Identifying a Browser Attack

Scenario

An interception proxy is software that sits between a client and server (a Man-In-The-Middle or On-Path attack) and allows requests from the client and responses from the servers to be analyzed and modified. In this activity, you will use the interception proxy Burp Suite to probe a web application for weaknesses and show how allowing a simple script to run can compromise browser security.

Objectives

This activity is designed to test your understanding of an ability to apply content examples in the following CompTIA Security+ objective:

- 1.3 Given a scenario, analyze potential indicators associated with application attacks.

Lab

- Kali VM
- LX1 VM
- pfSense VM

Task 1

Configure interception proxy

In this activity, you will see how XSS attacks take advantage of web applications that process user input to form the HTML output in some way. There are usually two sources of inputs:

- User typed input through a form or control.
- Parsing (interpreting) parameters from a URL.

XSS vulnerability testing on a website will consequently focus primarily on script-based pages (such as PHP) and on forms. You will use Burp Suite to probe a user form for XSS vulnerabilities. The form is hosted on Mutillidae, which is an intentionally vulnerable web application created by OWASP.

WARNING: Mutillidae contains pages with language that some may find offensive. If you are offended by bad language, please skip this activity.

To configure the browser to use Burp Suite as an interception proxy, complete the following steps.

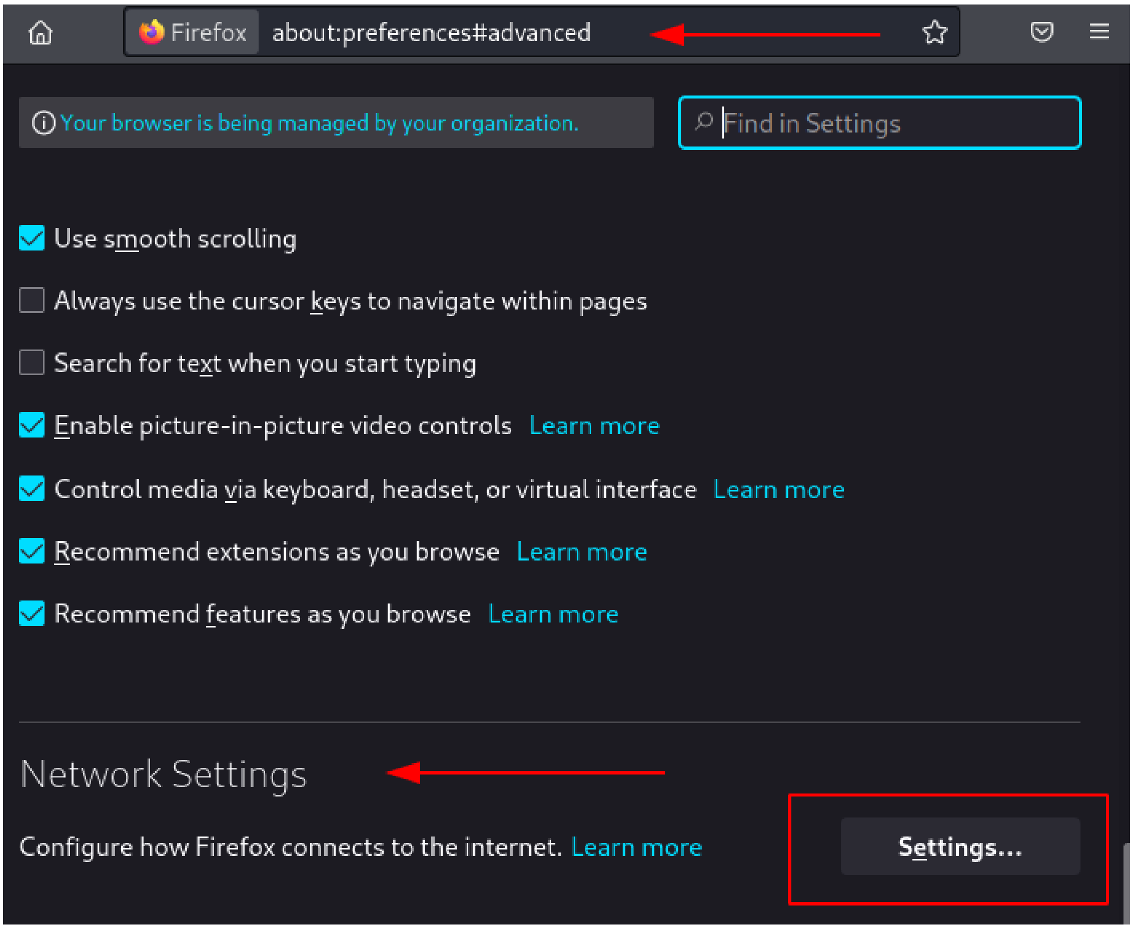
1. Select the **Kali** VM. Log on with the credentials **kali** and **Pa$$w0rd** as the password.

2. Open **Firefox ESR**.

3. In the browser bar, enter:

```
about:preferences#advanced
```

4. Scroll to the bottom of the configuration page, and then, under **Network Settings**, select the **Settings** button.



Your browser is being managed by your organization.

☑ Use smooth scrolling

□ Always use the cursor keys to navigate within pages

□ Search for text when you start typing

☑ Enable picture-in-picture video controls Learn more

☑ Control media via keyboard, headset, or virtual interface Learn more

☑ Recommend extensions as you browse Learn more

☑ Recommend features as you browse Learn more

Network Settings

Configure how Firefox connects to the internet. Learn more

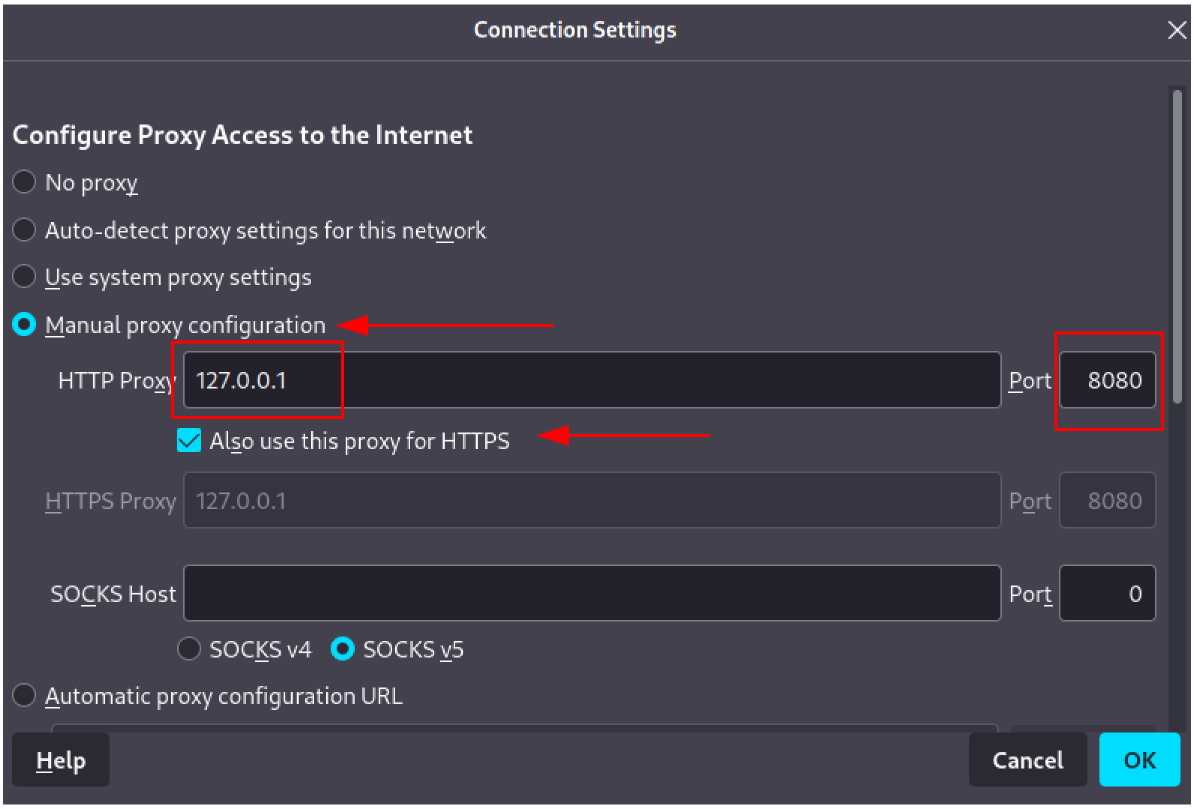
Figure 1.1 – Firefox Settings > Network Settings > Settings.

5. Select the **Manual Proxy configuration** radio button.

6. In the **HTTP proxy** box, type **127.0.0.1**

7. In the **Port** box, type **8080**

8. Check the **Also use this proxy for HTTPS** box.



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☑ Also use this proxy for HTTPS

HTTPS Proxy 127.0.0.1 Port 8080

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

Figure 1.2 – Connections settings – Manual proxy configuration.

9. Select **OK**.

10. **Minimize** Firefox.

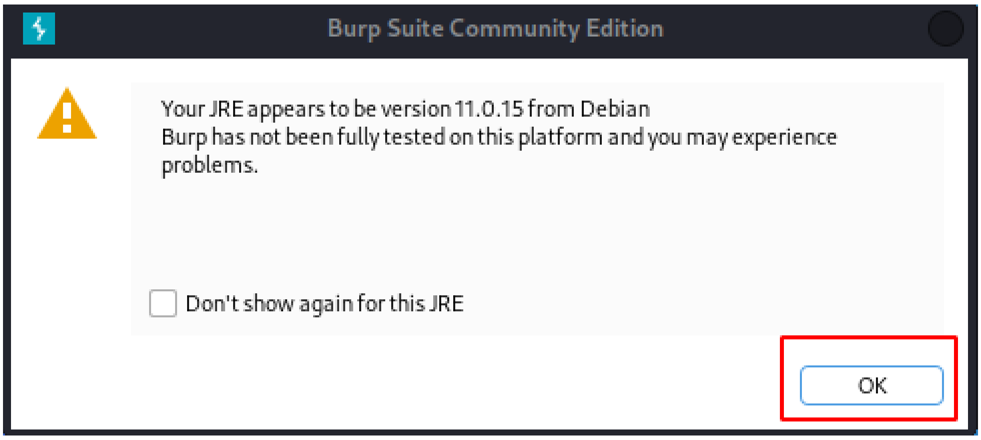
Task 2

Run interception proxy

Start Burp Suite and configure the proxy to intercept requests.

1. Open the **burpsuite** desktop shortcut.

2. **Accept** the license, and then select **Next** through the rest of the setup wizard to use the default settings. Do not be concerned with any warnings about Burp Suite being out of date – select **OK**.



Burp Suite Community Edition

Your JRE appears to be version 11.0.15 from Debian
Burp has not been fully tested on this platform and you may experience problems.

□ Don't show again for this JRE

Figure 2.1 – Warning message that Burp Suite is out of date. Click OK.

3. With the temporary project open, select the **Proxy** tab, **Intercept**, and ensure that the **Intercept is on** button is active.

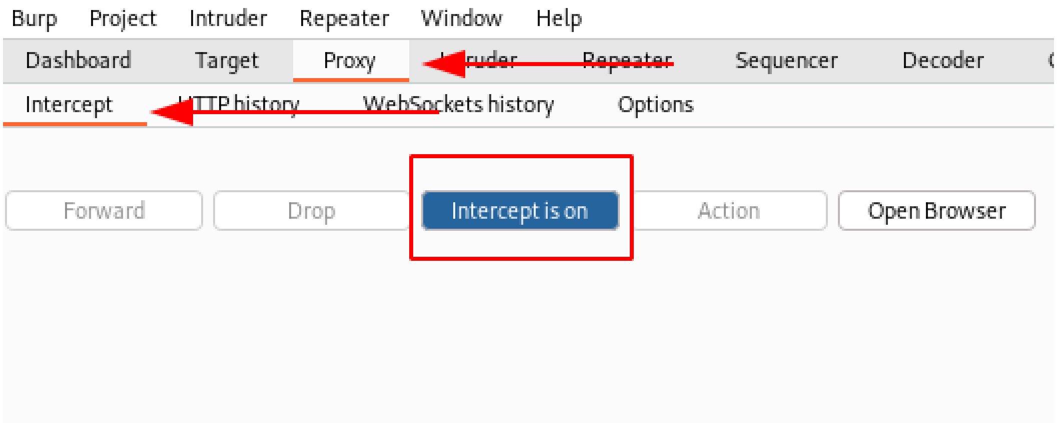


Figure 2.2 Intercept on button active.

4. Arrange the **Firefox** and **Burp Suite** windows so that you can use them both together easily.

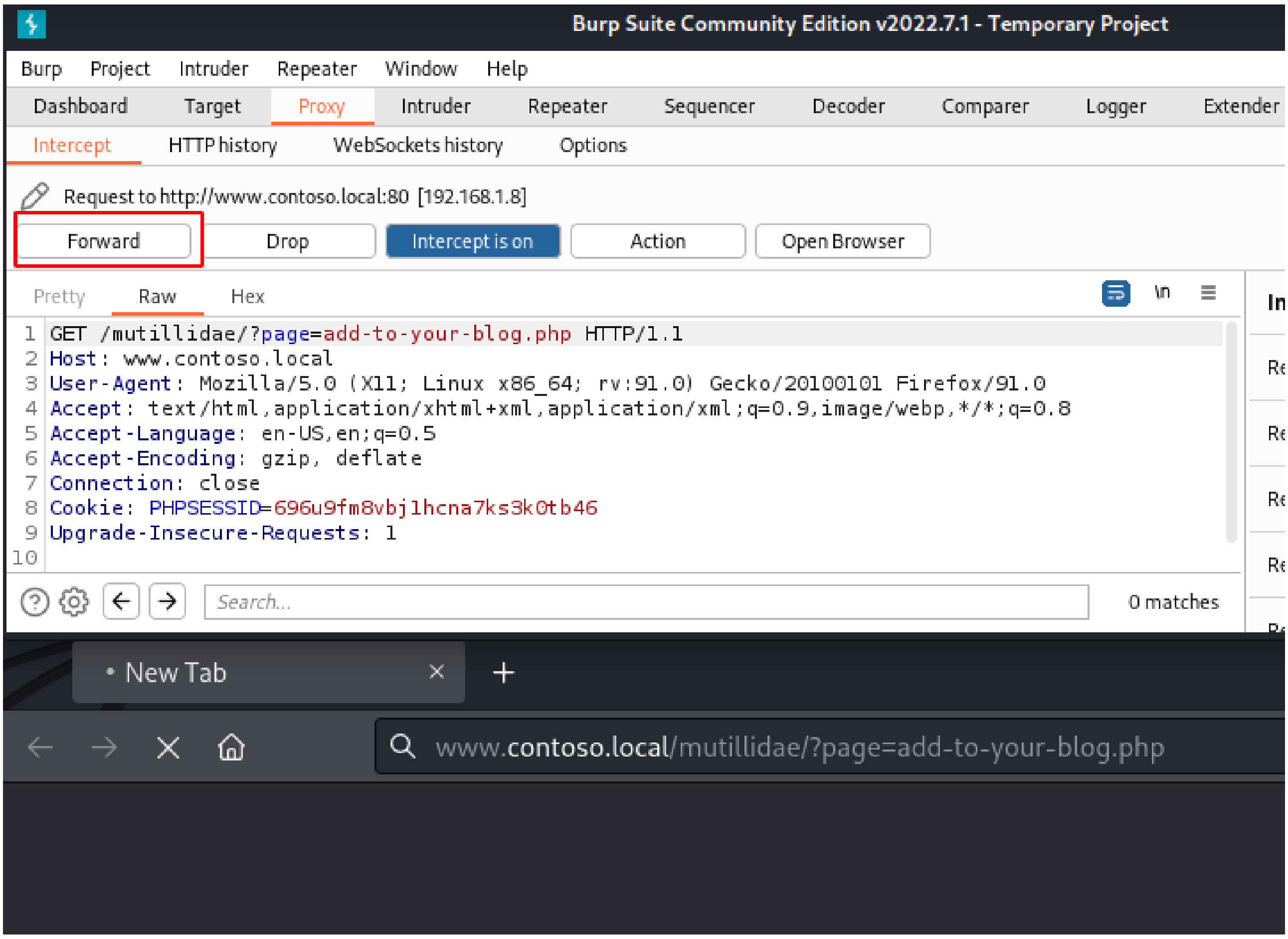
5. In the browser address bar, enter the following **URL**, taking care to type the address correctly:

```
http://www.contoso.local/mutillidae/?page=add-to-your-blog.php
```

The web page will not load. This is expected, because Burp Suite is intercepting the browser request.

Note the page file extension. PHP (PHP Hypertext Processor) is a scripting language widely used to create web applications.

6. In Burp Suite, note the content of what the browser is sending to the server – a simple page request along with some information about itself. Select the **Forward** button.

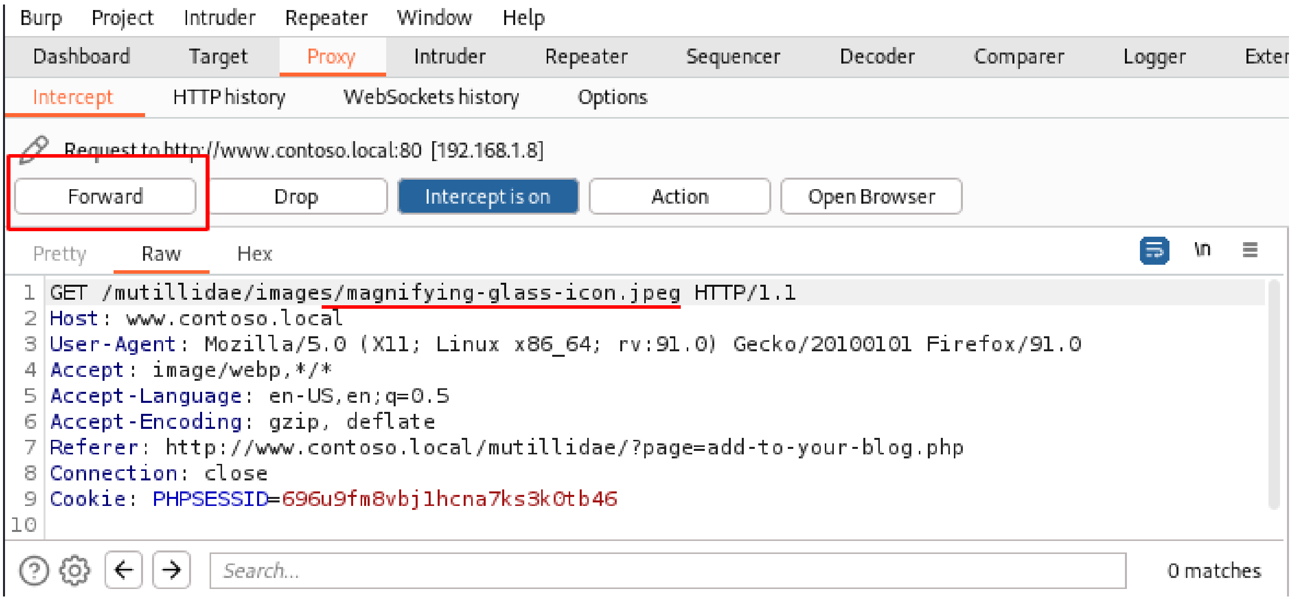

Burp Suite Community Edition v2022.7.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender
Intercept HTTP history WebSockets history Options
Request to http://www.contoso.local:80 [192.168.1.8]
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex
Search...
0 matches
New Tab
www.contoso.local/mutillidae/?page=add-to-your-blog.php

```
GET /mutillidae/?page=add-to-your-blog.php HTTP/1.1
Host: www.contoso.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=696u9fm8vbj1hcna7ks3k0tb46
Upgrade-Insecure-Requests: 1

```

Figure 2.3 – Burp Suite intercepting PHP page request.

7. Note that the browser has made another request (for a JPEG icon). Select the **Forward** button to let this through, too.


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Exter
Intercept HTTP history WebSockets history Options
Request to http://www.contoso.local:80 [192.168.1.8]
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex
Search...
0 matches

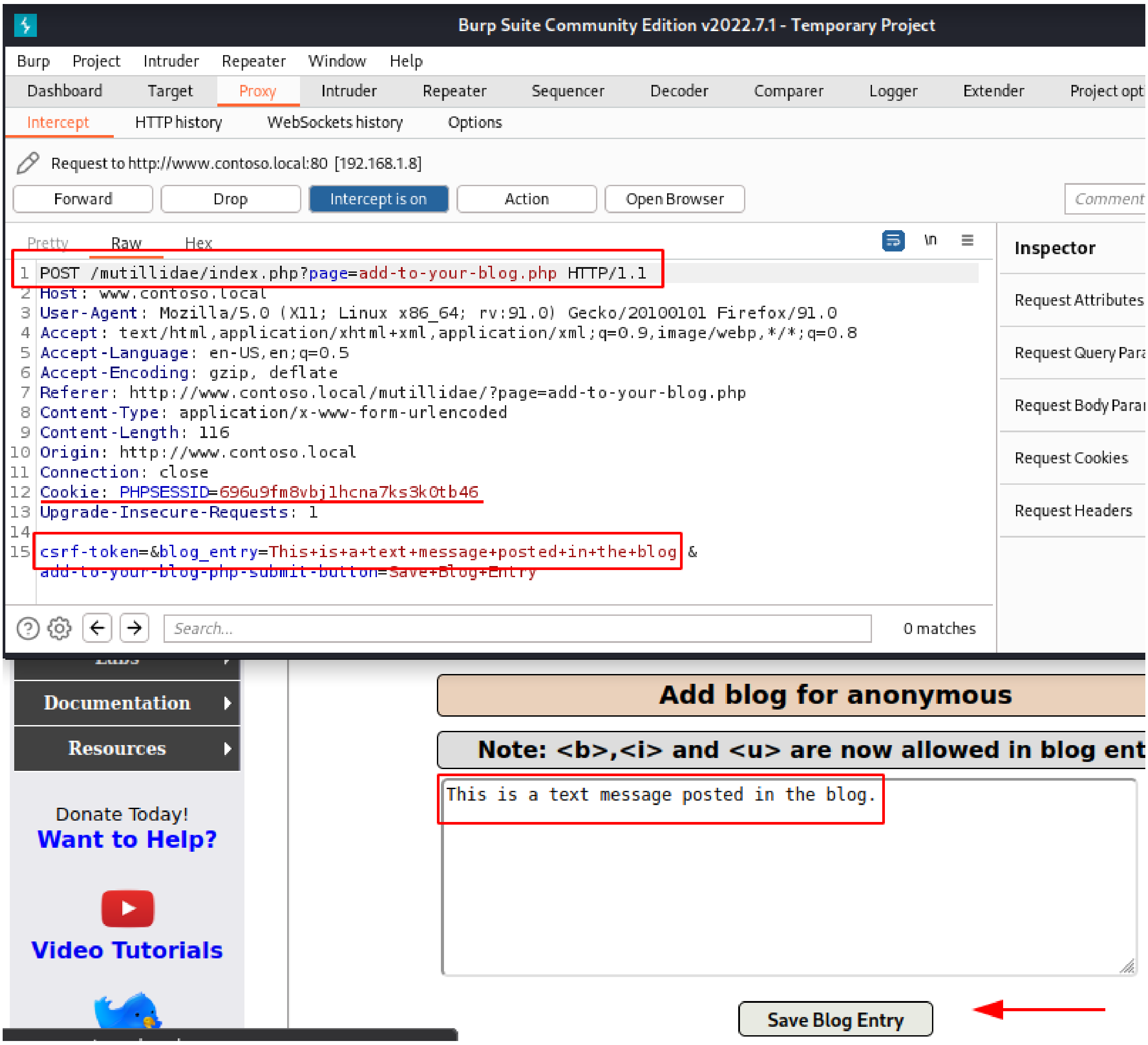
```
GET /mutillidae/images/magnifying-glass-icon.jpeg HTTP/1.1
Host: www.contoso.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.contoso.local/mutillidae/?page=add-to-your-blog.php
Connection: close
Cookie: PHPSESSID=696u9fm8vbj1hcna7ks3k0tb46

```

Figure 2.4 – Burp Suite interception a jpeg file icon.

8. In the Firefox browser, type a message into the box then select the **Save Blog Entry** button. Note that, again, nothing will happen.

9. In Burp Suite, analyze the contents of the new request. This is a POST request (compared to the previous GET) and contains the text you typed plus the control used. Note that the application has also set a session cookie. Select the **Forward** button.



```
POST /mutillidae/index.php?page=add-to-your-blog.php HTTP/1.1
Host: www.contoso.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.contoso.local/mutillidae/?page=add-to-your-blog.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 116
Origin: http://www.contoso.local
Connection: close
Cookie: PHPSESSID=696u9fm8vbj1hcna7ks3k0tb46
Upgrade-Insecure-Requests: 1

csrf-token=&blog_entry=This+is+a+text+message+posted+in+the+blog&
add-to-your-blog-php-submit-button=Save+Blog+Entry
```

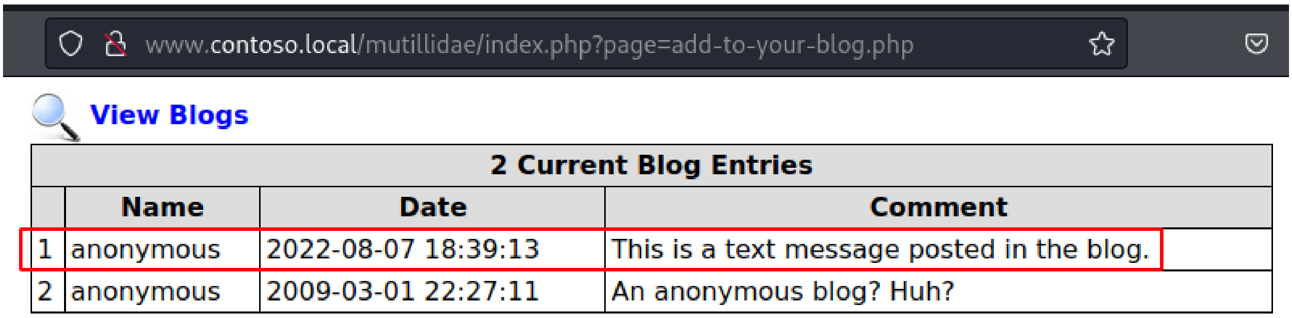
Add blog for anonymous

Note: <b>,<i> and <u> are now allowed in blog ent

This is a text message posted in the blog.

Figure 2.5 – POST request intercepted with the contents typed at the bottom in the form.

10. In the browser, observe that the message you typed is posted to the blog entries table.


www.contoso.local/mutillidae/index.php?page=add-to-your-blog.php
View Blogs

2 Current Blog Entries			
	Name	Date	Comment
1	anonymous	2022-08-07 18:39:13	This is a text message posted in the blog.
2	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?

Figure 2.6 – The blog post has been saved and shown at the bottom of the text box.

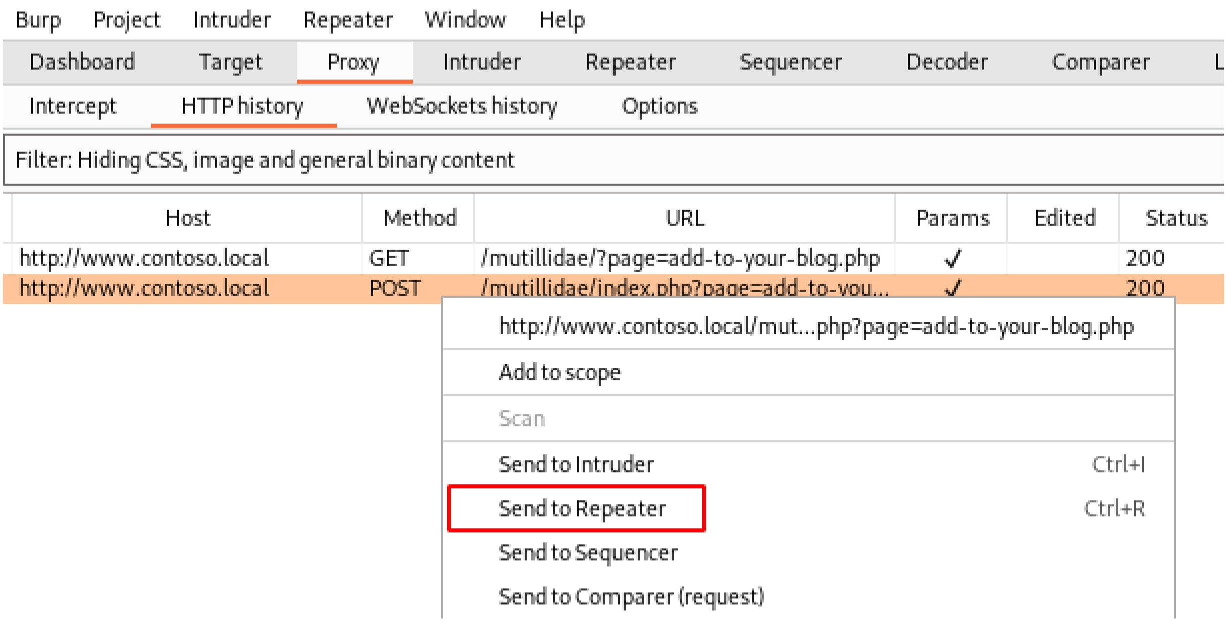
11. In Burp Suite, select the **Intercept is On** button to **switch it off**.

Task 3

Test injection vulnerability

If you want to probe this site for injection vulnerabilities, a basic test is to try to use some JavaScript to show an alert.

1. In Burp Suite, select the **HTTP history** tab. Locate the **POST** record then right-click it and select **Send to Repeater**.



Filter: Hiding CSS, image and general binary content

Host	Method	URL	Params	Edited	Status
http://www.contoso.local	GET	/mutillidae/?page=add-to-your-blog.php	✓		200
http://www.contoso.local	POST	/mutillidae/index.php?page=add-to-you...	✓		200

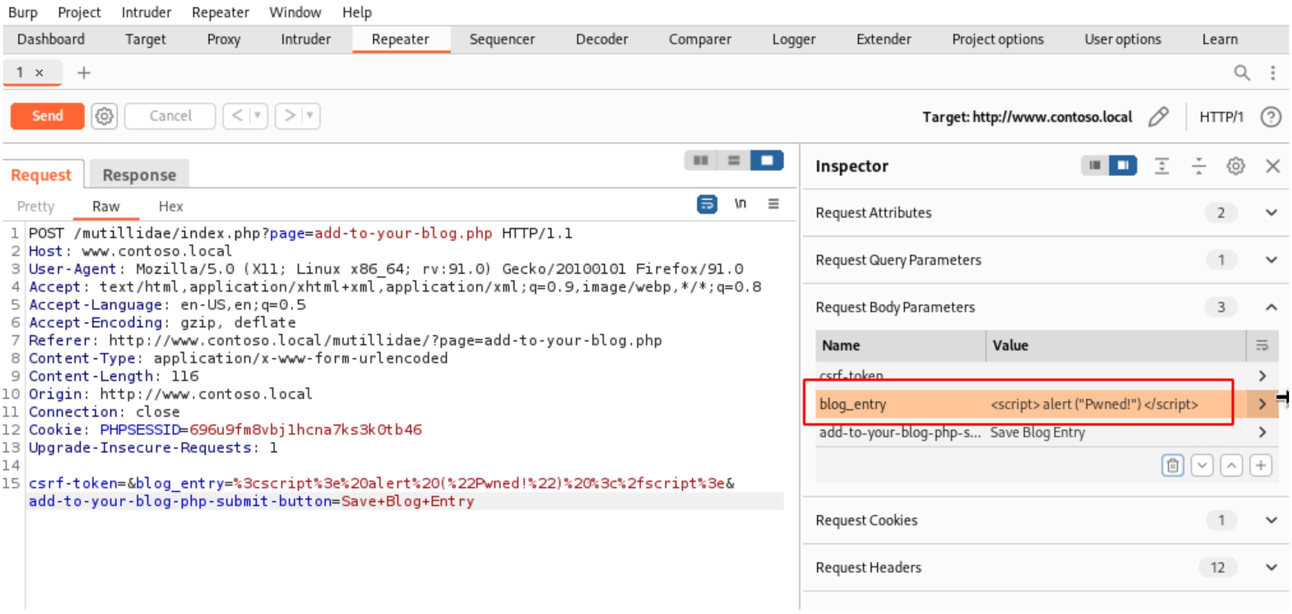
http://www.contoso.local/mut...php?page=add-to-your-blog.php
Add to scope
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer (request)

Figure 3.1 – Sending the POST request to Repeater.

2. Select the **Repeater** tab. In the Request panel, select the **Raw** tab.

3. Select to the right **Request body Parameters** and expand it. In the **blog_entry** box, add the following code to whatever you typed then press **ENTER**:

```
<script> alert (“Pwned!”) </script>
```


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 ×
Send
Cancel
Target: http://www.contoso.local
HTTP/1
Request
Response
Pretty
Raw
Hex
\n
Inspector

```
POST /mutillidae/index.php?page=add-to-your-blog.php HTTP/1.1
Host: www.contoso.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.contoso.local/mutillidae/?page=add-to-your-blog.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 116
Origin: http://www.contoso.local
Connection: close
Cookie: PHPSESSID=696u9fm8vbj1hcna7ks3k0tb46
Upgrade-Insecure-Requests: 1

csrf-token=&blog_entry=%3cscript%3e%20alert%20(%22Pwned!%22)%20%3c%2fscript%3e&
add-to-your-blog-php-submit-button=Save+Blog+Entry
```

Request Attributes 2

Request Query Parameters 1

Request Body Parameters 3

Name	Value
csrf-token	
blog_entry	<script> alert ("Pwned!") </script>
add-to-your-blog-php-s...	Save Blog Entry

Request Cookies 1

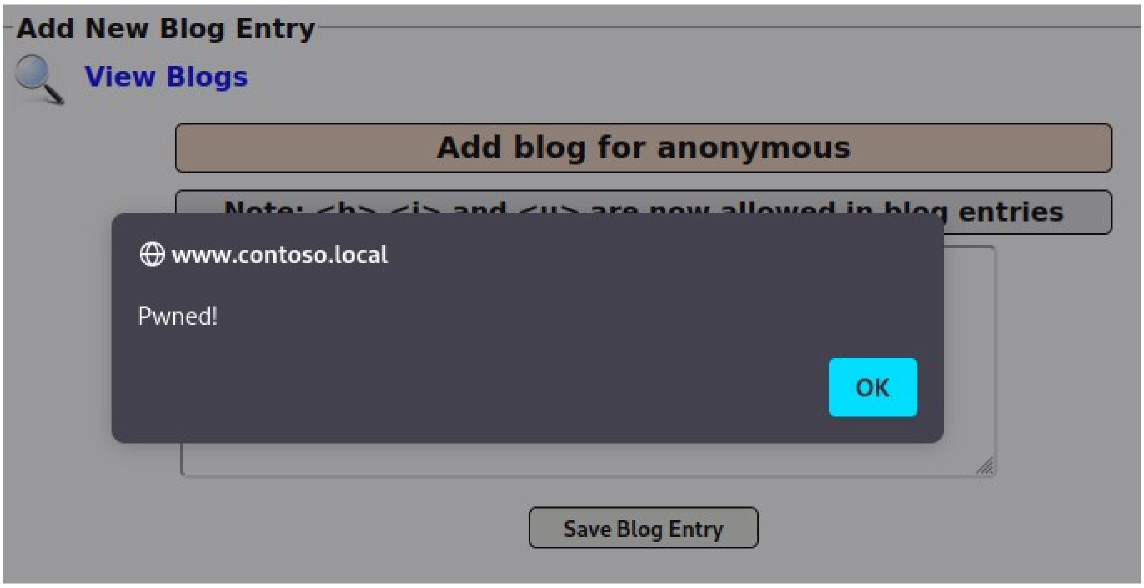
Request Headers 12

Figure 3.2 – Editing the blog_entry parameter.

4. Press the **Send** orange button to the upper left corner of the screen to send the modified request.

5. Switch to the browser and refresh or press F5 to update the blog entries. Press **ENTER** on the confirmation to resend the information.

The Pwned! Alert is displayed.



www.contoso.local

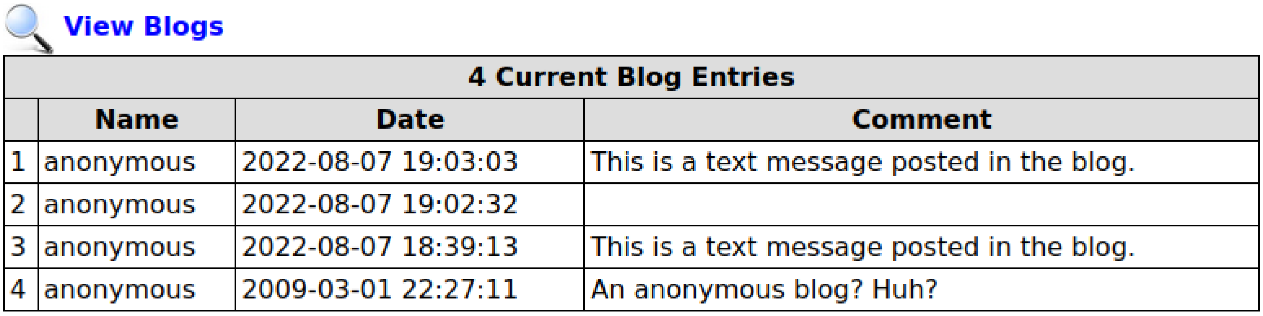
Pwned!

Figure 3.3 – The pwned alert.

The Pwned! Alert appears when a user visits the page. This is an example of a Cross Site Scripting attack (XSS) where the site allows messages posted as blog entries to execute embedded scripts.

6. Select **OK** to close the alert.

7. Scroll down the web page and note the duplicate blog entry that was created when you re-ran the request in Burp Suite.



View Blogs

4 Current Blog Entries			
	Name	Date	Comment
1	anonymous	2022-08-07 19:03:03	This is a text message posted in the blog.
2	anonymous	2022-08-07 19:02:32	
3	anonymous	2022-08-07 18:39:13	This is a text message posted in the blog.
4	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?

Figure 3.4 – Duplicated blog entries when sending the request with the malicious code.

8. Close Burpsuite.