

UTILISATION DE BURPSUITE

EFFECTUER UNE REQUÊTE POST DEPUIS UNE LISTE DÉROULANTE

The screenshot shows the Burp Suite interface with the HTTP history tab active. A table lists three requests:

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP
1	http://192.168.1.39	GET	/vulnerabilities/sqli/			200	4908	HTML		Vulnerability: SQL Injectio...			192.168.1.39
2	https://push.services.mozilla.com	GET	/			101	240					✓	34.117.65.55
3	http://192.168.1.39	POST	/vulnerabilities/sqli/		✓	200	4967	HTML		Vulnerability: SQL Injectio...			192.168.1.39

The selected request (3) is shown in the Request pane:

```
1 POST /vulnerabilities/sqli/ HTTP/1.1
2 Host: 192.168.1.39
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
  Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
  /webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 18
9 Origin: http://192.168.1.39
10 Connection: close
11 Referer: http://192.168.1.39/vulnerabilities/sqli/
12 Cookie: PHPSESSID=9avgut3kkm1pq4db0tv0udr1u4; security=medium
13 Upgrade-Insecure-Requests: 1
14
15 id=16Submit=Submit
```

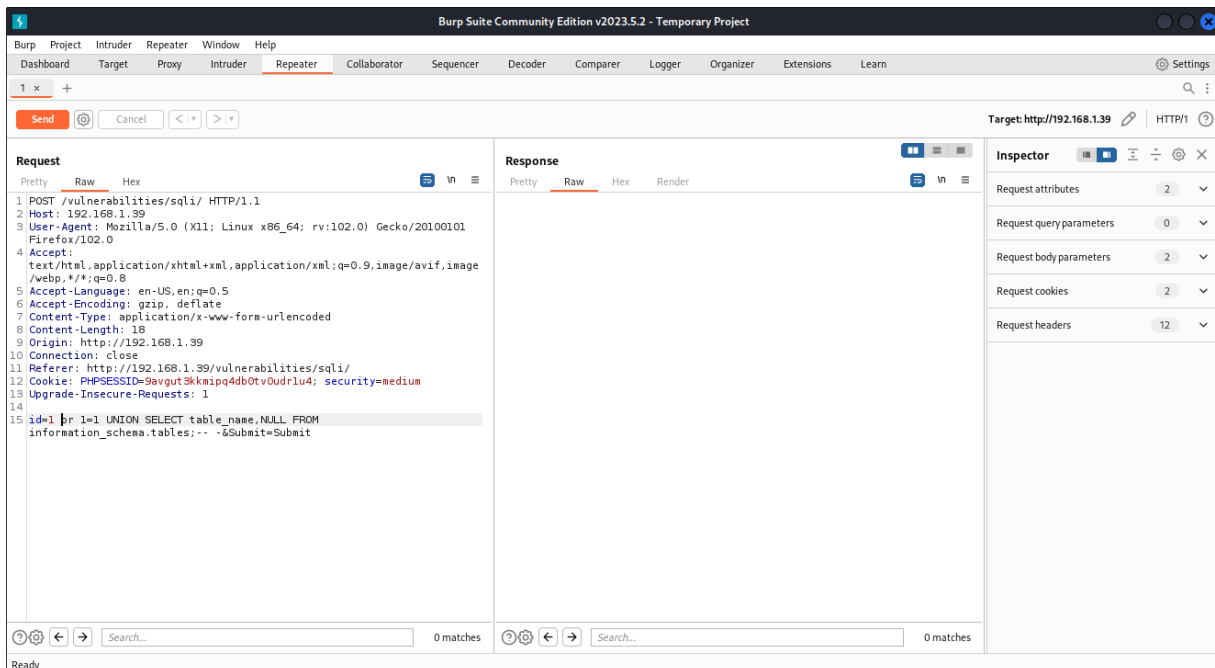
Repérer la requête POST. On repère le paramètre id (ici égal à 1)

The screenshot shows the Burp Suite interface with the Repeater tab active. The request from the previous screenshot is loaded into the Repeater:

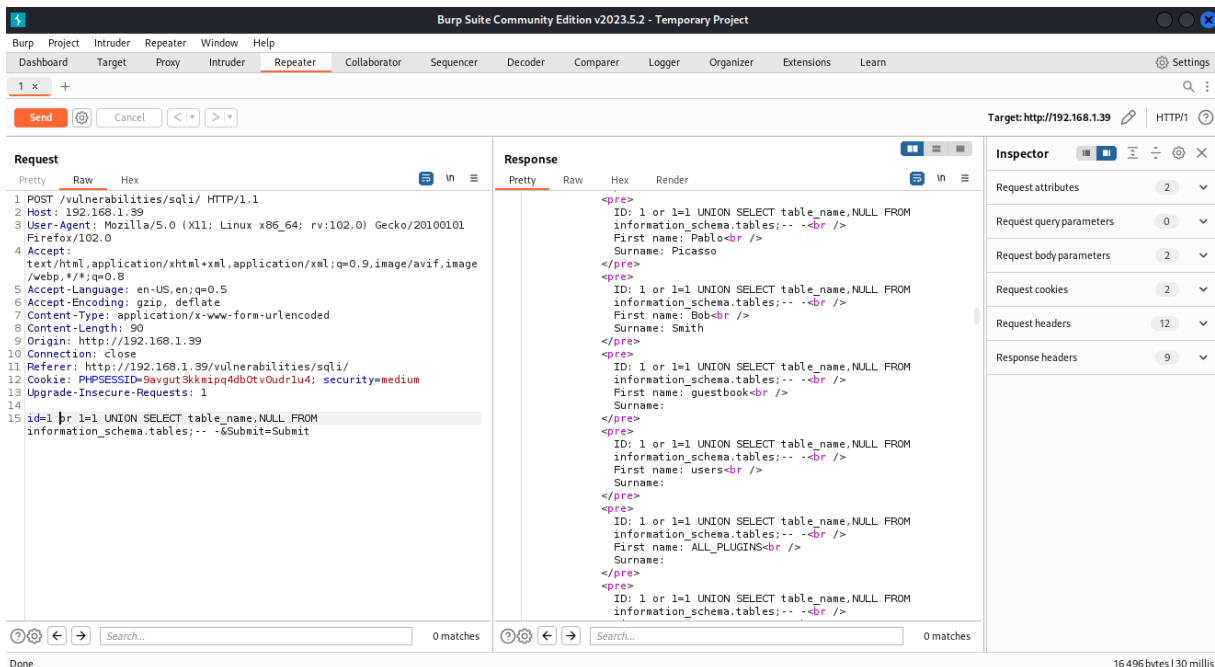
```
1 POST /vulnerabilities/sqli/ HTTP/1.1
2 Host: 192.168.1.39
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
  Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
  /webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 18
9 Origin: http://192.168.1.39
10 Connection: close
11 Referer: http://192.168.1.39/vulnerabilities/sqli/
12 Cookie: PHPSESSID=9avgut3kkm1pq4db0tv0udr1u4; security=medium
13 Upgrade-Insecure-Requests: 1
14
15 id=16Submit=Submit
```

The 'Send' button is highlighted, indicating the next step in the process.

On clique droit sur la zone request et on choisit « envoi vers repeater »



On insère la requête sql après id.



On clique sur send et on observe la réprety dans la zone « réponse »