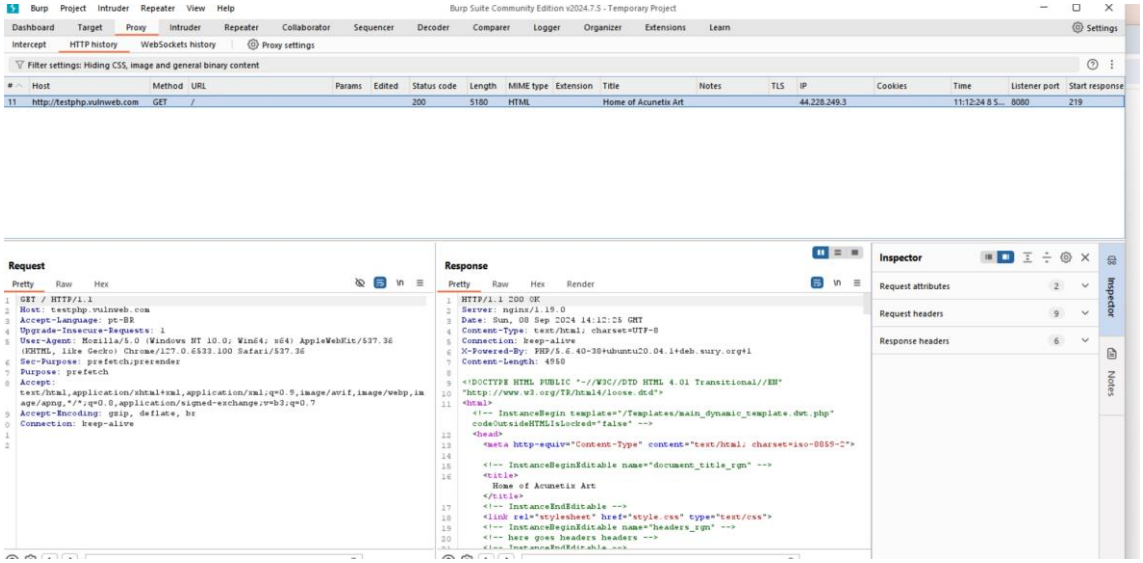
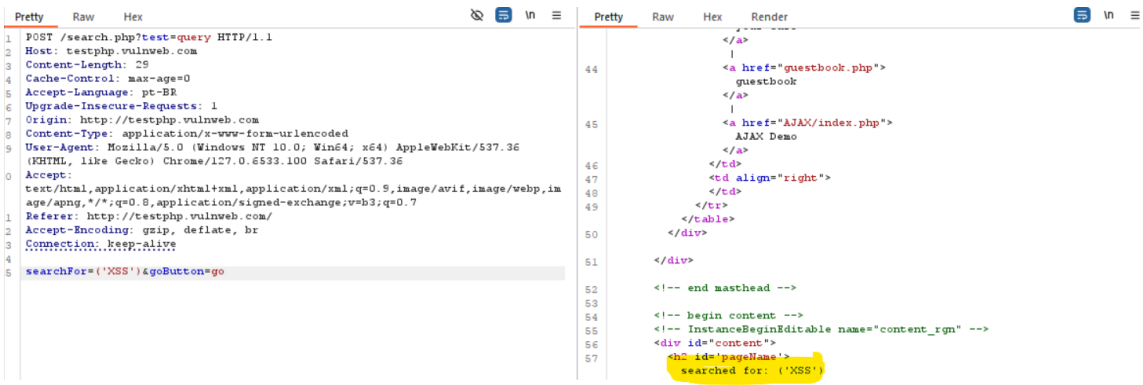
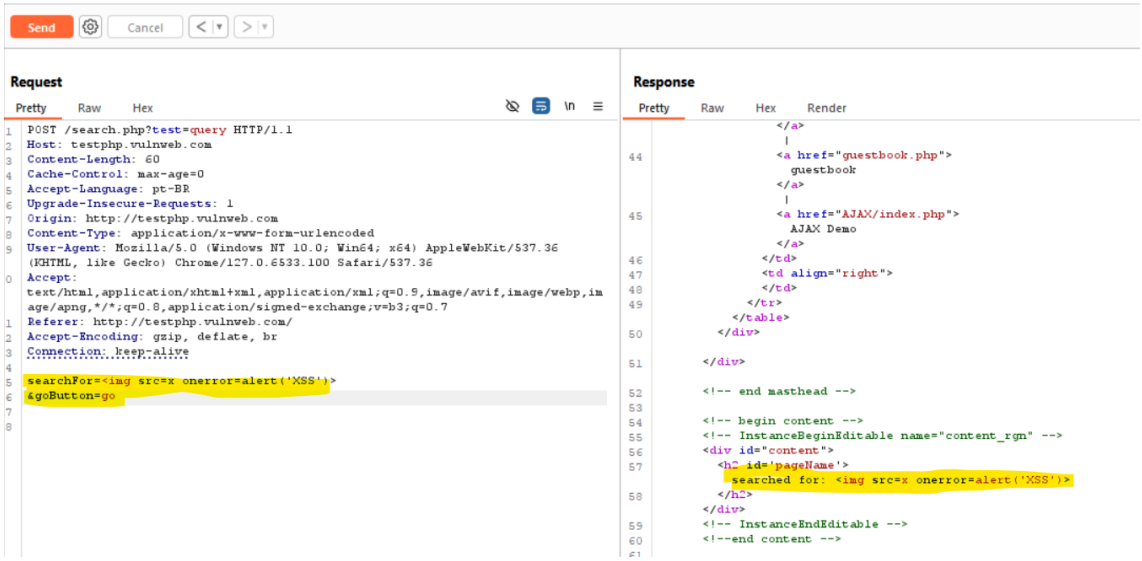
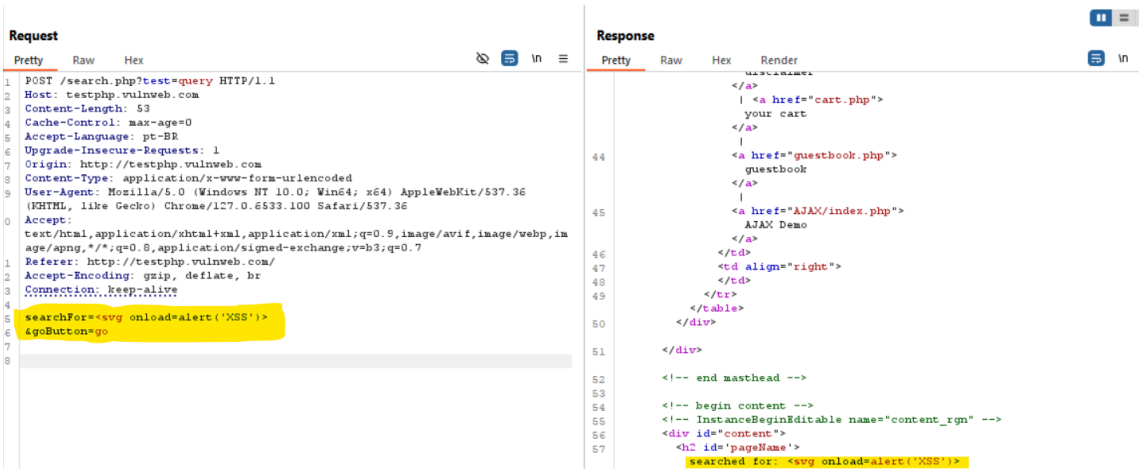
Através do Repeater, realize testes de XSS no campo de pesquisa do site http://testphp.vulnweb.com/.

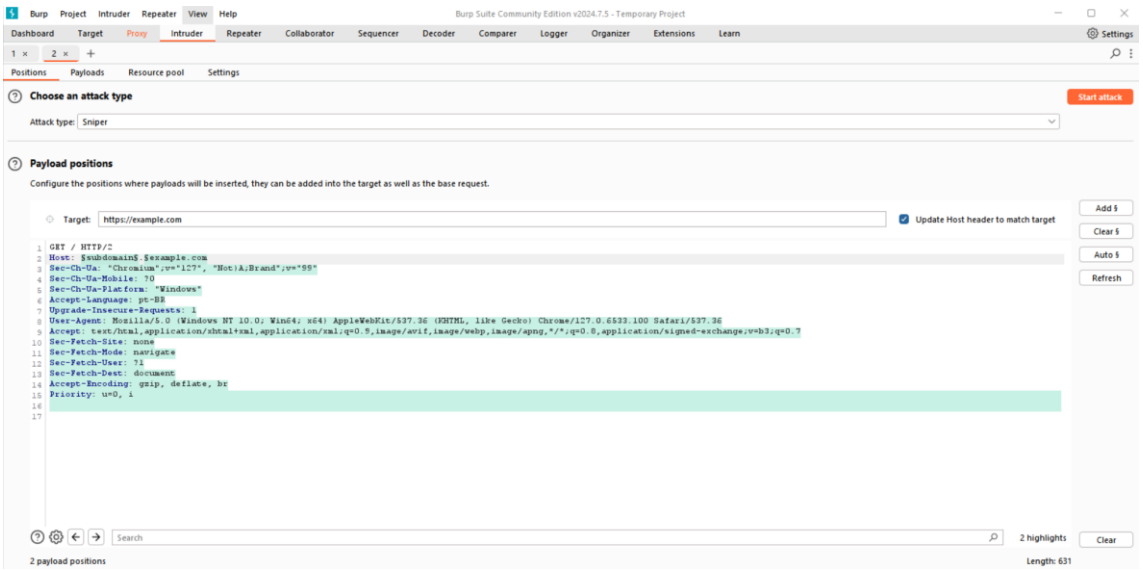


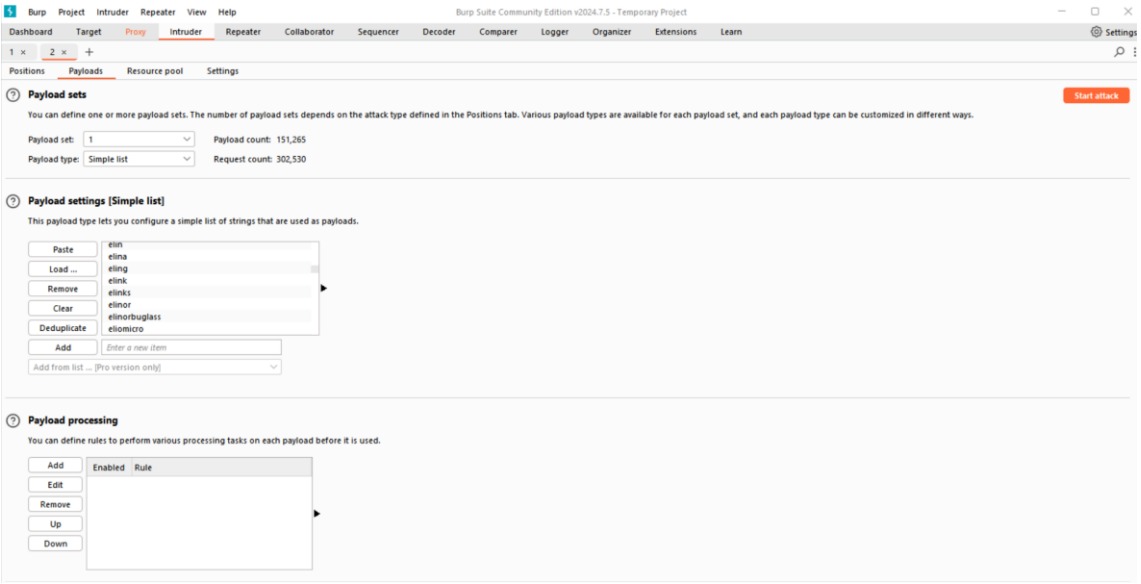


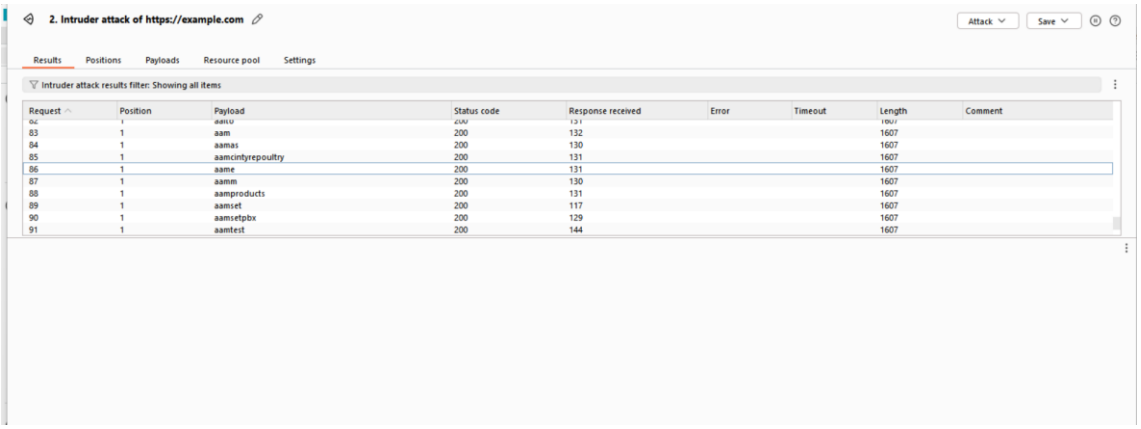




Realize uma enumeração de subdomínios em domínios à sua escolha e utilize a wordlist Discovery/DNS/namelist.txt. Utilize o Intruder.




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
Settings
1 × 2 ×
Positions Payloads Resource pool Settings
Payload sets
Start attack
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
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
elin
elina
eling
elink
elinks
elinor
elinorbuglass
eliomicro
Add
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.
Add
Edit
Remove
Up
Down
Enabled
Rule


2. Intruder attack of https://example.com
Attack
Save
Results Positions Payloads Resource pool Settings
Intruder attack results filter: Showing all items
Request Position Payload Status code Response received Error Timeout Length Comment
83 1 aam 200 132 1607
84 1 aamas 200 130 1607
85 1 aamcintyrepoultry 200 131 1607
86 1 aame 200 131 1607
87 1 aamm 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