HTML Injection:-

HTML Injection is a type of vulnerability that occurs when an attacker is able to inject arbitrary HTML into a web page, causing unintended behavior. This can lead to various security risks, such as altering the structure of the webpage, stealing sensitive information, or executing malicious scripts.

How HTML Injection Works:-

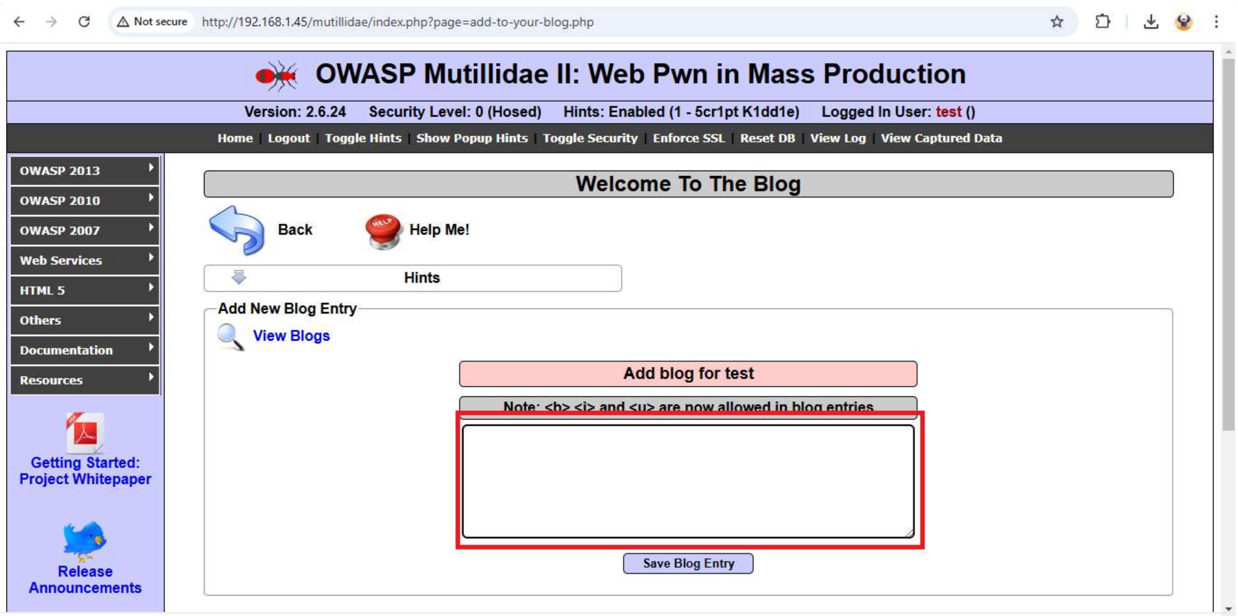
HTML injection happens when user input is not properly sanitized, allowing the attacker to inject HTML tags or scripts into the page. These malicious tags or scripts can then be rendered by the browser and executed.

In this case, the application allows users to input data into fields such as:

- **Comment boxes**
- **User profile fields**
- **Search bars**
- **Feedback forms**

Potential Impact

- **UI Manipulation: The attacker can manipulate the layout of the page, making it look suspicious or misleading.**
- **Session Hijacking: If JavaScript is injected, an attacker can potentially steal session cookies using methods like document.cookie.**
- **Phishing Attacks: The attacker may inject malicious HTML that tricks users into providing sensitive information.**
- **Cross-Site Scripting (XSS): HTML Injection often leads to a more severe XSS vulnerability if JavaScript execution is allowed.**
- **Reputation Damage: If the injected content is offensive or malicious, it could damage the trust of users or customers.**



Not secure http://192.168.1.45/mutillidae/index.php?page=add-to-your-blog.php

OWASP Mutillidae II: Web Pwn in Mass Production

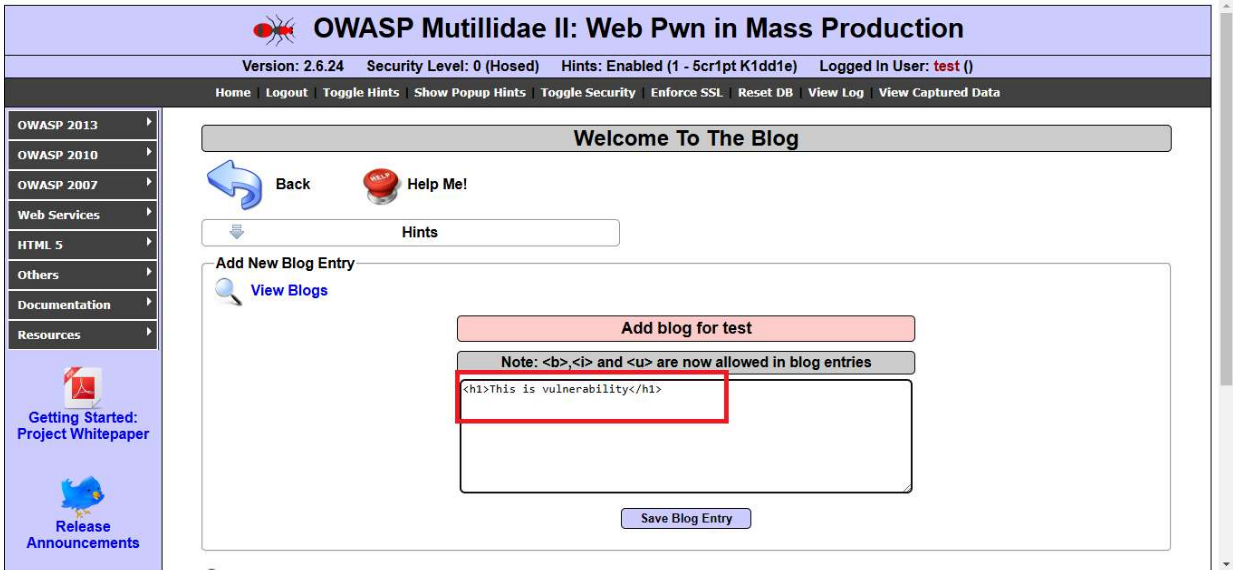
Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Logged In User: test ()

Welcome To The Blog

Add New Blog Entry

Add blog for test

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



OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Logged In User: test ()

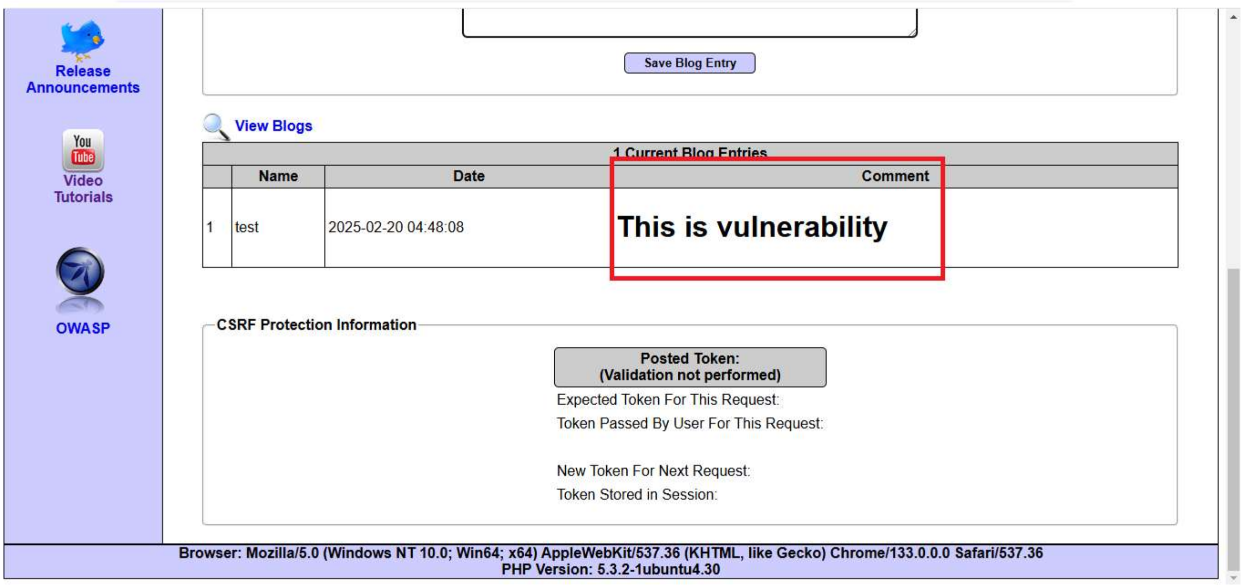
Welcome To The Blog

Add New Blog Entry

Add blog for test

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

```
<h1>This is vulnerability</h1>
```



		1 Current Blog Entries	
	Name	Date	Comment
1	test	2025-02-20 04:48:08	**This is vulnerability**

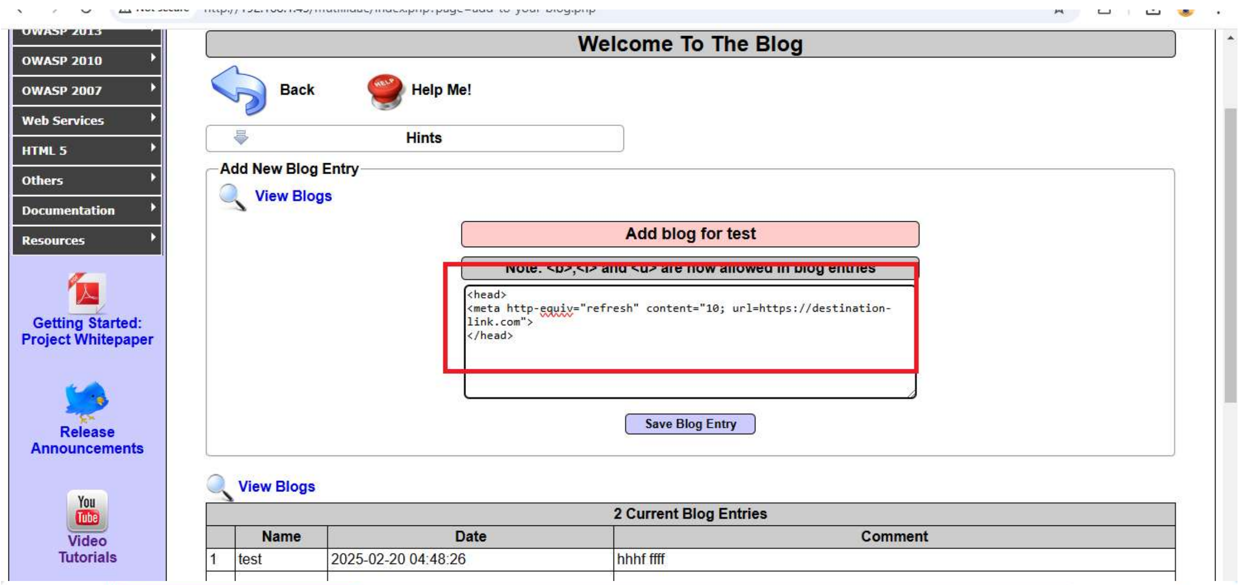
CSRF Protection Information

Posted Token:
(Validation not performed)

Expected Token For This Request:
Token Passed By User For This Request:

New Token For Next Request:
Token Stored in Session:

Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
PHP Version: 5.3.2-1ubuntu4.30



Welcome To The Blog

Add New Blog Entry

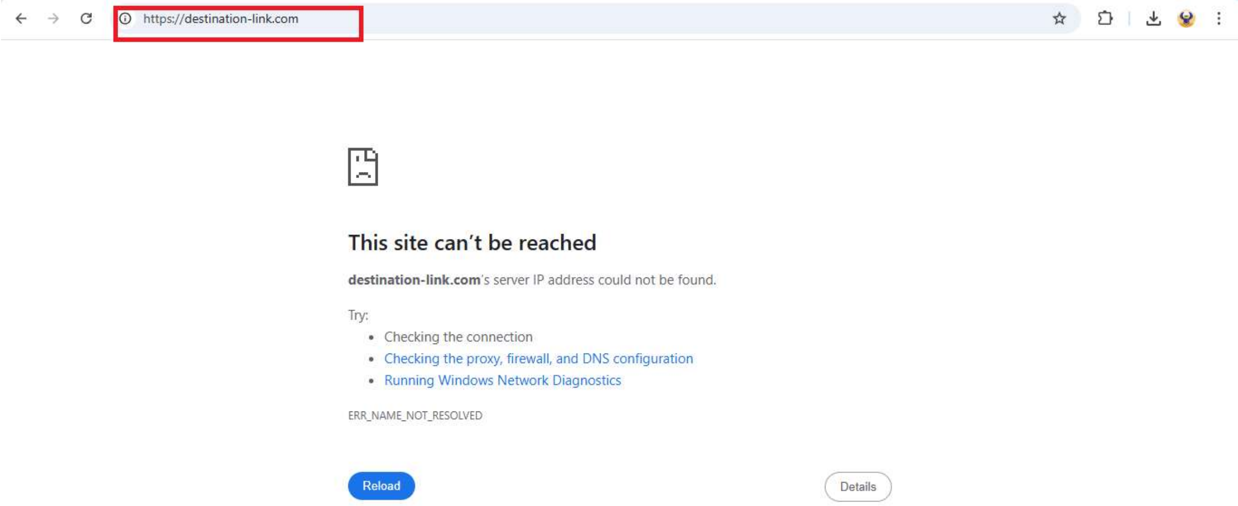
Add blog for test

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

```
<head>
<meta http-equiv="refresh" content="10; url=https://destination-
link.com">
</head>
```

2 Current Blog Entries

	Name	Date	Comment
1	test	2025-02-20 04:48:26	hhhf ffff



https://destination-link.com

This site can’t be reached

destination-link.com’s server IP address could not be found.

Try:

- Checking the connection
- Checking the proxy, firewall, and DNS configuration
- Running Windows Network Diagnostics

ERR_NAME_NOT_RESOLVED