Hacking Vulnhub VM BadStore.iso

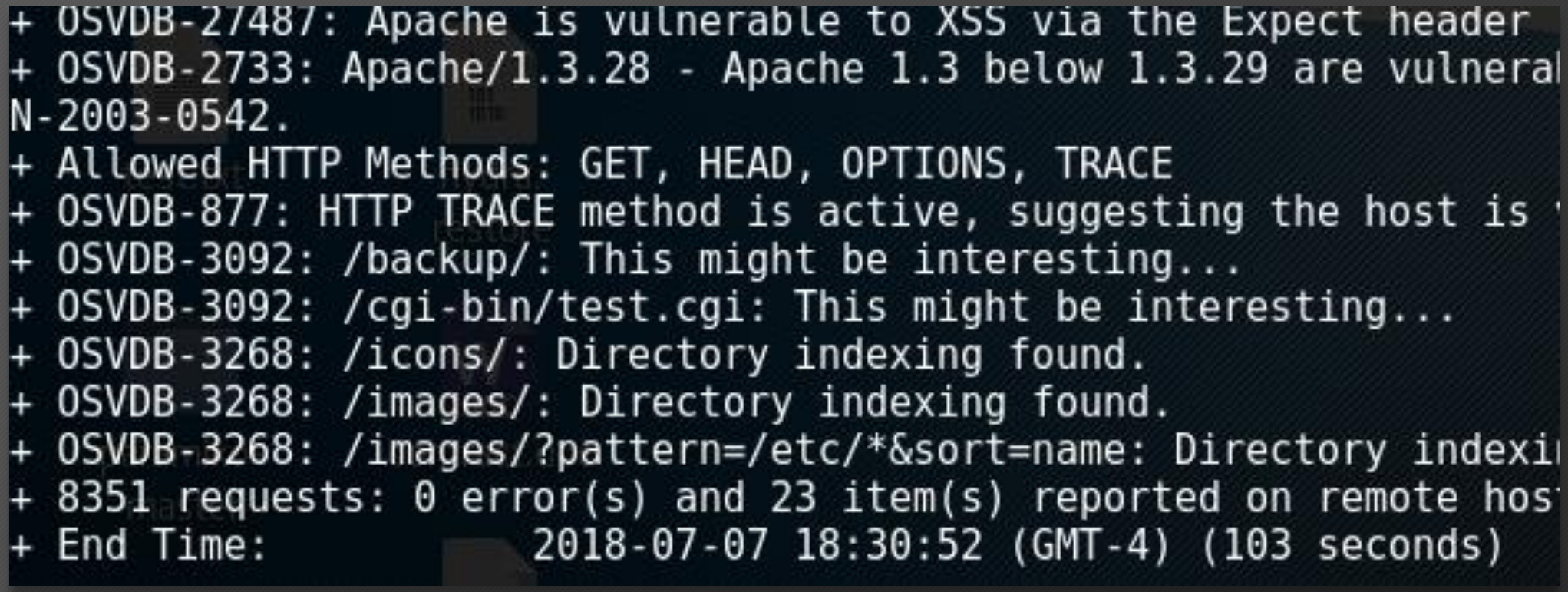
Gladiola

https://gladiola.github.io/blog/

https://github.com/gladiola/blackmagic/tree/Demo/agkistrodon/contortix/Penelope/BadStore

BadStore Initial Characteristics

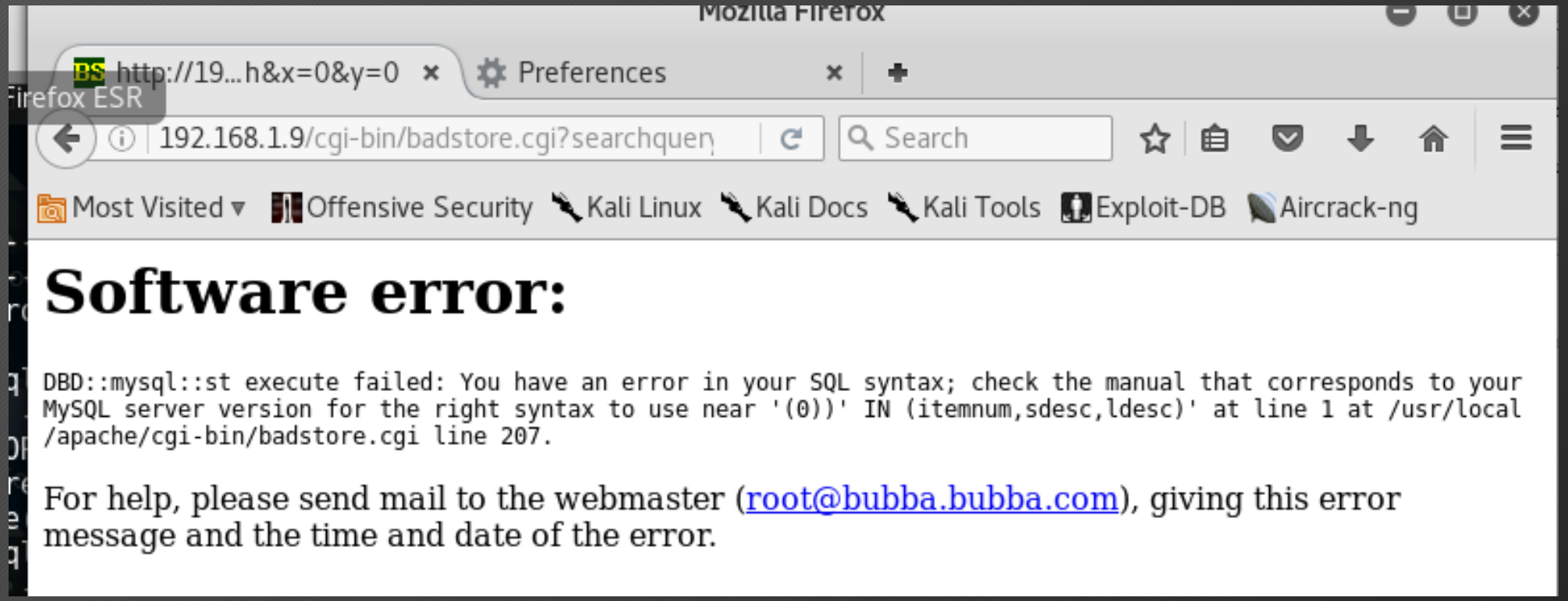
- Perl CGI, MySQL 4.x, Apache 1.3
- No JSP, ASP, PHP limited use of prefab msf scripts
- Open on 80, 443, and 3306
- ISO file will reset on restart
- File upload buttons and some supporting directories nearby
- Built-in PDF with “Directions”

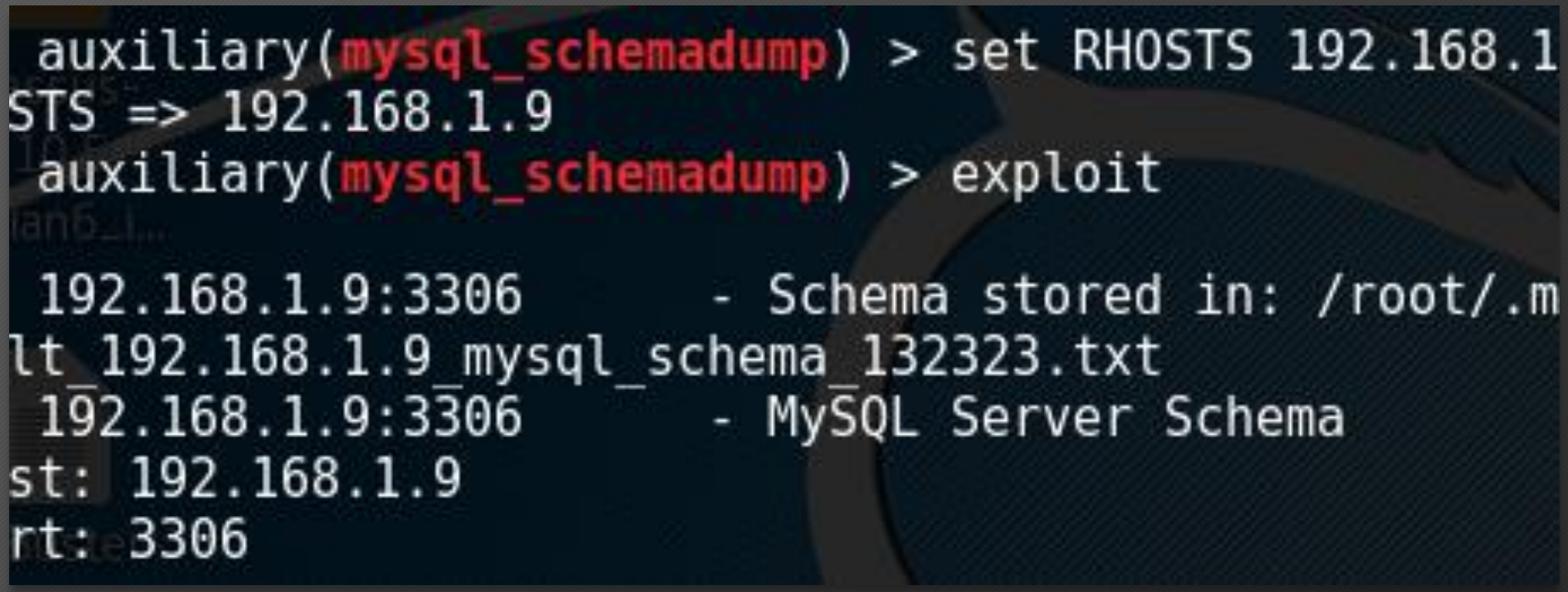


Nikto, Nessus (basic net and web), msf scanner, and manual

Historic vulns like heartbleed and shellshock came up also.

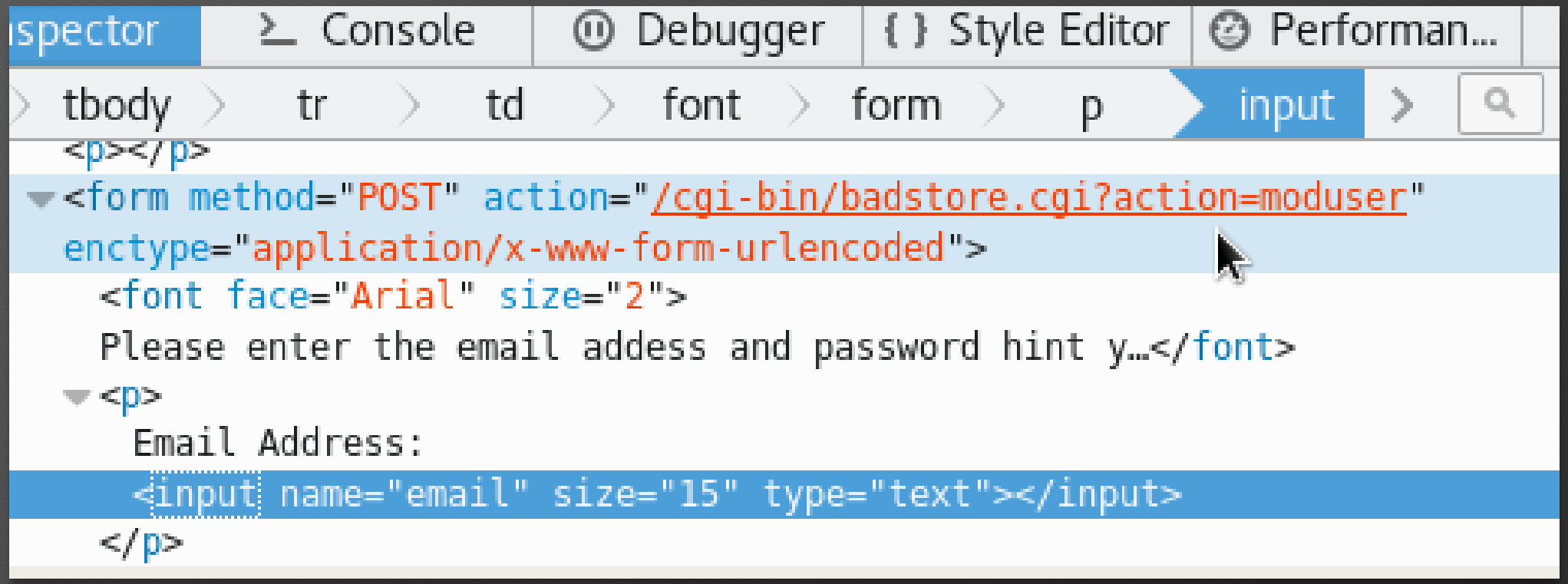
Injectable


Mozilla Firefox
http://19...h&x=0&y=0
Preferences
Firefox ESR
192.168.1.9/cgi-bin/badstore.cgi?searchquery
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Software error:
DBD::mysql::st execute failed: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '(0))' IN (itemnum,sdesc,ldesc)' at line 1 at /usr/local/apache/cgi-bin/badstore.cgi line 207.
For help, please send mail to the webmaster (root@bubba.bubba.com), giving this error message and the time and date of the error.



Msf mysql_schemadump

No “INFORMATION_SCHEMA” and none of the usual default table names in there anywhere.



Associating POST form with field for crafting call

Burp Suite form interception to draft a sqlmap POST file upload in an attempt to pop a shell.

Later, just called database directly after some sqlmap; got any table we wanted with direct remote calls.

AAA_Test_User	098F6BCD4621D373CADE4E832627B4F6	black	Test User	U
admin	5EBE2294ECD0E0F08EAB7690D2A6EE69	black	Master System Administrator	A
joe@supplier.com	62072d95acb588c7ee9d6fa0c6c85155	green	Joe Supplier	S
big@spender.com	9726255eec083aa56dc0449a21b33190	blue	Big Spender	U
ray@supplier.com	99b0e8da24e29e4ccb5d7d76e677c2ac	red	Ray Supplier	S
robert@spender.net	e40b34e3380d6d2b238762f0330fbd84	orange	Robert Spender	U
bill@gander.org	5f4dcc3b5aa765d61d8327deb882cf99	purple	Bill Gander	U
steve@badstore.net	8cb554127837a4002338c10a299289fb	red	Steve Owner	U
fred@whole.biz	356c9ee60e9da05301adc3bd96f6b383	yellow	Fred Wholesaler	U
debbie@supplier.com	2fbd38e6c6c4a64ef43fac3f0be7860e	green	Debby Supplier	S
mary@spender.com	7f43c1e438dc11a93d19616549d4b701	blue	Mary Spender	U
sue@spender.com	ea0520bf4d3bd7b9d6ac40c3d63dd500	orange	Sue Spender	U
curt@customer.com	0DF3DBF0EF9B6F1D49E88194D26AE243	green	Curt Wilson	U
paul@supplier.com	EB7D34C06CD6B561557D7EF389CDDA3C	red	Paul Rice	S
kevin@spender.com	NULL	NULL	Kevin Richards	U
ryan@badstore.net	40C0BBDC4AEEAA39166825F8B477EDB4	purple	Ryan Shorter	A
stefan@supplier.com	8E0FAA8363D8EE4D377574AEE8DD992E	yellow	Stefan Drege	S
landon@whole.biz	29A4F8BFA56D3F970952AFC893355ABC	purple	Landon Scott	U
sam@customer.net	5EBE2294ECD0E0F08EAB7690D2A6EE69	red	Sam Rahman	U
david@customer.org	356779A9A1696714480F57FA3FB66D4C	blue	David Myers	U
john@customer.org	EEE86E9B0FE29B2D63C714B51CE54980	green	John Stiber	U
heinrich@supplier.de	5f4dcc3b5aa765d61d8327deb882cf99	red	Heinrich Hâ^šÂºber	S
tommy@customer.net	7f43c1e438dc11a93d19616549d4b701	orange	Tom O'Kelley	U
blipblap@somemail.com	202cb962ac59075b964b07152d234b70	green	blipblap	U
blipblap@somemail.com	202cb962ac59075b964b07152d234b70	green	blipblap	U
	d41d8cd98f00b204e9800998ecf8427e	green		U

Lessons Learned

- Separate db and file accounts effective
- Does anybody still have write permission on this box?
- One writer; programs installed; deleted user; no writers
- “No”
  - ports open
  - normal services running
  - cronjobs running
- “No” normal, contemporary server-side languages in use
- Aside from the targeted site deliberately left vuln, hard to find an opening. Burned the back door shut on the way out.

```
################
# Admin Portal #
################

sub adminportal
{
        local ($aquery, $email, $newpasswd, @data
        &printheaders;
        print @header,
        start_html("Private Administration Portal
        h1("Secret Administration Portal"), hr, p
        $aquery=$query->param('admin');
```

```
, size=> -2 }, $value )));
  }
  print "</TABLE>",p,
  h2("Recent Apache Error Log"),p,hr,
  `tail /usr/local/apache/logs/error_log`,
  p, h2("Apache Access Log"),p,hr,
  `cat /usr/local/apache/data/userdb`;
```

```
_bin_sh                    _etc_rc.local
_etc_badstore              _etc_shadow
_etc_fstab                 _etc_version
_etc_group                 _home_root_.bash_history
_etc_HOSTNAME              _root_.ssh
_etc_hosts                 _usr_local_apache_backup_userdb.bak
_etc_init.d                _usr_local_apache_cgi-bin_*
_etc_init.d_apache         _usr_local_apache_cgi-bin_badstore.cgi
_etc_inittab               _usr_local_apache_cgi-bin_test.cgi
_etc_issue                 _usr_local_apache_htdocs_backup_orderdb.bak
_etc_network_interfaces    _usr_local_apache_htdocs_backup_userdb.bak
_etc_passwd                _usr_local_apache_htdocs_uploads
_etc_profile               _var_adm
_etc_rc1.d                 _var_log
_etc_rc.d                  _var_log_apache_access.log
_etc_rc.d_rc.local         _var_spool_cron
root@kali:~/.sqlmap/output/192.168.1.9/files# ls -lisa
total 464
793384   4 drwxr-xr-x 2 root root   4096 Jul  8 05:54 .
811503   4 drwxr-xr-x 4 root root   4096 Jul  8 05:54
```

```
### Connect to the SQL Database ###
my $dbh = DBI->connect("DBI:mysql:database=badstoredb;host=localhost", "root", "secret",{'RaiseError' => 1})
or die "Cannot connect: " . $DBI::errstr;
```

Hacking Vulnhub VM BadStore.iso

Gladiola

https://gladiola.github.io/blog/

https://github.com/gladiola/blackmagic/tree/Demo/agkistrodon/contortix/Penelope/BadStore