HyperionDev

A Toolbox for Ethical Hacking

Model Answer

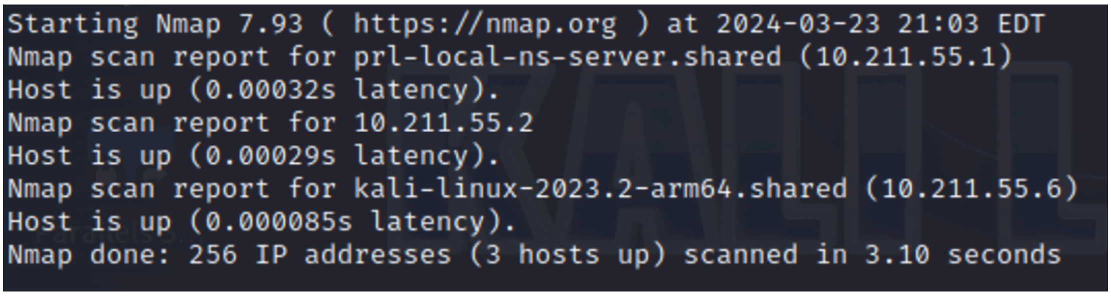
Visit our website

Auto-graded task

1. Mapping out the network topology:
    a. The correct tool for this task is **Nmap**.
    b. To perform a comprehensive scan of your local network and identify active hosts, you can use the following command:

```
nmap -sn 10.211.55.0/24
```

In this command, the target IP address range `10.211.55.0/24` specifies the network address and the subnet mask. **Replace this with the appropriate IP address range for your local network.** Here is a sample output:

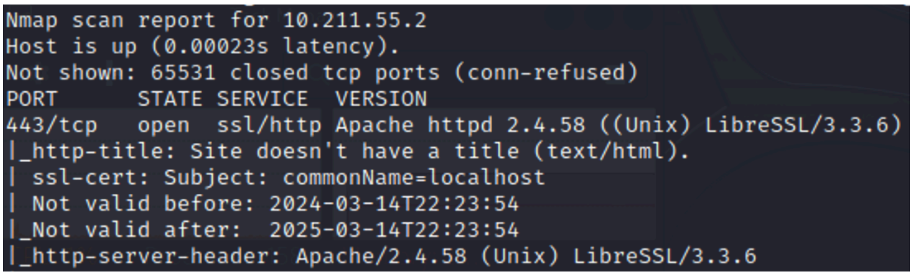


```
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-23 21:03 EDT
Nmap scan report for prl-local-ns-server.shared (10.211.55.1)
Host is up (0.00032s latency).
Nmap scan report for 10.211.55.2
Host is up (0.00029s latency).
Nmap scan report for kali-linux-2023.2-arm64.shared (10.211.55.6)
Host is up (0.000085s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.10 seconds
```

To identify open ports and services running on those ports, use the following command:

```
nmap -p- -A -T4 10.211.55.2
```

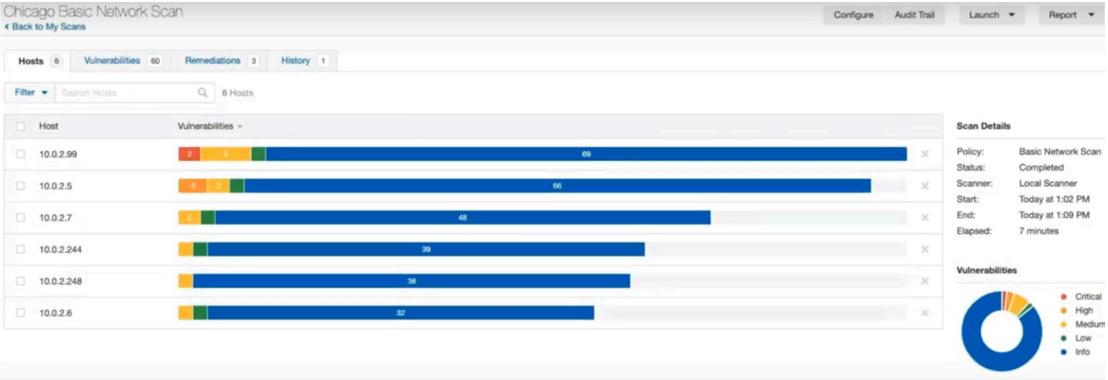
Replace this address `10.211.55.2` with your own IP address. Here is a sample output showing a poorly configured web server:



```
Nmap scan report for 10.211.55.2
Host is up (0.00023s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT      STATE SERVICE  VERSION
443/tcp   open  ssl/http Apache httpd 2.4.58 ((Unix) LibreSSL/3.3.6)
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2024-03-14T22:23:54
|_Not valid after:  2025-03-14T22:23:54
|_http-server-header: Apache/2.4.58 (Unix) LibreSSL/3.3.6
```

2. Vulnerability scan:
    a. The correct tool for the vulnerability scan is **Nessus**.

b. Here is a sample screenshot of a basic scan of a local network:



Chicago Basic Network Scan

‹ Back to My Scans

Host	Vulnerabilities
10.0.2.99	2 5 69
10.0.2.5	3 2 66
10.0.2.7	2 48
10.0.2.244	39
10.0.2.248	38
10.0.2.6	32

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 1:02 PM
End:	Today at 1:09 PM
Elapsed:	7 minutes

Vulnerabilities

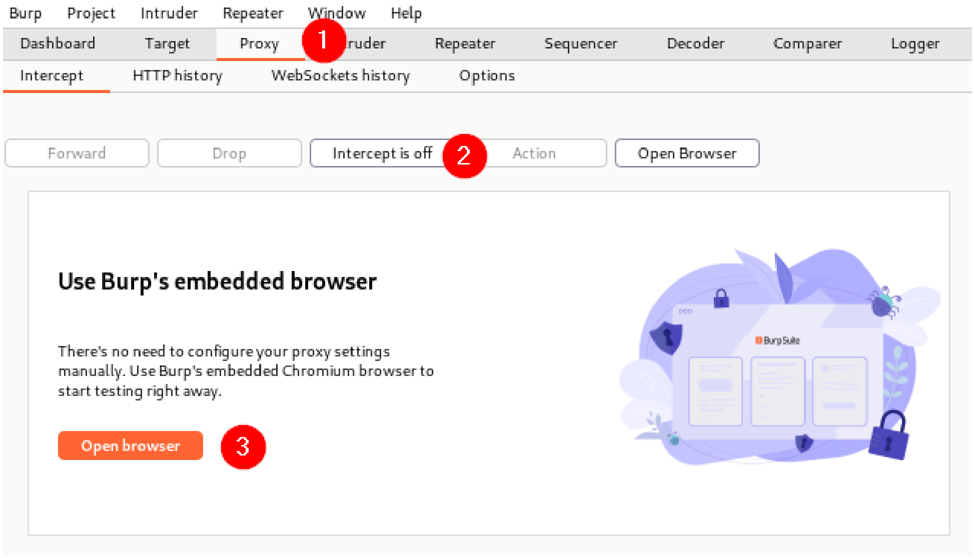
Notice that the scan provides results for each host, with the criticality of each discovered vulnerability clearly marked. Continue to investigate your results by clicking on each host's results to obtain more information about each vulnerability.

c. Numbers in each category (critical, high, medium, and low) will depend on the individual network scanned. The criticality numbers are shown in the scan results.

Optional task

1. Go to Kali Linux and open Burp Suite.

2. On Burp Suite, locate the "Proxy" tab and ensure the intercept is off, then open the embedded browser.

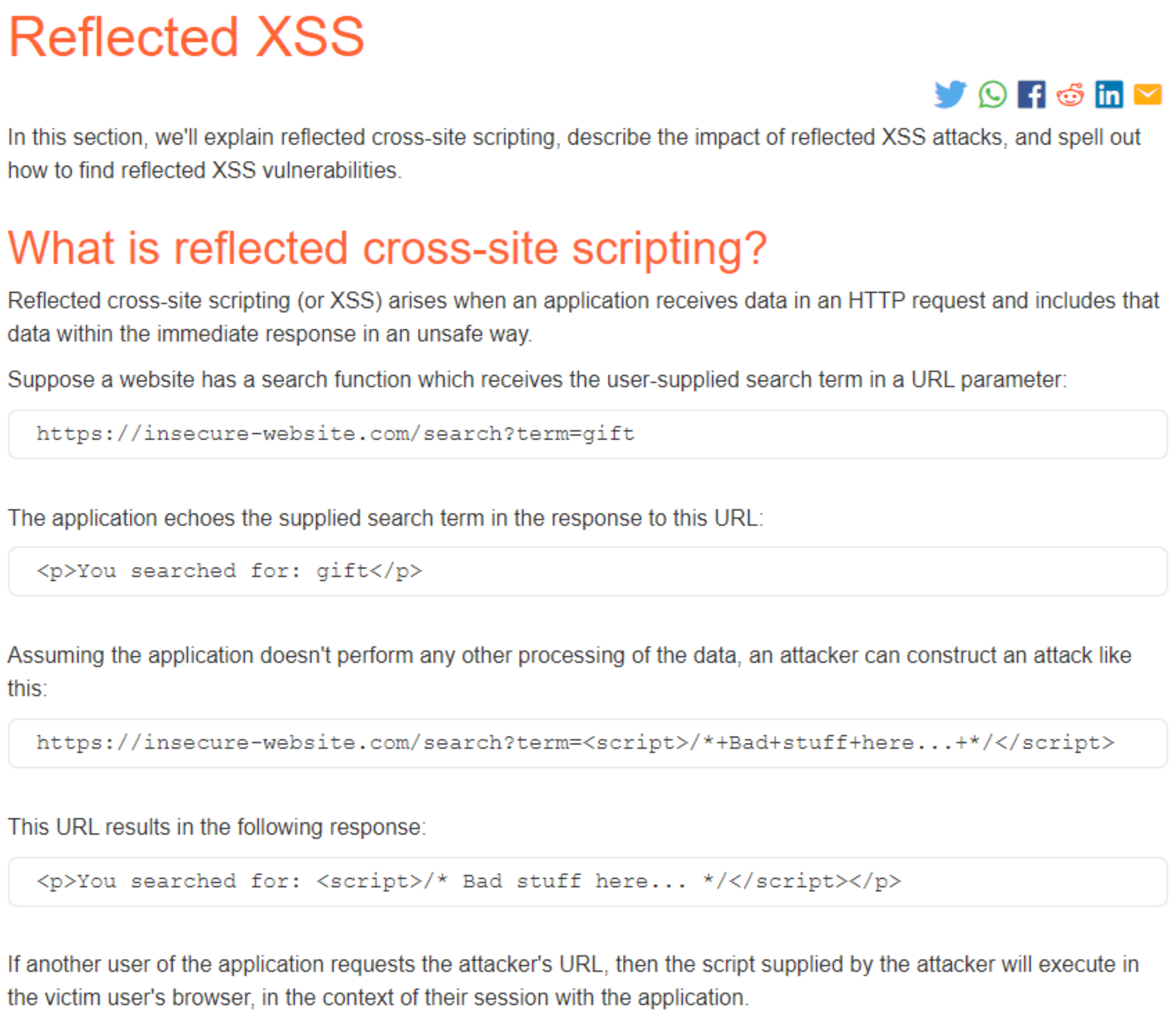


Use Burp's embedded browser

There's no need to configure your proxy settings manually. Use Burp's embedded Chromium browser to start testing right away.

Open browser

3. Please visit **Reflected XSS** to read up on the topic.



Reflected XSS

In this section, we'll explain reflected cross-site scripting, describe the impact of reflected XSS attacks, and spell out how to find reflected XSS vulnerabilities.

What is reflected cross-site scripting?

Reflected cross-site scripting (or XSS) arises when an application receives data in an HTTP request and includes that data within the immediate response in an unsafe way.

Suppose a website has a search function which receives the user-supplied search term in a URL parameter:

```
https://insecure-website.com/search?term=gift
```

The application echoes the supplied search term in the response to this URL:

```
<p>You searched for: gift</p>
```

Assuming the application doesn't perform any other processing of the data, an attacker can construct an attack like this:

```
https://insecure-website.com/search?term=<script>/*+Bad+stuff+here...+*/</script>
```

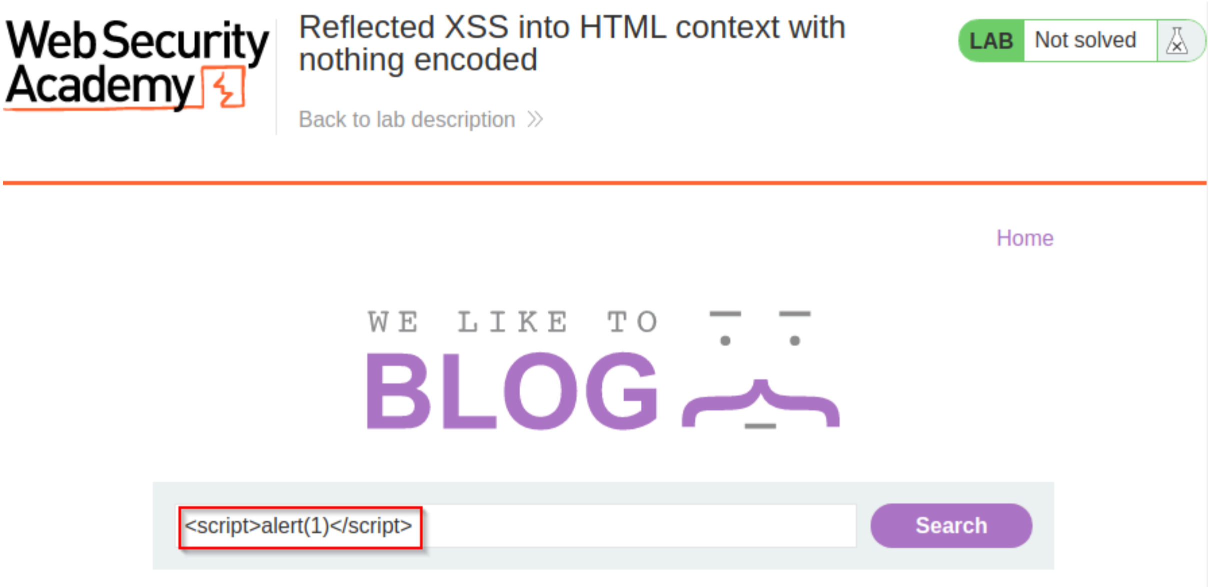
This URL results in the following response:

```
<p>You searched for: <script>/* Bad stuff here... */</script></p>
```

If another user of the application requests the attacker's URL, then the script supplied by the attacker will execute in the victim user's browser, in the context of their session with the application.

4. After reading about reflected XSS, log in to your Burp Suite account and complete the **lab on reflected XSS**.

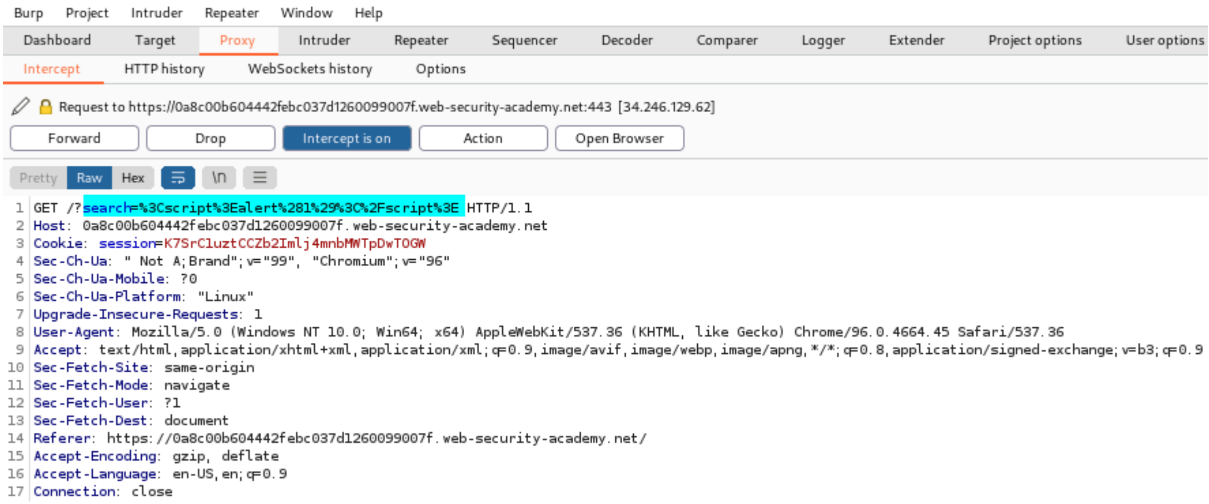
5. Turn on the intercept and refresh the webpage once you have copied and pasted `<script>alert(1)</script>` into the blog search box.



Reflected XSS into HTML context with nothing encoded

<script>alert(1)</script>

6. Look at the response captured by Burp Suite.

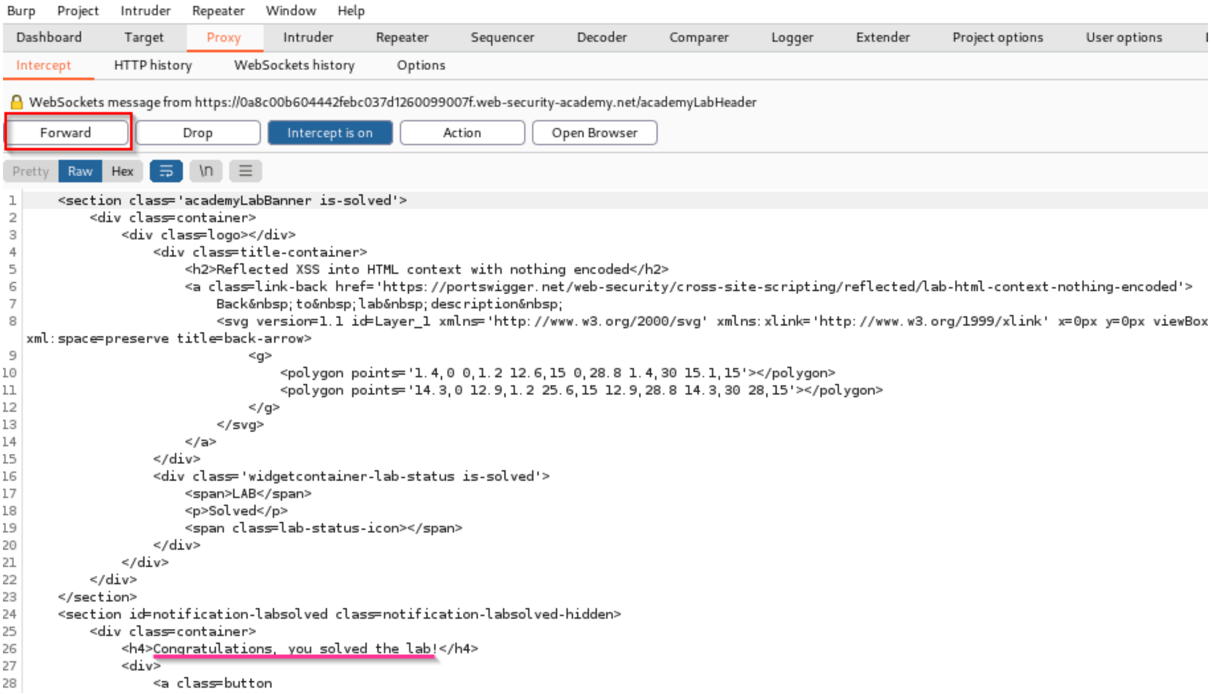


Request to https://0a8c00b604442febc037d1260099007f.web-security-academy.net:443 [34.246.129.62]

```
GET /?search=%3Cscript%3Ealert%281%29%3C%2Fscript%3E HTTP/1.1
Host: 0a8c00b604442febc037d1260099007f.web-security-academy.net
Cookie: session=K7SrCluztCCZb2Imlj4mnbMWTpDwTOGW
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a8c00b604442febc037d1260099007f.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

7. Click on “Forward” and check the responses on both Burp Suite and the lab (example screenshots on the next page).

Burp Suite:

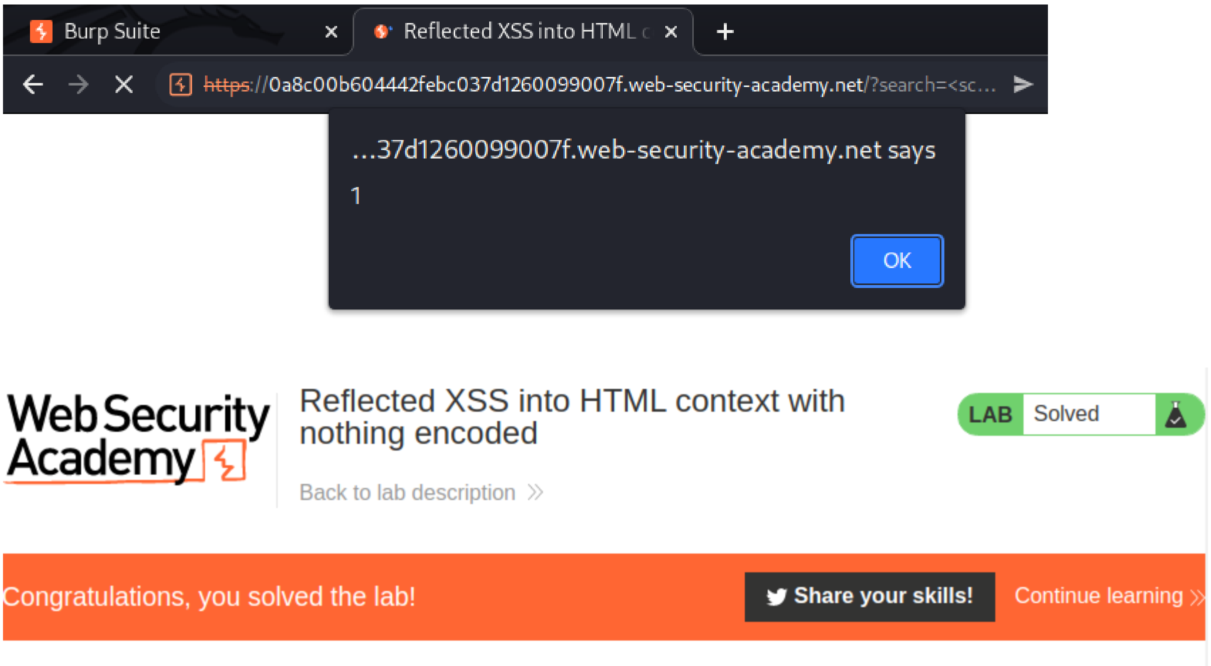

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Intercept HTTP history WebSockets history Options

WebSockets message from https://0a8c00b604442febc037d1260099007f.web-security-academy.net/academyLabHeader

Forward
Drop
Intercept is on
Action
Open Browser
Pretty Raw Hex \n

```
    <section class='academyLabBanner is-solved'>
        <div class=container>
            <div class=logo></div>
                <div class=title-container>
                    <h2>Reflected XSS into HTML context with nothing encoded</h2>
                    <a class=link-back href='https://portswigger.net/web-security/cross-site-scripting/reflected/lab-html-context-nothing-encoded'>
                        Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
                        <svg version=1.1 id=Layer_1 xmlns='http://www.w3.org/2000/svg' xmlns:xlink='http://www.w3.org/1999/xlink' x=0px y=0px viewBox
xml:space=preserve title=back-arrow>
                            <g>
                                <polygon points='1.4,0 0,1.2 12.6,15 0,28.8 1.4,30 15.1,15'></polygon>
                                <polygon points='14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28,15'></polygon>
                            </g>
                        </svg>
                    </a>
                </div>
                <div class='widgetcontainer-lab-status is-solved'>
                    <span>LAB</span>
                    <p>Solved</p>
                    <span class=lab-status-icon></span>
                </div>
            </div>
        </div>
    </section>
    <section id=notification-labsolved class=notification-labsolved-hidden>
        <div class=container>
            <h4>Congratulations, you solved the lab!</h4>
            <div>
                <a class=button
```

Lab:


Burp Suite
Reflected XSS into HTML c
https://0a8c00b604442febc037d1260099007f.web-security-academy.net/?search=<sc…

...37d1260099007f.web-security-academy.net says

1

Reflected XSS into HTML context with nothing encoded

LAB Solved
Back to lab description »

Congratulations, you solved the lab!

Share your skills!
Continue learning »