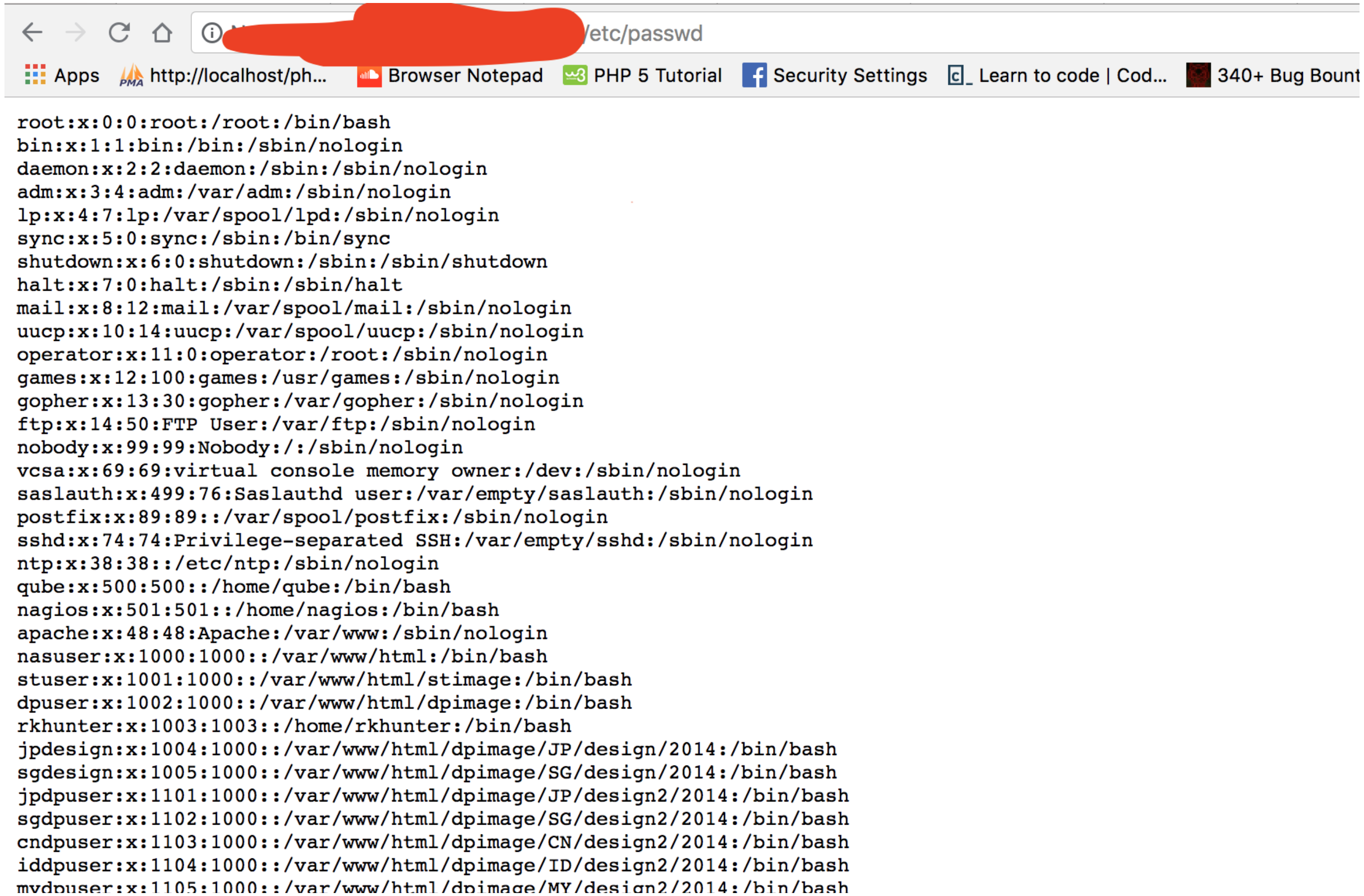
Chain The Bugs to Pwn an Organisation (LFI + Unrestricted File Upload = Remote Code Execution)

Armaan Pathan Follow
Sep 18, 2018 · 2 min read

Hi everyone,
After completing my OSCP certification I thought to give a try to bug bounty, as OSCP has sharpened my exploitationSkills.

I will use lol.com to represent an application as can not disclose the website’s name.

While i was enumerating an application i got a domain which was basically an image server and was managing the images which has uploaded by a user, while enumerating more, i got an endpoint which was allowing me to call the server local files such as passwd , cron jobs and current running services on the server.



```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
saslauth:x:499:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
qube:x:500:500::/home/qube:/bin/bash
nagios:x:501:501::/home/nagios:/bin/bash
apache:x:48:48:Apache:/var/www:/sbin/nologin
nasuser:x:1000:1000::/var/www/html:/bin/bash
stuser:x:1001:1000::/var/www/html/stimage:/bin/bash
dpuser:x:1002:1000::/var/www/html/dpimage:/bin/bash
rkhunter:x:1003:1003::/home/rkhunter:/bin/bash
jpdesign:x:1004:1000::/var/www/html/dpimage/JP/design/2014:/bin/bash
sgdesign:x:1005:1000::/var/www/html/dpimage/SG/design/2014:/bin/bash
jpdpuser:x:1101:1000::/var/www/html/dpimage/JP/design2/2014:/bin/bash
sgdpuser:x:1102:1000::/var/www/html/dpimage/SG/design2/2014:/bin/bash
cndpuser:x:1103:1000::/var/www/html/dpimage/CN/design2/2014:/bin/bash
iddpuser:x:1104:1000::/var/www/html/dpimage/ID/design2/2014:/bin/bash
mydpuser:x:1105:1000::/var/www/html/dpimage/MY/design2/2014:/bin/bash
```

As it was a image server means the server stores all the images which user uploads form his/her profiles.

I again went back to lol.com and started looking for photo upload functionality that from where i can upload the photo and i got the profile photo option which is allowing me to upload the photos to an application and the photos were storing to the image server.

Now photo upload functionality has ext parameter which is used for file extensions checks but due to improper validations on the parameter, i was able to tamper the values and can upload unrestricted files on the server, i tried to upload php shell but as it was image server so it was not serving the php but by reconig more via lfi i came to know that i can get a shell via perl so i uploaded a perl reverse shell to get a reverse shell on my public IP.

And with the use of LFI I called the file and i got the reverse shell on my public IP.

Thanks for reading, Hope you guys liked it.

JavaScript Hacking Remote Code Execution Lfi Hackerone

181 claps

WRITTEN BY

Armaan Pathan

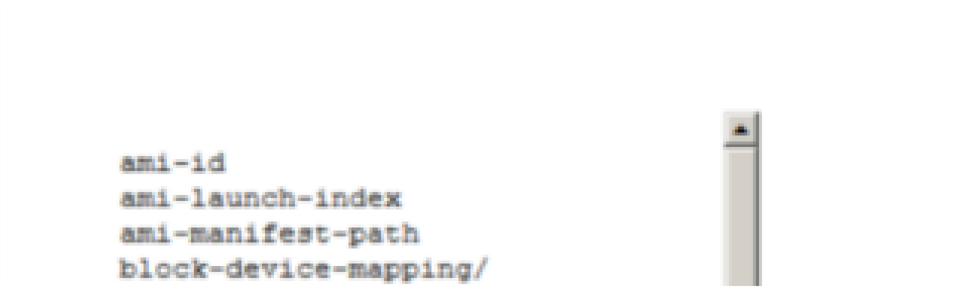
Follow

See responses (2)

More From Medium

Related reads

The Bugs Are Out There, Hiding in Plain Sight



```
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
```

The Bugs Are Out There, Hiding in Plain Sight

A Bug’z Life in A Bug’z Life
Jul 15 · 6 min read ★

709

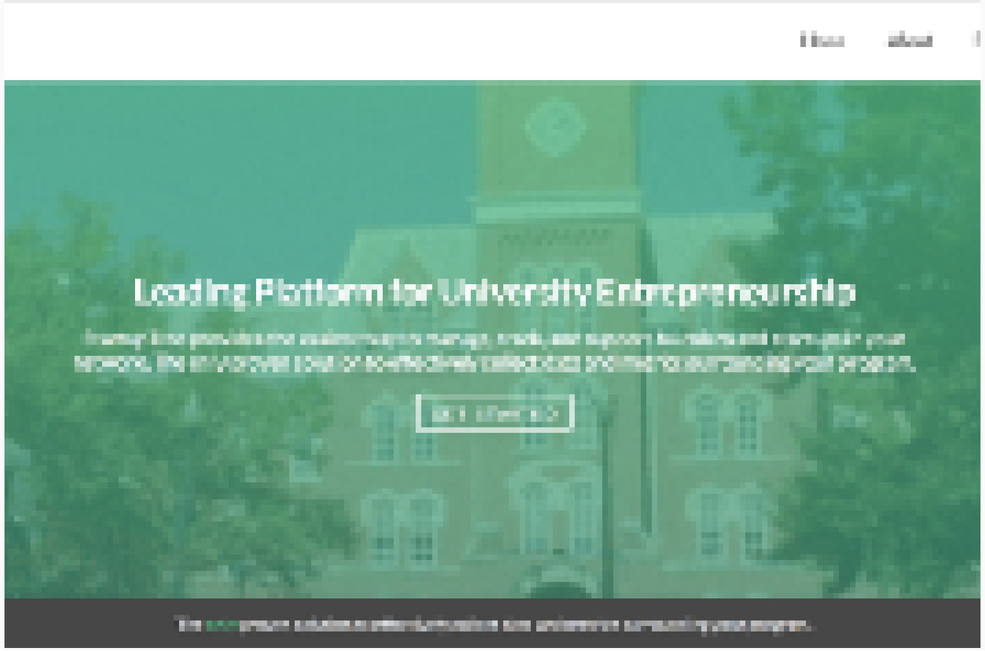
```
s great   events/
          hostname
          iam/
          identity-credentials/
```

Related reads

Open Redirects & Security Done Right!

Akshay ‘Ax’ Sharma
Jun 19, 2018 · 3 min read ★

490



Leading Platform for University Entrepreneurship

Related reads

The BatchOverflow Bug and How to Catch All Bugs

Kiran Garimella

May 11, 2018 · 12 min read ★

319

Discover Medium

Welcome to a place where words matter. On Medium, smart voices and original ideas take center stage - with no ads in sight. Watch

Make Medium yours

Follow all the topics you care about, and we'll deliver the best stories for you to your homepage and inbox. Explore

Become a member

Get unlimited access to the best stories on Medium — and support writers while you're at it. Just $5/month. Upgrade

Medium

About Help Legal