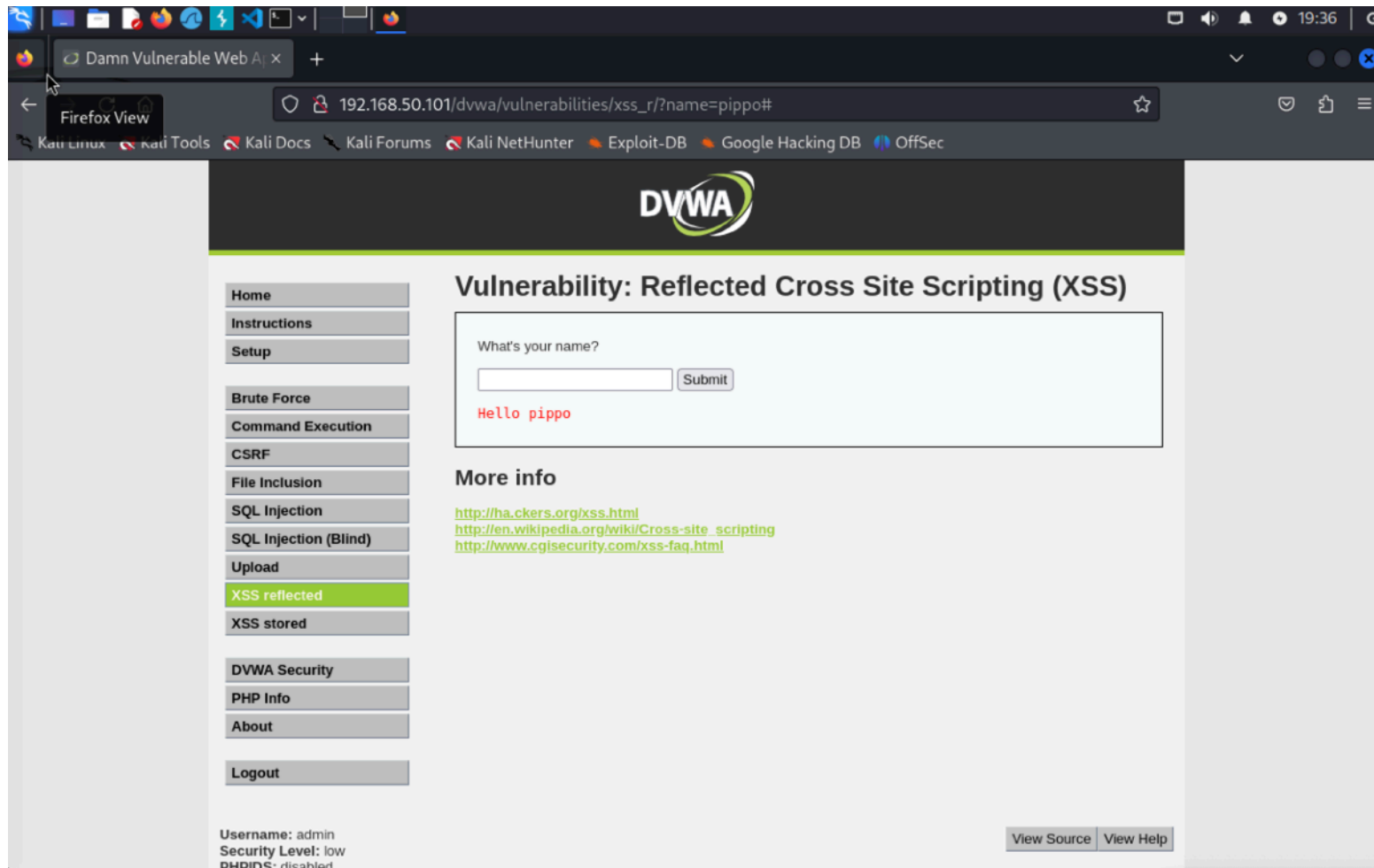


Testiamo se la webapp è affetta da XSS ed effettivamente il nostro input del form viene riportato sia sotto che nel campo URL



Iniettiamo codice HTML, utilizziamo il tag <i> con un input(es.pluto) e come output ci aspettiamo il nostro input ma in corsivo

The screenshot shows a web browser window with the address bar displaying the URL: `192.168.50.101/dvwa/vulnerabilities/xss_r/?name=<i>pluto<%2Fi>#`. The browser's tab is labeled "Applications in Vulnerable Web A". The browser's address bar also shows a list of bookmarks: "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", and "OffSec".

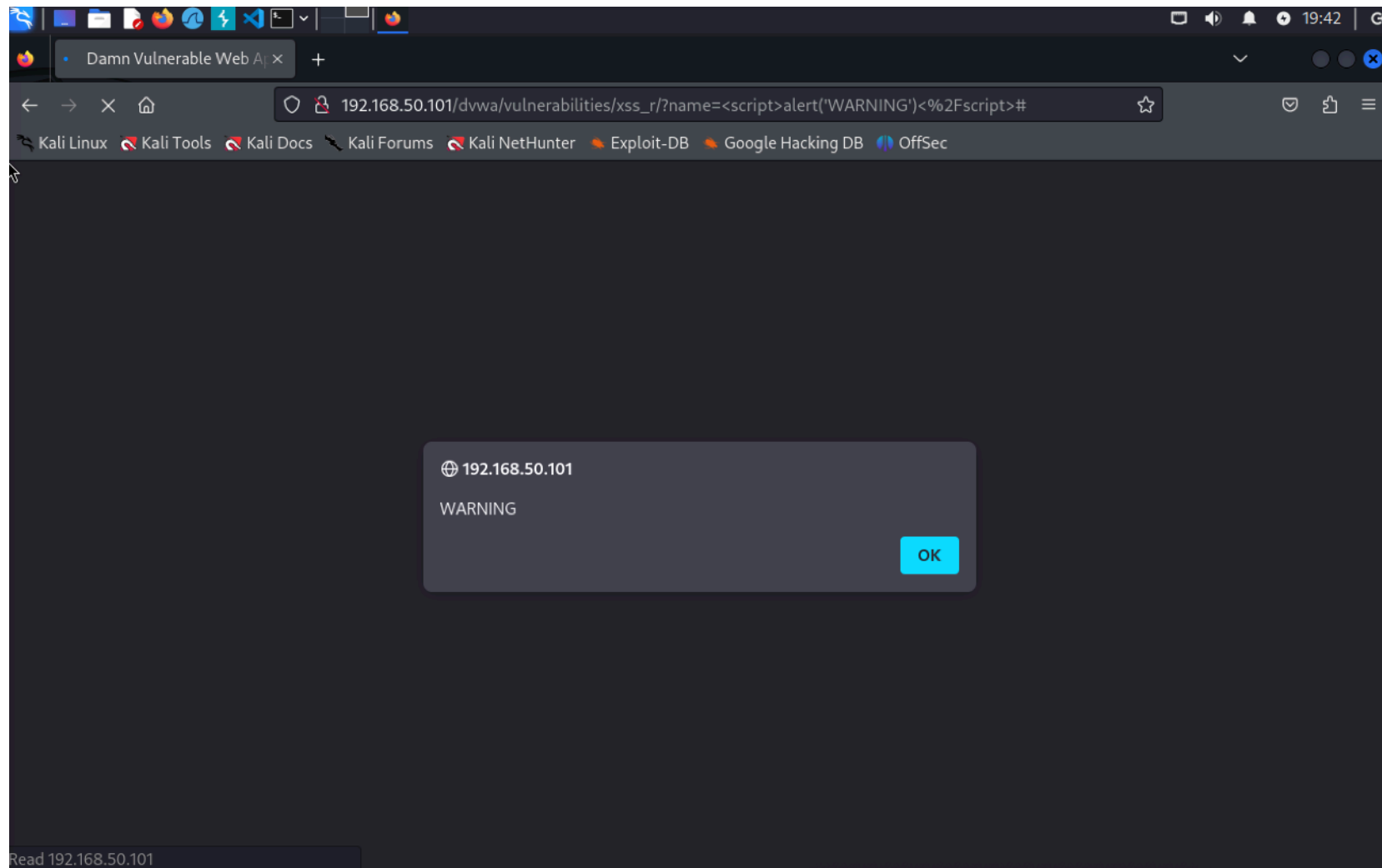
The DVWA application interface is visible. The top navigation bar includes the DVWA logo and a list of menu items: "Home", "Instructions", "Setup", "Brute Force", "Command Execution", "CSRF", "File Inclusion", "SQL Injection", "SQL Injection (Blind)", "Upload", "XSS reflected" (highlighted in green), "XSS stored", "DVWA Security", "PHP Info", "About", and "Logout".

The main content area is titled "Vulnerability: Reflected Cross Site Scripting (XSS)". It contains a form with the label "What's your name?". The input field contains the text "<i>pluto" and a "Submit" button. Below the input field, the output is displayed as "Hello *pluto*".

Below the form, there is a section titled "More info" with three links: <http://ha.ckers.org/xss.html>, [http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting), and <http://www.cgisecurity.com/xss-faq.html>.

At the bottom of the page, the status bar shows "Username: admin" and "Security Level: low". There are also "View Source" and "View Help" buttons.

Iniettiamo uno script con codice HTML per aprire un pop-up con la scritta “WARNING”



Intercettiamo con Burpsuite per conoscere i cookies di sessione e le varie info contenute nella chiamata.

The screenshot shows the Burp Suite Community Edition v2024.5.3 interface. The 'Proxy' tab is active, and the 'Intercept' sub-tab is selected. A request to http://192.168.50.101:80 is intercepted, and the 'Intercept is on' button is highlighted. The request is displayed in the 'Pretty' view, and the 'Inspector' panel on the right shows the request details.

Request to http://192.168.50.101:80

Forward Drop Intercept is on Action Open browser

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 3

Request cookies 2

Request headers 13

Notes

Event log All issues

Memory: 136.5MB

```
1 POST /dvwa/login.php HTTP/1.1
2 Host: 192.168.50.101
3 Content-Length: 44
4 Cache-Control: max-age=0
5 Accept-Language: en-US
6 Upgrade-Insecure-Requests: 1
7 Origin: http://192.168.50.101
8 Content-Type: application/x-www-form-urlencoded
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
10 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=0.7
11 Referer: http://192.168.50.101/dvwa/login.php
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=low; PHPSESSID=1994440d3f0c8ea974038a327845e195
14 Connection: keep-alive
15
16 username=admin&password=password&Login=Login
```