



XSS ATTACK LAB REPORT

WEB SECURITY

Lecturer: Hoang Xuan Dau

Student: Nguyen Khang Ninh

Class: Cyber Security

Student ID: BI12-341

1- Stored XSS

Leave a comment

Comment:

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

Name: KN

Email: jb@gmail.com

Website: https://www.trollge.com

Post Comment

WebSecurity Academy

Stored XSS into HTML context with nothing encoded

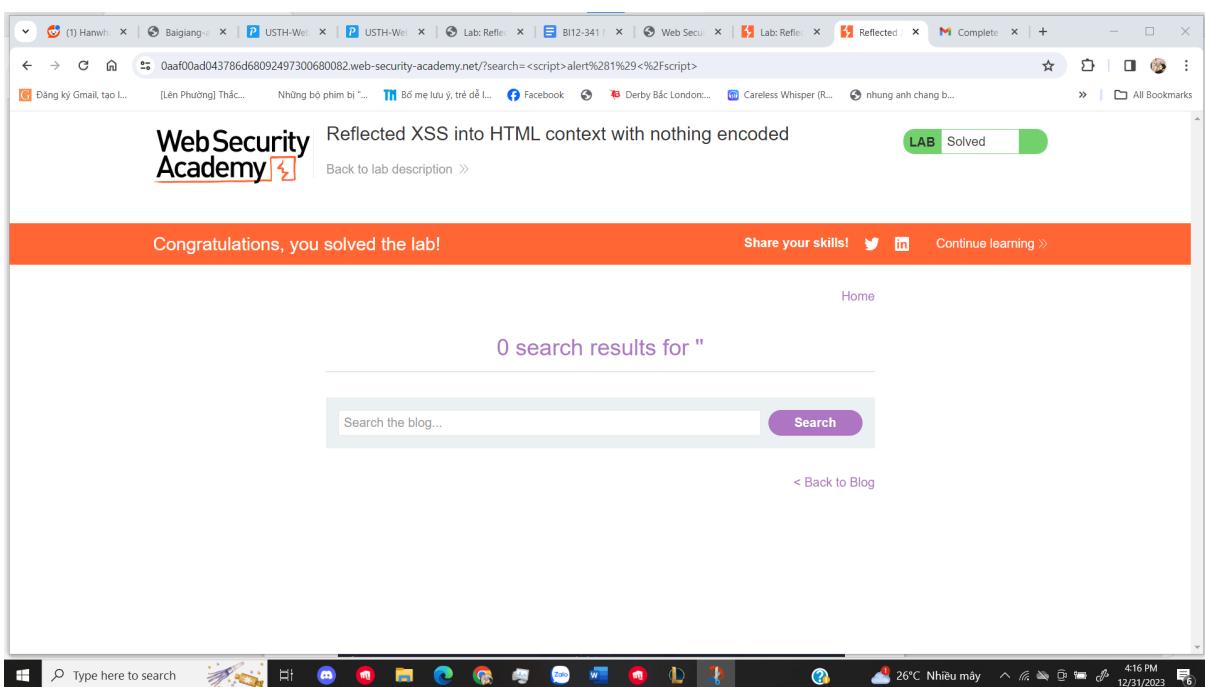
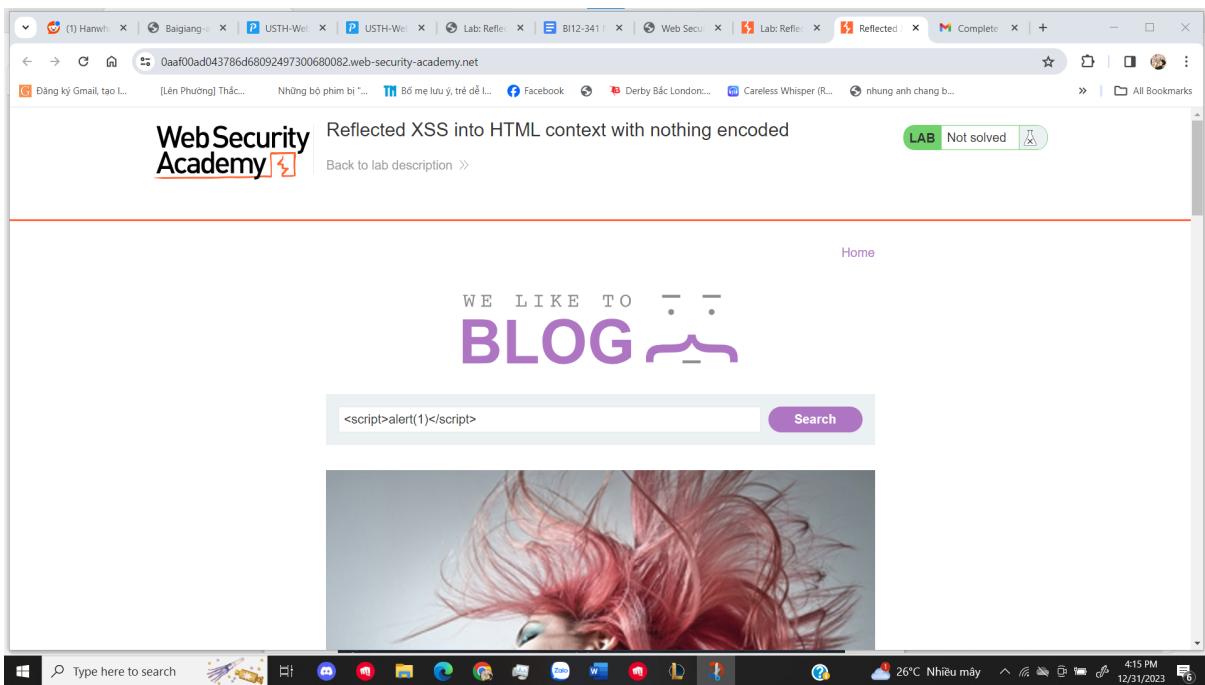
LAB Solved

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) Continue learning »

Home

2- Reflected XSS:



3- DOM-based XSS

The screenshot shows a browser window with multiple tabs open. The active tab is titled "DOM XSS in document.write sink using source location.search inside a select element" from "Web Security Academy". The page content includes a success message: "Congratulations, you solved the lab!", a rating of 5 stars, and a price of \$45.61. Below this is a large image of a woman in a blue dress standing in a park. At the top right of the page, there is a green button labeled "LAB Solved". The browser's address bar shows a URL related to the lab. The taskbar at the bottom of the screen displays various pinned icons.

4-Practice more XSS labs

a- Reflected XSS with event handlers and href attributes blocked

The screenshot shows a browser window with multiple tabs open. The active tab is titled "Reflected" from "Web Security Academy". The page content features a large image of a surgeon wearing a mask and gloves. Below the image is a purple header with the text "Video Games Made Me A Better Surgeon". Underneath the header is a paragraph of text: "Recently there was an article on this very subject. I felt it was slightly lacking in depth, there was a lot of input from professionals discussing dexterity, did video games improve that or make it worse. I imagine the surgeon...". At the bottom of the page is a purple "View post" button. The browser's address bar shows a URL related to the lab. The taskbar at the bottom of the screen displays various pinned icons.

The screenshot shows a browser window with multiple tabs open. The active tab is titled "Reflected XSS with event handlers and href attributes blocked" from "Web Security Academy". The page content includes a success message "Congratulations, you solved the lab!", a "Home" link, and a "Click me" button. Below the button, it says "0 search results for '" and has a search bar. At the bottom, there's a navigation bar with links like "Share your skills!" and "Continue learning >". The status bar at the bottom of the screen shows a Windows taskbar with various icons and the date/time as 4:25 PM 12/31/2023.

b- Reflected XSS in a JavaScript URL with some characters blocked

The screenshot shows a browser window with multiple tabs open. The active tab is titled "Reflected XSS in a JavaScript URL with some characters blocked" from "Web Security Academy". The page content includes a success message "Congratulations, you solved the lab!", a "Home" link, and a large image of a man with white paint on his face. Below the image, there's a navigation bar with links like "Share your skills!" and "Continue learning >". The status bar at the bottom of the screen shows a Windows taskbar with various icons and the date/time as 4:29 PM 12/31/2023.

c- Exploiting XSS to perform CSRF:

The screenshot shows a browser window with multiple tabs open. The active tab is a comment form for a post on 'web-security-academy.net'. The form includes fields for 'Comment' (containing a JavaScript exploit), 'Name' (KN), 'Email' (jb@gmail.com), and 'Website' (https://www.trollge.com). A 'Post Comment' button is visible. Below the form, a link '[< Back to Blog](#)' is present. The browser's taskbar at the bottom shows various pinned icons.

The screenshot shows a browser window displaying the confirmation page for a solved lab. The title is 'Exploiting XSS to perform CSRF'. A green 'Solved' button is visible. The message 'Congratulations, you solved the lab!' is displayed in an orange bar. Below it, a 'Share your skills!' button with social media links (Twitter, LinkedIn) and a 'Continue learning >' link are shown. Navigation links for 'Home' and 'My account' are at the top right. A link '[Back to lab description >](#)' is also present. The browser's taskbar at the bottom shows various pinned icons.

5- Web/JavaScript/SQL vulnerability challenges

a- Challenge 1

Challenge 1: Comment to Comments

It looks like this page may have some useful information hiding in its source code. See if you can answer these questions and find the flag.

Hint: Right click the page and select "View Page Source" or input "Ctrl+U" to view the HTML code and find the comments!

Question 1: What is the developer's nickname?

Sir Code-a-lot

Good job! Try the next question.

Submit

Question 2: What month of the year was this webpage written in?

April

Good job! Try the next question.

Submit

Challenges

Challenge 1

Challenge 2

Challenge 1

Challenge 2

Challenge 3

Question 3: What is the name of the webpage that the developer has not finished making (and therefore not linked to)?

Admin.html

Good job! Try the next question.

Submit

Challenge 1: Find the flag and input the answer.

Input Flag

ctfa{Quest for Comments}

Good job! Click here for the explanation.

Submit

b- Challenge 2

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "ctfacademy.github.io/web/challenge2/index.htm". On the left, there's a sidebar with sections like "2.3 JavaScript Vulnerabilities", "2.4 Database Vulnerabilities", and "3. Summary". Below that is a "Challenges" section with "Challenge 1", "Challenge 2", and "Challenge 3". The main content area has a question: "Question 1: What is the administrator's username?". A green input field contains "admin". Below it, a message says "Good job! Try the next question." and a green "Submit" button is visible. Another question follows: "Question 2: What is the administrator's password?". An input field contains "SuperSecretPassword". The message "Good job! Try the next question." is shown again, along with a "Submit" button.

This screenshot shows the same browser window after navigating to the "2.4 Database Vulnerabilities" section. The sidebar now includes "1.2 CSS", "1.3 JavaScript", "1.4 Databases", "2. Security Vulnerabilities", "2.1 HTML Vulnerabilities", "2.2 CSS Vulnerabilities", "2.3 JavaScript Vulnerabilities", "2.4 Database Vulnerabilities", and "3. Summary". The main content area displays a hint: "Hint: The login form is processed with JavaScript; remember what you learned earlier in this module about JavaScript logins.". Below this is a "Sign in" form with two input fields: one for "admin" and another for a password represented by a series of dots. A message "Great job! The flag is below." is displayed. A green "Sign in" button is present. A green box at the bottom right contains the text "ctfa{Client-side_Validation}".

The screenshot shows a browser window with multiple tabs open. The active tab is titled "ctfacademy.github.io/web/challenge2/index.htm". The page content includes a green "Submit" button at the top, followed by the text "Challenge 2: Find the flag and input the answer." Below this is an orange "Input Flag" box containing a text input field with the value "ctfa(Client-side_Validation)". A message below the input field says "Good job! Click here for the explaination." and another green "Submit" button. At the bottom of the page are links for "Back to Top", a navigation bar with pages 1 through 7, and footer sections for "CONTACT US" (links to Gmail, Glossary, Quick Start Guide, Legal Disclaimer), "ABOUT US" (links to Jacob Corley, James Corley, John Reiman), and copyright information ("© 2019 Cyber Training Force Academy"). The status bar at the bottom shows a Windows taskbar with various icons and the date/time "12/31/2023 4:42 PM".

c- Challenge 3

The screenshot shows a browser window with multiple tabs open. The active tab is titled "ctfacademy.github.io/web/challenge3/index.htm". On the left, there's a sidebar with a navigation menu: "1.4 Databases", "2. Security Vulnerabilities", "2.1 HTML Vulnerabilities", "2.2 CSS Vulnerabilities", "2.3 JavaScript Vulnerabilities", "2.4 Database Vulnerabilities", and "3. Summary". Below this is a "Challenges" section with links to "Challenge 1", "Challenge 2", and "Challenge 3". The main content area features an orange "Sign in" box with input fields for "admin" and "*****". A message below the box says "Great job! The flag is below." and a green "Sign in" button. Below the sign-in box is a green box containing the flag "ctfa{sequel}". To the right of the sign-in box is a "Question 1" section with a text input field containing "WHERE" and a green "Submit" button. The status bar at the bottom shows a Windows taskbar with various icons and the date/time "12/31/2023 4:45 PM".

(1) Hanwh... | Baigiang... | USTH-We... | USTH-We... | Lab: Refle... | BI12-341 | Download | Web Secu... | CTF Acad... | view-sour... | +

Đăng ký Gmail, tạo L... [Lên Phương] Thắc... Nhũng bộ phim bi "... T! Bố mẹ lưu ý; trẻ dễ l... Facebook Derby Bắc London... Careless Whisper (R... nhung anh chàng b...

ctfacademy.github.io/web/challenge3/index.htm

WHERE
Good job! Try the next question.

Submit

Challenge 3: Find the flag and input the answer.

Input Flag

ctfa[sequel]

Good job! Click here for the explanation.

Submit

Back to Top

« 1 2 3 4 5 6 7 »

CONTACT US
GLOSSARY
QUICK START GUIDE
LEGAL DISCLAIMER

ABOUT US
JACOB CORLEY
JAMES CORLEY
JOHN REIMAN

Type here to search

Windows Start button, taskbar icons, weather (26°C), date (12/31/2023), time (4:45 PM)