dvcs-ripper:专门用于从web服务器提取和恢复元数据，如.git .hg .svn

```
rip-hg -u http://www.example.com还原.hg
rip-git -u http://www.example.com还原.git
rip-svn -u http://www.example.com还原.svn
```

chrl+U：查看源码

请求头，响应头

robots.txt泄露

phps源码泄露

.git泄露，可用githack工具还原.git文件夹中的文件，在arch的默认目录为/usr/share/githack

.hg泄露，可用dvcs-ripper

.DS-Store泄露，直接wget下载好，string提取

```
wget http://www.example.com/.DS_Store
strings .DS_Store
```

vim缓存信息泄露：用vim编辑文件时，为了防止丢失会生成一个<文件名>.swp文件，如果不及时删除，会造成信息泄露

Cookie泄露

有时候域名有隐藏信息，可以上 https://boce.aliyun.com/detect/http查看

有时候网站上的公开信息，就是管理员常用密码

php 探针：用来探测空间、服务器运行状况和 PHP 信息，探针可以实时查看服务器硬盘资源、内存占用、网卡流量、系统负载、服务器时间等信息，常见tz.php

探针类型	探针名称	常见默认文件名
经典PHP探针	雅黑PHP探针	`y.php`、`yah.php`、`yahei.php`、`tz.php`
	X探针	`x.php`、`x_probe.php`、`probe.php`
	UPUPW PHP 探针	`phpinfo.php`、`upupw.php`、`info.php`
	LNMP一键包探针	`p.php`、`probe.php`、`tz.php`
通用测试文件	PHPInfo 函数	`phpinfo.php`、`info.php`、`test.php`、`i.php`
	环境探针	`env.php`、`environment.php`、`status.php`
	数据库测试文件	`db_test.php`、`mysql_test.php`、`test_db.php`
其他技术栈	ASP.NET 探针	`aspxspy.aspx`、`aspnet.aspx`、`status.aspx`
	JSP 探针	`jsp-probe.jsp`、`status.jsp`、`test.jsp`1