



Recon & Information Leak

@splitline



基礎思路

觀察建置環境 (Recon)

- 用什麼語言？
- 什麼版本？
- 什麼框架？
- 架在什麼伺服器？
- ...

尋找漏洞 / fuzz

- 理解語言特性/框架原理
- 網站邏輯
- 已知框架/套件漏洞

實際攻擊

- 將漏洞轉為實體危害
- 擴張漏洞的危害性

Recon (Reconnaissance) / 偵查

- 網站指紋辨識
 - Special URL path
 - Error message
 - HTTP Response Header
 - Session ID
 - (And more)
- 自動分析網站技術的 browser extension : <https://www.wappalyzer.com/>

Infomation Leak / 資訊洩漏

- 開發人員忘記關閉 debug mode 或錯誤訊息
- 不小心把不該公開的東西推到 production 上
 - 例如：備份、設定檔
- CTF 怕太通靈，只好偷偷給你原始碼（0）

常見套路

- robots.txt
- .git / .svn / .bzz
- .DS_Store
- .index.php.swp
- Backup files

常見套路

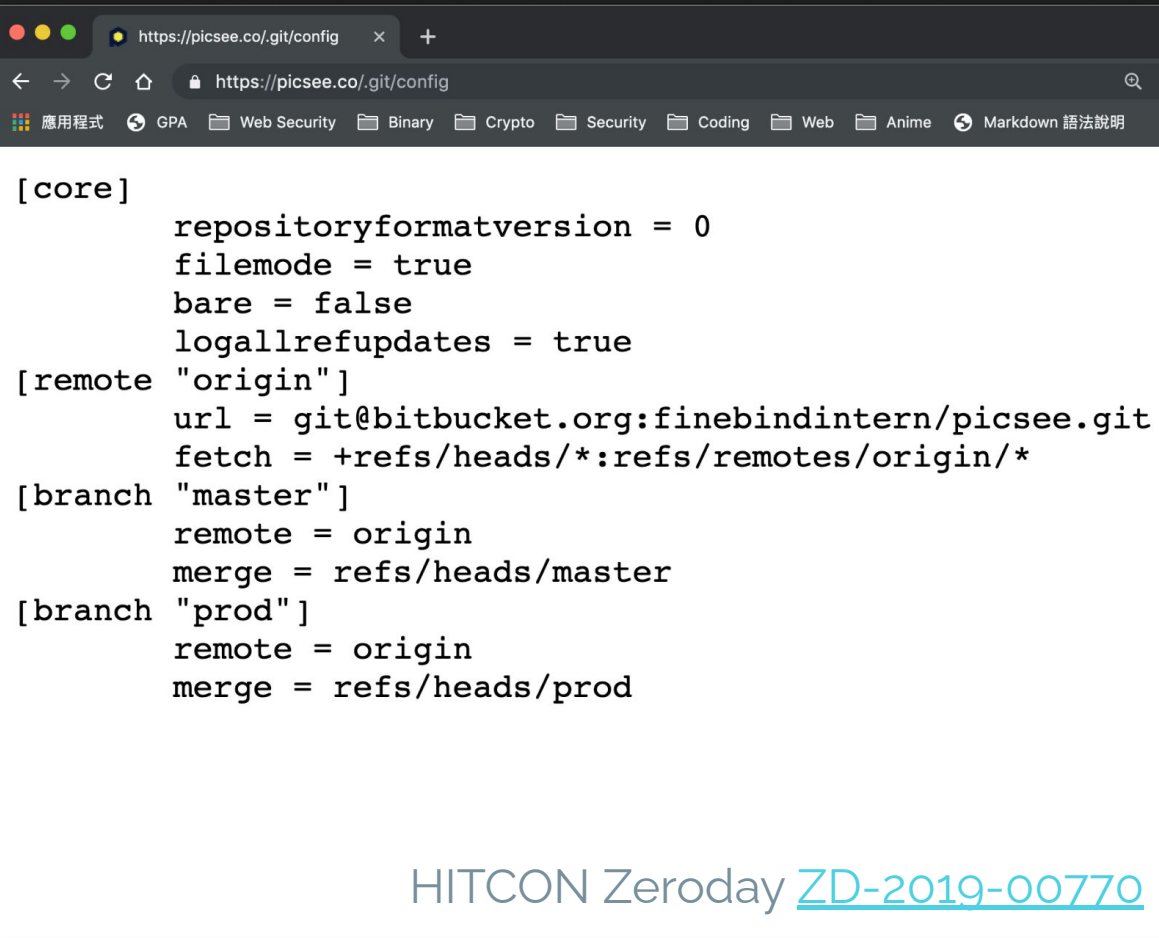
- robots.txt
 - 告訴爬蟲什麼該看什麼不該看
 - 可能包含 **不想被爬取** 的路徑
 - 管理後台？
- .git / .svn / .bzip
- .DS_Store
- .index.php.swp
- Backup files



```
User-Agent: *
Disallow: /posts/
Disallow: /posts?
Disallow: /amzn/click/
Disallow: /questions/ask/
Disallow: /questions/ask?
Disallow: /search/
Disallow: /search?
Disallow: /feeds/
Disallow: /feeds?
Disallow: /users/login/
Disallow: /users/login?
Disallow: /users/logout/
Disallow: /users/logout?
Disallow: /users/filter/
Disallow: /users/filter?
Disallow: /users/signup
Disallow: /users/signup/
Disallow: /users/signup?
Disallow: /users/authenticate/
Disallow: /users/authenticate?
Disallow: /users/oauth/*
Disallow: /users/flag-summary/
Disallow: /users/flair/
Disallow: /users/flair?
Disallow: /users/activity/
Disallow: /users/activity/?
Disallow: /users/stats/
Disallow: /users/*?tab=accounts
Disallow: /users/*?tab=activity
Disallow: /users/rep/show
Disallow: /users/rep/show?
Disallow: /users/prediction-data
Disallow: /users/prediction-data/
Disallow: /users/prediction-data?
Disallow: /unanswered/
Disallow: /unanswered?
```

常見套路

- robots.txt
- .git / .svn / .bzip
 - 版本控制系統
 - 可還原 source code
 - Tools (for git)
[denny0223/scrabble](#)
[lijiejie/GitHack](#)
- .DS_Store
- .index.php.swp
- Backup files



The screenshot shows a web browser window with the address bar displaying `https://picsee.co/.git/config`. The browser's bookmark bar includes links for 應用程式, GPA, Web Security, Binary, Crypto, Security, Coding, Web, Anime, and Markdown 語法說明. The main content area displays the configuration file's text:

```
[core]
    repositoryformatversion = 0
    filemode = true
    bare = false
    logallrefupdates = true
[remote "origin"]
    url = git@bitbucket.org:finebindintern/picsee.git
    fetch = +refs/heads/*:refs/remotes/origin/*
[branch "master"]
    remote = origin
    merge = refs/heads/master
[branch "prod"]
    remote = origin
    merge = refs/heads/prod
```

HITCON Zeroday [ZD-2019-00770](#)

常見套路

- robots.txt
- .git / .svn / .bzip
- .DS_Store
 - macOS 上自動產生的隱藏檔
 - 可得知資料夾內的文件名稱、路徑
 - [lijiejie/ds_store_exp](#)
- .index.php.swp
- Backup files

常見套路

- robots.txt
- .git / .svn / .bzip
- .DS_Store
- .index.php.swp
 - vim 暫存檔
 - 可以直接還原原本的 source
- Backup files

常見套路

- robots.txt
- .git / .svn / .bzip
- .DS_Store
- .index.php.swp
- Backup files
 - www.tar.gz
 - backup.zip
 - ...

Google Hacking

- `site:nycu.edu.tw`
- `intext:"管理介面"`
- `filetype:sql`

Google Hacking Database (GHDB):

<https://www.exploit-db.com/google-hacking-database>

Other tricks

- Dirsearch
- Subdomain enumeration