Webguneen segurtasuna aztertzen

Webgune baten teknologiak identifikatzen

Segurtasunaren ikuspegitik, funtsezkoa da web orri batean erabiltzen diren teknologiak eta tresnak ezagutzea. Teknologia horiek identifikatzeak aukera ematen die segurtasuneko adituei webgune baten arrisku potentzialak ebaluatzeko, urrakortasunak identifikatzeko eta informazio sentikorra eta datu kritikoak babesteko estrategia eraginkorrak diseinatzeko.

Lineako hainbat tresna eta utilitate daude web orri batean erabiltzen diren teknologiak identifikatzeko. Tresna ezagunenetako batzuk Whatweb, Wappalyzer eta builtwith.com dira. Tresna horiek web-orria eskaneatzen dute, eta erabilitako teknologiei buruzko informazio zehatza ematen dute, hala nola programazio-lengoaiari, web-zerbitzariari eta edukia kudeatzeko sistemei buruzkoa, besteak beste.

Whatweb tresna urrakortasunak aztertzeko erabilgarritasun bat da, web-orria eskaneatzen duena eta erabilitako teknologiei buruzko informazio zehatza ematen duena. Tresna hori erabil daiteke, halaber, web-orrian egon daitezkeen ahulguneak eta ahulguneak identifikatzeko.

Wappalyzer, bestalde, web orrian erabiltzen diren teknologiak detektatu eta erakusten dituen nabigatzailearen luzapena da. Tresna hau bereziki erabilgarria da web-orri batean erabilitako teknologiak berehala identifikatu nahi dituzten segurtasuneko adituentzat, eskaneatze osoa egin behar izan gabe.

Builtwith.com web-orri batean erabiltzen diren teknologiak identifikatzeko aukera ematen duen lineako tresna bat da. Tresna honek erabilitako teknologiei buruzko informazio zehatza ematen du, baita estatistika erabilgarriak ere, hala nola trafikoa eta webgunearen ospea.

Ikusitako tresnak:

- Whatweb
- Wappalyzer
- Builtwith

Fuzzying eta webguneen fitxategi bilaketa

Klase honetan, Wfuzz eta Gobuster tresnak erabiltzen ditugu Fuzzing aplikatzeko. Teknika hau web zerbitzari batean ezkutatuta dauden ibilbideak eta baliabideak aurkitzeko erabiltzen da, indar gordineko erasoen bidez. Asmo txarreko erasotzaileek zerbitzarira baimenik gabe sartzeko erabil ditzaketen ezkutuko baliabideak aurkitzea da helburua.

Wfuzz edukia deskubritzeko tresna bat eta datuak injektatzeko tresna bat da. Funtsean, web aplikazioetako kalteberatasunak probatzeko prozesuak automatizatzeko erabiltzen da.

Web aplikazio baten parametroetan eta direktorioetan indar gordineko erasoak egiteko aukera ematen du, dauden baliabideak identifikatzeko. Wfuzzen abantailetako bat da oso pertsonalizagarria dela eta hainbat proba-beharretara egokitu daitekeela. Wfuzzen desabantailetako batzuk bere komandoen sintaxia ulertzeko beharra dute, eta mantsoagoa izan daiteke edukia aurkitzeko beste tresna batzuekin alderatuta.

Bestalde, Gobuster edukia aurkitzeko tresna bat da, web-aplikazio batean ezkutuko fitxategiak eta direktorioak bilatzeko ere erabiltzen dena. Wfuzz bezala, Gobuster indar gordineko erasoetan oinarritzen da ezkutuko fitxategi eta direktorioak aurkitzeko. Gobusterren abantaila nagusietako bat abiadura da, ezaguna baita edukia aurkitzeko tresna azkarrenetako bat delako. Erabilerraza ere bada eta sintaxia sinplea da. Hala ere, Gobusterren desabantaila bat da agian ez dela Wfuzz bezain pertsonalizagarria.

Laburbilduz, Wfuzz eta Gobuster web-aplikazioetan kalteberatasun-probak egiteko tresna erabilgarriak dira, baina ikuspegian eta ezaugarrietan desberdintasunak dituzte. Bata edo bestea aukeratzea zure beharren eta lehentasun pertsonalen araberakoa izango da.

Jarraian, tresna hauetarako esteka emango dizugu:

- Wfuzz
- Gobuster

Gobuster instalatu

1. Klonatu repositorioa /opt karpetan Gobuster.
2. Konpilatu proiektua, gobuster karpeta barruan

```
go build .
```

Go instalatu

2. Instalatu go lenguaia konpilatzailea
    1. Deskargatu tarball https://go.dev/dl/go1.21.6.linux-amd64.tar.gz

```
curl -OL https://golang.org/dl/go1.21.6.linux-amd64.tar.gz
```

3. Deskonprimitu paketea

```
tar -C /usr/local -xvf go1.21.6.linux-amd64.tar.gz
```

4. Go routa ezarri

```
nano ~/.profile
```

Gehitu linea hau fitxategira

```
export PATH=$PATH:/usr/local/go/bin
```

5. Refresh profila

```
source ~/.profile
```

6. Ziurtatu bertsio go `version` idatziz

Gobuster erabili

```
.\gobuster dir -u  [weguneare helbidea] -w [seclist ruta] -t 200
```

- https://tolosaldea.hezkuntza.net/
- /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt

```
.\gobuster dir -u https://tolosaldea.hezkuntza.net/ -w /usr/share/SecLists/D
```

Irteera gorde.

```
./gobuster dir -u https://ikasgela.tolosaldealh.eus/ -w /usr/share/SecLists
```

```
-b 403,404
```

Deskargatu seclist /usr/share karpetan

```
git clone https://github.com/danielmiessler/SecLists
```

WFUZZ trensa erabiltzen

Instalatu tresna

```
apt install wfuzz
```

Adibide agindu bat

```
wfuzz -c --hc=404,403 -t 200 -w /usr/share/SecLists/Discovery/Web-Content/di
```

Parametro batzuk:

```
# Show line
--sl=216

# Hide line
--hl=216

# Bi paiload eribiliz bata, hitzekin rutarako eta beztea zerrenda bat fitxat

wfuzz -c --hc=404,403 -t 200 -w /usr/share/SecLists/Discovery/Web-Content/di


# Rangoak erabiltzen adibidez produktu ideak identfikatzeko

wfuzz -c -t 200 -z range,1-20000 'https://www.mi.com/shop/buy/detail?product
```