



TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

WEB SECURITY



Content

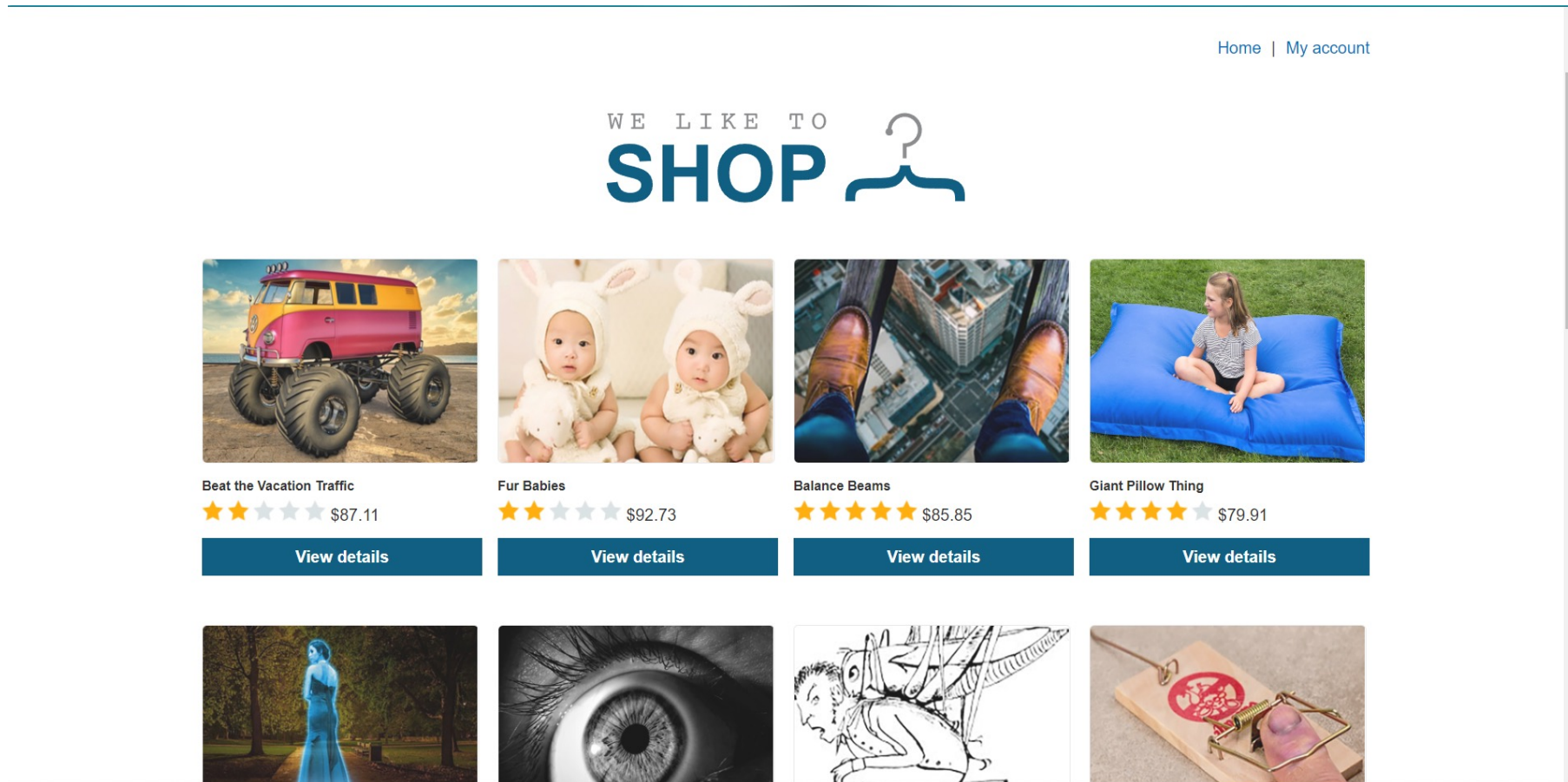
1. SQL Injection
2. XSS

Content

1. SQL Injection
2. XSS

SQL Injection

Eg: Perform an SQL injection attack that logs in to the application as the administrator user.



SQL Injection

Step 1: Open Devtools → Network to intercept http request, then try login with username is **administrator** and password is anything.

👉 We can see the browser send a http request with payload have 2 fields that we just enters.



SQL injection vulnerability allowing login bypass

[Back to lab description >>](#)

LAB Not solved

[Home](#) | [My account](#)

Login

Invalid username or password.

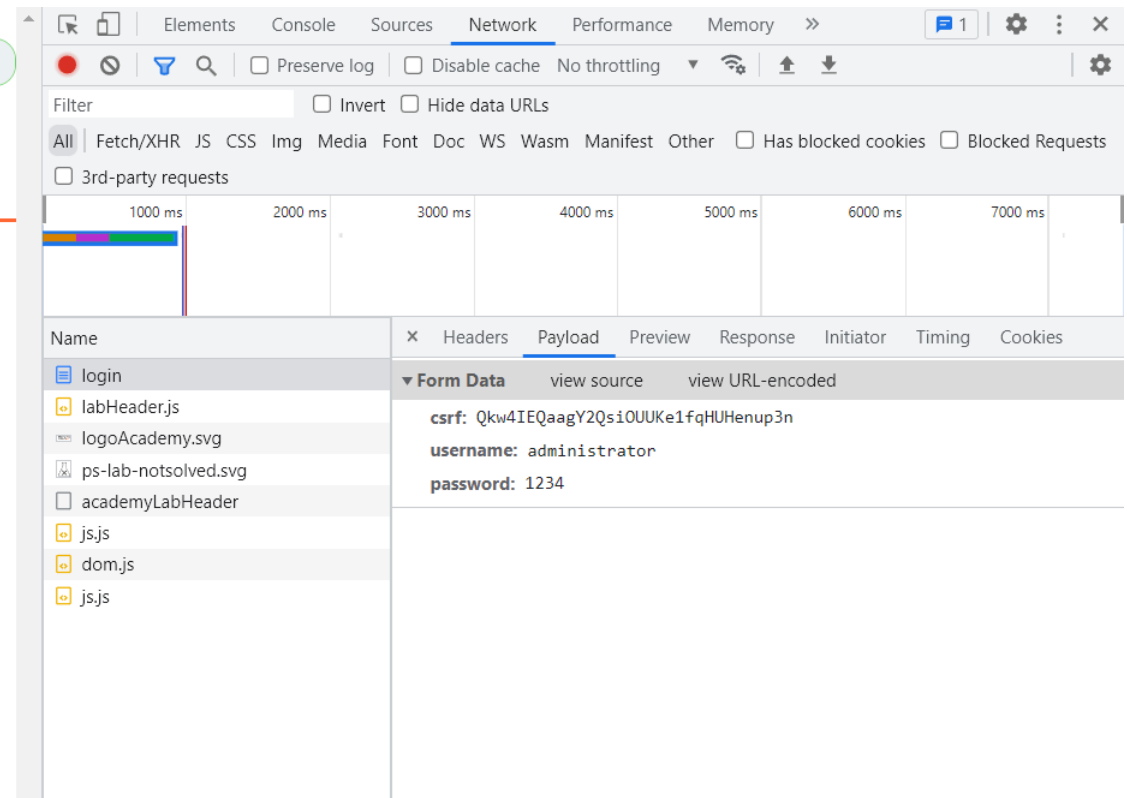
Username

administrator

Password


....

Log in



SQL Injection

Step 2: From http request, we can guess that SQL query will be like:



```
1 SELECT * FROM USER WHERE username='administrator' AND password='1234'
```

Step 3: So if we enter username with value `administrator' --` the query will be like:



```
1 SELECT * FROM USER WHERE username='administrator' -- 'and password='1234'
```




👉 In SQL, after “--” is comment so the query will select the account with username is `administrator` without any password

SQL Injection

Step 4: We can test our predictions:


Web Security Academy 

SQL injection vulnerability allowing login bypass

LAB Solved 

Back to lab description >>

Congratulations, you solved the lab!

 Share your skills!

Continue learning >>

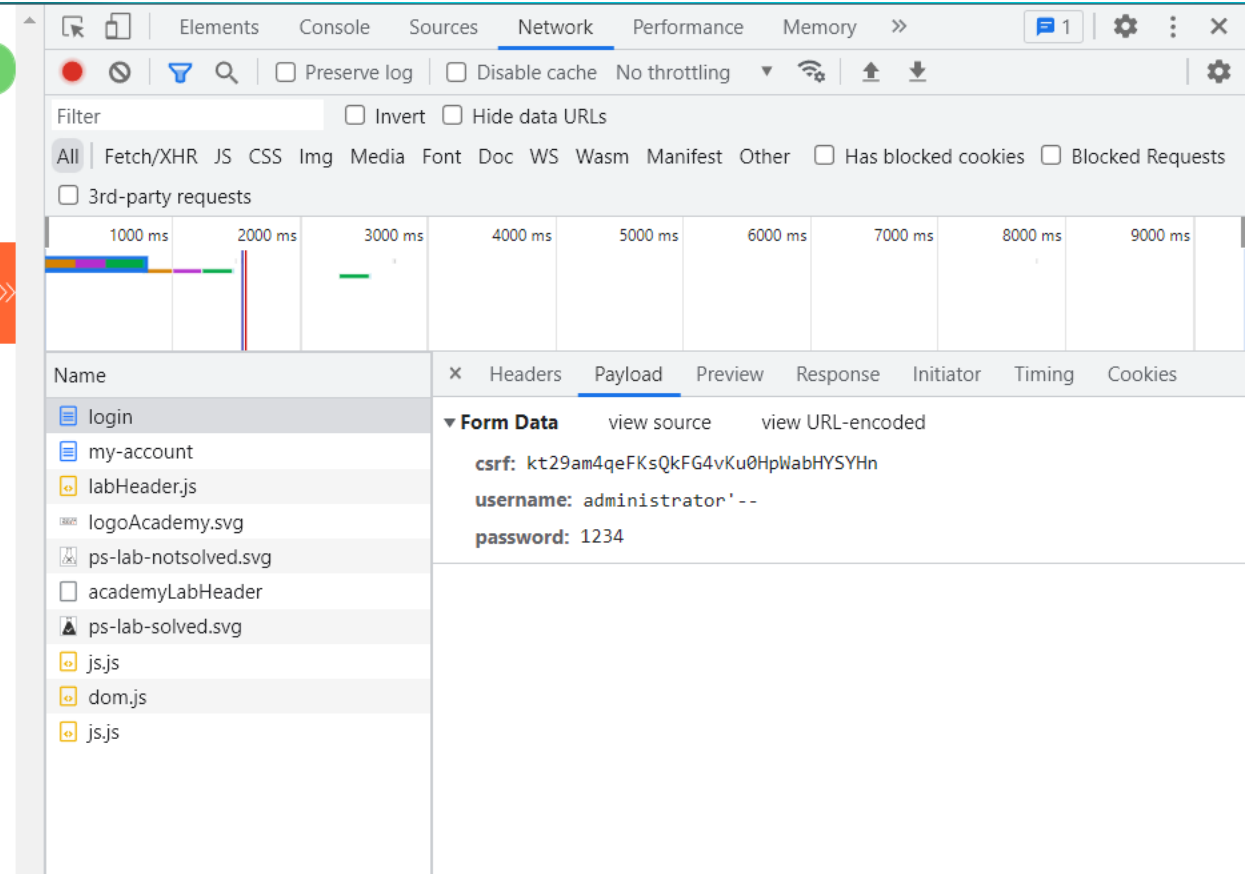
Home | My account | Log out

My Account

Your username is: administrator

Email

Update email



The screenshot shows the Network tab of a web browser. The filter is set to 'All'. The list of requests includes 'login', 'my-account', 'labHeader.js', 'logoAcademy.svg', 'ps-lab-notsolved.svg', 'academyLabHeader', 'ps-lab-solved.svg', 'js.js', 'dom.js', and 'js.js'. The 'login' request is selected, and the 'Payload' tab is active. The form data shows the following values:

Field	Value
csrf	kt29am4qeFKsQkFG4vKu0HpWabHYSYHn
username	administrator'--
password	1234

Content

1. SQL Injection
2. XSS

Eg: This sites contains a stored cross-site scripting vulnerability in the comment functionality. We will submit a comment that calls the alert function when the blog post is viewed.

Step 1: We will try to submit a comment:

Comments

 Harry Legs | 05 December 2022

How long does it take to write stuff like this?

Leave a comment

Comment:

This post is awesome

Name:

ducnm

Email:

ducnm@gmail.com

Website:

Post Comment

Step 2: After submit, we reload the post and see our new comment, we can use Devtools → Elements to see our comment in raw HTML:

The image shows a web application interface on the left and a Chrome DevTools window on the right. The web application displays a comment by 'Harry Legs' from December 5, 2022, with the text 'How long does it take to write stuff like this?'. Below it is a comment by 'ducnm' from December 27, 2022, with the text 'This post is awesome'. A tooltip for the comment shows its dimensions (668 x 71.8) and styling (color #333332, font 16px Arial, Helvetica Neue, Helvetica, sans-serif, margin 16px 0px, padding 16px 0px 0px 16px). The DevTools window shows the 'Elements' panel with the raw HTML of the comment. The comment is contained within a `<div class='comment'>` block, which contains a `<p>` element with the text 'This post is awesome'. The `<p>` element is highlighted with a green box. The 'Styles' panel on the right shows the default styling for the `p` element, including display, margin, and font properties. A blue arrow points from the `<p>` element in the HTML to a callout box on the right.

Comments

Harry Legs | 05 December 2022
How long does it take to write stuff like this?

ducnm | 27 December 2022
This post is awesome

section.comment 668 x 71.8
Color #333332
Font 16px Arial, "Helvetica Neue", Helvetica, s...
Margin 16px 0px
Padding 16px 0px 0px 16px
ACCESSIBILITY
Name
Role
Keyboard-focusable

Name:

Email:

Website:

Elements Console Sources Network Performance Memory

```
<!DOCTYPE html>
<html>
<head>...</head>
<body>
  <script src="/resources/labheader/js/labHeader.js"></script>
  <div id="academyLabHeader">
    <section class="academyLabBanner">...</section>
  </div>
  <div theme="blog">
    <section class="maincontainer">
      <div class="container is-page">
        <header class="navigation-header">...</header>
        <header class="notification-header"> </header>
        <div class="blog-post">
          
          <h1>Hobbies</h1>
          <p>...</p>
          <hr>
          <p>...</p>
          <p>...</p>
          <p>...</p>
          <p>...</p>
          <p>...</p>
          <p>...</p>
          <div>
            <hr>
            <h1>Comments</h1>
            <section class="comment">...</section>
            <section class="comment">
              <p>...</p>
              <p>This post is awesome</p>
            </section>
            <section class="add-comment">...</section>
            <div class="is-linkback">...</div>
          </div>
        </div>
      </div>
    </section>
  </div>
</body>
</html>
```

Styles Computed Layout

Filter: show .cls +

element.style {
}

p { labsBlog.css:581
margin: 0 0 10px;
}

*, *:before, labsBlog.css:432
*:after {
-moz-box-sizing: border-box;
-webkit-box-sizing: border-box;
box-sizing: border-box;
}

p { user agent stylesheet
display: block;
margin-block-start: 1em;
margin-block-end: 1em;
margin-inline-start: 0px;
margin-inline-end: 0px;
}

Inherited from body
body { labsBlog.css:569
background: #fff
!important;
color: #333332;
font-size: 16px;
-webkit-font-smoothing: antialiased;
-moz-osx-font-smoothing: grayscale;
font-family: Arial, "Helvetica Neue", Helvetica, sans-serif;
line-height: 1.4;
overflow-wrap: break-word;
word-wrap: break-word;
}

Inherited from html
:root { labsBlog.css:25
--text-base-size: 1em;
--text-scale-ratio: 1.1;
--text-xs: calc(1em / (var(--text-scale-ratio) * 1.1));
}

1 <p>This post is awesome</p>

Step 3: We can guess that the database store comments in raw text, so if we comment a script tag, it will trigger when any user open the post, like this:



```
1 <script> /** bad stuff... </script>
```

XSS

Step 4: We will try our predictions to comment a script which will alert 1 when any user open the post:



Leave a comment

Comment:

`<script>alert(1)</script>`

Name:

hacker

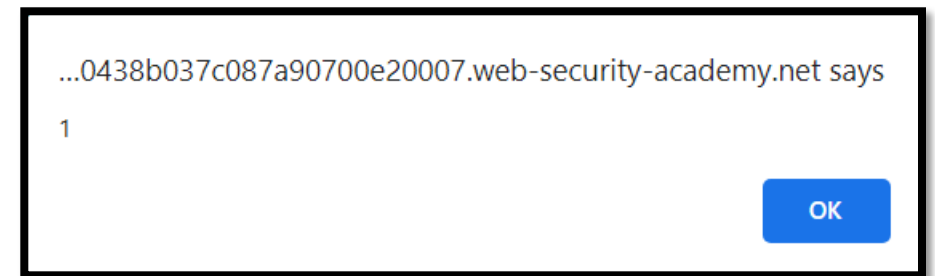
Email:

evil@gmail.com

Website:

Post Comment

👉 After submit, when back to blog post, we will see an alert



XSS

With the Devtools, we can see raw HTML:

The image shows a Chrome DevTools interface with the 'Elements' panel on the left and a web page on the right. The 'Elements' panel displays the DOM tree of a comment section. A comment with the text 'This post is awesome' is selected, and its raw HTML is shown in the 'Elements' panel. A green box highlights the following HTML snippet:

```
<p>  
<script>alert(1)</script>  
</p>
```

The 'Styles' panel on the right shows the default styles for the selected paragraph element. The web page on the right shows a comment form with the text 'This post is awesome' and a 'Post Comment' button. A blue box highlights the raw HTML snippet from the 'Elements' panel, showing the injected script:

```
1 <p>  
2   <script> alert(1) </script>  
3 </p>
```

Exercise

? Lab 01: Retrieve hidden data

This lab contains an SQL injection vulnerability in the product category filter. You must perform an SQL injection attack that causes the application to display details of all products in any category, both released and unreleased.

Exercise

? Lab 02: Determine the number of columns

This lab contains an SQL injection vulnerability in the product category filter. You must determine the number of columns returned by the query by performing an SQL injection UNION attack that returns an additional row containing null values.

Exercise

? Lab 03: Reflected XSS into attribute with angle brackets HTML-encoded

This lab contains a reflected cross-site scripting vulnerability in the search blog functionality where angle brackets are HTML-encoded. You must perform a cross-site scripting attack that injects an attribute and calls the alert function.

Excercise

? **Lab 04:** Stored XSS into anchor href attribute with double quotes HTML-encoded

This lab contains a stored cross-site scripting vulnerability in the comment functionality. You must submit a comment that calls the alert function when the comment author name is clicked.

