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 Udemy 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.



Sources:-

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

CVE-2023-41507

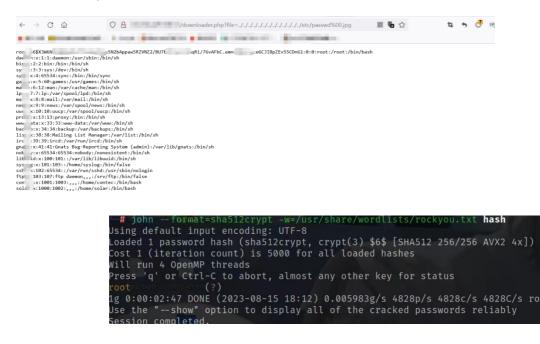
Super Store Finder v3.6 was discovered to contain multiple SQL injection vulnerabilities in the store locator component via the products, distance, lat, and lng parameters.

Re	Request							Response III = =						
Pro	Pretty Raw Hex 🚍 IN 🚍								Pretty Raw Hex Render 🚍 \N =					
2 3	1 POST /locations/index.php HTTP/2 2 Rost: 3 Concent-Length: 102 4 Cookie:							1 HTTP/2 200 OK						
6 7 9 10 11 12 13 14 15 16 17 18 19		: en-US,er : grip, de pplication h: XMLHttp empty cors same-orig se ducts=!	n;q=0.5 eflate n/x-www-form pRequest /10	-urlencoded;	charset=UTF-	-8	14 15 16 17	Array ([0] => Inv that corre '''' HAVIN line 1) ((pre> (pre> SELECT latitu RADIAN stores 39.915 ("su sea	alid query: You have an errot in y sponds to your NySQL server versio 5 distance <- 35.915051442750454 O *, (3955 * ACOS(COS(RADIANS(-2 de)) * COS(RADIANS(longitude) 5(-27.4704528)) * SIN(RADIANS(l WHERE status=1 AND approved=1 AN 051442758454 ORDER BY distance ASO cesses":0,mmsg": "No nearby stores w rch") seed SQL injection	n for t RDER BY 7.47045 - RADI atitude D cat_i LIMIT	he right synt distance ASC 28)) * COS(ANS(153.02603))) AS d d=''' HAVING 0,60	ax to use near LIMIT 0,60' at RADIANS(41)) + SIN(istance FROM distance <=		
entr	users ry]	ocation	+	+		+						++		
id	facebook_id	email	address	created	status	lastname	modified		password		username	firstname		
	NULL	NULL	NULL	NULL	1	NULL			4481	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: <u>https://www.contecinc.com/</u>



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

