

WebGoat WebWolf

Twitter: @BlackSheepSpicy

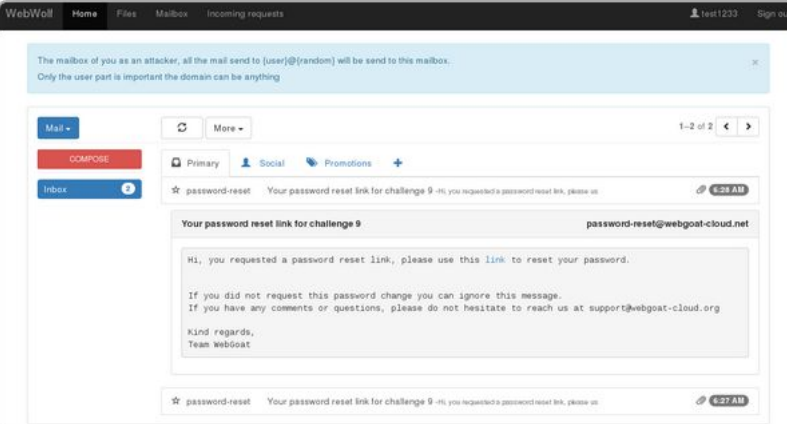
Twitch: <https://twitch.tv/BlackSheepSpicy>

Keep in mind these aren't necessarily challenges, the main focus of them is to get you familiar with webgoat for later challenges. In short WebWolf is a learning tool provided alongside webgoat in order to simulate attacks that use email and can also be used as a file upload server.

3.

Your own mailbox

WebWolf offers a mail client which will contain the e-mail sent during a lesson. This mailbox is user specific so each user has a separate mailbox. All e-mail sent to {user}@.... wil end up in this inbox.

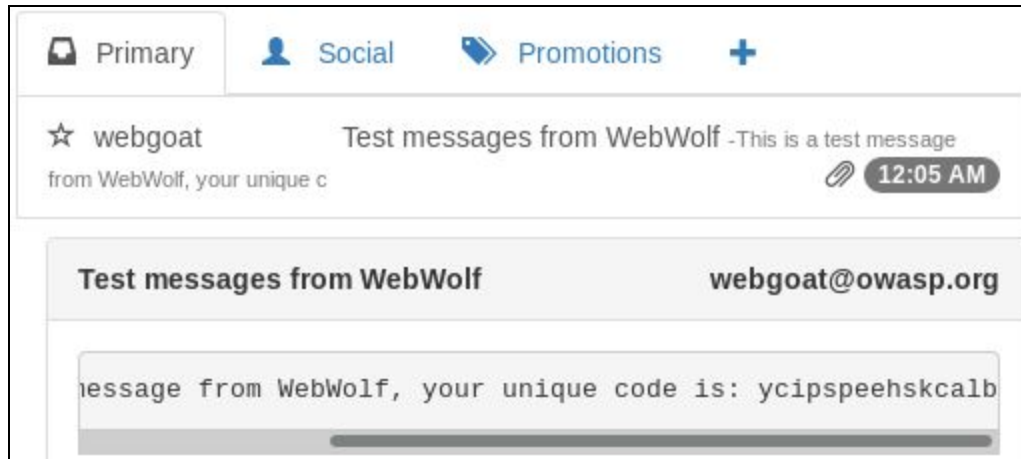


Try it, type in your e-mail address below and check your inbox in WebWolf. Then type in the unique code from the e-mail in the field below.



Biggest thing to note here (aka the one thing that tripped me up) the challenge automatically resolves where the server is so in my case i used the email **blacksheepspicy@localhost**

If all goes according to plan this should pop up in your WebWolf inbox:



Slap that bad boy into the code input back on webgoat for a winner:

Try it, type in your e-mail address below and check your inbox in WebWolf. Then type in the unique code from the e-mail in the field below.

A screenshot of the WebWolf challenge input form. It features two input fields with checkmarks on the left. The first field contains the code 'ycipspeehskcalb' and has a 'Go' button to its right. The second field contains an '@' symbol and the email address 'blacksheepspicy@localhost'. Below these fields is a large blue button labeled 'Send e-mail'. At the bottom of the form, a message reads 'Congratulations. You have successfully completed the assignment.'

4.

Suppose we tricked a user to click on a link he/she received in an email, this link will open up our crafted password reset link page. The user does not notice any differences compared to the normal password reset page of the company. The user enters a new password and hits enter. The new password will be sent to your host. In this case the new password will be sent to WebWolf. Try to locate the unique code.

Please be aware that after resetting the password the user will receive an error page. In a real attack scenario the user would probably see a normal success page (this is due to a limit what we can control with WebWolf)



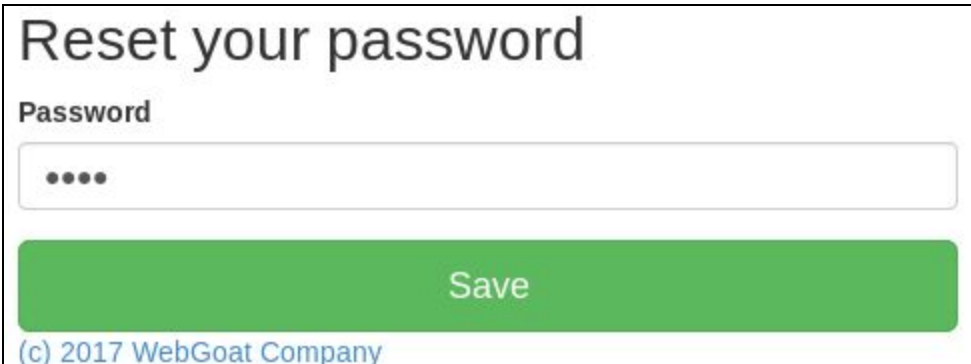
Click here to reset your password

Type in your unique code

Go

The screenshot shows a light gray rectangular box with rounded corners. At the top left, there is a blue hyperlink that says "Click here to reset your password". On the right side of the box, there is a small green checkmark icon and a black silhouette of a wolf's head. Below the link, there is a white input field with the placeholder text "Type in your unique code". To the right of the input field is a blue button with the text "Go" in white.

Alright time to build some character and pwn ourselves by going to that password reset link (don't worry this won't actually reset our password), I used **test** as our password here:



Reset your password

Password

.....

Save

(c) 2017 WebGoat Company

The screenshot shows a white rectangular box with a black border. At the top, the text "Reset your password" is displayed in a large, dark font. Below this, the word "Password" is written in a smaller, bold font. Underneath "Password" is a white input field containing five dots, indicating a masked password. Below the input field is a large green button with the word "Save" in white text. At the bottom left of the box, the text "(c) 2017 WebGoat Company" is written in a small, blue font.




As soon as we hit **save** webgoat will fire a response to our WebWolf page, giving us not only the password we specified but also the unique code needed to complete this challenge:


```
^ Tue Aug 27 00:09:49 EDT 2019 | /landing

{
  "method" : "POST",
  "path" : "/landing",
  "headers" : {
    "request" : {
      "host" : "localhost:9090",
      "user-agent" : "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/57.0",
      "accept" : "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8",
      "accept-language" : "en-US,en;q=0.5",
      "accept-encoding" : "gzip, deflate",
      "referrer" : "http://localhost:8080/WebGoat/WebWolf/landing/password-reset",
      "content-type" : "application/x-www-form-urlencoded",
      "content-length" : "40",
      "cookie" : "WEBWOLFSESSION=AFC3A5EC0E42A164A4925B8D70F12A7D",
      "connection" : "close",
      "upgrade-insecure-requests" : "1",
      "cache-control" : "max-age=0"
    },
    "response" : {
      "X-Application-Context" : "application:9090",
      "status" : "200"
    }
  },
  "parameters" : {
    "uniqueCode" : [ "ycipspeehskalb" ],
    "password" : [ "test" ]
  },
  "timeTaken" : "1"
}
```

Thanks OWASP very unique wow.



[Click here to reset your password](#)



Congratulations. You have successfully completed the assignment.



I hope you enjoyed this write up! If you want to see me do these challenges live be sure to drop by my Twitch when I'm live and also follow my Twitter for some fresh memes!

