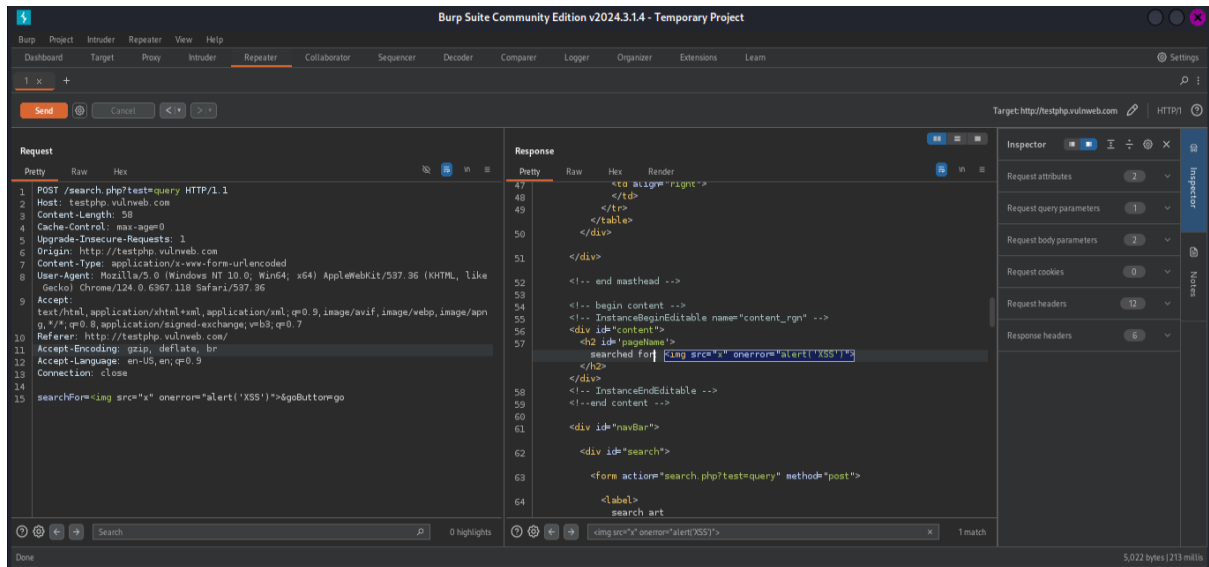
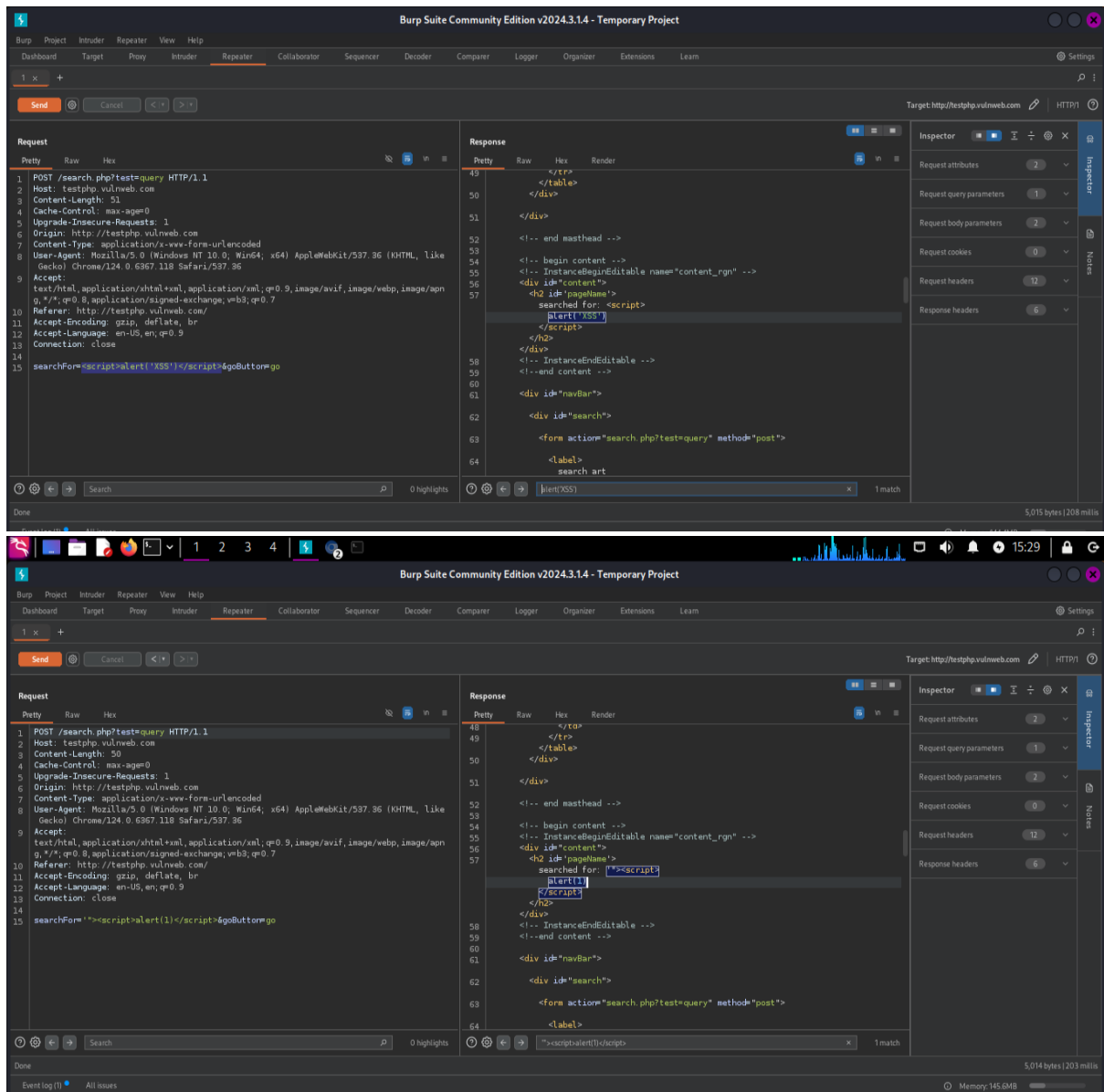


Através do Repeater, realize testes de XSS no campo de pesquisa do site <http://testphp.vulnweb.com/>.





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

2. Intruder attack of http://testphp.vulnweb.com

Attack Save

2. Intruder attack of http://testphp.vulnweb.comAttack Save

ResultsPositionsPayloadsResource poolSettings

Intruder attack results filter: Showing all items

| Request | Payload | Status code | Response received | Error | Timeout | Length | Comment |
|---------|---------------|-------------|-------------------|-------|---------|--------|---------|
| 93 | aandigaming | 200 | 211 | | | 5180 | |
| 94 | aandc | 200 | 219 | | | 5180 | |
| 95 | aanddcurlains | 200 | 201 | | | 5180 | |
| 96 | aandrewtest | 200 | 205 | | | 5180 | |
| 97 | aandreux | 200 | 305 | | | 5180 | |
| 98 | aaret | 200 | 239 | | | 5180 | |
| 99 | aap | 200 | 222 | | | 5180 | |
| 100 | aapo | 200 | 199 | | | 5180 | |
| 101 | aappi | 200 | 203 | | | 5180 | |
| 102 | aapras | 200 | 224 | | | 5180 | |
| 103 | aaprecherche | 200 | 202 | | | 5180 | |
| 104 | aaps | 200 | 236 | | | 5180 | |
| 105 | aapiest | 200 | 210 | | | 5180 | |

RequestResponse

PrettyRawHexRender

1 HTTP/1.1 200 OK

2 Server: nginx/1.19.0

3 Date: Sun, 08 Sep 2024 19:58:51 GMT

4 Content-Type: text/html; charset=UTF-8

5 Connection: keep-alive

6 X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

7 Content-Length: 4958

8

9 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"

10 "http://www.w3.org/TR/html4/loose.dtd">

11 <html>

12 <!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false" -->

13 <head>

14 <meta http-equiv="Content-Type" content="text/html; charset=utf-8">

Search0 highlights

105 of 151265