

Pillaging DVCS Repos

...for fun and profit

DEFCON 19 // Adam Baldwin

\$ whoami

@adam_baldwin

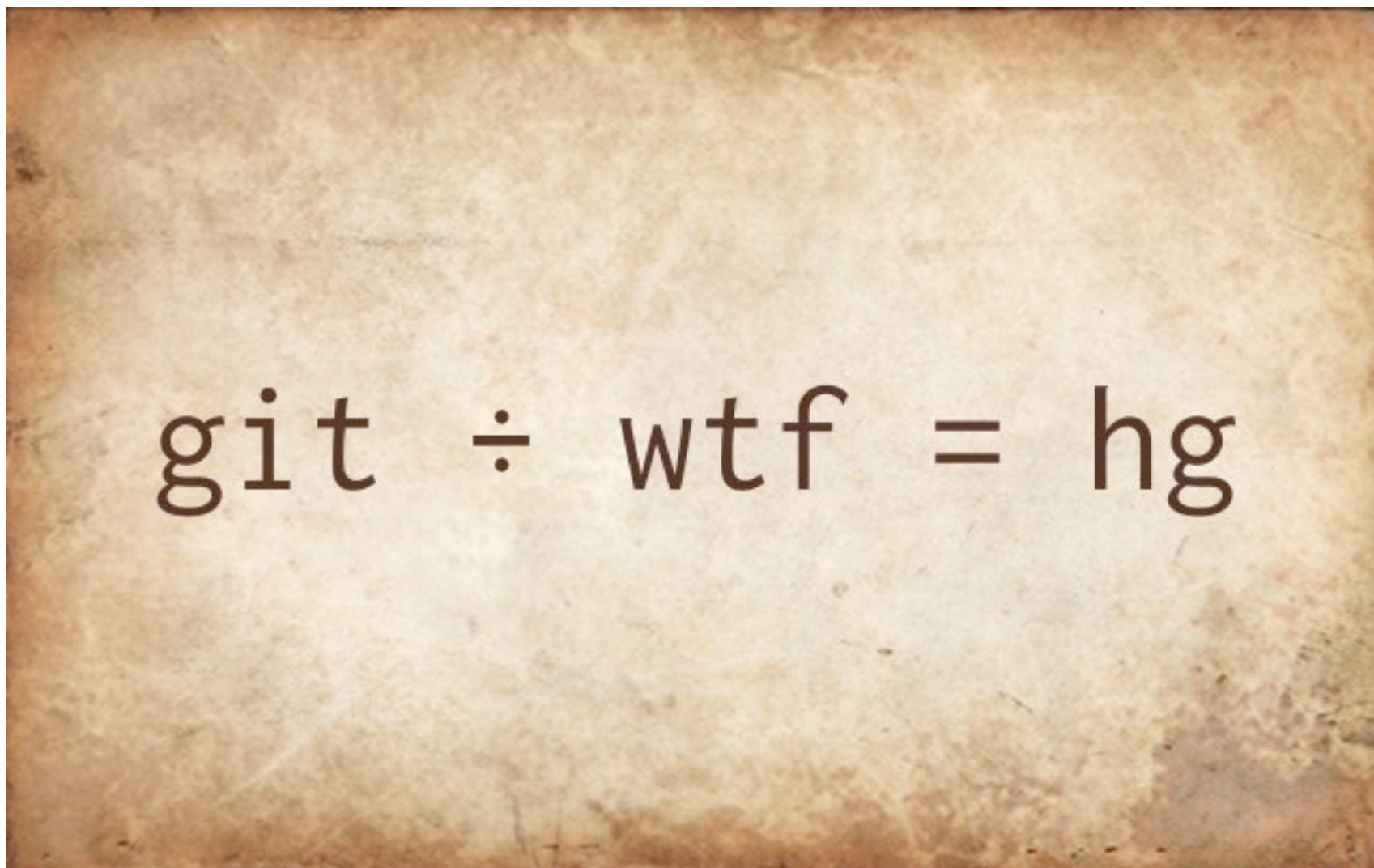
Co-Founder of nGenuity

Pentester of webs

evilpacket.net



WTF is DVCS



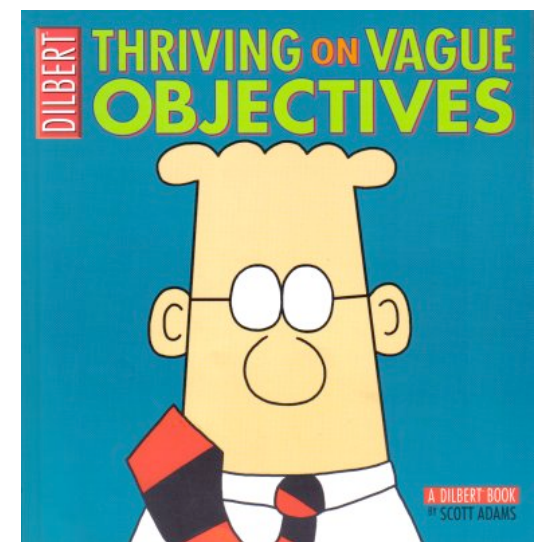
Objectives

Identify web accessible repos

Pillage as much info as possible

???

Profit

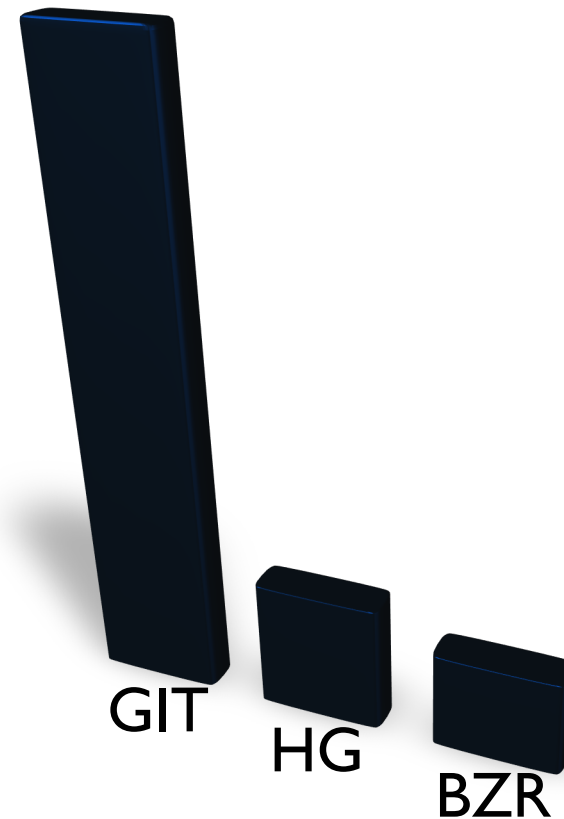


Alexa top million sites

GIT: 1498 repos

HG: 312 repos

BZR: 235 repos



Repo Identification

GIT: `.git/HEAD`

HG: `.hg/requirements`

BZR: `.bzr/README`

`http://example.com/.git/HEAD`



W3AF Plugin

Scan config | Log | Results | Exploit

Profiles

- empty_profile
- OWASP_TOP10
- audit_high_risk
- bruteforce
- fast_scan
- full_audit
- full_audit_manual_di**
- sitemap
- web_infrastructure

Target:

Plugin	Active
dnsWildcard	<input type="checkbox"/>
domain_dot	<input type="checkbox"/>
dotNetErrors	<input type="checkbox"/>
favicon_identification	<input type="checkbox"/>
findBackdoor	<input type="checkbox"/>
findCaptchas	<input type="checkbox"/>
findDVCS	<input checked="" type="checkbox"/>
findGit	<input type="checkbox"/>
findvhost	<input type="checkbox"/>
fingerBing	<input type="checkbox"/>
fingerGoogle	<input type="checkbox"/>

findDVCS

This plugin search for evidence of git, hg or bzz metadata in a directory. For example, if the input is:
- http://host.tld/w3af/index.php

The plugin will perform a request to:
- http://host.tld/w3af/.git/HEAD
- or
- http://host.tld/w3af/.hg/requirements
- or
- http://host.tld/w3af/.bzz/README

Plugin	Active
▶ output	<input checked="" type="checkbox"/>

Cloning

0. Check for dir browsing
1. Get predictable files
2. List repo files
3. Download references to files
4. Restore the repo (if possible)

Pillaging

Platform details (.php, .cgi, etc)

Downloadable files (.old, .sql)

Source Code

Credentials / Certs / API Keys

Pillaging Ideas


.sql / .sql.bz2	.pem	config	.bak
.sql.gz	.xls / .xlsx	.ini	.cfg
.tar / .tar.gz	.doc / .docx	.sh	export
htpasswd	private	.qbw / .mny	backup
id_rsa	.pst / .ost	confidential	dump / .dmp
id_dsa	settings	.csv	.txt

Thanks to @flirzan & @quitlahok for some of these!

Montage of fail



https://www.██████████/admin/data/csv_export/bankdaten_██████████.csv



The site's security certificate is not trusted

You attempted to reach www.██████████. This site's security certificate is not trusted by your computer's operating system. This may be because you are trying to access a site that you have never seen this warning before for this site.

[Proceed anyway](#) [Back to safety](#)

The server www.██████████:443 requires a username and password. The server says: www.██████████:cooladmin.

User Name:

Password:

[Cancel](#) [Log In](#)

Auth Required?

```
From the Terminal — bash — 108x28
~/hgpillage/██████████/admin/data/csv_export$ls
bankdaten_██████████.csv
~/hgpillage/██████████/admin/data/csv_export$\
> head -5 bankdaten_██████████.csv
"3000";"Felicity";"maria gato";"Dresdner Bank Hilden";"██████████";"30080000";
"3002";"Die Kleidmanufaktur";"doris ivanschitz";"Postbank Essen";"██████████";"36010043";
"3003";"PerfectEvent";"Mechthild Anfang";"Volksbank Münster";"██████████";"40160050";
"3004";"SAGT JA Hochzeitsplanung";"Katrin Glaser";"Cronbank AG";"██████████";"50530000";
"3008";"Brämer Maßbekleidung";"kathrin brämer";"Sparkasse Erlangen";"██████████";"76350000";
~/hgpillage/██████████/admin/data/csv_export$
```

Nope

Database Passwords

```
dump.sh
#!/bin/sh

DBHOST=debbie
DBUSER=hees
DBPASS=
DATABASES="nuke handy _"
#DATABASES="nuke handy"

for d in $DATABASES
do
    mysqldump -h$DBHOST -u$DBUSER -p$DBPASS
--add-drop-table --quick $d `cat $d.tables |
sed -e 's/#.*$/g'` | gzip > $d-dump.sql.gz
done
```

```
backup.sh
#!/bin/sh

date=`date "+%Y-%m-%d"`
started=`date`

mysqldump -u bob_wordpressmu -p bob_wordpressmu | gzip > backup-
$date-wpmu.sql.gz
mysqldump -u openx -p986b openx | gzip >
backup-$date-openx.sql.gz
echo "Started: ".$started
echo "Ended: ".$date`
```

```
Stinky-Dingus:gitshort adambaldwin$ ./search.sh list id_rsa
```

```
**** [redacted].com ****
```

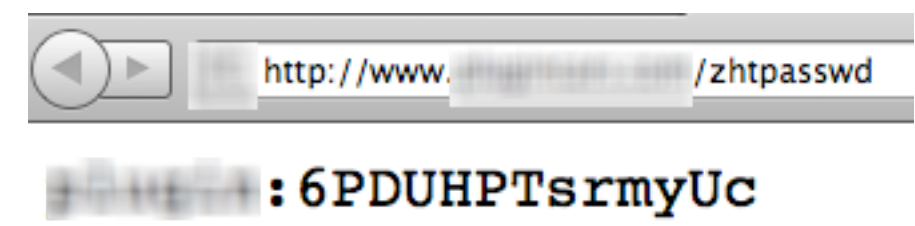
```
config/ec2tools/id_rsa-[redacted]-ec2-keypair  
config/ec2tools/id_rsa-[redacted]-ec2-keypair.pub
```

← **SSH Keys**

```
**** www.[redacted].com ****
```

```
config/id_rsa  
config/id_rsa.pub  
config/templates/[redacted]/home/[redacted]/.ssh/id_rsa.erb
```

htpasswd →



Customer Invoices

[Redacted]

Denver, CO 80216

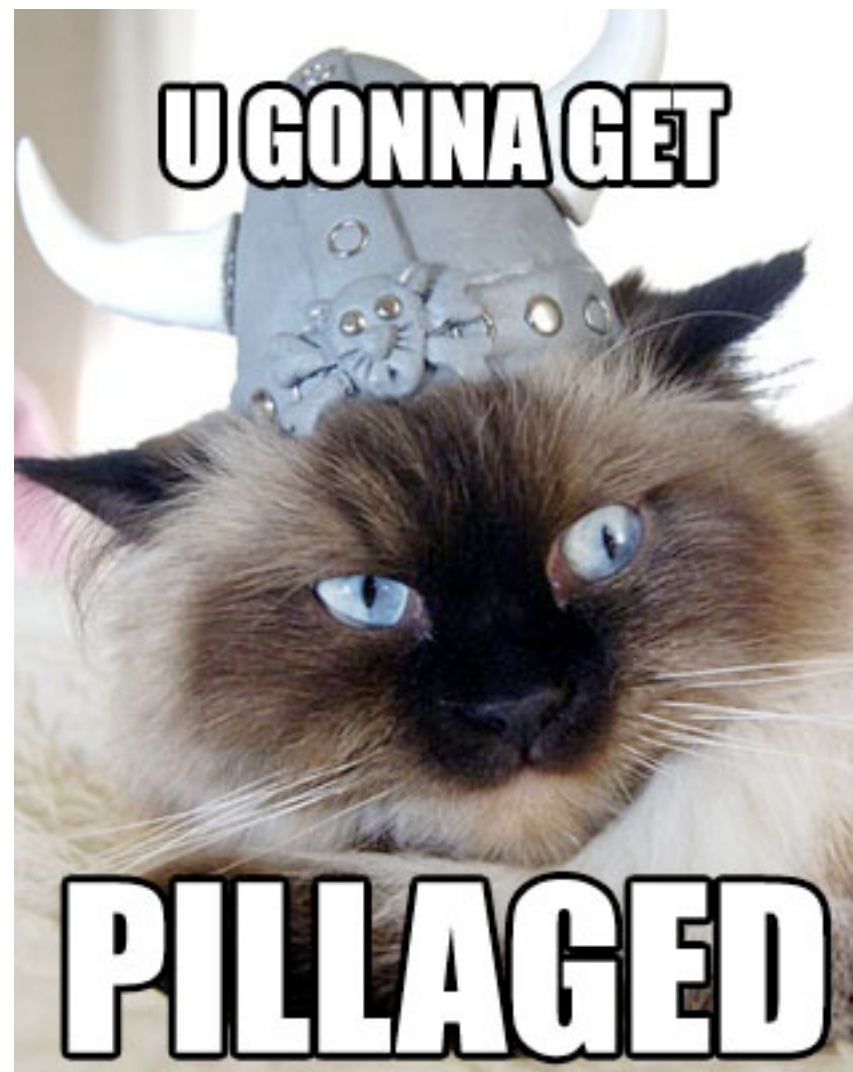
Phone (303) [Redacted] Fax (303) [Redacted]

Payment To: [Redacted]

DATE: 1/15/2011
CHECK# ACH

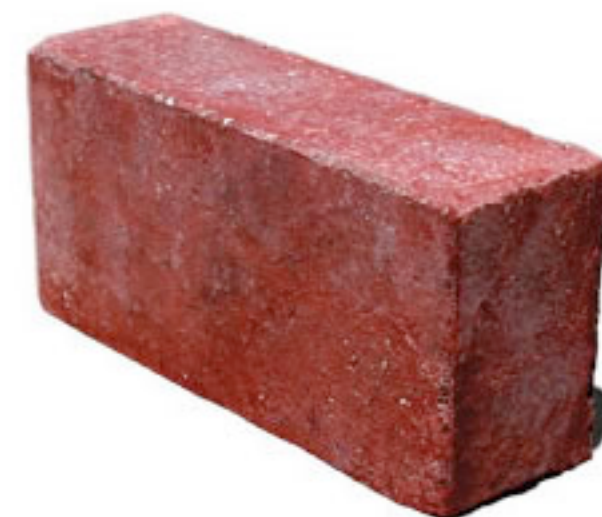
Dates			Revenue Share	Revenue Pending *	Amount Due
[Redacted] 11/1-11/30			\$3,885.39		\$3,885.39
[Redacted] 11/1-11/30			\$3,286.10		\$3,286.10
			\$7,171.49	\$0.00	\$7,171.49

Demo



The Tool

<https://github.com/ngenuity/DVCS-Pillage>





Questions?

adam@ngenuity-is.com // [@adam_baldwin](https://twitter.com/adam_baldwin)

References

nGenuity:

<http://ngenuity-is.com>

<http://ngenuity-is.com/blog/2011/mar/22/gotta-git-up-to-get-down/>

<http://ngenuity-is.com/blog/2011/apr/30/git-pillaging-revisited/>

Evilpacket:

<http://evilpacket.net>

W3AF:

<http://w3af.sourceforge.net/>

DVCS Pillage Toolkit:

<http://github.com/ngenuity/dvcs-pillage>