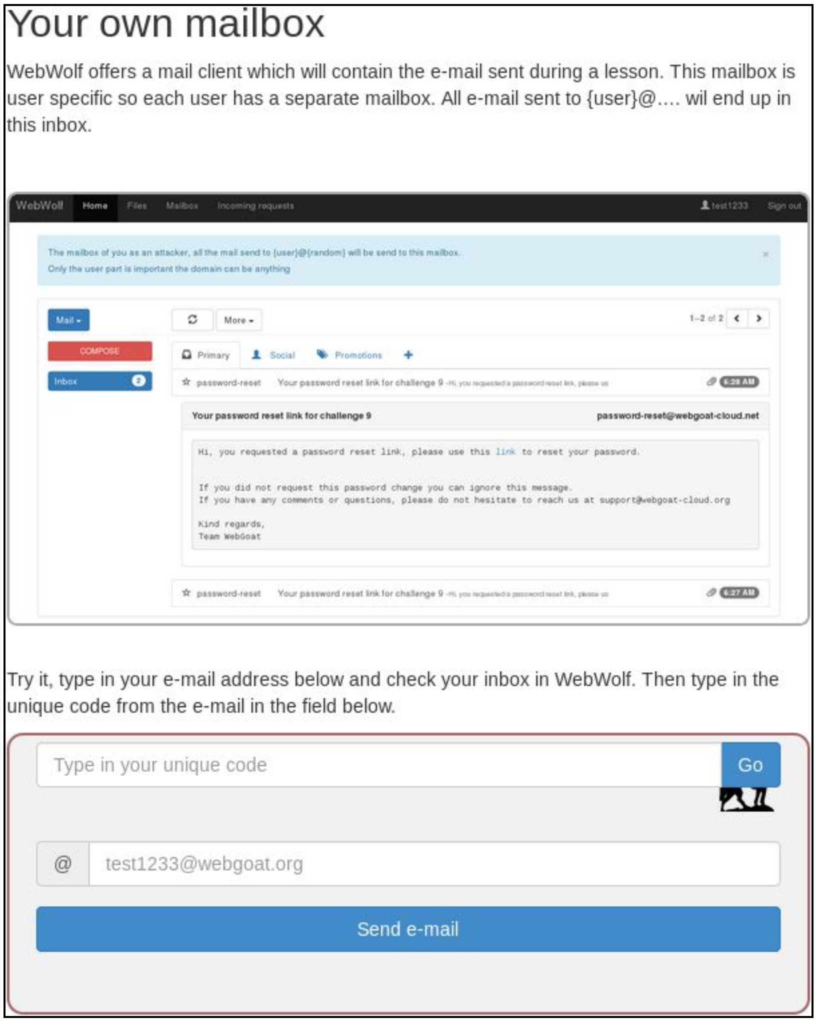
WebGoat WebWolf

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.

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.

The mailbox of you as an attacker, all the mail send to {user}@{random} will be send to this mailbox.
Only the user part is important the domain can be anything

☆ password-reset Your password reset link for challenge 9 -Hi, you requested a password reset link, please us 6:28 AM

Your password reset link for challenge 9 **password-reset@webgoat-cloud.net**

```
Hi, you requested a password reset link, please use this link to reset your password.


If you did not request this password change you can ignore this message.
If you have any comments or questions, please do not hesitate to reach us at support@webgoat-cloud.org

Kind regards,
Team WebGoat
```

☆ password-reset Your password reset link for challenge 9 -Hi, you requested a password reset link, please us 6:27 AM

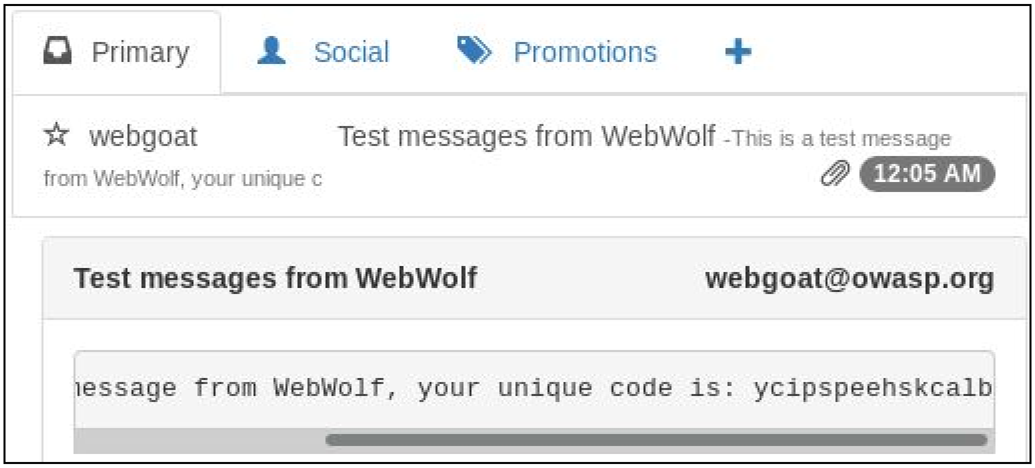
Try it, type in your e-mail address below and check your inbox in WebWolf. Then type in the unique code from the e-mail in the field below.

Type in your unique code

@ test1233@webgoat.org

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:

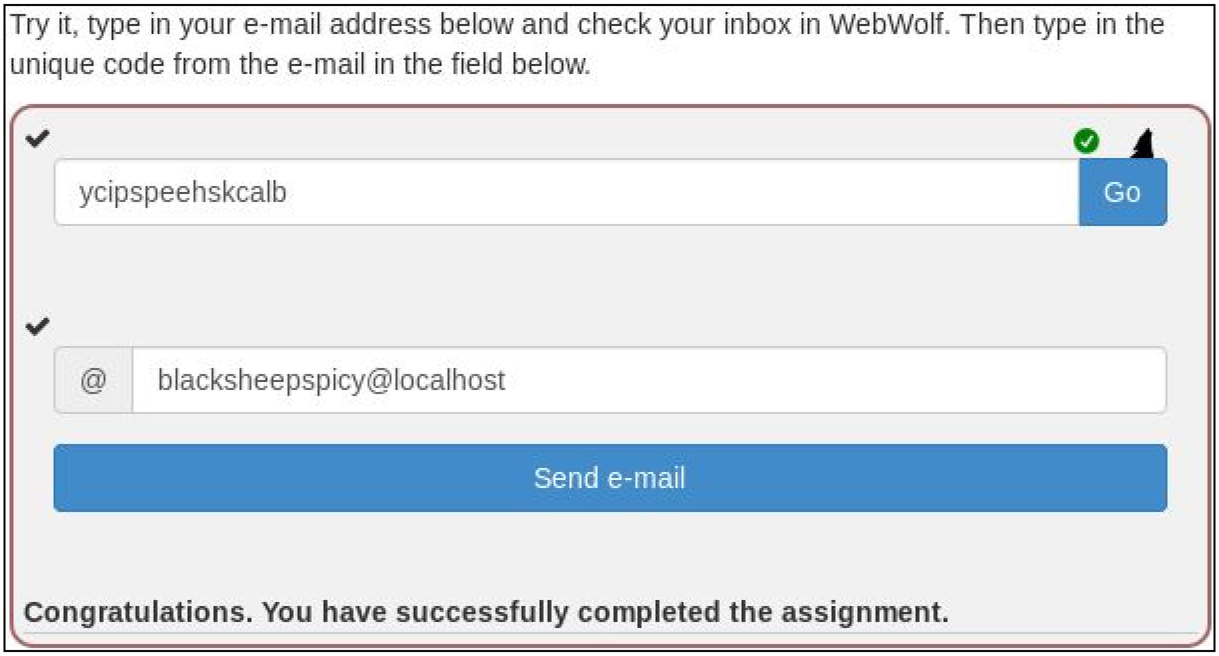


☆ webgoat Test messages from WebWolf -This is a test message from WebWolf, your unique c 12:05 AM

Test messages from WebWolf **webgoat@owasp.org**

```
ıessage from WebWolf, your unique code is: ycipspeehskcalb
```

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.

✓

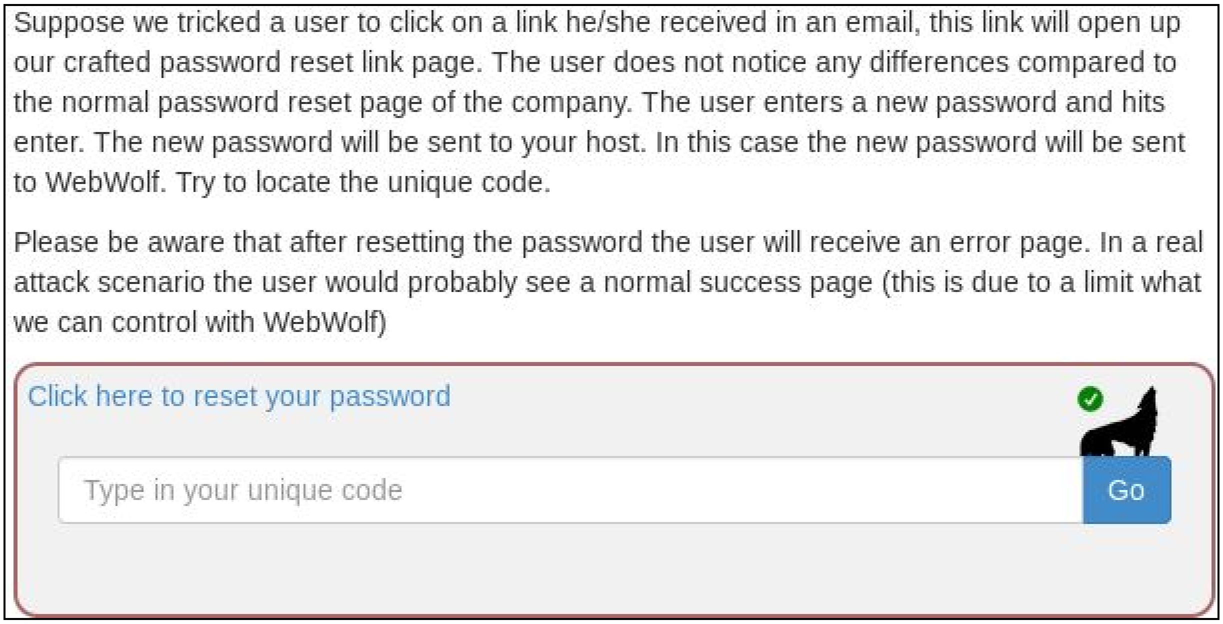
ycipspeehskcalb

✓

@ blacksheepspicy@localhost

Congratulations. You have successfully completed the assignment.

4.

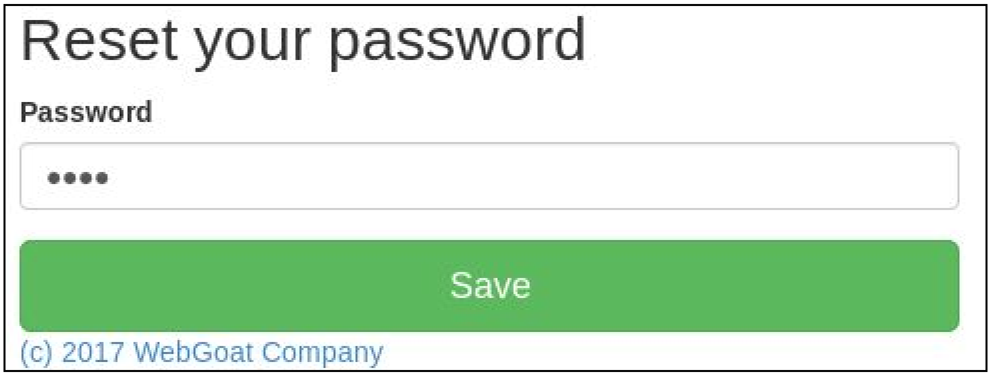


Suppose we tricked a user to click on a link he/she received in an email, this link will open up our crafted password reset link page. The user does not notice any differences compared to the normal password reset page of the company. The user enters a new password and hits enter. The new password will 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

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:



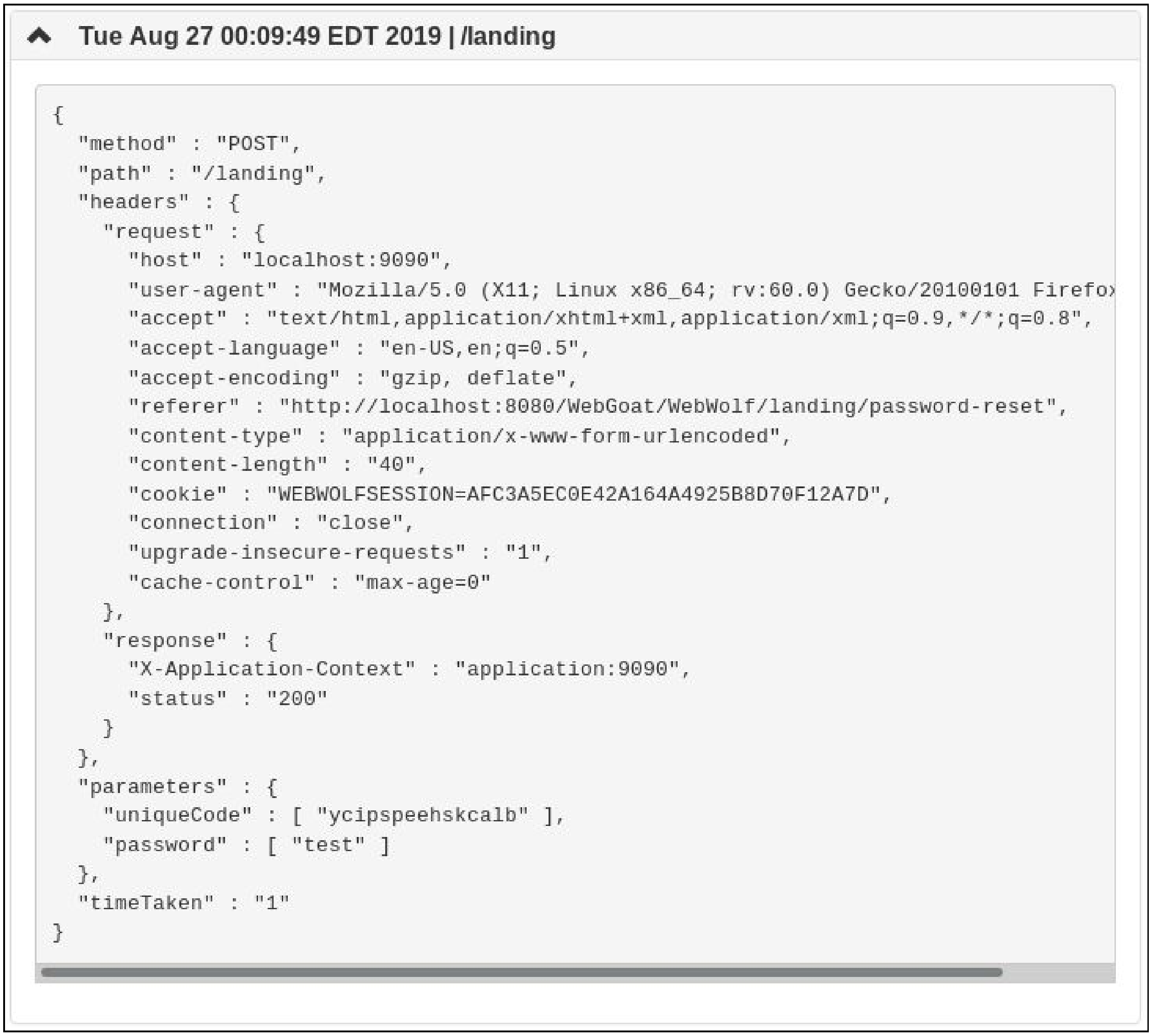
Reset your password

Password

●●●●

(c) 2017 WebGoat Company

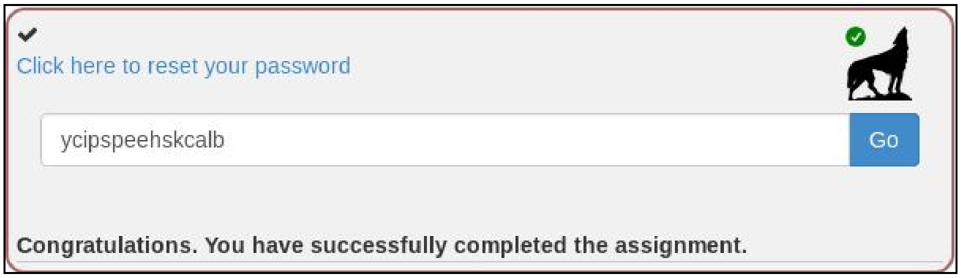
As soon as we hit **save** webgoat will fire a response to our webwolf page, giving us not only the password we specified but also the unique code needed to complete this challenge:



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 Firefo
      "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",
      "referer" : "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" : [ "ycipspeehskcalb" ],
    "password" : [ "test" ]
  },
  "timeTaken" : "1"
}
```

Thanks OWASP very unique wow.



✓

Click here to reset your password

ycipspeehskcalb

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!