

I'm Richard

Welcome

To my talk about:

**WAFP**

# Web Application Finger Printer

How does it  
work?

- Fetching static files
- Matching checksums
- Calculating match

Why?

Automated Web  
Application Finger  
Printing is cool ! ;)

Sometimes you can't tell  
which Application is  
powering a Website  
because its HTML output  
is modified too much...

USAGE: ./wafp.rb [Options] {URL}

--

- p, --product STRING a string which represents the name of the product to check for; STRING can be something like: "wordpress"
- v, --pversion STRING a string which represents the versions of the product to check for; STRING can be something like: "2.2.1" or "%.2" or "1.%".
- P, --dump-products STRING this will dump all products for which fingerprints are available; STRING can be something like: "%bb%" which will select all products having bb|BB in their name.
- s, --store STRING write the fetched data to the database for later use; STRING is used as an identifier.
- f, --fetch fetch only - do not fingerprint the app. (mostly used in conjunction with -s)
- l, --list STRING list the stored data archives containing STRING. STRING is optional in this case.
- d, --dry STRING perform the fingerprint on the stored data STRING instead of fetching it.
- t, --threads INT this is the count of threads to use. [8]
  - user-agent STRING a STRING which holds the User-Agent headerfield contents.
  - outlines INT number of results to print. [10]
  - timeout INT connection timeout in seconds. [10]
  - retries INT maximum retries per file to fetch. [3]
  - any this causes wafp to fetch all files known by fingerprints of all products.
  - verbose turns on verbose output.
  - debug turns on debug output.
  - quiet output off - besides the final results.
  - dbinfo prints some database stats.
  - version print WAFP version and exit.
- h, --help print this help and exit.

#### EXAMPLES:

```
./wafp.rb -p 'wordpress' -v '2%' http://blog.example.com/
```

```
./wafp.rb -f -t 32 -s phpmy-save01 -p 'phpmyadmin' -v '1.1.%'
```

```
https://user:pass@www.example.com/phpmyadmin/
```

```
./wafp.rb -d phpmy-save01 -p 'phpmyadmin' -v '1.1.%'
```

./wafp.rb -p phpmyadmin https://phpmyadmin.example.com/

Collecting the files we need to fetch ...

Fetching needed files (#426), calculating checksums and storing the results to  
the database:

.....  
.....  
.....

.....  
Checking gathered/stored checksums (#426) against the selected product  
(phpmyadmin) versions (#81) checksums:

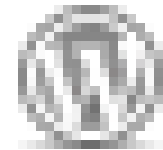
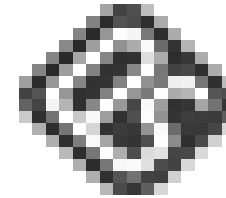
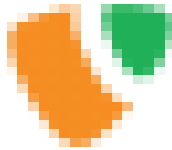
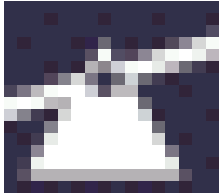
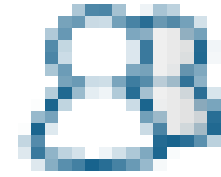
.....

found the following matches (limited to 10):

Product	Count	Percentage
phpmyadmin-2.11.9.1	297 / 299	(99.33%)
phpmyadmin-2.11.9	295 / 299	(98.66%)
phpmyadmin-2.11.8	295 / 299	(98.66%)
phpmyadmin-2.11.9.2	295 / 299	(98.66%)
phpmyadmin-2.11.9.5	295 / 299	(98.66%)
phpmyadmin-2.11.9.3	295 / 299	(98.66%)
phpmyadmin-2.11.9.4	295 / 299	(98.66%)
phpmyadmin-2.11.8.1	295 / 299	(98.66%)
phpmyadmin-2.11.7	294 / 299	(98.33%)
phpmyadmin-2.11.5	294 / 299	(98.33%)

+-----+

WAFP 0.01-alpha9 - - - - - http://mytty.org/wafp/



More than 600 different versions can already be identified!

**WARNING: It's still under  
heavy development!**

- New features
- New fingerprints
- More documentation

You can get it

Here:

<http://mytty.org/wafp>

# Thank you

Richard Sammet - [richard.sammet@gmail.com](mailto:richard.sammet@gmail.com)  
<http://www.mytty.org>

## Business Contact

**Deloitte.**

**Richard Sammet**  
Manager  
Enterprise Risk Services

**Deloitte & Touche GmbH**  
Wirtschaftsprüfungsgesellschaft  
Franklinstraße 50  
60486 Frankfurt  
Germany  
[rsammet@deloitte.de](mailto:rsammet@deloitte.de)

Member of  
Deloitte Touche Tohmatsu