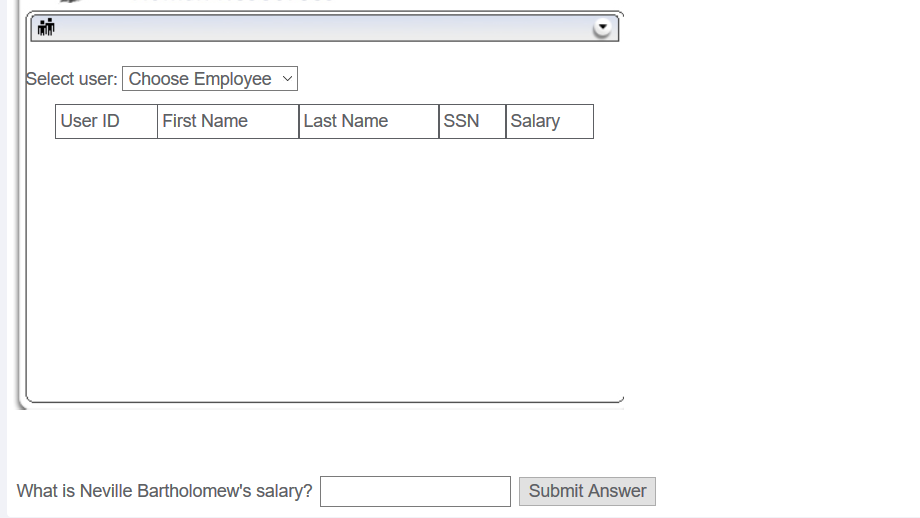
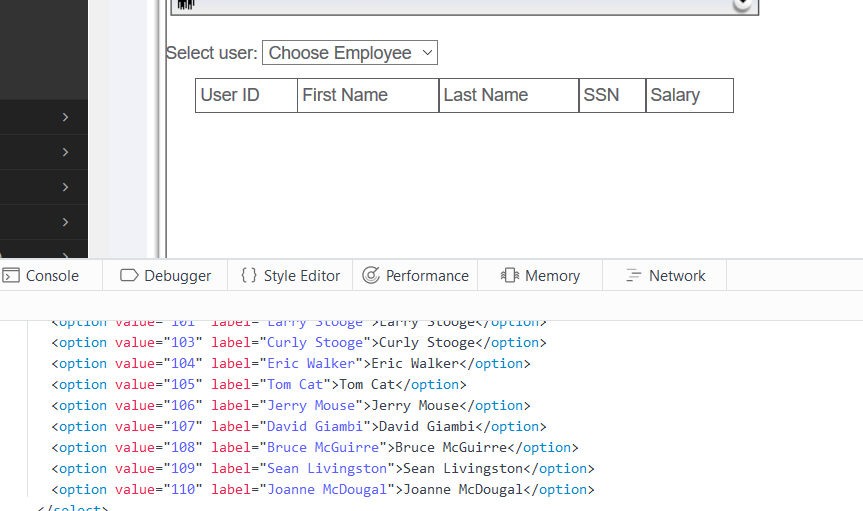
AJAX SECUTIRY

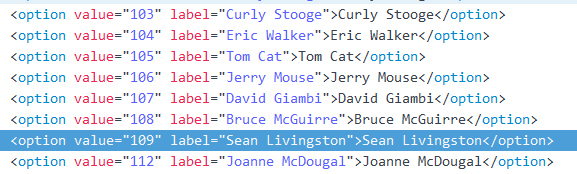
LAB: CLIENT SIDE FILTERING

STAGE 1:

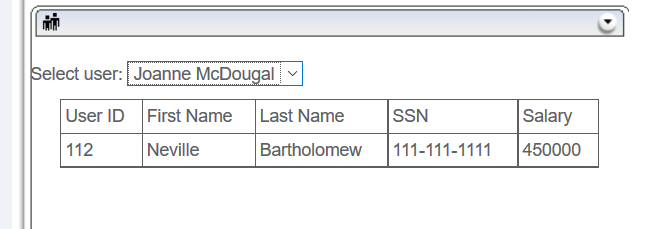


Inspect element thay đổi giá trị value là 112





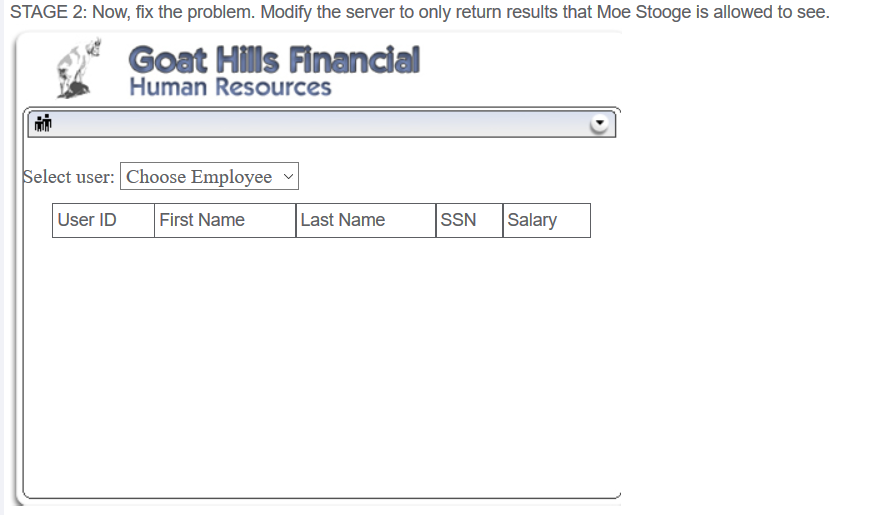
Chọn trong combo box giá trị vừa thay đổi



Nhập vào salary input 450000



STAGE 2:

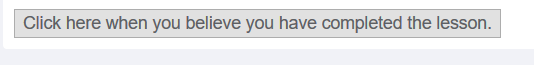


Thay đổi trong file clientSideFiltering.jsp trong project webgoat tìm đến đoạn

StringBuffer sb = new StringBuffer();  
sb.append("/Employees/Employee/UserID | ");  
sb.append("/Employees/Employee/FirstName | ");  
sb.append("/Employees/Employee/LastName | ");  
sb.append("/Employees/Employee/SSN | ");  
sb.append("/Employees/Employee/Salary ");  
String expression = sb.toString();

Thay bằng đoạn code sau:

StringBuffer sb = new StringBuffer();  
sb.append("/Employees/Employee[Managers/Manager/text() = " + userId + "]/UserID | ");  
sb.append("/Employees/Employee[Managers/Manager/text() = " + userId + "]/FirstName | ");  
sb.append("/Employees/Employee[Managers/Manager/text() = " + userId + "]/LastName | ");  
sb.append("/Employees/Employee[Managers/Manager/text() = " + userId + "]/SSN | ");  
sb.append("/Employees/Employee[Managers/Manager/text() = " + userId + "]/Salary ");  
String expression = sb.toString();

Click button 

# LAB: DOM-Based cross-site scripting

# 

# Thêm vào input <IMG SRC="images/logos/owasp.jpg"/> và submit

# STAGE 1:

# 

# STAGE 2:

# 

# Nhập vào input <img src=x onerror=;;alert('XSS') /> submit

# 

# STAGE 3:

# 

# Nhập vào <IFRAME SRC="javascript:alert('XSS');"></IFRAME> submit

# 

# 

# STAGE 4:

# 

# Nhập vào input Please enter your password:<BR><input type = "password" name="pass"/><button onClick="javascript:alert('I have your password: ' + pass.value);">Submit</button><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR> submit

# 

# Nhập vào password kết quả

# 

# STAGE 5:

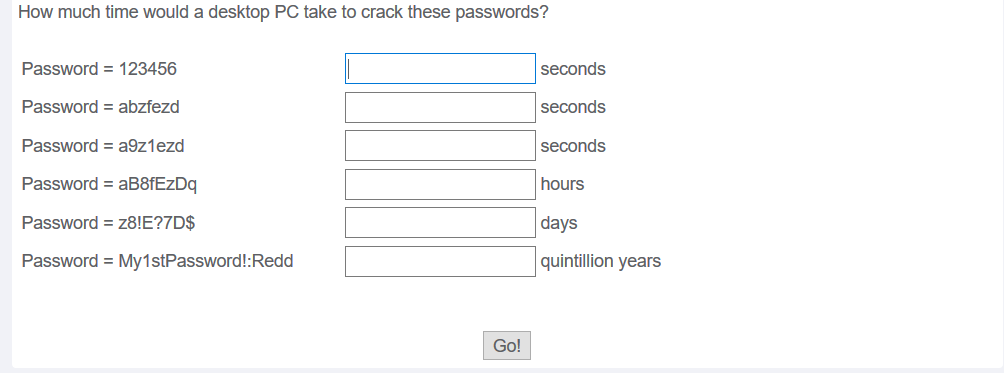
# 

# DOM Injection

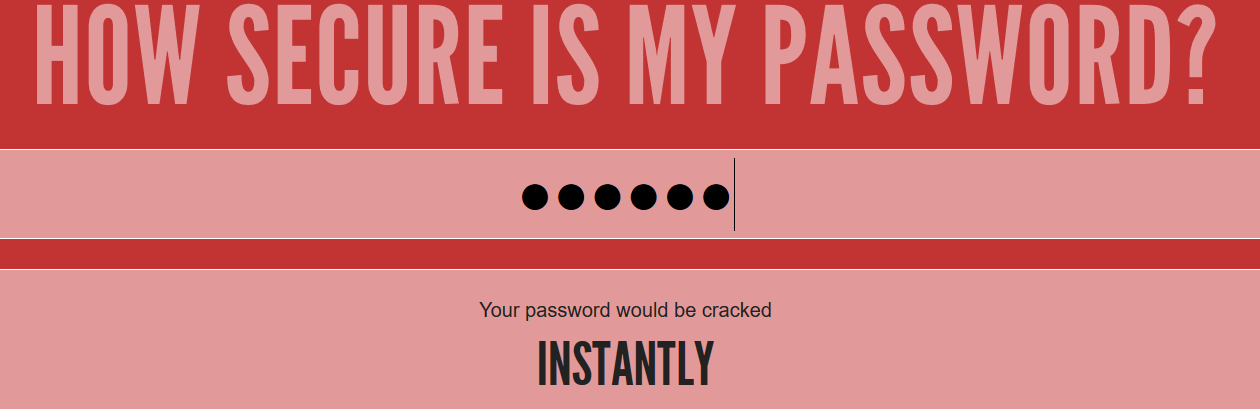
# 

AUTHENTICATION FLAW

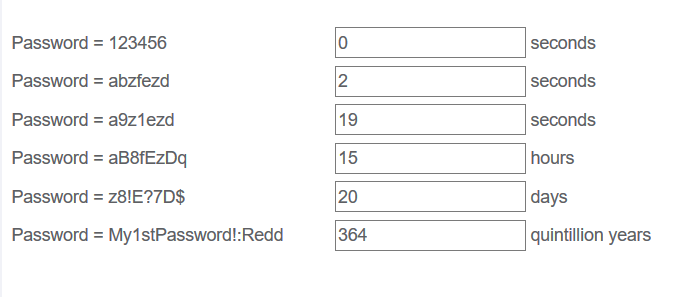
PASSWORD STRENGTH

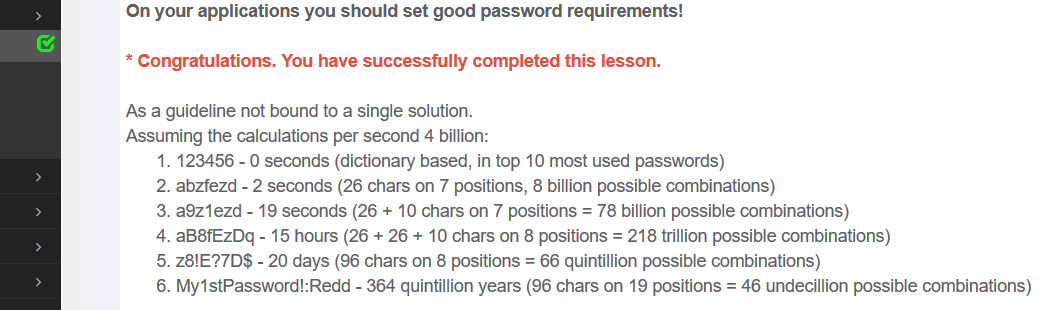


Lên trang web <https://howsecureismypassword.net> điền pass vào input

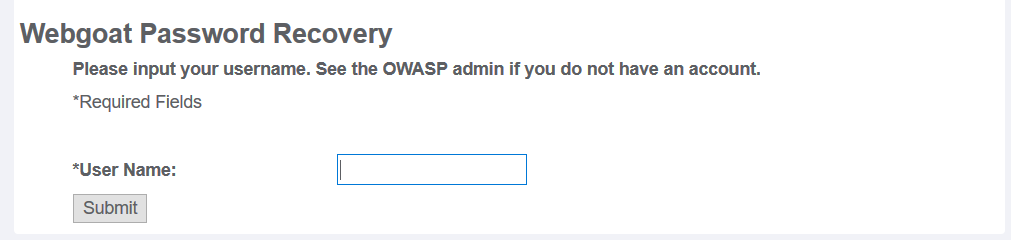


Kết quả:

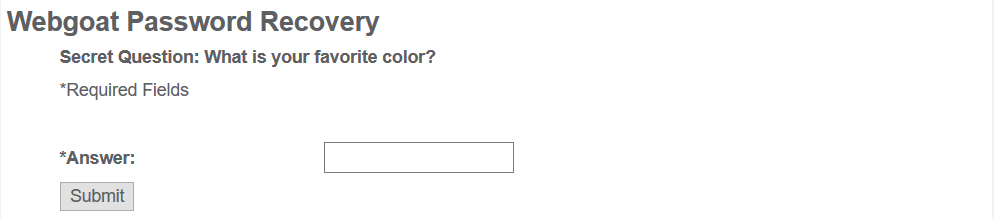




FORGOT PASSWORD



Điền vào username là admin



Câu hỏi bí mật điền vào 3 màu cơ bản red hoặc blue hoặc green

Kết quả là green

