

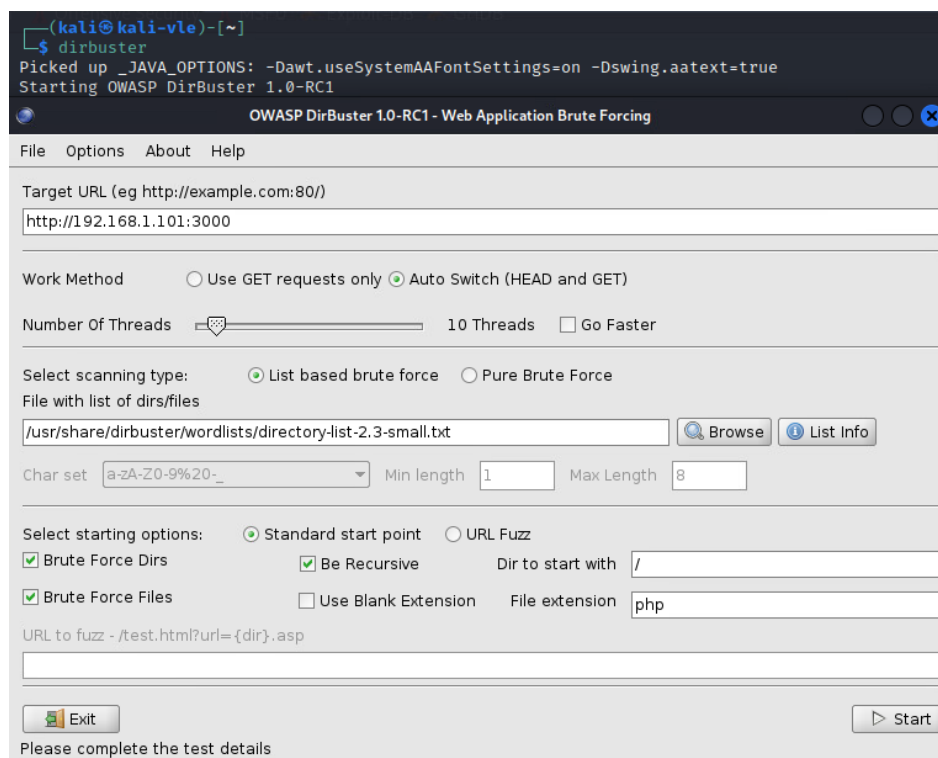
Juice Shop - Easter Egg

Description

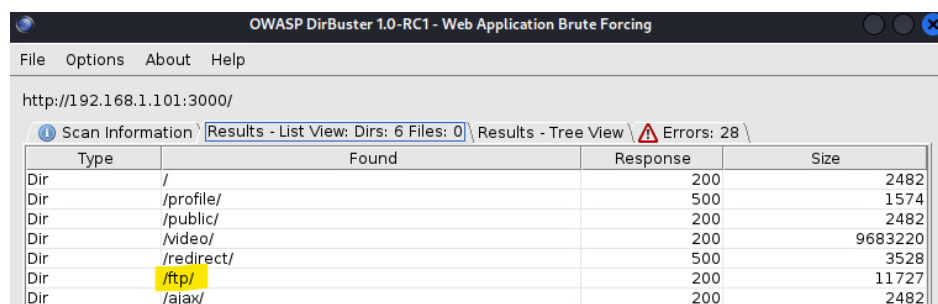
Website stores sensitive information to websites directories and they are easy to access.

Steps to produce

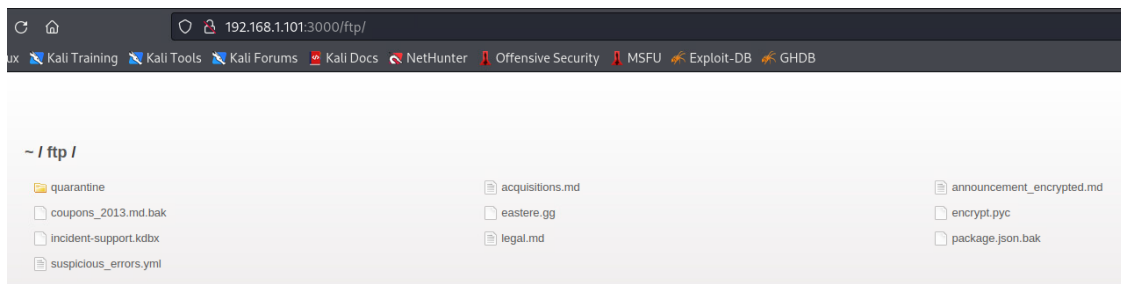
Open DirBuster and put <http://192.168.1.101:3000> to target field. Then select wordlist to be used for example I used DirBusters own 'directory-list-2.3-small.txt' file. Then hit start.



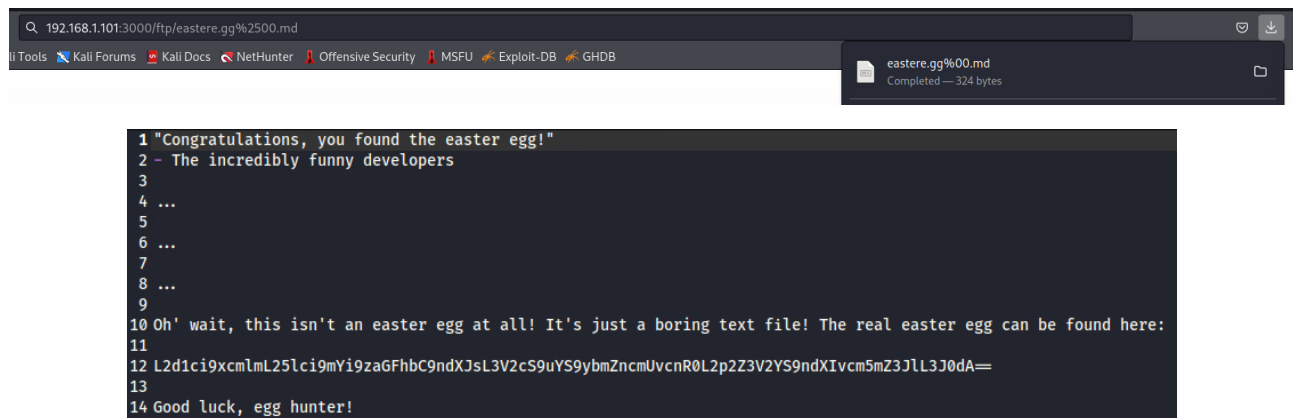
Here is directory list that it found.



Open web browser and go to <http://192.168.1.101:3000/ftp> .



There is 'eastere.gg' file. To open it we need to go <http://192.168.1.101:3000/ftp/eastere.gg%2500.md> . We need to add ' %2500.md ' to the end because it only allows access to .md and .pdf file types.



Impact estimation

High severity. With this attacker can get sensitive information about website/company.

Mitigation

You should not store this kind of information straightly to the website. If you still have to store it use some kind of encryption to it. For hiding sensitive directories use noindex instead of robots.txt.

<https://developers.google.com/search/docs/crawling-indexing/block-indexing> .

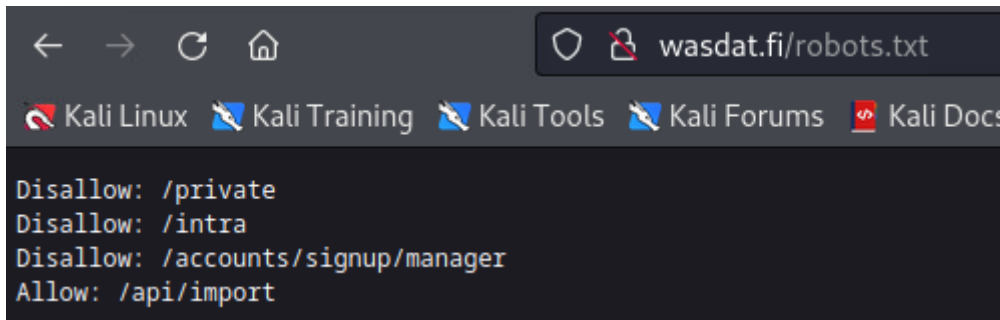
Main target - Coupon codes stored in plain text

Description

Website stores sensitive information to websites directories and they are easy to access. In this example attacker can get the coupon codes.

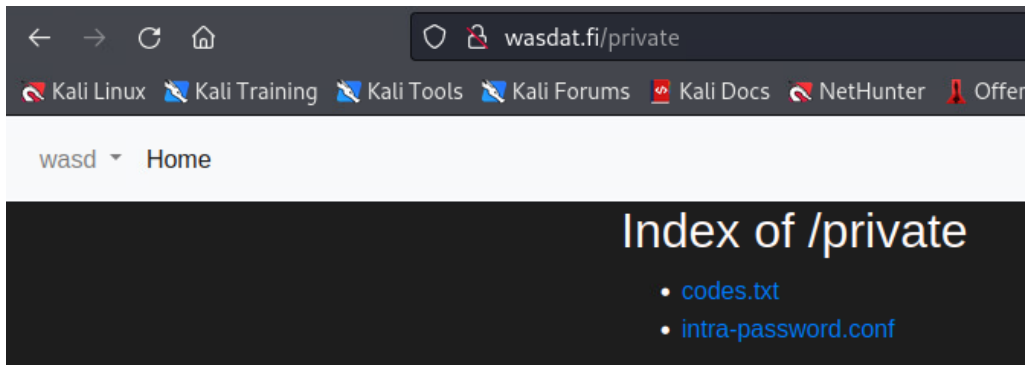
Steps to produce

Open your browser and go to <http://wastad.fi/robots.txt> .



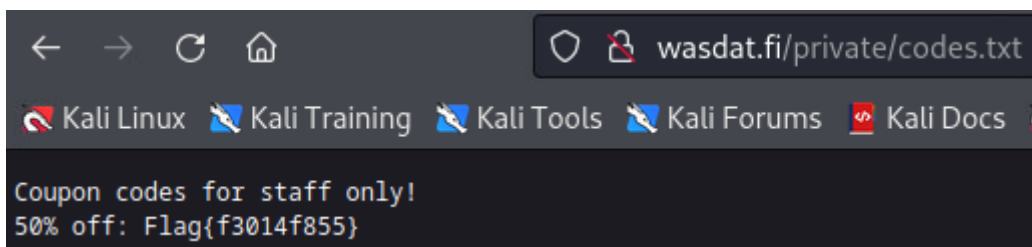
```
← → ↻ 🏠 wasdat.fi/robots.txt
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs
Disallow: /private
Disallow: /intra
Disallow: /accounts/signup/manager
Allow: /api/import
```

Then go to <http://wasdat.fi/private> .



```
← → ↻ 🏠 wasdat.fi/private
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offer
wasd ▾ Home
Index of /private
• codes.txt
• intra-password.conf
```

There is codes.txt file. Open it.



```
← → ↻ 🏠 wasdat.fi/private/codes.txt
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs
Coupon codes for staff only!
50% off: Flag{f3014f855}
```

Impact estimation

High severity. With this attacker can get sensitive information about website/company.

Mitigation

You should not store this kind of sensitive information to the public website directories. Give this kind of information privately to employees. You can also use noindex instead of robots.txt to hide directories.

<https://developers.google.com/search/docs/crawling-indexing/block-indexing> .

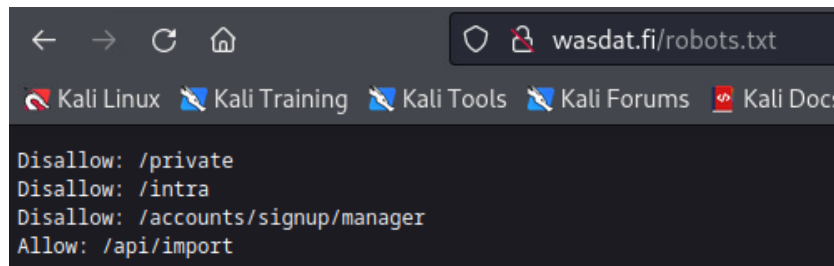
Main target - Login intra

Description

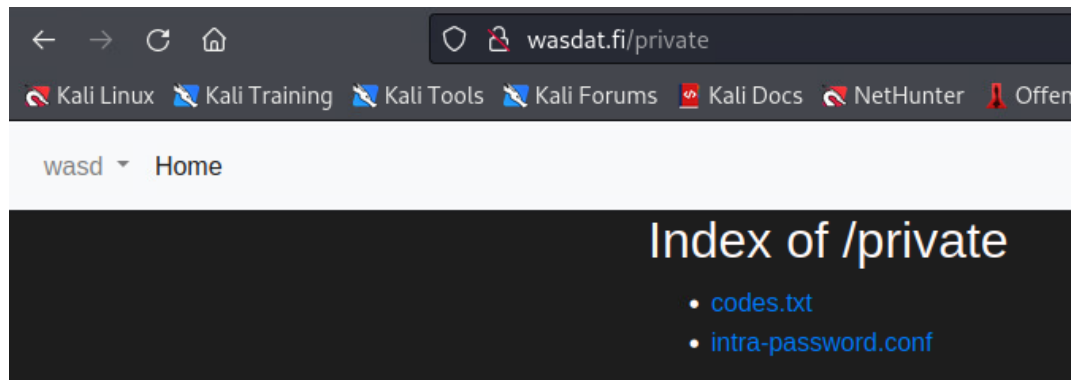
Website has intra login password stored to it and it is easy to access with help of /robots.txt file.

Steps to produce

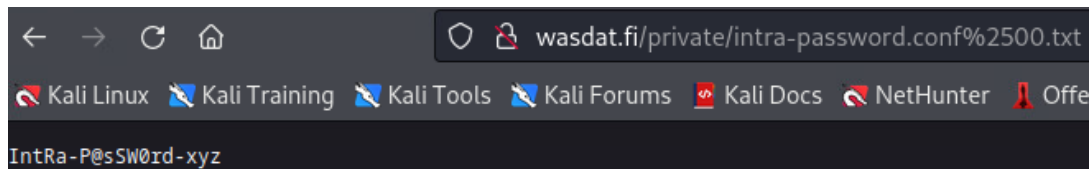
Open your browser and go to <http://wasdat.fi/robots.txt> .



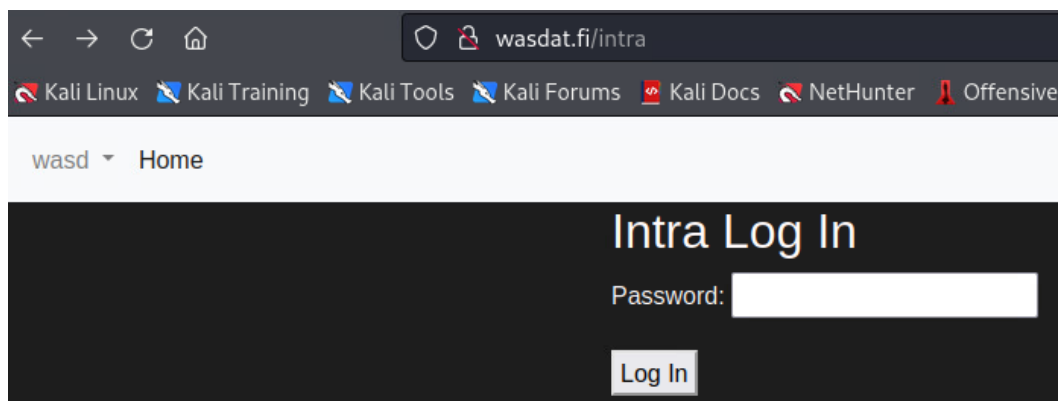
Then go to <http://wasdat.fi/private> .



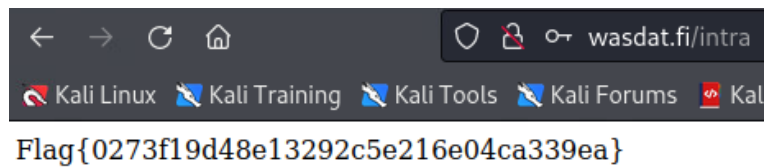
There is 'intra-password.conf' file. To open it we need to change file format because it only allows open .txt files. Open that .conf file and add %2500.txt to end of URL. <http://wasdat.fi/private/intra-password.conf%2500.txt>



It has password inside. Now go to intra login page <http://wasdat.fi/intra> that we found from <http://wasdat.fi/robots.txt>.



Write password 'IntRa-P@sSw0rd-xyz' and log in.



Impact estimation

High severity. With this attacker can get sensitive information. And when he gets password to intra, attacker can get business secrets that only employees should know.

Mitigation

You should never store passwords to the website directories. Another good thing to do is require username on intra login. You can also use noindex instead of robots.txt to hide directories you want keep hidden.

<https://developers.google.com/search/docs/crawling-indexing/block-indexing> .