



SYSTEM HARDENING

~ hardening?

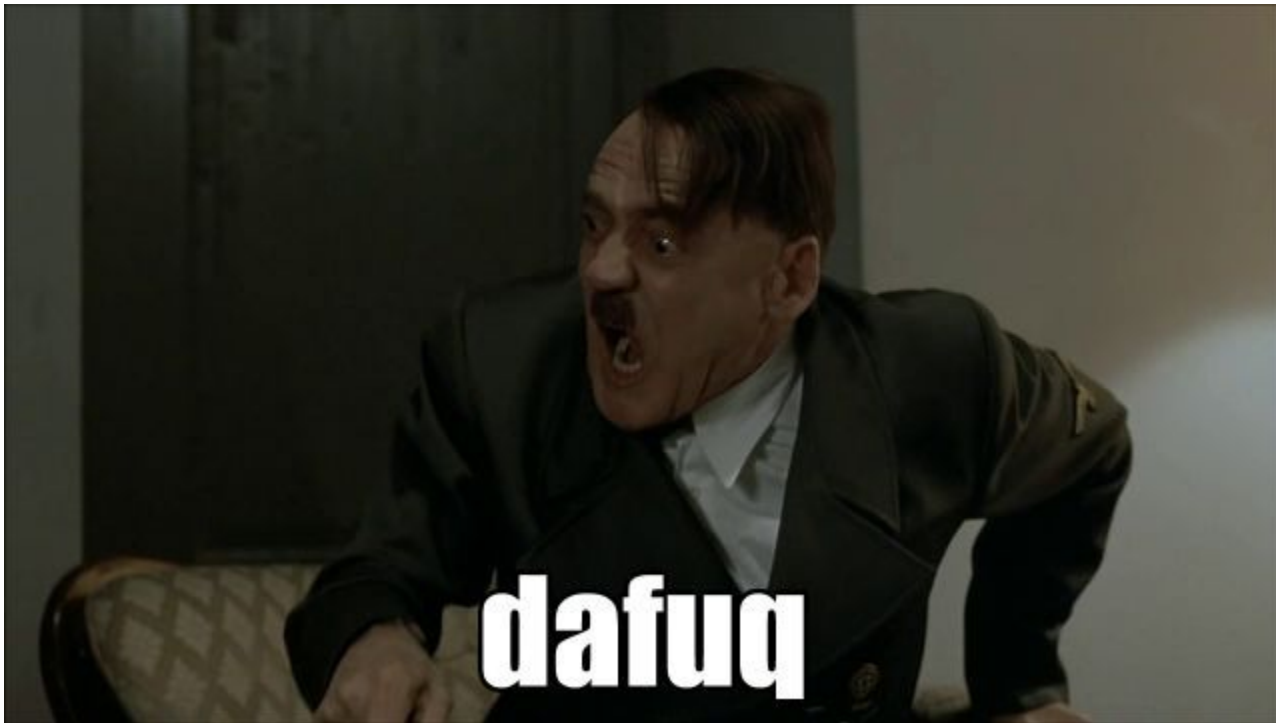




~ hardening?

- Fiziksel Sıkılaştırma
- Sistem Sıkılaştırma
- Uygulama Sıkılaştırma
- Servis Sıkılaştırma

~ fiziksel sıkılaştırma



~ fiziksel sıkılaştırma

- BIOS
- Fiziksel Erişim
 - Sunucuların barındırılması
 - BadUSB
 - EvilUSB



~ sistem sıkılaştırma

- Windows
- Unix Türevleri

~ sistem sıkılaştırma

- Parola politikaları
- Dosya erişim izinleri
- Kullanıcı/Grup izinleri
- Ağ katmanında güvenlik

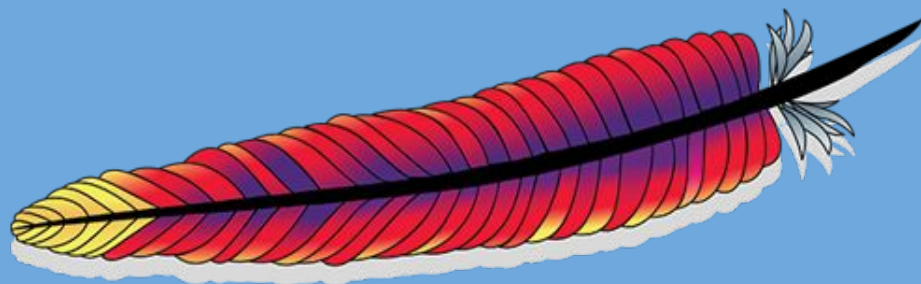
~ uygulama sıkılaştırma

- php, python, java ...
- version tabanlı zafiyetler, güvenli olmayan fonksiyon/method/kütüphane tabanlı zafiyetler,
- statik/dinamik kod analizi

~ servis sıkılaştırma

VSFTPD
FtpServer





A P A C H E

~ apache http server





~ apache http server

- /etc/apache2/
- /var/www/
- /var/log/apache2/



~ apache http server banner

- banner nedir ?
- banner bilgisi kaynaklı tehlikeler ?
- banner gizleme
 - ServerTokens
 - ServerSignature

~ apache http server directory listing

- directory listing nedir ?
- directory listing kaynaklı tehlikeler ?
- directory listing engelleme
 - <Directory ..



~ apache http server user

- `groupadd -r apache`
- `useradd apache -r -g apache -d /var/www -s /sbin/nologin`
- `passwd -l apache`
- `apache2.conf - envvars`

~ apache http server limit http methods

- <Directory /usr/local/apache2/cgi-bin
 - <LimitExcept GET POST OPTIONS>
 - deny from all



~ apache http server disable trace

- /etc/apache2/confs-enabled/security.conf
- TraceEnable Off



~ apache http server timeout

- /etc/apache2/
- timeout

~ apache http server disable other http versions

- mod_rewrite.so
- LoadModule rewrite_module modules/mod_rewrite.so
- RewriteEngine On

```
RewriteCond %{THE_REQUEST} !HTTP/1\..1$
```

```
RewriteRule .* - [F]
```

~ apache http server disable .htaccess

- `<FilesMatch "^\.ht">`

`Order allow,deny`

`Deny from all`

`Satisfy All`

`</FilesMatch>`

~ apache http server disable file ext.

- `<FilesMatch`

```
"^.*\.(css|html?|js|pdf|txt|xml|xsl|gif|ico|jpe?g|png)$">
```

```
Order Deny,Allow
```

```
Allow from all
```

```
</FilesMatch>
```



~ apache http server

- ssl
- mod_security



~ SSH





~ SSH - Key

- ssh-keygen
- public/private key
- authorized_keys



~ SSH

- `/etc/ssh/`
- `/home/{user}/.ssh`



~ SSH root login

- PermitRootLogin no



~ SSH empty password

- `PermitEmptyPassword no`



~ SSH auth try

- MaxAuthTries #



~ SSH pubkey auth

- PubkeyAuthentication yes
- PasswordAuthentication no



~ SSH users

- AllowUsers/Groups