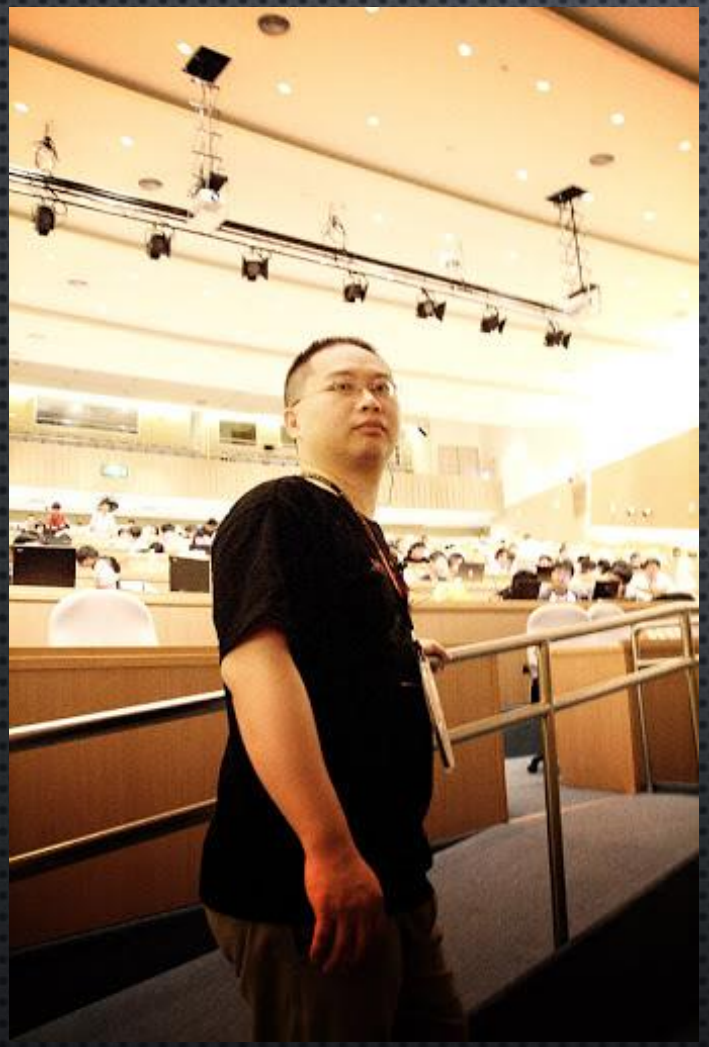
如何利用 DOCKER 強化網站安全

Containersummit.ithome.com.tw

Tim Hsu



徐千洋 (TIM HSU)

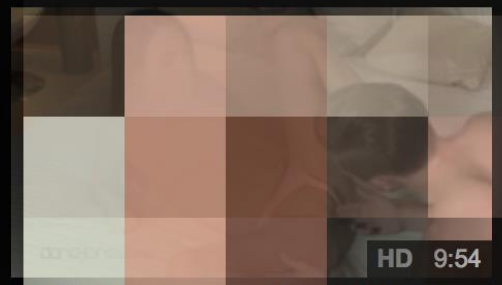
CHROOT 創辦人
HITCON　創辦人
網駭科技　創辦人

曾任:
台灣大哥大 資安部經理
現職:
VARMOUR 美商安連網路公司台灣分公司

NEW CONTEST : 50 SHADES OF PORNHUB! Upload your wildest BDSM videos for a chance to win a kinky sexy toy bundle! See the details on our blog!

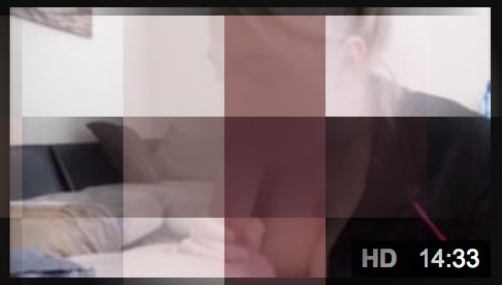
Hot Videos Internationally

+ More Videos



Lexi Dona Forcing Him To Cum Inside Her

515,116 views 78%



LittleOralAndie vs. First Monster Cock: Fans Raffle Winning

536,267 views 87%

SisLovesMe - Sis Finds My Hidden Cam & Masturbates

554,498 views 76%

TUSHY.com Hot Sister Gets Anal from Brothers Friend

716,366 views 80%

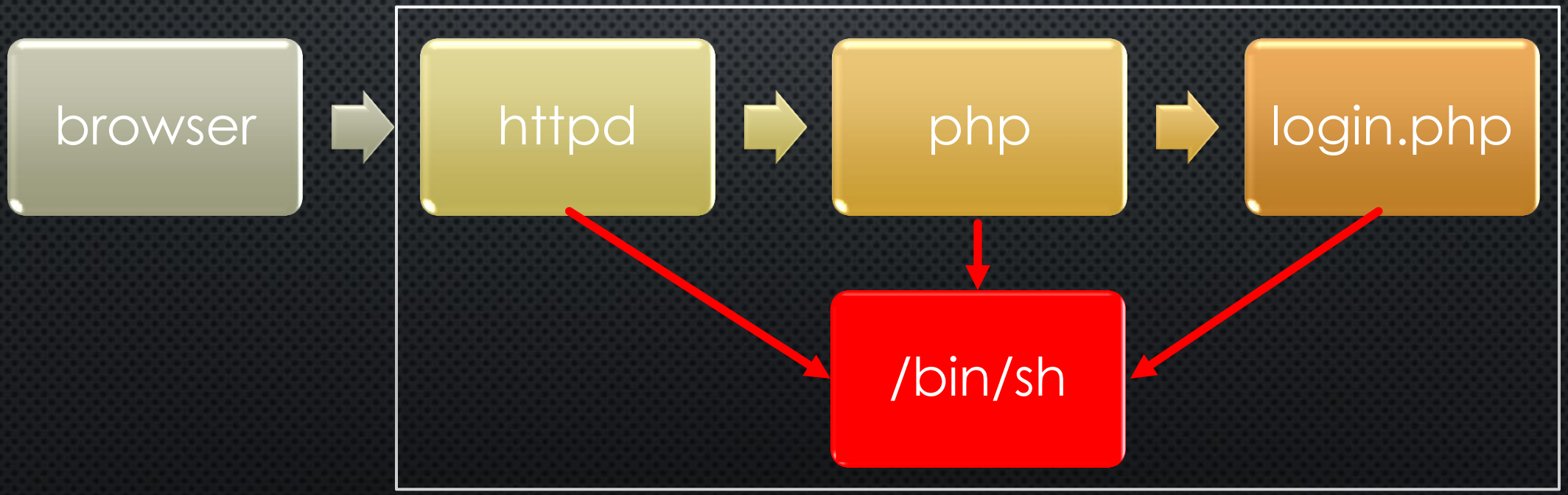
Rewards

Pornhub may provide rewards to eligible reporters of qualifying vulnerabilities. Our minimum reward is $50 USD, and our maximum rewards is $25,000 USD. Reward amounts may vary depending upon the severity of the vulnerability reported.

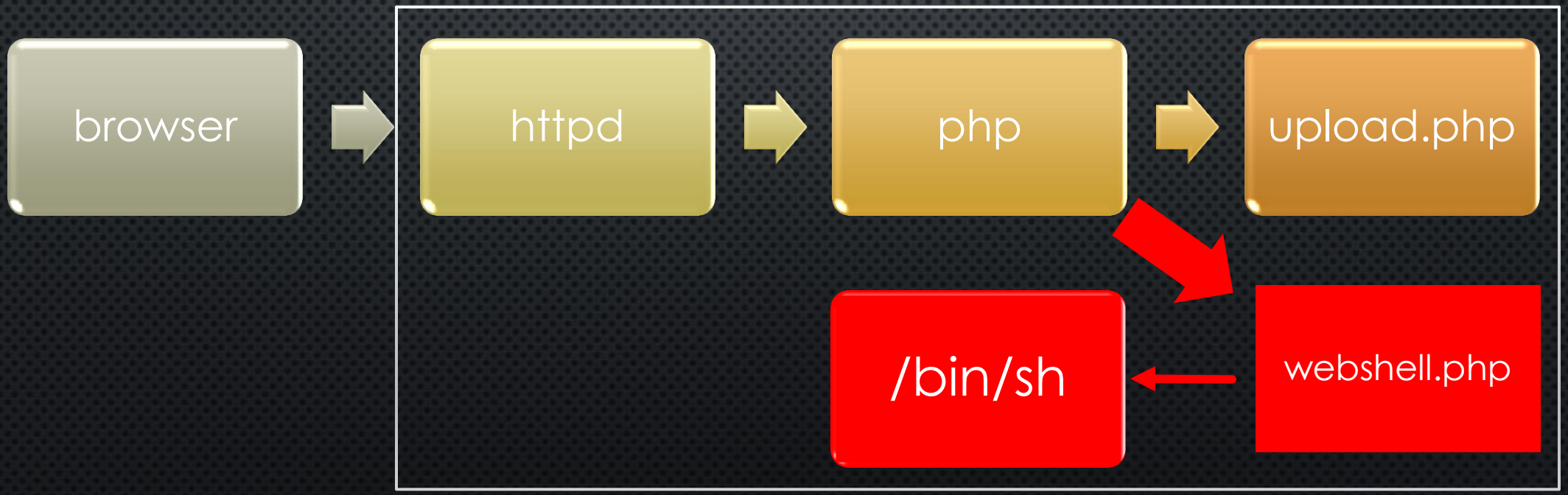
The following table outlines the average rewards for specific classes of vulnerabilities:

Vulnerability Types	Core Pornhub *	All Other
Remote Shell / Command Execution	$15,000	$5,000
Remote Code Execution	$10,000	$2,500
SQL Injection (with output)	$5,000	$2,500
Significant Authentication Bypass	$5,000	$1,000
Local file Inclusion	$2,500	$1,000
SQL Injection (blind)	$2,500	$1,000
Insecure Direct Object References	$1,500	$750
Server Side Request Forgery	$1,500	$750
Stored Cross Site Scripting	$1,500	$500
Other Cross Site Scripting	$250	$50

遠端命令執行(REMOTE CODE EXECUTION)



遠端命令執行(REMOTE CODE EXECUTION)



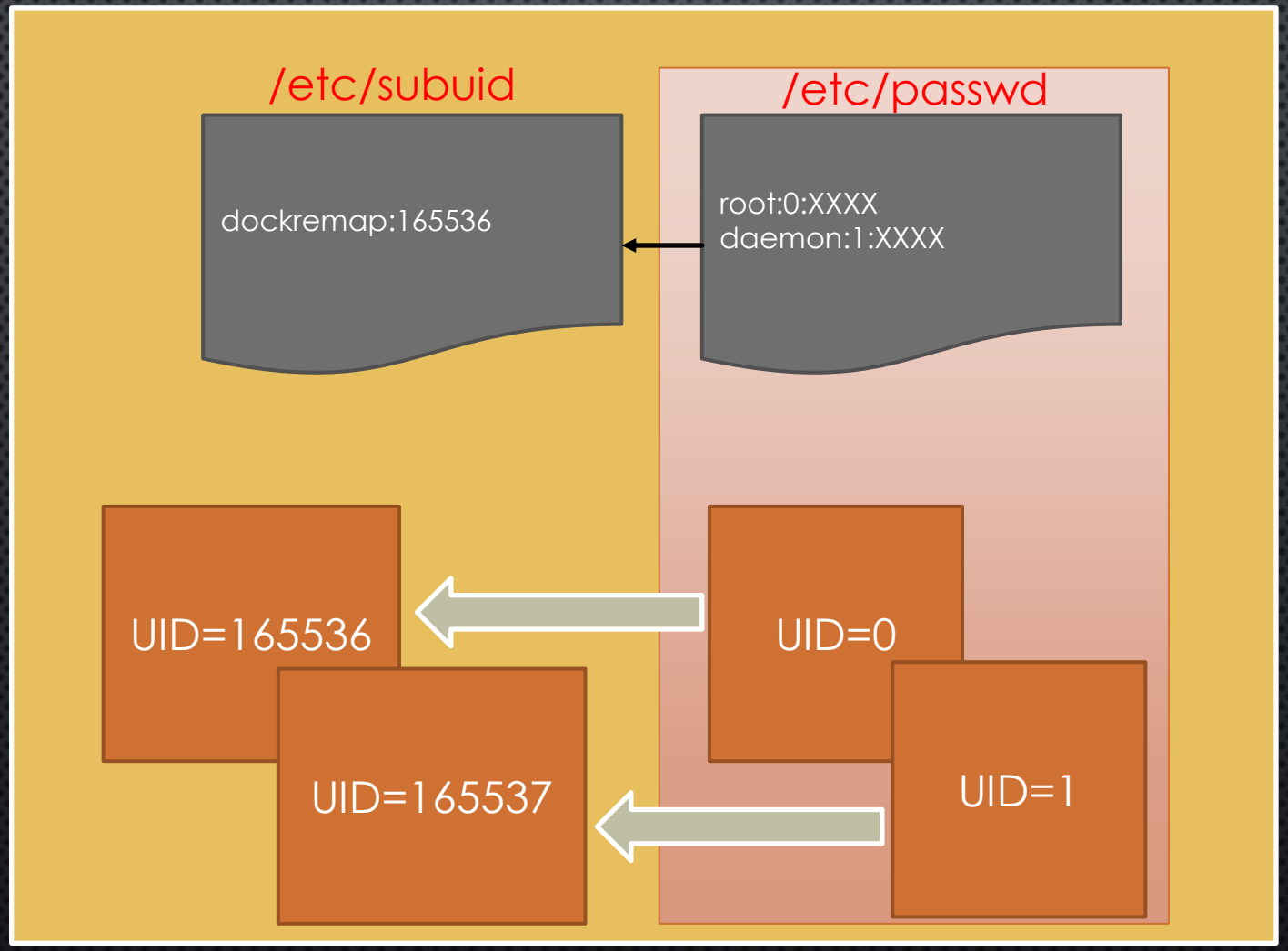
DOCKER CONTAINER 的安全強化

三個強化技術

- USER-NAMESPACE
- CAPABILITIES
- APPARMOR

USER-NAMESPACE

- Container 不再用 root 權限執行
- 在 Container 底下的 root 帳號其實會對應對 HOST 的一般權限帳號
- 從 host 來看，所有在 Container 下的執行程序都會是一般權限執行


/etc/subuid
dockremap:165536
/etc/passwd
root:0:XXXX
daemon:1:XXXX
UID=165536
UID=165537
UID=0
UID=1

CAPABILITIES

- 將特權帳號能做的事，切割成數十個，並給予控制
- 例如: /BIN/PING 傳統上必須為 SETUID-ROOT 權限的程式
- 如今，它只要有 CAP_NET_RAW CAPABILITY

```
# ls -al /bin/ping
-rwxr-xr-x 1 root root 44168 Mar 15
2014
# getcap /bin/ping
/bin/ping = cap_net_raw+p
```

APPARMOR

- 針對程序作存取控制

```
/usr/sbin/nginx {

#include <abstractions/apache2-common>
#include <abstractions/base>

    capability dac_override,
    capability net_bind_service,
    capability setgid,
    capability setuid,

    /etc/passwd r,
    /etc/group r,
    deny /bin/sh mrwklx,
}
```

CONTAINER 的網站服務強化術

基本強化法則

- 避免服務程序用 ROOT 權限執行
- 服務程序的權限不可寫入網頁程式或設定檔
- 服務程序有權寫入的檔案，不能被執行

針對 CONTAINER 安全強化

- 設定 USER NAMESPACE
- 去除不必要的 CAPABILITIES
- 利用 APPARMOR 作存取限制

針對 IMAGE 最佳化

- 移除不需要的檔案或程式
- 重設所有指令的權限
- 檢視所有可讀和可寫的檔案及目錄

其它想法

- 將偵測到 RCE 的記錄送往 SOC/SIEM
- 對所有 CONTAINER 新增的檔案，進行分析、記錄、隔離、告警
- 限制 CONTAINR 無法對外部建立網路連線

結論

- 依服務量身打造運行的 CONTAINER 環境
- 利用 USER-NAMESPACE、CAPABILITIES、APPARMOR 強化安全
- CONTAINER 可以讓服務多一層安全保障

Q&A

感謝各位聆聽

TIMHSU.TW@GMAIL.COM

HTTP://GITHUB.COM/TIMHSUTW

DEMO: HTTPS://GITHUB.COM/TIMHSUTW/CONTAINERSUMMIT2016_ITHOME

參考資料

1. AppArmor security profiles for Docker
   https://docs.docker.com/engine/security/apparmor/
2. VulApps
   https://hub.docker.com/r/medicean/vulapps/
   https://github.com/Medicean/VulApps/
3. Pornhub bug bounty
   https://hackerone.com/pornhub
4. Docker security
   https://docs.docker.com/engine/security/security/
5. Critical: Remote Command Execution in WordPress Form Manager Plugin (CVE-2015-7806)
   http://appcheck-ng.com/remote-command-execution-in-wordpress-form-manager-plugin-cve-2015-7806/
6. Struts2 RCE PoC
   https://github.com/coffeehb/Some-PoC-oR-ExP/tree/master/Struts2