RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: PROF-M02

Hackers Hiring Hackers – How to Do Things Better

Tim O’Brien

Director, Threat Research Palerra
CTO/CISO, Xero Equipment
@obrientg

Magen Wu

Security Consultant
Rapid7
@Tottenkoph

#RSAC

Target Audience

- Hiring managers
  - On the quest to hire information security professionals
  - People who will stay and grow with the company
- Hackers
  - In the traditional sense, not the 'new' definition by the press
  - Those with little to no “professional” experience
  - Those with plenty of experience looking for next opportunity

Inspiration For This Talk

- Little light being shed on this topic
- “It is hard to find people to hire”
- Both sides of the hiring practice have problems
  - Setting expectations
  - Applications and resume gathering/submissions
  - Interviewing
  - Post-interview

Expectations

Expectations

“We can't find anyone to hire!”

Vs

“Must work in our corporate office in Wichita, initially on a six month contract to fire with a rotating SOC shift cycle. Oh, and you start on night shift.

Readjust Expectations

“Over the years, what we have essentially done—intentionally or not—is create a sub-category of talent whom we will never hire. The Unhireable. ...

-Winn Schwartau, “Hiring the unhireable”

Hiring Manager, What Do You Want?

- Use the right title for the role
  - A majority of titles being posted don’t match with the expectations
- Be clear and concise with position descriptions (PDs)
  - It is easy (and common) to see PDs that are all over the place
  - It’s ok to say you’re looking for a generalist
  - Avoid misrepresentation

Hiring Manager, What Do You Need?

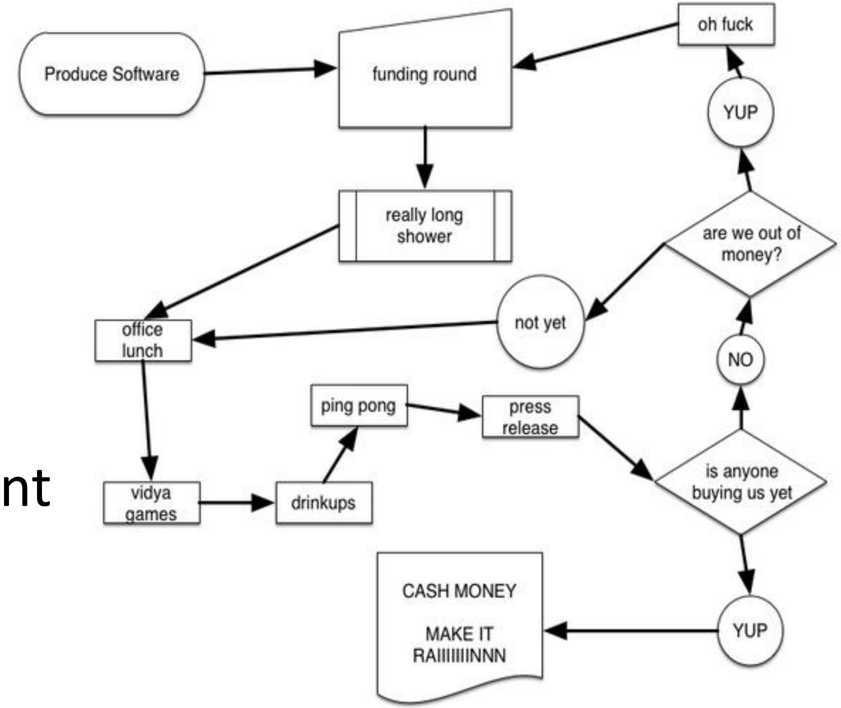
- Consider what matters
  - Experience (need vs affordability)
  - Certifications and degrees
    - Are they relevant to the position?
    - Can the business afford reimbursement if passed a certain amount of time after being hired?
- Conciseness can reduce the likelihood of alienating potential applicants

Scoping The Role

- Contractor or full time employee?
- Specialty roles versus “Jack of All Trades”
  - Both have their benefits and drawbacks
  - Consider type of specialty roles (analysts, engineers, architects)
- State the realm that applicants will be working in
  - Application, network, or system security?
  - Vendor-specific preferences

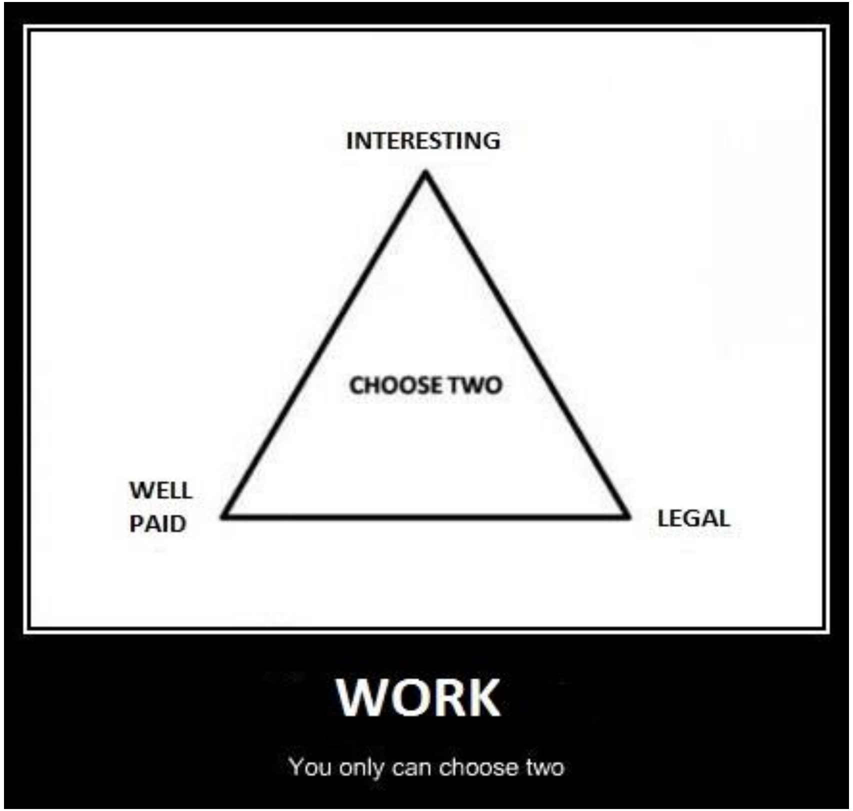
Organizational Placement

- Who will be their direct report? Report to?
- Does the team report to IT, compliance, or Legal?
  - Consider conflicts of interest
- Over-extension of new and current employees
- Start ups & small companies



Hacker Expectations

- Sometimes unrealistic…
  - High pay
  - With no bureaucracy
  - All the tools you want – or the freedom to build new
  - With a free pass to hacker summer camp (BlackHat/DEFCON)
- Sometimes realistic, but not doable



WORK

You only can choose two

Application Process

The Application Process

- Prepare
  - Both sides struggle with this
  - Know what questions you want to ask
  - Understand how to measure and determine “good fit”
- Consider the timing
  - Determine when in the year is best to recruit for the role
  - Applicants should look at dates jobs are posted before applying to set expectations

Hiring Managers Finding Candidates

- Get involved in your
  - Local IT & InfoSec communities and Meetup groups
  - Mailing lists and forums
  - Local tech/college professional meetings
- Posting online
  - Monster, CareerBuilder, Beyond, Indeed, etc.
  - Craigslist
  - Technical & topic related forums on Reddit, Stack Overflow, etc.
  - Work with your marketing team for social media exposure
  - Closed, invite only IT/InfoSec communities & lists (NinjaJobs.org)

Finding Candidates

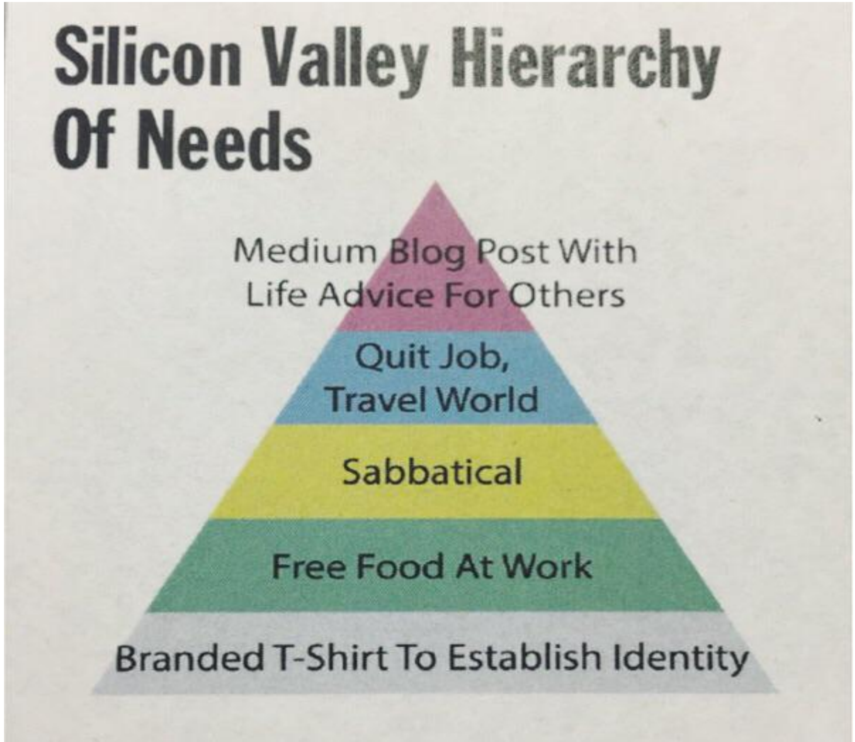
- What is your role in talent?
  - One of your obligations as a hiring manager, as a leader in InfoSec is to nurture talent in our field
  - Your involvement in the local groups helps promote (your team, your company, the industry) & screen potential candidates

HR And Recruiters

- Paid recruiters, overseas body shops are helping perpetuate the contractor class; avoid please
- Recruiter roadblocks or helping you attract talent?
  - Your HR/recruiting staff and their initial contacts and conversations with candidates set the tone for the process, ensure they are good ones
    - Sets up expectations for the next step(s)
  - Sends the screening questionnaire, expecting the applicant to do their work
    - Starts off with a poor experience
    - Candidates will go elsewhere

Questioning Compensation

- Salary history
  - You know the range, pay them what they are worth
  - Incentives
    - Flexible work schedule
    - Work from home/remote
    - Training budget
    - Conferences
    - PTO



Silicon Valley Hierarchy Of Needs

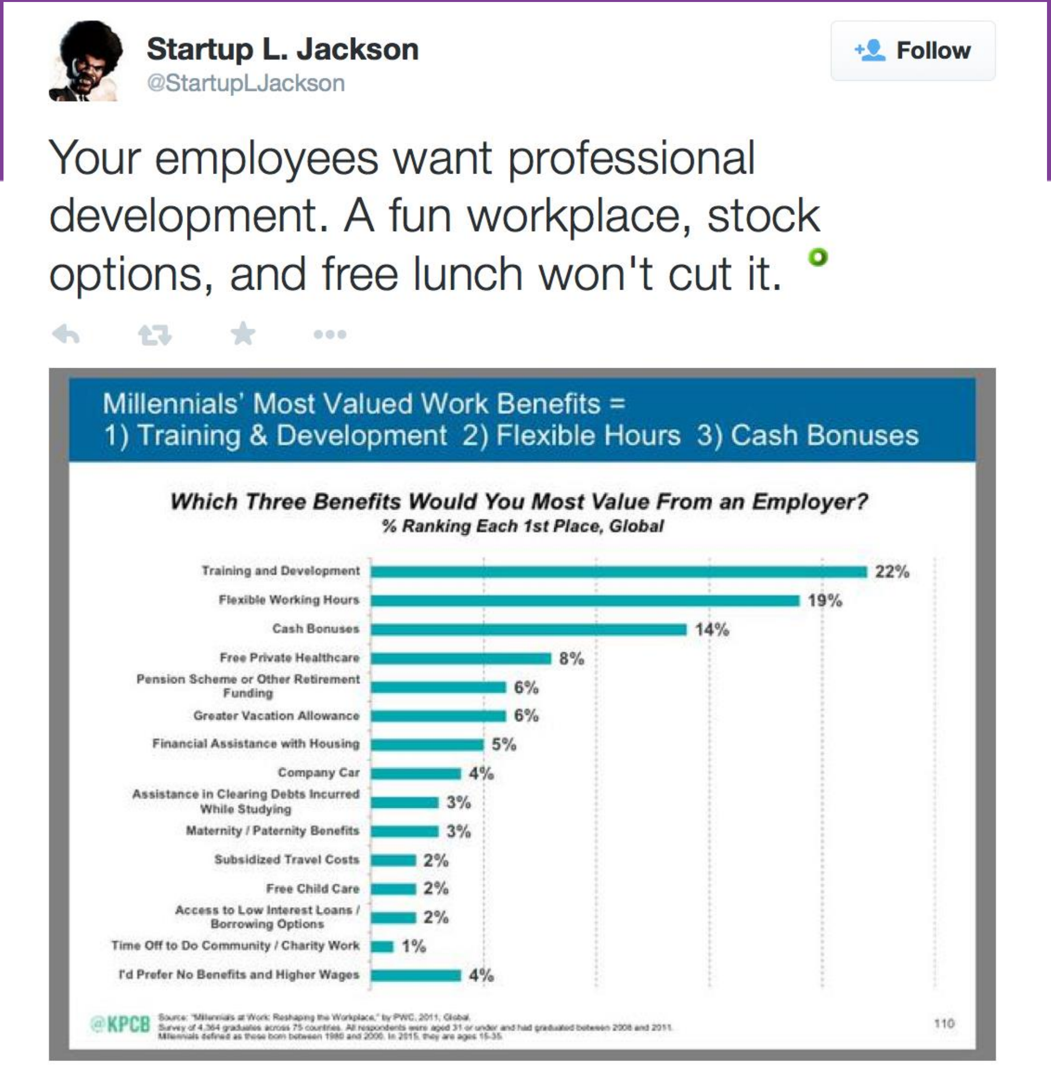
Medium Blog Post With Life Advice For Others

Quit Job, Travel World

Sabbatical

Free Food At Work

Branded T-Shirt To Establish Identity



Startup L. Jackson
@StartupLJackson

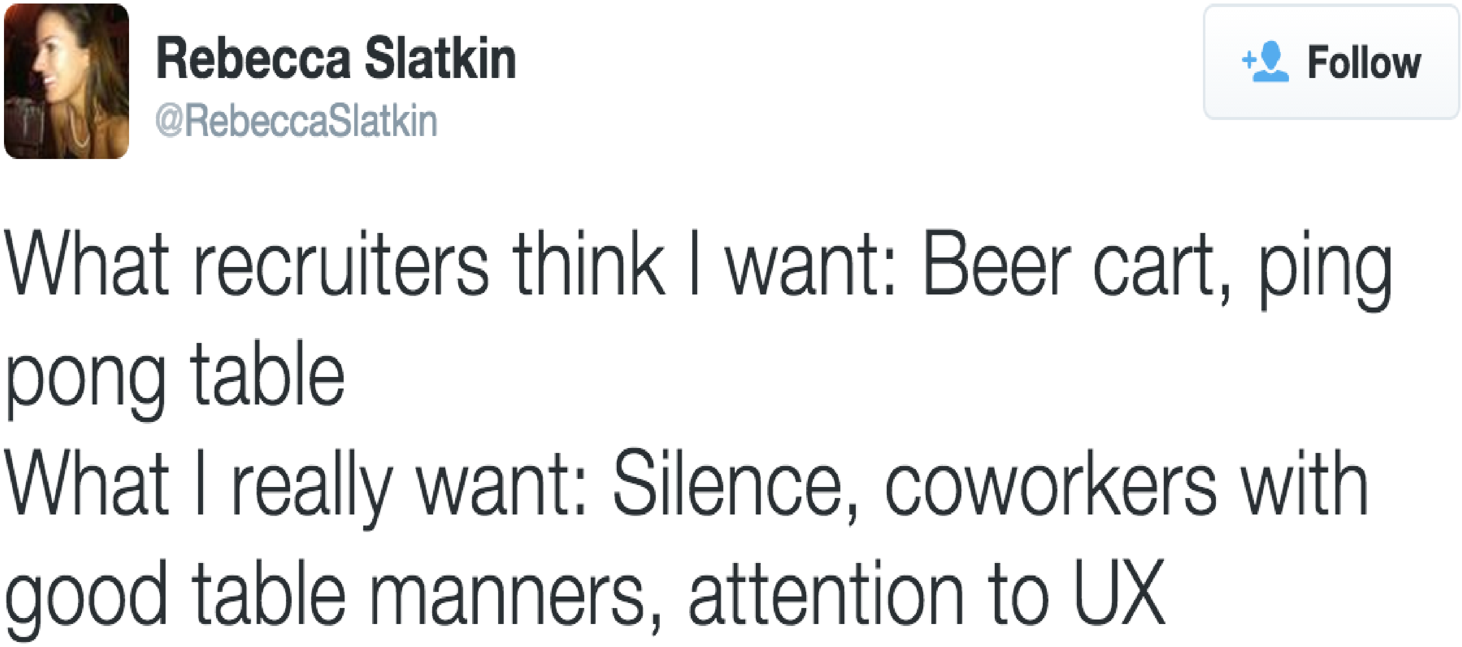
Your employees want professional development. A fun workplace, stock options, and free lunch won't cut it.

Millennials' Most Valued Work Benefits =
1) Training & Development 2) Flexible Hours 3) Cash Bonuses

Which Three Benefits Would You Most Value From an Employer?
% Ranking Each 1st Place, Global

Training and Development 22%
Flexible Working Hours 19%
Cash Bonuses 14%
Free Private Healthcare 8%
Pension Scheme or Other Retirement Funding 6%
Greater Vacation Allowance 6%
Financial Assistance with Housing 5%
Company Car 4%
Assistance in Clearing Debts Incurred While Studying 3%
Maternity / Paternity Benefits 3%
Subsidized Travel Costs 2%
Free Child Care 2%
Access to Low Interest Loans / Borrowing Options 2%
Time Off to Do Community / Charity Work 1%
I'd Prefer No Benefits and Higher Wages 4%
@KPCB
110

Source: "Millennials at Work: Reshaping the Workplace," by PWC, 2011, Global.
Survey of 4,364 graduates across 75 countries. All respondents were aged 31 or under and had graduated between 2008 and 2011.
Millennials defined as those born between 1980 and 2000. In 2015, they are ages 15-35.



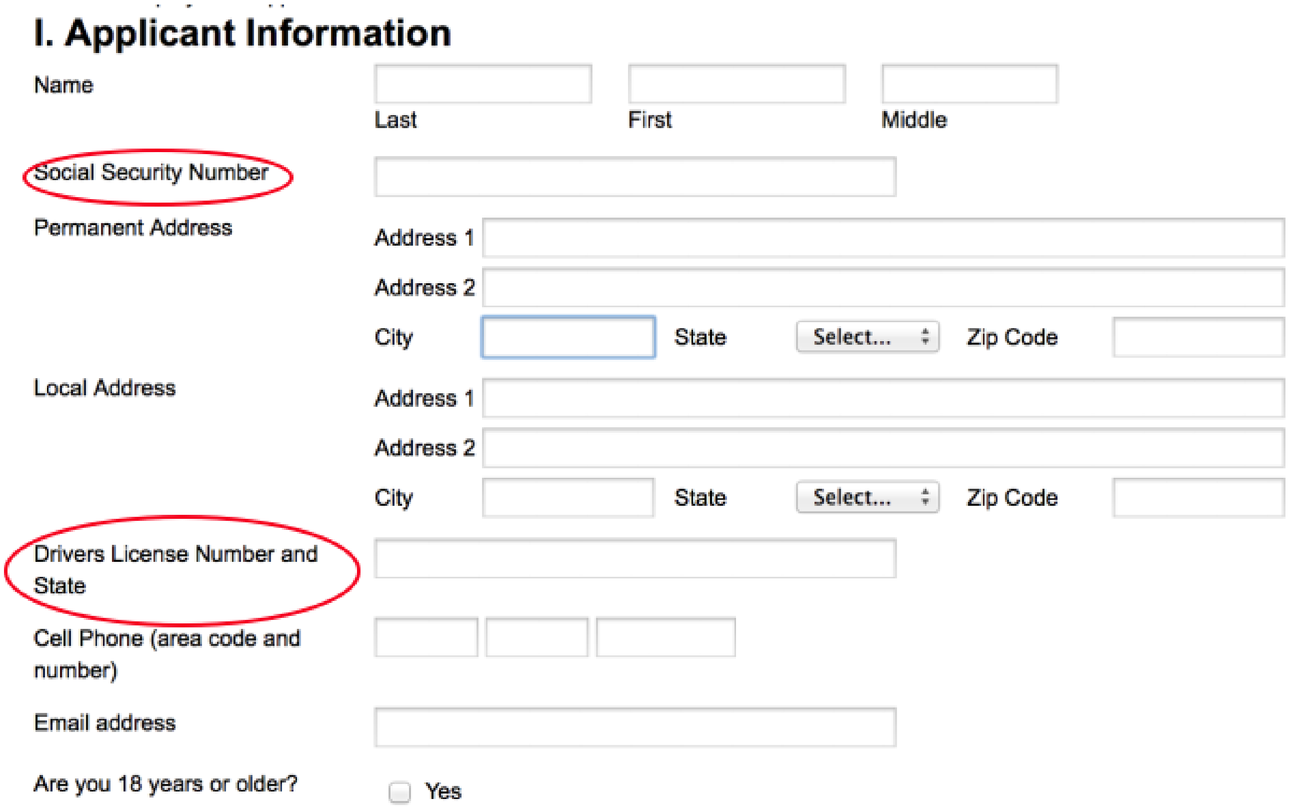
Rebecca Slatkin
@RebeccaSlatkin

What recruiters think I want: Beer cart, ping pong table
What I really want: Silence, coworkers with good table manners, attention to UX

Application Tracking Systems

- Ensure the ATS you use doesn’t require PII/NPPI
  - SSANs in BrassRing
- Test and validate your application process
  - Get a friend to apply, do they make it through the process? Past HR at least?
- Avoid the common application fails
  - The initial impressions last

ATS Fails – PII & NPPI



I. Applicant Information

Name

Last First Middle

Social Security Number

Permanent Address

Address 1

Address 2

City State Select... Zip Code

Local Address

Address 1

Address 2

City State Select... Zip Code

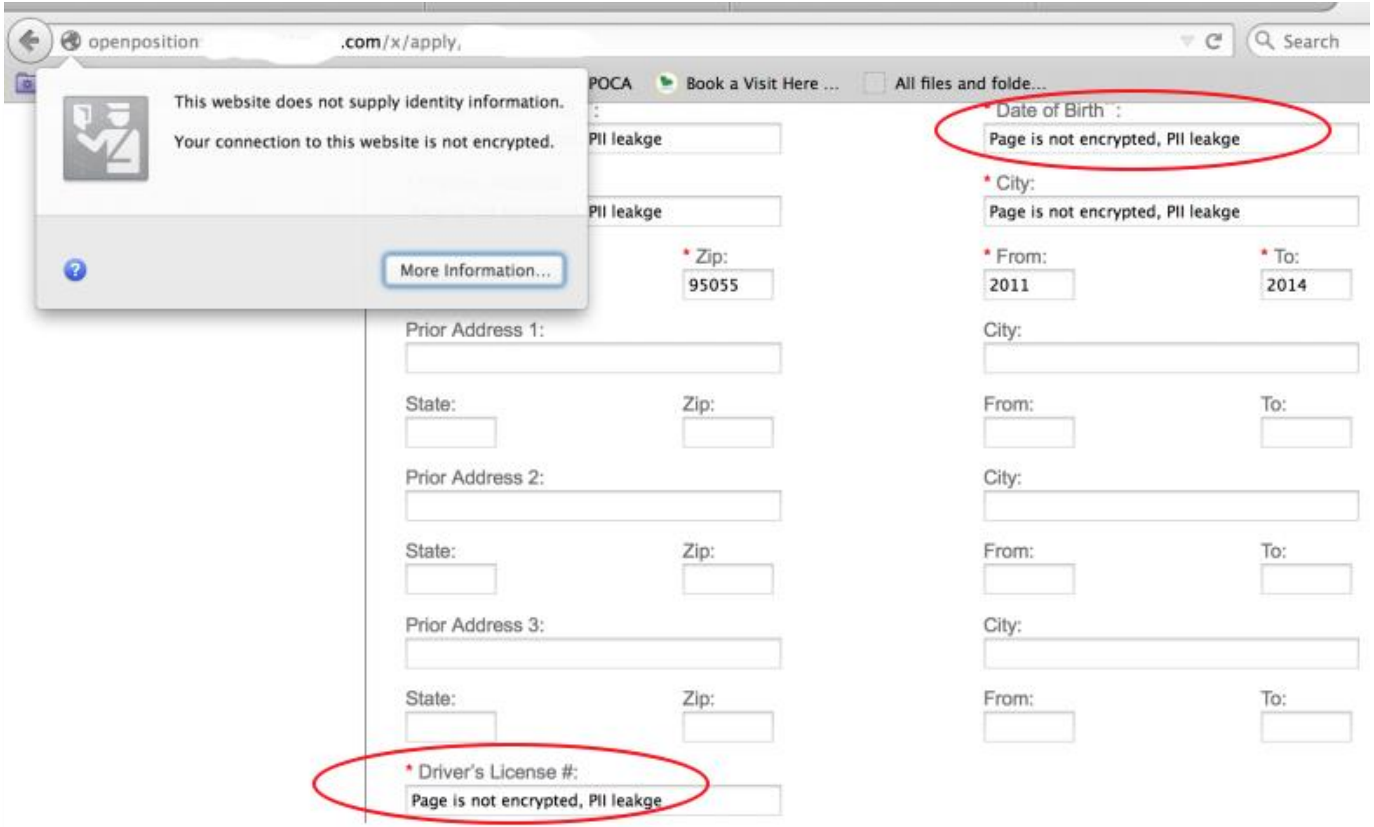
Drivers License Number and State

Cell Phone (area code and number)

Email address

Are you 18 years or older? □ Yes

ATS Fails – PII & NPPI & Certs



openposition .com/x/apply,

This website does not supply identity information.

Your connection to this website is not encrypted.

PII leakge

PII leakge

* Date of Birth :

Page is not encrypted, PII leakge

* City:

Page is not encrypted, PII leakge

* Zip: 95055

* From: 2011

* To: 2014

Prior Address 1:

City:

State:

Zip:

From:

To:

Prior Address 2:

City:

State:

Zip:

From:

To:

Prior Address 3:

City:

State:

Zip:

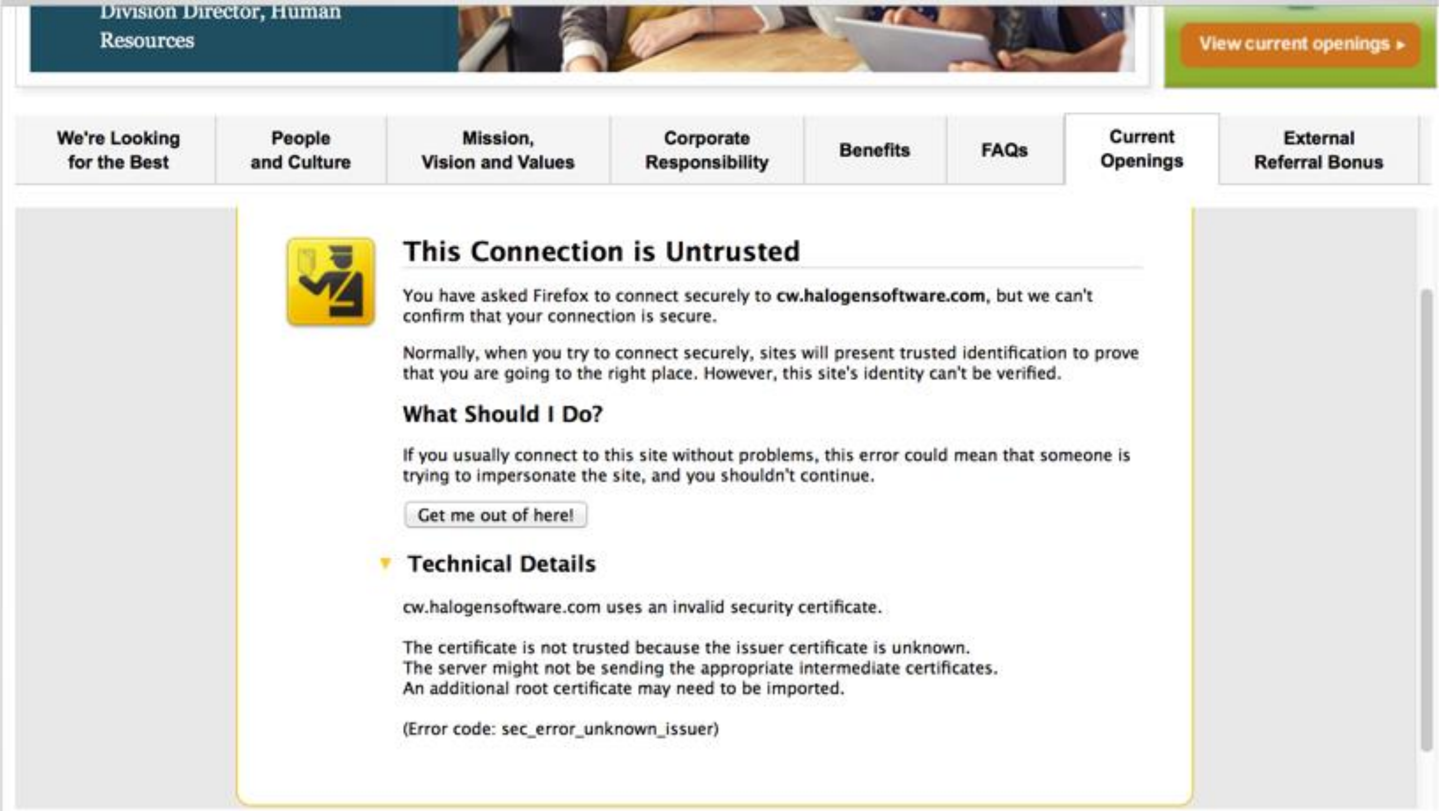
From:

To:

* Driver's License #:

Page is not encrypted, PII leakge

ATS Fails – HTTPS & Certs



This Connection is Untrusted

You have asked Firefox to connect securely to **cw.halogensoftware.com**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

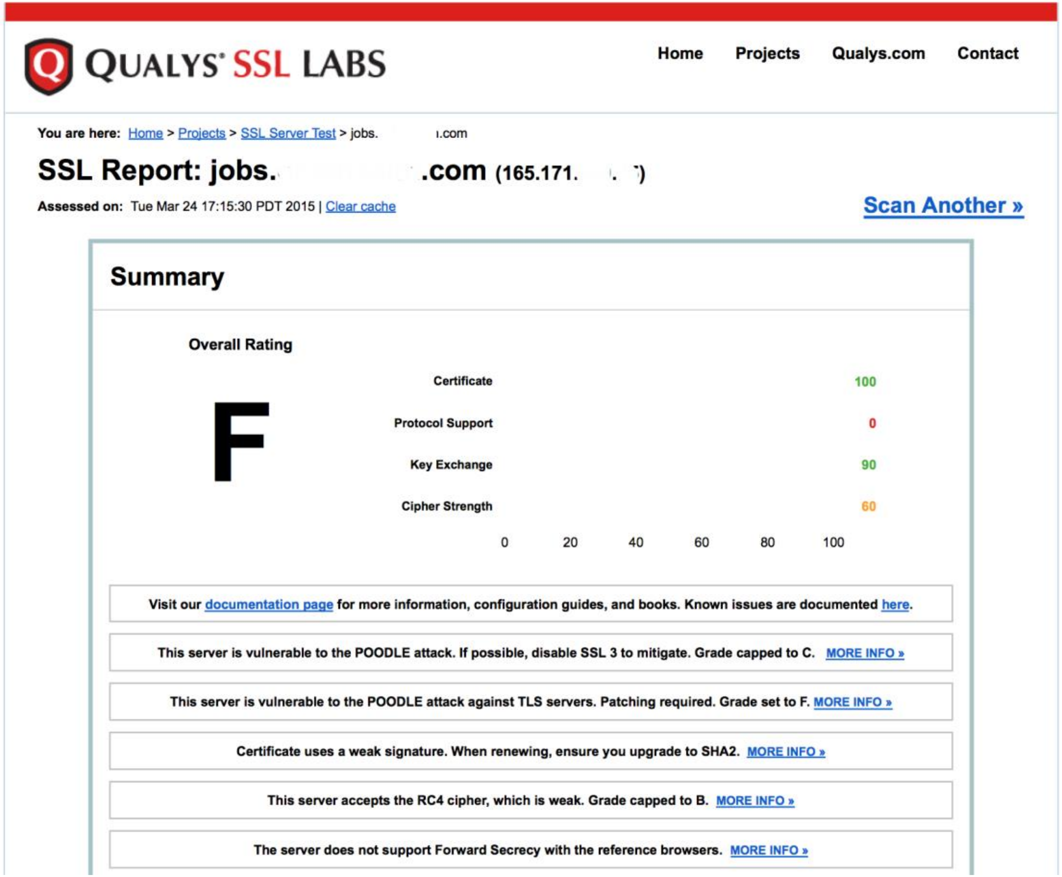
▾ Technical Details

cw.halogensoftware.com uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is unknown.
The server might not be sending the appropriate intermediate certificates.
An additional root certificate may need to be imported.

(Error code: sec_error_unknown_issuer)

ATS Fails – HTTPS & Certs



QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > jobs.[redacted].com

SSL Report: jobs.[redacted].com (165.171.[redacted])

Assessed on: Tue Mar 24 17:15:30 PDT 2015 | Clear cache

Scan Another »

Summary

Overall Rating

F

Certificate	100
Protocol Support	0
Key Exchange	90
Cipher Strength	60

0 20 40 60 80 100

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

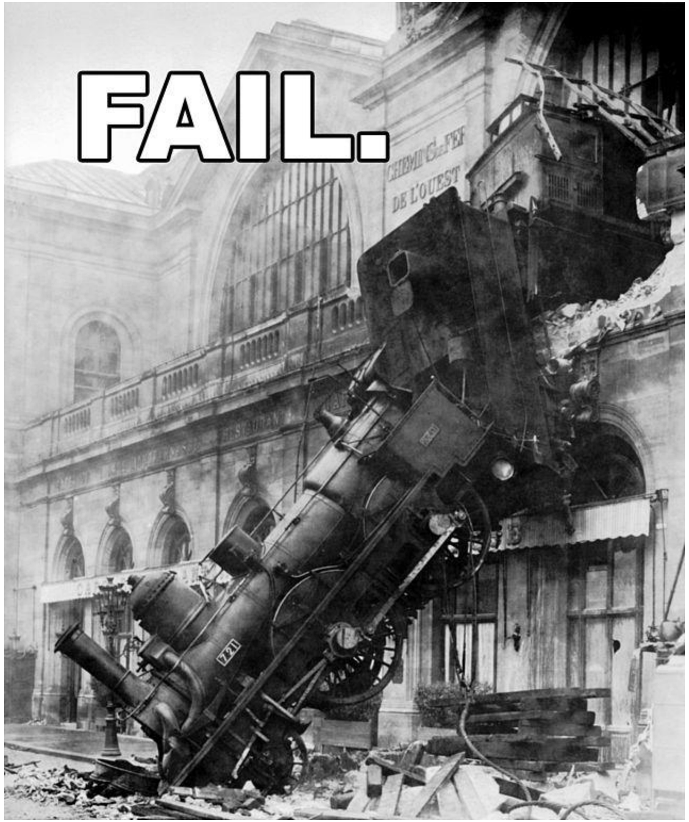
This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. MORE INFO »

This server is vulnerable to the POODLE attack against TLS servers. Patching required. Grade set to F. MORE INFO »

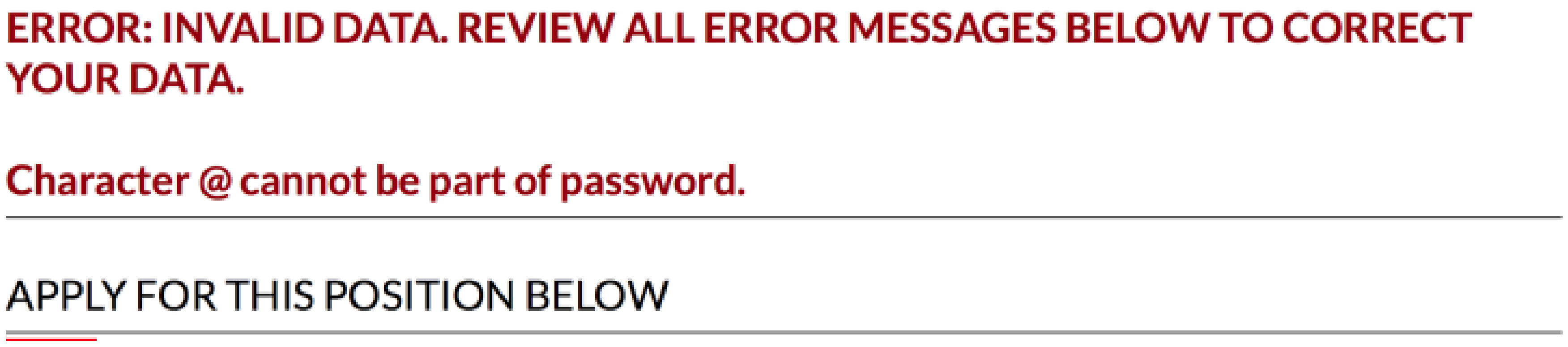
Certificate uses a weak signature. When renewing, ensure you upgrade to SHA2. MORE INFO »

This server accepts the RC4 cipher, which is weak. Grade capped to B. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »



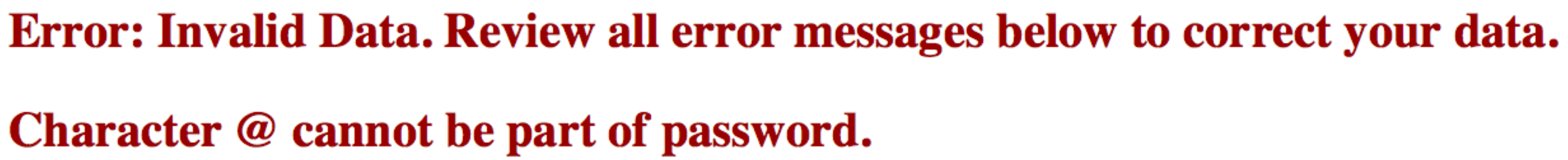
ATS Fails – Passwords



ERROR: INVALID DATA. REVIEW ALL ERROR MESSAGES BELOW TO CORRECT YOUR DATA.

Character @ cannot be part of password.

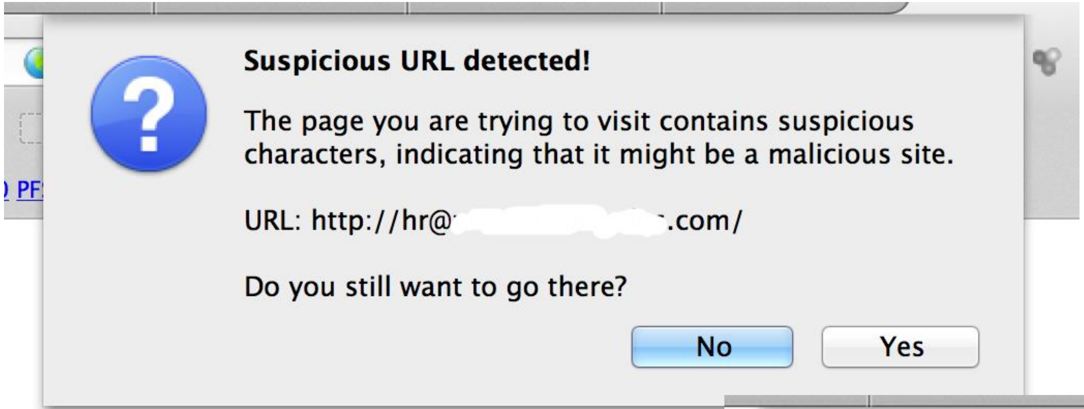
APPLY FOR THIS POSITION BELOW



Error: Invalid Data. Review all error messages below to correct your data.

Character @ cannot be part of password.

ATS Fails – Bad UI & AppSec

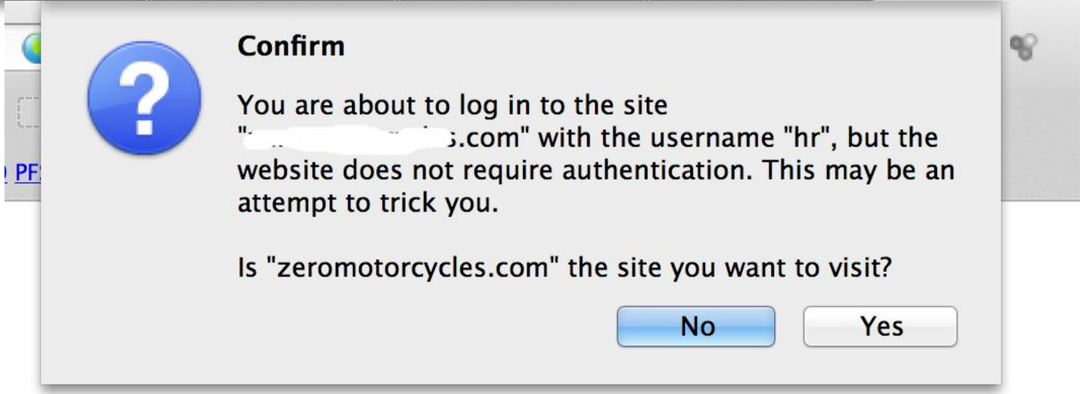


Suspicious URL detected!

The page you are trying to visit contains suspicious characters, indicating that it might be a malicious site.

URL: http://hr@[redacted].com/

Do you still want to go there?

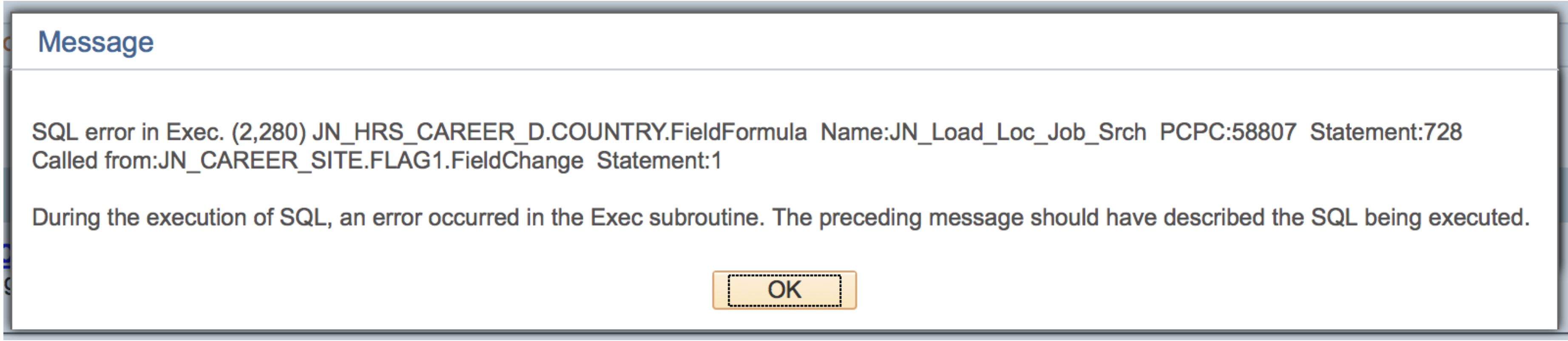


Confirm

You are about to log in to the site "[redacted]s.com" with the username "hr", but the website does not require authentication. This may be an attempt to trick you.

Is "zeromotorcycles.com" the site you want to visit?

ATS Fails – Bad Error Handling

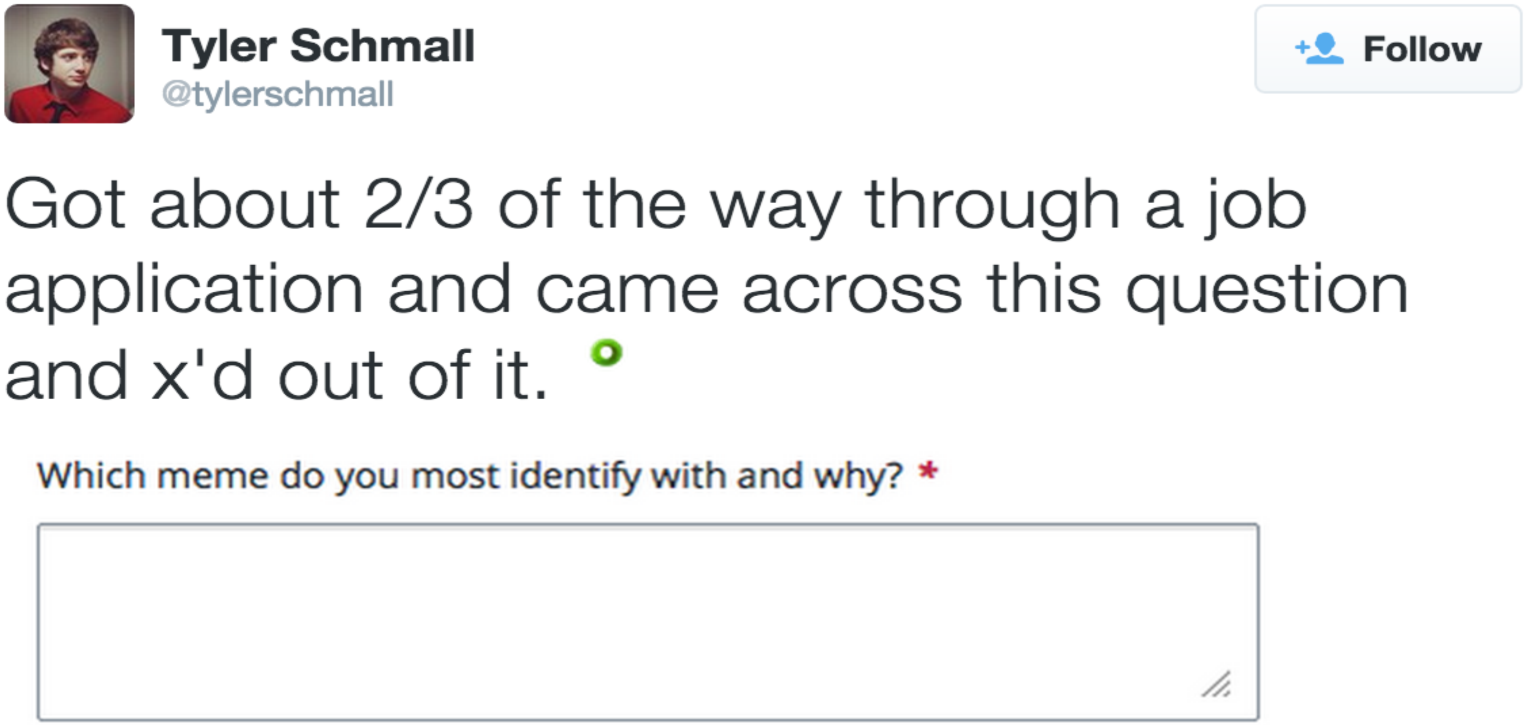


Message

SQL error in Exec. (2,280) JN_HRS_CAREER_D.COUNTRY.FieldFormula Name:JN_Load_Loc_Job_Srch PCPC:58807 Statement:728
Called from:JN_CAREER_SITE.FLAG1.FieldChange Statement:1

During the execution of SQL, an error occurred in the Exec subroutine. The preceding message should have described the SQL being executed.

The Owl Question



Tyler Schmall
@tylerschmall

Got about 2/3 of the way through a job application and came across this question and x'd out of it.

Which meme do you most identify with and why? *

Hackers: Hack Your Resume

- Experience reflects your background and the role
  - No stretching the truth
- Careful on the buzzword bingo
  - Enough to match the role in the big HR and ATS matching
  - Know what the terms mean
- Tailor your resume to make it relevant to the employer/hiring manager and the role

Hackers: Hack The File Name

- Have your resume/CV as long as it needs to be.
  - Is your resume long enough so it reaches where it's supposed to go?
- 1 or 2 page resume, and a full CV
  - Different hiring managers, different preferences
- File names make a difference
  - Distinguish yourself from other candidates
  - Managers and HR make mistakes, and lose documents; good labeling helps you out.
- Sanitize the metadata

Customized Resumes

- The full CV with buzzword bingo for the heavyweight application tracking systems
  - Import, then tweak details
- The 1 or 2 page resume for human digestion
  - Include with the ATS application as well

Security Clearances

- Do not belong on the resume or your social media profiles
- Broadcasting makes you a bigger target and look unprofessional
- DSS/OPM does not look kindly on this
  - Read the NDA you signed
  - Does not matter that the APT$ stole it all
- When asked by HR, the proper answer: “That information can be verified with a conversation with your Personal Security Officer.”
  - If this answer is not satisfactory, do you want to work for them?

Don’t Pen Test With Your Resume

- Submit resumes as text, RTF, and/or PDF
- Do not insert malicious code or trackers into your resume or cover letter
    - Nor should you conduct a penetration test on the application systems

Am I Qualified?

Remember:

Determining if you are qualified for the role is not your job.

It is the job of HR (and perhaps the ATS), the Hiring Manager and perhaps their leadership to make that determination.

Application Tracking System

- There are different Application Tracking Systems (ATS)
  - Heavyweight application systems with data mining looking for keywords & application management
    - Taleo, iCIMS, SuccessFactors, PeopleSoft, Bullhorn, Brassring
  - Lightweight application tracking
    - Workday, Jobvite, SilkRoad, LinkedIn, SmartRecruiter
  - Human

ATS Recommendations

- Be one of the first to apply
- Fill out every applicable text box that you feel comfortable with
- Resume/CV formatting for computer readable
  - No graphics or special characters
  - Web safe fonts
  - Spell check
  - Skills section as complete and truthful as possible

Email Applications

- Quick and easy to apply, easy to get lost
- Subject line is important
- Include a cover letter in the body of the email
- Digital signature is a bonus

USAJobs Applications

- Government roles have dedicated websites for applications
  - For USA, USAJobs
    - Mostly, some .GOV still have their own
- Similar to the heavyweight ATS
  - Unwieldy
  - Be sure to answer the qualifier questions
  - Review the application process for the surprise essay questions

Hacking Back To The Basics

- Use a professional looking email address
  - Don’t send it from l33tH4x0rz666@caturday.net
  - Caution on Google data mining
  - Best keep personal & work email separate
    - Conduct a search on your self & your email address

The Basics: Cover Letter

- What role are you applying for?
- Why do you want the role?
- No letter indicates you are not interested, or just spamming applications
- Just five (5) minutes spent on why this role sounds interesting makes a difference

Hackers: Meet Hiring Managers

- Reach out to your network regarding specific companies and roles
  - Social media
- Get involved!
  - Local IT & InfoSec communities/Meetups
  - Mailing lists & forums
  - Conferences
  - Online communities

Hackers: Working With Recruiters

- There are different types of recruiters
  - Technical recruiters
    - Company
    - Agencies (boutique and otherwise)
  - Agencies just looking for a body to fill a seat
    - Spamming of the PDs, unable to answer follow-up questions
    - Helping perpetuate the sub class of contractor/consultant workers

Hackers: Understand The Odds

- Connect with others before the search officially begins
- Diversify your applications
- Location
  - Depth of the labor pool
  - Who else applied for the role
- You may not have the buzzword bingo or the industry background they want

Hackers: Keep Perspective

- Try not to get too discouraged
- Have patience
- Keep in mind the other requirements and stressors the hiring managers have
  - Outside influences on the process
- Get feedback from mentors & peers
- Remember, it is not you – it is not personal (normally)

The Interview

Pre-Interview

- Consider the types of questions you want to ask BEFORE the interview
  - Respect the sensitivities of the applications in your questions
- Creating the interviews
  - Balancing fact based questions vs essay/short
- Does your team share questions?
  - Figure out who asks what
  - Avoid duplication

Define Key Areas

- How do you define key areas/topics?
- Testing/evaluating for specific skills? Or more General?
- How do you match up skills to the position description (PD), then the areas to question per candidate?

Hiring Managers

- “Stump the monkey” isn’t fun for anyone
  - Trick questions, the Google stumpers
  - Does not convey how good of an analyst they are or could be
    - How the candidate processing information to mitigate the threat/risk/vulnerability
    - Not how fast they can recite knowledge
  - Could dissuade a good candidate from accepting an offer

“Stump The Monkey”

- The intent is to find individuals for your team, not prove how smart you are - or how dumb they are
- Lasting impression on you & company
    - See the Glassdoor interview ratings & feedback
- Sometimes there is more than one answer
    - With the answer different than yours
    - See Wheaton's law

Question Bias

- So what if the candidate does not know how to work with oak
  - Can they learn to work with mahogany?
- Avoid close-ended questions
  - “Have you worked with Oak”?
  - “What is the UDP flag on a DNS request that fails”
  - “What protocol uses port 0”

Toolset Bias

- Best to use situational, exploratory conversations
  - What are some of the ways you have used wood to address vulnerabilities?
  - Not: Have you ever used maple wood?
- Review: If Carpenters Were Hired Like Programmers

Hiring Bias

- Stop passing judgment
  - Piercings and tattoos no longer mean that they’re ex-convicts
- See Wheaton’s Law
  - People get nervous and forget things
- So what if they self-identify as a hacker?
- Lookup: Evaluate the Scrapper

Time In A Role

- Why does the length of time in a role matter?
  - Most are out of the candidate's control
    - Startups
    - Company failure or change of direction
    - Contract work
    - Layoff, unemployment

Periods Of Unemployment

- Unemployment does not mean untouchable
  - Put aside your bias
  - Listen to the reason(s) and don’t assume they’re excuses
- Discrimination
- Not all gaps between jobs should be a (bad) reflection on the candidate

The InfoSec Question

- Can the candidate explain how you can reduce Risk by affecting Vulnerability, Threat, Asset or Cost?
  - Most technical folk focus on Vulnerability.
  - Most nontechnical folk focus on Threat
- We need to reduce Vulnerability and Threat, but also work on Cost

The Trifecta

- Ability to learn (and want to learn skills)
- Passion
  - What is this person passionate about?
- Ability to be wrong/fail, and to do so well.
  - We will all fail.
  - Can you learn and grow from it, or do you hide it and try to blame others?

Hacker Wear

- Leave the ski mask at home
- Appropriateness
  - A bank vs. a startup?
  - East or West coast? Southwest?
- Determine the daily dress and take it up a notch

Mind Your Manners

- Don’t ducking swear
- Watch your personal sharing & stories
- Personal hygiene
- Mind the other person’s bubble
- Manners still count

Hack the Interview

- Research on company and interviewees
  - Glassdoor
  - Wikipedia
  - Crunchbase
  - Social media
    - LinkedIn, with your alternate profile & proxy
  - Review rating Web sites, GTFG

Knowing Your Target

- Understand the target organization and hiring manager
  - Their product, company values and culture
- Able to explain why & how you are the best person for the role and the team at that company
- Have your message (your three bullets) and stick to them

Question Everything

- From your research, have questions to ask them
  - Get them to sell you the role & the company
  - This is an interview on both sides of the table
    - Would you want to work for the manager?
    - Do you like the company, what they produce and stand for?

Question Everything

- Have appropriate answers for every InfoSec related interview question online
  - How would you figure something you don’t know out?
- It is a judgment call on calling out interviewers regarding inappropriate questions

Question The Timing

- Did the interviewees give you enough time to ask questions?
- Was it the token five minutes at the end of their questions?
- Was it a conversation between peers, or individuals in the industry - or a grilling?

Post-Interview

Provide Reasons, Not Excuses

- In your team interviews, use a scoring system and average the scores to help eliminate bias
- People should be hired for aptitude, but attitude is important to an extent
- Think about whether you would want to work with this individual, but do not use it as an excuse when someone ”better” comes along
- Do you think the person can do the job - or can learn?
- Diversity is good

Post-Interview Etiquette

- Don’t leave people hanging
  - Send an email or call with status updates
  - Contact within 3-4 weeks at maximum
- Provide feedback
  - If HR/Legal will allow
  - Builds relationships within the community
  - Helps improve the pool of candidates

Feedback

- Glaring resume issues/errors
- Topics to review
  - Tools, Techniques, Procedures (TTPs)
  - Protocols
- Interview tips
  - Talk more/don’t talk as much
  - Etiquette

Hacker Follow-Up

- Send a “thank you” email to all you talked and interacted with. Consider snail mail card
- Follow-up
  - When should you reach out if you have not heard back?
  - Don’t panic, it may take a while to hear back
- Be realistic in your expectations
  - Know the local/regional/national market

Social Networking

- Leverage your network to provide insight & potential references to the company/hiring manager
- How do you get previous supervisors as references?
- Hold off on sending social media connection requests
- Leave feedback on Glassdoor, Indeed, etc.

“Employers forget that the impression they leave on their employees, past & present, influences income, rep and biz dev in ways unknown.”

-@kjvalentine

Applying What You Learned

- Connect with at least 2 people post-conference; learn how their application and selection process works (or not work).
- How can you be more active and involved in your local IT/InfoSec community?
- What can you do to mentor younger/less experienced?
- How can we improve our application process? Our screening process and criteria?
- Have you ran a ‘pen test’ on your application process?

Summary

- Set and adjust our expectations
- Our application processes are typically cumbersome and unwieldy, aim to improve them
- Our interviews may not provide the best opportunities for assessing capabilities and talent
- Our post-interview follow up is reflective of our communication styles and capabilities
- All areas for improvement, on both sides

Thank you

@StartUpJackson, @RebeccaSlatkin, @TylerSchmall,

Trey Ford aka @treyford

roadtociso.wordpress.com - Jesika McEvoy

jasonbock.net - Jason Bock

@kjvalentine

John Omernik aka Chief Ten Beers

Winn Schwartau

All those applications we submitted, those folks we interviewed with, and those we have interviewed

References & Resources

Winn Schwartau, “Hiring the unhireable”

http://techspective.net/2015/07/06/hiring-the-unhireable-its-time-we-get-over-ourselves/

If Carpenters Were Hired Like Programmers

http://www.jasonbock.net/jb/News/Item/7c334037d1a9437d9fa6506e2f35eaac

Why 'True Recruiters' are actually Super Unicorns

https://www.linkedin.com/pulse/why-true-recruiters-actually-super-unicorns-ingeborg-van-harten

Evaluate the Scrapper

http://www.ted.com/talks/regina_hartley_why_the_best_hire_might_not_have_the_perfect_resume