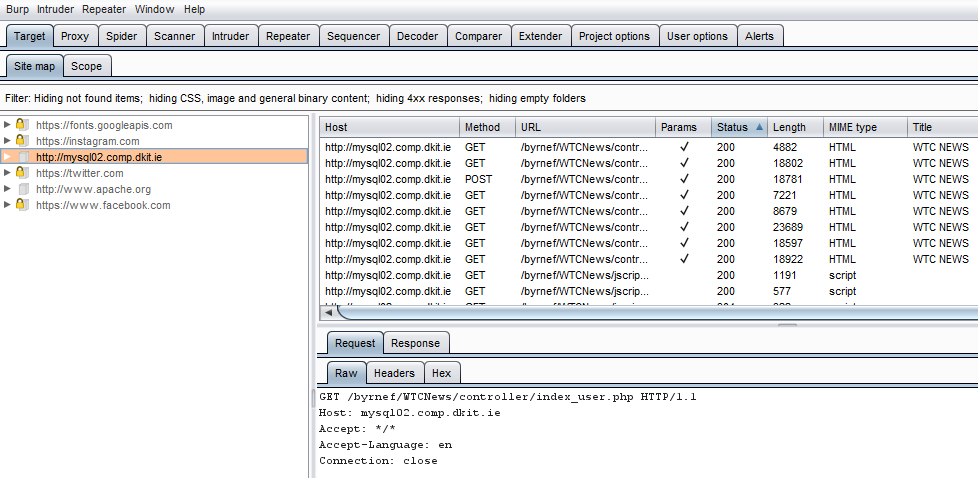
1. Configured my wed browser to use the Burp application as a proxy server.

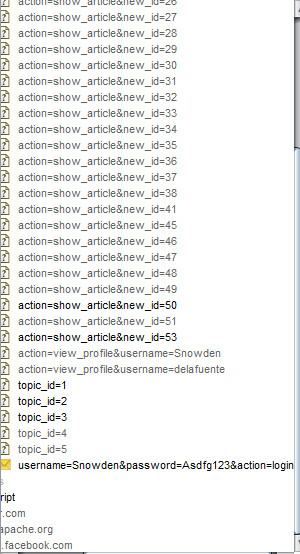
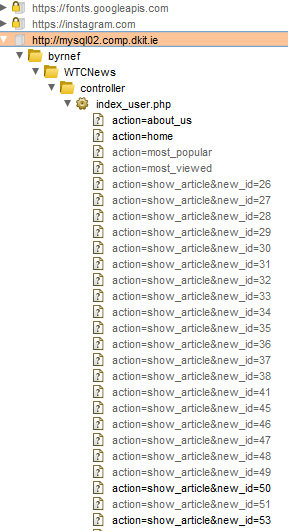


1. (a) Intercepts are turned off

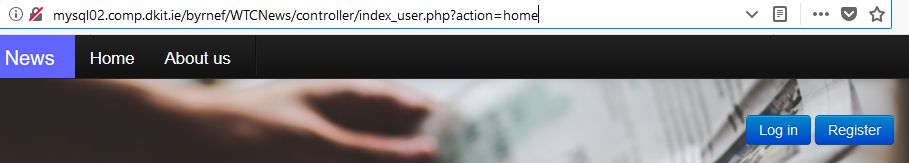


(b)(c)

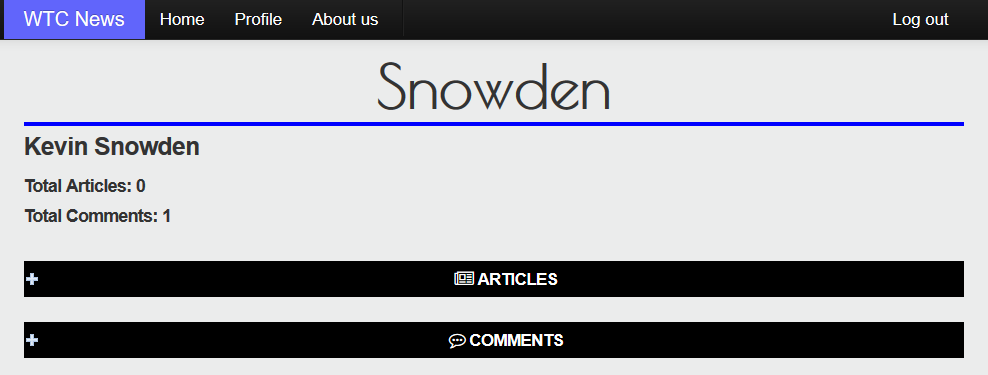
After manually stepping through the website with Burp running it shows my requested items while stepping through, but also shows quite a few items that I have not requested. One of the most alarming bits of information I can take from this is knowing my username and password are stored in plain text. I performed this step through whilst logged out. 



I’ve noticed that I encounter a login error where I’m no longer logged in but the URL informs me that I’m currently here as a user. To fix this I have to delete everything proceeding WTCNews and reload the site, once completed it allows me to login normally.

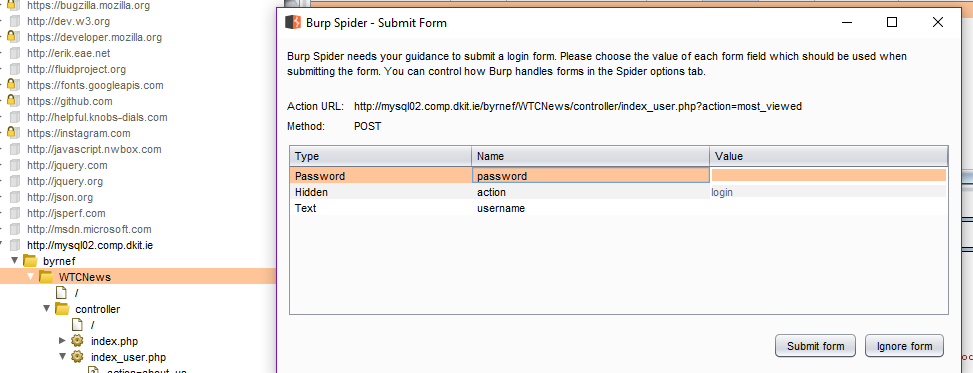


I have also found that the site doesn’t seem to keep a record of the articles I have created on my profile but they do still exist on the site. It does keep a record of my comments.

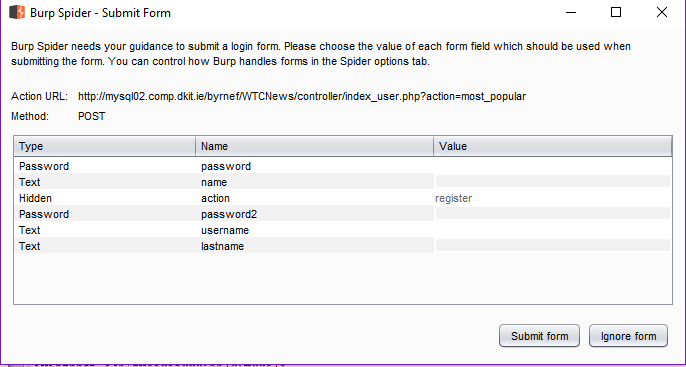


(d)

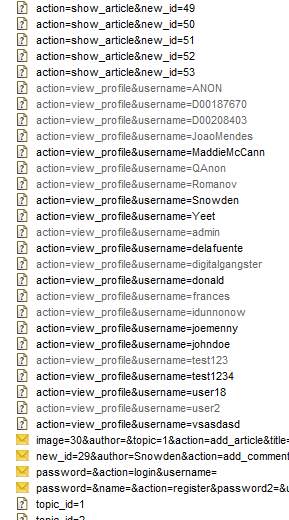
After choosing to spider WTCNews exclusively and click yes to modify to modify the scope, Burp requested my assistance in getting past the login screen by requesting I manually enter my username and password so it can access user.php areas



Clicking submit without filling the fields brings you to the create a new user options. Clicking submit again leaving them blank brings you back to the login options. The ignore form button gives the same result, it loops endlessly through them on repeated clicks. I opted to close this down and not login to see what I can accomplish as a site visitor.

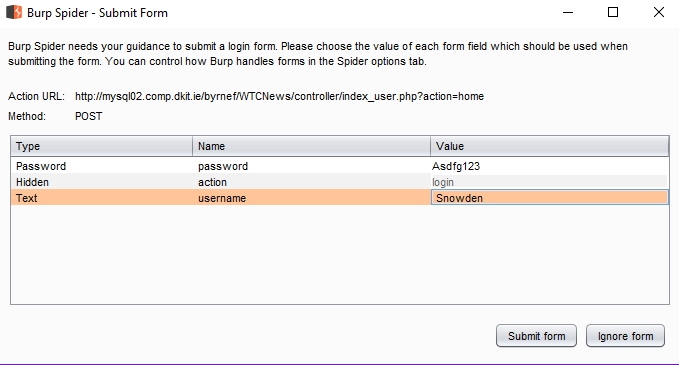


Spidering has revealed the usernames of all who have registered with the site, effectively halving the difficulty of a brute force attack with only the password field left to fill in.

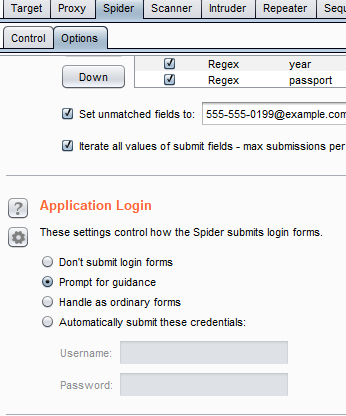


(e)

After searching through and finding new information like the hidden jscript folder, I decided to revisit Burps submit form and enter the correct details.

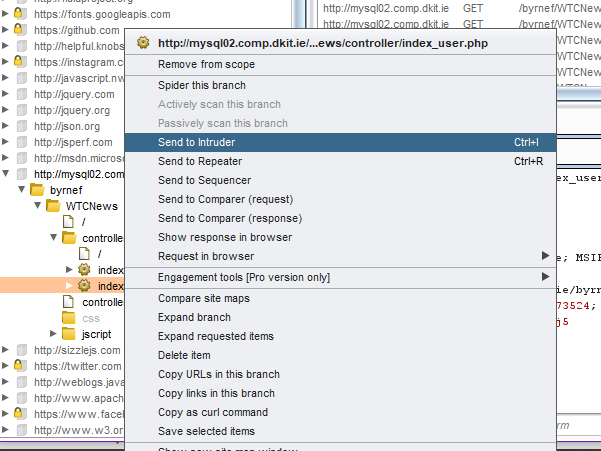


Here you can modify what Burp should automatically send an application when asked for a username and password.

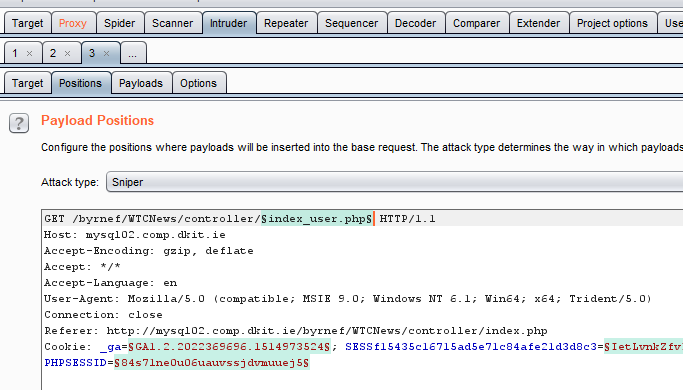


1. While Burps spidering has seemingly successfully visited every area a user can enter both registered and unregistered, all pages and articles are recorded as are the login and signup menus, as well as the create a new article menu though it has not actually created a new article. It doesn’t seem to be able to pick up or interact with any user comments whatsoever but it can identify all members usernames.
2. To access areas closed off to users an attacker should guess the page name based in information already acquired, such as index\_user.php.

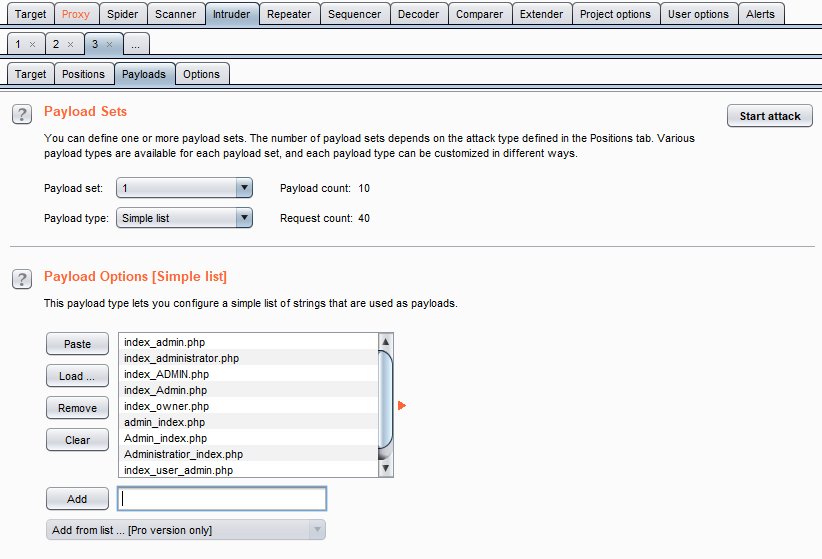
right click on inde\_user.php and send it to the intruder.



Next select the right position to attack



In payloads an attacker needs to enter possible names for other hidden pages and the start the attack.



After initialising the attack, the results show the existing page under status 200, non-existing under 404 and re-directs under 301.

