



# Fortify on Demand Security Review

<b>Company:</b>	<b>DOBT_FMA_343719085</b>
<b>Project:</b>	<b>DOBT Screendoor</b>
<b>Version:</b>	<b>8-7-15</b>
<b>Latest Analysis:</b>	<b>8/8/2015 2:27:40 AM</b>

# Executive Summary

Company: DOBT\_FMA\_343719085

Project: DOBT Screendoor

Version: 8-7-15

Static Analysis Date:

Dynamic Analysis Date: 8/8/2015 2:27:40 AM

**Fortify Security Rating**

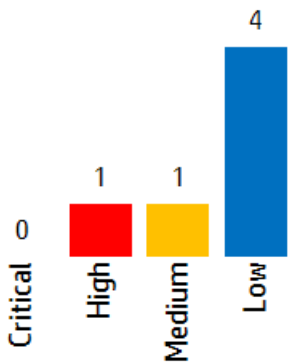
★★★★☆13 issues

Static: ❌Dynamic: ✔️

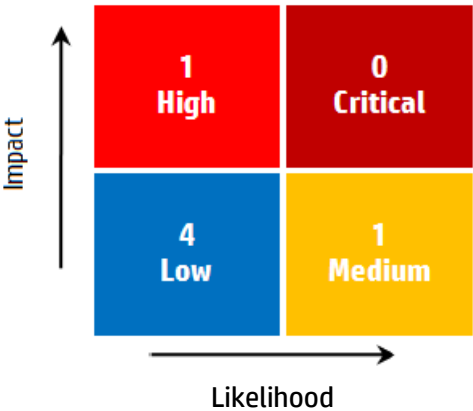
## Application Details

Business criticality	Medium	Application type	Software Development
Interface type	Web Access	Project type	Application

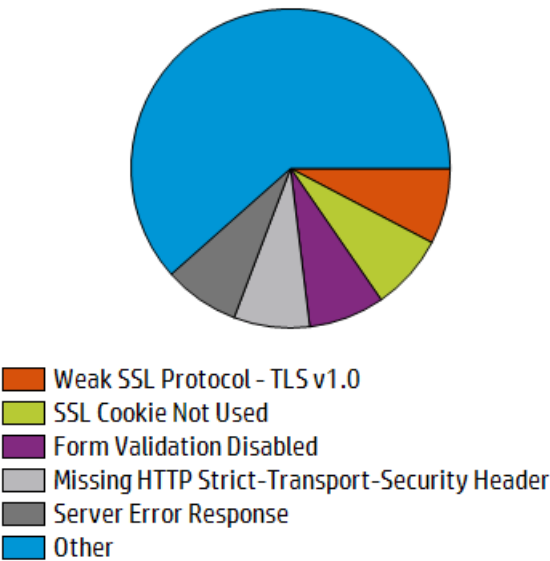
Risk Totals by Severity



Risk Totals by Instance Count



Most Prevalent Issues (by Category)



Remediation Roadmap

To Achieve	Major Fixes	Minor Fixes
★★★★★	0	0
★★★★☆	1	0
★★★☆☆	1	0
★★★☆☆	4	0
★★★★★	0	0

Issue Status

New	Existing	Reopened
13	0	0

# Issue Breakdown

Issues are divided based on their impact (potential damage) and likelihood (probability of identification and exploit).

High impact / high likelihood issues represent the highest priority and present the greatest threat.

Low impact / low likelihood issues are the lowest priority and present the smallest threat.

See Appendix for more information.

Rating	Category	Test Type	Instance Count
High	Weak SSL Protocol - TLS v1.0	Dynamic	1
Medium	SSL Cookie Not Used	Dynamic	1
Low	Form Validation Disabled	Dynamic	1
Low	Missing HTTP Strict-Transport-Security Header	Dynamic	1
Low	Server Error Response	Dynamic	1
Low	Set-Cookie does not use HTTPOnly Keyword	Dynamic	1

# Issue Breakdown by OWASP Top 10 2013

## PCI Sections 6.3, 6.5 & 6.6

The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

The PCI compliance standards, particularly sections 6.3, 6.5, and 6.6, reference the OWASP Top Ten vulnerability categories as the core categories that must be tested for and remediated.

OWASP 2013 Category	Severity			
	Critical	High	Medium	Low
None		1	1	4
Total		1	1	4

# Issue Breakdown by Analysis Type

Issues are divided based on their impact (potential damage) and likelihood (probability of identification and exploit).

High impact / high likelihood issues represent the highest priority and present the greatest threat.

Low impact / low likelihood issues are the lowest priority and present the smallest threat.

See Appendix for more information.

Category	Static	Dynamic
Form Auto Complete Active	0	1
Form Validation Disabled	0	1
Hidden Form Value	0	1
Missing HTTP Strict-Transport-Security Header	0	1
Possible Authentication Misconfiguration (WWW-Authenticate)	0	1
Possible File Upload Capability	0	1
Possible Insecure Cryptographic Hash (MD Family)	0	1
Possible Insecure Cryptographic Hash (SHA-0/SHA-1)	0	1
Privacy Policy Not Present	0	1
Server Error Response	0	1
Set-Cookie does not use HTTPOnly Keyword	0	1
SSL Cookie Not Used	0	1
Weak SSL Protocol - TLS v1.0	0	1
Total	0	13

# Issue Details

Below is an enumeration of all issues found in the project. The issues are organized by priority and category and then broken down by the package, namespace, or location in which they occur.

The priority of an issue can be Critical, High, Medium, or Low.

Issues from static analysis reported on at same line number with the same category originate from different taint sources.

## 6.1.1 Weak SSL Protocol - TLS v1.0

**High**

**None**

**OWASP Top 10: None**

**PCI 3.0: None**

### Summary

The Transport Layer Security (TLS) protocol provides a protection mechanism to better protect authenticity, confidentiality and integrity of the data transmitted between a client and a web server. The TLS protocol has undergone various revisions resulting in periodic version updates. Each revision tries to address security weakness in prior versions and incorporate support for the latest in security measures. It is strongly recommended to use the latest version of the available protocol, whenever possible.

TLS 1.0 is considered insecure as it lacks support for strong ciphersuites and is known to be plagued by several known vulnerabilities. It either uses RC4 cipher, which is prone to bias attacks or uses Cipher Block Chaining (CBC) mode cipher, which enables condition for POODLE (Padding Oracle On Downgraded Legacy Encryption) attacks.

NIST Special Publication 800-52 Revision 1 no longer considers TLS 1.0 as strong cryptography. TLS 1.0 is also no longer in compliance with PCI DSS v3.1 requirements. PCI does not consider TLS 1.0 to be adequate to protect cardholder data and has deprecated its use starting June 2016.

Use of insecure protocol versions will weaken the strength of the transport protection and could allow an attacker to compromise, steal or modify sensitive information. Configuring the web server to use the most secure protocol, TLS 1.1 or TLS 1.2 is highly recommended.

### Explanation

Use of a weak protocol such as TLS 1.0 leaves the connection vulnerable to man-in-the-middle attacks. This would allow the attacker to read and modify data on a secure TLS connection, thus compromising user security and privacy. Its use would also limit the use of strong cipher suites that help protect data integrity and confidentiality.

### Recommendation

Disable support for the TLS 1.0 protocol on the server. Both NIST 800-52 and PCI DSS v3.1 strongly recommend upgrade to the latest version of TLS available, TLS 1.2. Or, at a minimum an upgrade to TLS 1.1.

- For Apache, modify the following lines in the server configuration
  - SSLProtocol ALL -SSLv2 -SSLv3 -TLSv1
- For Nginx, modify the following lines in server configuration:
  - ssl\_protocols TLSv1.1 TLSv1.2;
- For IIS, please refer to Microsoft Knowledge Base Articles:
  - <https://technet.microsoft.com/library/security/3009008>
- For other servers, please refer to vendor specific documentation.

### References

**OWASP:**

[Transport Layer Protection Cheat Sheet](#)

**NIST:**

[NIST SP 800-52 Revision 1](#)

**PCI Security Standards Council:**

[PCI DSS v3.1](#)  
[Migrating from SSL and Early TLS](#)  
[PCI SSC FAQ on impending revisions to PCI DSS, PA-DSS to address SSL protocol vulnerability](#)

**Microsoft:**  
[Knowledge Base Article ID: 187498](#)  
[Knowledge Base Article ID: 245030](#)  
[Security Guidance for IIS](#)

**Apache:**  
[SSL/TLS Strong Encryption: FAQ](#)

**CVE-2014-8730**  
[CVE-2014-8730](#)

**POODLE Vulnerability Expands Beyond SSLv3 to TLS 1.0 and 1.1**  
<https://www.globalsign.com/en/blog/poodle-vulnerability-expands-beyond-ssl3-to-tls/>

**TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks**  
<https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-001>

**RC4 in TLS is Broken: Now What ?**  
<https://community.qualys.com/blogs/securitylabs/2013/03/19/rc4-in-tls-is-broken-now-what>

## Instances

Weak SSL Protocol - TLS v1.0	High
Location	
ID 6319938 - <a href="https://screendoor.dobt.co:443/account/projects">https://screendoor.dobt.co:443/account/projects</a>	

## 6.2.1 SSL Cookie Not Used

Medium

None

OWASP Top 10: None

PCI 3.0: None

### Summary

This policy states that any area of the website or web application that contains sensitive information or access to privileged functionality such as remote site administration requires that all cookies are sent via SSL during an SSL session. The URL: ~FullURL~ has failed this policy. If a cookie is marked with the "secure" attribute, it will only be transmitted if the communications channel with the host is a secure one. Currently this means that secure cookies will only be sent to HTTPS (HTTP over SSL) servers. If secure is not specified, a cookie is considered safe to be sent in the clear over unsecured channels.

### Recommendation

#### For Development:

This issue will ultimately need to be rectified by your Network or Security Operations team. If necessary, implement the change in your development environment.

#### For Security Operations:

IIS 4.0 and 5.0 Fix Information:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;274149>

Remediation for IIS 6.x:

<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/0d49cbc8-10e1-4fa8-ba61-c34e524a3ae6.mspx?mfr=true>

<http://msdn2.microsoft.com/en-us/library/ms998310.aspx>

Require SSL for an Authentication Cookie (IIS 7):

[http://technet.microsoft.com/en-us/library/cc771633\(W5.10\).aspx](http://technet.microsoft.com/en-us/library/cc771633(W5.10).aspx)

AnonymousIdentificationSection Class [IIS 7]:

<http://msdn.microsoft.com/en-us/library/ms689482.aspx>

Use the following links to remediate this issue on an Apache server:

<http://search.cpan.org/~jkrasnoo/ApacheCookieEncrypted-0.03/Encrypted.pm>

<http://hc.apache.org/httpclient-3.x/apidocs/org/apache/commons/httpclient/class-use/Cookie.html>

#### For QA:

This issue will ultimately need to be rectified by your Network or Security Operations team. If necessary, implement the change in your testing environment.

### References

General Information:

[The Unofficial Cookie FAQ](#)

### Instances

SSL Cookie Not Used

Medium

Location

ID 6319945 - <https://screendoor.dobt.co:443/>



6.3.1 Form Validation Disabled

Low

None

OWASP Top 10: None

PCI 3.0: None

**Summary**

HTML5 provides a convenient way to add client-side input form field validation by simply including a "required" attribute for required fields or "fieldtype" attribute for common input types or, more granularly, by enabling users to specify a data type-sensitive context that allows pattern-based validation. Developers can supply a customizable "pattern" attribute that checks the input against a regular expression. However, this validation gets disabled when adding a "novalidate" attribute on a form field or a "formnovalidate" attribute on a submit input form field. This check detects whether the "novalidate" or "formnovalidate" attributes are used which may lead to a security vulnerability depending on how securely the application is developed.

**Explanation**

HTML forms with disabled validation can potentially expose the server to numerous types of attacks. Unchecked input is the root cause of vulnerabilities like cross-site scripting and SQL injection.

**Recommendation**

While it is much more important to validate input on the server side, validation on the client side adds another layer of protection and makes the process of completing HTML forms more user-friendly and responsive. Avoid using the "novalidate" or "formnovalidate" attributes alone unless compensating methods of validation are being used in their place, and always implement complementary form field validation from the application server; never relying solely on client-side validation routines in the browser.

**References**

**HTML5 <form> novalidate Attribute**  
[http://www.w3schools.com/html5/att\\_form\\_novalidate.asp](http://www.w3schools.com/html5/att_form_novalidate.asp)

**HTML5 <input> formnovalidate Attribute**  
[http://www.w3schools.com/html5/att\\_input\\_formnovalidate.asp](http://www.w3schools.com/html5/att_input_formnovalidate.asp)

Instances	
Form Validation Disabled	Low
Location	
ID 6319947 - <a href="https://screendoor.dobt.co:443/account/settings">https://screendoor.dobt.co:443/account/settings</a>	

## 6.3.2 Missing HTTP Strict-Transport-Security Header

Low

None

OWASP Top 10: None

PCI 3.0: None

### Summary

Http Strict Transport Security (HSTS) policy enables web applications to enforce web browsers to restrict communication with the server over an encrypted SSL/TLS connection for a set period. Policy is declared via special Strict Transport Security response header. Encrypted connection protects sensitive user and session data from attackers eavesdropping on network connection.

Consider following attack scenarios:

- Users often omit the URI scheme i.e. https:// when typing a URL in location bar to access a website. Also third party websites can link to the site using the "http" scheme instead of "https". This could result in an initial connection to a HTTPS-enabled site over an unencrypted channel. An eavesdropping attacker can hijack this unencrypted connection and replace the intended use of HTTPS protocol with HTTP in an attack known as SSLStrip, granting unauthorized access to all subsequent traffic.
- Websites often transfer non-sensitive resources such as help documents over an unencrypted HTTP connection. Any cookies without a secure flag are sent along with such requests potentially disclosing sensitive user and session data to eavesdropper.
- Man-in-the-Middle attacks that exploit user tendencies to override invalid certification warnings, e.g. SSLSniff.

For web sites configured with an accurate HSTS policy, browsers automatically upgrade any HTTP connections to HTTPS. Furthermore, browsers prevent users from overriding any host certificate warnings. HSTS offers an effective defense against above attack scenarios.

### Explanation

A successful MiTM attack such as SSLStrip or SSLsniff can lead to the compromise of sensitive user data such as financial information, Social Security Number, personal information etc. as well as grant unauthorized access to user accounts enabling attackers to perform privileged actions on client's behalf.

### Execution

Access location ~FullURL~ and notice the absence of the Strict Transport Security header in the HTTP response.

### Recommendation

Configure the web application under test to include Strict Transport Security header in every response generated by an HTTPS-enabled site. Any HTTP version of site on the same domain should permanently redirect to the secure encrypted site. Header should not be added to HTTP response as browsers will ignore it.

It is important to note that this header does not prevent from above mentioned attack scenarios during the very first connection to the site or any connections established after the set period has expired. To prevent such a scenario, the site must be added to the pre-loaded HSTS hosts list embedded in both Google Chrome and Mozilla Firefox browsers.

### References

<http://tools.ietf.org/html/rfc6797>

### Instances

Missing HTTP Strict-Transport-Security Header

Low

Location

ID 6319939 - <https://screendoor.dobt.co:443/>

## 6.3.3 Server Error Response

Low

None

OWASP Top 10: None

PCI 3.0: None

### Summary

A server error response was detected. The server could be experiencing errors due to a misbehaving application, a misconfiguration, or a malicious value sent during the auditing process. While error responses in and of themselves are not dangerous, per se, the error responses give attackers insight into how the application handles error conditions. Errors that can be remotely triggered by an attacker can also potentially lead to a denial of service attack or other more severe vulnerability. Recommendations include designing and adding consistent error handling mechanisms which are capable of handling any user input to your web application, providing meaningful detail to end-users, and preventing error messages that might provide information useful to an attacker from being displayed.

### Explanation

The server has issued a 500 error response. While the body content of the error page may not expose any information about the technical error, the fact that an error occurred is confirmed by the 500 status code. Knowing whether certain inputs trigger a server error can aid or inform an attacker of potential vulnerabilities.

### Recommendation

#### For Security Operations:

Server error messages, such as "File Protected Against Access", often reveal more information than intended. For instance, an attacker who receives this message can be relatively certain that file exists, which might give him the information he needs to pursue other leads, or to perform an actual exploit. The following recommendations will help to ensure that a potential attacker is not deriving valuable information from any server error message that is presented.

- **Uniform Error Codes:** Ensure that you are not inadvertently supplying information to an attacker via the use of inconsistent or "conflicting" error messages. For instance, don't reveal unintended information by utilizing error messages such as Access Denied, which will also let an attacker know that the file he seeks actually exists. Have consistent terminology for files and folders that do exist, do not exist, and which have read access denied.
- **Informational Error Messages:** Ensure that error messages do not reveal too much information. Complete or partial paths, variable and file names, row and column names in tables, and specific database errors should never be revealed to the end user. Remember, an attacker will gather as much information as possible, and then add pieces of seemingly innocuous information together to craft a method of attack.
- **Proper Error Handling:** Utilize generic error pages and error handling logic to inform end users of potential problems. Do not provide system information or other data that could be utilized by an attacker when orchestrating an attack.

#### Removing Detailed Error Messages

Find instructions for turning off detailed error messaging in IIS at this link:

<http://support.microsoft.com/kb/294807>

#### For Development:

From a development perspective, the best method of preventing problems from arising from server error messages is to adopt secure programming techniques that prevent problems that might arise from an attacker discovering too much information about the architecture and design of your web application. The following recommendations can be used as a basis for that.

- Stringently define the data type (for instance, a string, an alphanumeric character, etc) that the application will accept.
- Use what is good instead of what is bad. Validate input for improper characters.
- Do not display error messages to the end user that provide information (such as table names) that could be utilized in orchestrating an attack.
- Define the allowed set of characters. For instance, if a field is to receive a number, only let that field accept numbers.
- Define the maximum and minimum data lengths for what the application will accept.
- Specify acceptable numeric ranges for input.

#### For QA:

The best course of action for QA associates to take is to ensure that the error handling scheme is consistent. Do you receive a different type of error for a file that does not exist as opposed to a file that does? Are phrases like "Permission Denied" utilized which could reveal the existence of a

file to an attacker? Inconsistent methods of dealing with errors gives an attacker a very powerful way of gathering information about your web application.

## References

**Apache:**  
[Security Tips for Server Configuration](#)  
[Protecting Confidential Documents at Your Site](#)  
[Securing Apache - Access Control](#)

**Microsoft:**  
[How to set required NTFS permissions and user rights for an IIS 5.0 Web server](#)  
[Default permissions and user rights for IIS 6.0](#)  
[Description of Microsoft Internet Information Services \(IIS\) 5.0 and 6.0 status codes](#)

## Instances

Server Error Response	Low
Location	
ID 6319949 - <a href="https://screendoor.dobt.co:443/dobt_hooks/session?payload=%5b%2224a2f1e394a28901d943bf0c8e524d8e5a7f1cda%22%2c%7b%22verification_token%22%3a%22QKs7uVmaw6YqoDiz_HsK9qUt5w%22%2c%22state%22%3a%7b%22redirect%22%3a%22https%3a%5c%2f%5c%2fscreendoor.dobt.co%5c%2f%5cr%5cnSPIHeader%3a+SPIValue%22%7d%7d%5d">https://screendoor.dobt.co:443/dobt_hooks/session?payload=%5b%2224a2f1e394a28901d943bf0c8e524d8e5a7f1cda%22%2c%7b%22verification_token%22%3a%22QKs7uVmaw6YqoDiz_HsK9qUt5w%22%2c%22state%22%3a%7b%22redirect%22%3a%22https%3a%5c%2f%5c%2fscreendoor.dobt.co%5c%2f%5cr%5cnSPIHeader%3a+SPIValue%22%7d%7d%5d</a>	

6.3.4 Set-Cookie does not use HTTPOnly Keyword

Low

None

OWASP Top 10: None

PCI 3.0: None

**Summary**

The web application does not utilize HTTP only cookies. This is a new security feature introduced by Microsoft in IE 6 SP1 to mitigate the possibility of a successful Cross-Site scripting attack by not allowing cookies with the HTTP only attribute to be accessed via client-side scripts. Recommendations include adopting a development policy that includes the utilization of HTTP only cookies, and performing other actions such as ensuring proper filtration of user-supplied data, utilizing client-side validation of user supplied data, and encoding all user supplied data to prevent inserted scripts being sent to end users in a format that can be executed.

**References**

**References:**

<https://social.msdn.microsoft.com/Search/en-US?query=HTTPOnly%20Cookie&emptyWatermark=true&ac=5>

**Instances**

Set-Cookie does not use HTTPOnly Keyword	Low
Location	
ID 6319943 - <a href="https://screendoor.dobt.co:443/hp-scan/12345/admin/collaborators?direction=asc&amp;sort=user_name">https://screendoor.dobt.co:443/hp-scan/12345/admin/collaborators?direction=asc&amp;sort=user_name</a>	

6.4.1 Form Auto Complete Active

Best Practice

None

OWASP Top 10: None

PCI 3.0: None

**Summary**

Most recent browsers have features that will save form field content entered by users and then automatically complete form entry the next time the fields are encountered. This feature is enabled by default and could leak sensitive information since it is stored on the hard drive of the user. The risk of this issue is greatly increased if users are accessing the application from a shared environment. Recommendations include setting autocomplete to "off" on all your forms.

**References**

Microsoft:  
[Autocomplete Security](#)

**Instances**

Form Auto Complete Active	Best Practice
Location	
ID 6319944 - <a href="https://screendoor.dobt.co:443/account/projects">https://screendoor.dobt.co:443/account/projects</a>	

## 6.4.2 Possible Insecure Cryptographic Hash (MD Family)

### Best Practice

None

OWASP Top 10: None

PCI 3.0: None

### Summary

A string of hexadecimal digits matching the length of a cryptographic hash from the MD family was detected. Cryptographic hashes are often used to protect passwords, session information, and other sensitive data. There are multiple hashing algorithms in the MD family. By far the most commonly used algorithm is MD5, though MD4 and MD2 are still used with various public key and digital certificate systems. There are known attacks against MD5, MD4, and MD2. These hashes are also susceptible to Rainbow table attacks unless the input is properly salted. As such the MD family of cryptographic hashing functions should not be considered secure and should only be used in certain situations.

### Explanation

Hashes produced by the MD family should only be used for short-lived uses where the hash and/or hashed data is not highly security sensitive, or for uses where uniqueness is not a critical requirement. MD Hashes should not be used for any type of long term application such as verifying the integrity of a file or for password storage.

### Recommendation

#### For Development:

The application should only use cryptographically secure hashing algorithms, such as SHA-224, SHA-256, SHA-384, or SHA-512. Hashes representing sensitive data should be salted to reduce the effectiveness of rainbow tables.

#### For Security Operations:

Implement a security policy that precludes the use of MD5, MD4, or MD2 for cryptographic functionality.

#### For QA:

Make sure that the application is not relying on MD5, MD4, or MD2 for cryptographic functionality.

### References

#### MD5

<http://en.wikipedia.org/wiki/MD5>

#### Cryptographic Salting

[http://en.wikipedia.org/wiki/Salt\\_%28cryptography%29](http://en.wikipedia.org/wiki/Salt_%28cryptography%29)

#### Project Rainbow Crack

<http://www.antsight.com/zsl/rainbowcrack/>

### Instances

#### Possible Insecure Cryptographic Hash (MD Family)

#### Best Practice

##### Location

ID 6319948 - <https://screendoor.dobt.co:443/>

## 6.4.3 Possible Insecure Cryptographic Hash (SHA-0/SHA-1)

### Best Practice

None

OWASP Top 10: None

PCI 3.0: None

### Summary

A string of hexadecimal digits matching the length of a cryptographic SHA-0 or SHA-1 hash was detected. Cryptographic hashes are often used to protect passwords, session information, and other sensitive data. There are known attacks against SHA-0 and SHA-1. While not broken, SHA-0 and SHA-1 are considered weak. Various organizations, such as NIST in the United States, no longer recommend SHA-0 or SHA-1 and these algorithms should only be used in certain situations.

### Explanation

The SHA-0 and SHA-1 cryptographic hashing functions are considered weak. You should consider upgrading to a strong hash unless the hash is used for short-lived uses, where the hash and/or hashed data is not highly security sensitive, or for uses where uniqueness is not a critical requirement.

### Recommendation

#### For Development:

Consider upgrading to a secure hashing algorithms, such as SHA-224, SHA-256, SHA-384, or SHA-512. Hashes representing sensitive data that is stored for long periods of time should be salted to reduce the effectiveness of rainbow tables.

#### For Security Operations:

Implement a security policy that precludes the use of SHA-0 and SHA-1 for cryptographic functionality.

#### For QA:

Make sure that the application is not relying on SHA-0 and SHA-1 for cryptographic functionality.

### References

#### SHA Hash Functions

[http://en.wikipedia.org/wiki/SHA\\_hash\\_functions](http://en.wikipedia.org/wiki/SHA_hash_functions)

#### New Cryptoanalytic Results Against SHA-1

[http://www.schneier.com/blog/archives/2005/08/new\\_cryptanalyt.html](http://www.schneier.com/blog/archives/2005/08/new_cryptanalyt.html)

#### NIST Approved Secure Hashing Algorithms

[http://csrc.nist.gov/groups/ST/toolkit/secure\\_hashing.html](http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html)

#### Cryptographic Salting

[http://en.wikipedia.org/wiki/Salt\\_%28cryptography%29](http://en.wikipedia.org/wiki/Salt_%28cryptography%29)

#### Project Rainbow Crack

<http://www.antsight.com/zsl/rainbowcrack/>

### Instances

#### Possible Insecure Cryptographic Hash (SHA-0/SHA-1)

#### Best Practice

Location

ID 6319941 - <https://screendoor.dobt.co:443/>



## 6.4.4 Privacy Policy Not Present

## Best Practice

**None**

**OWASP Top 10: None**

**PCI 3.0: None**

### Summary

A privacy policy was not supplied by the web application within the scope of this audit. Many legislative initiatives require that organizations place a publicly accessible document within their web application that defines their website's privacy policy. As a general rule, these privacy policies must detail what information an organization collects, the purpose for collecting it, potential avenues of disclosure, and methods for addressing potential grievances.

Various laws governing privacy policies include the Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act (HIPAA), the California Online Privacy Protection Act of 2003, European Union's Data Protection Directive and others.

### Explanation

Most privacy laws are created to protect residents who are users of the website. Hence, organizations from any part of the world must adhere to these laws if they cater to customers residing in these geographical areas. Failing to do so could result in a lawsuit by the corresponding government against the organization.

### Execution

All of the web pages accessible within the scope of the scan are sampled for textual content that often constitutes a privacy policy statement. A violation is reported upon completion of the web application crawl without a successful match against any of the web pages.

Note that the privacy policy of your application could be located on another host or within a section of the site that was not configured as part of the scan. To validate, please try to access the privacy policy of your website and check to see if it was part of the scan.

### Recommendation

Declare a comprehensive privacy policy for the website, and ensure that it is accessible from every page that seeks personal information from users. To verify the fix, rescan the site in order to discover and audit the newly added resources.

#### Descriptions:

Any standard web application privacy policy should include the following components:

- A description of the intended purpose for collecting the data.
- A description of the use of the data.
- Methods for limiting the use and disclosure of the information.
- A list of the types of third parties to whom the information might be disclosed.
- Contact information for inquiries and complaints.

### References

#### California Online Privacy Protection Act

<http://oag.ca.gov/privacy/COPPA>

#### National Conference of State Legislation

<http://www.ncsl.org/issues-research/telecom/state-laws-related-to-internet-privacy.aspx>

#### Gramm-Leach-Bliley Act

<http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf>

#### Health Insurance Portability and Accountability Act of 1996

<https://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/downloads/HIPAALaw.pdf>

#### Health Insurance Portability and Accountability Act of 1996

[http://ec.europa.eu/justice/policies/privacy/docs/guide/guide-ukingdom\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/guide/guide-ukingdom_en.pdf)

# Instances

Privacy Policy Not Present

Best Practice

Location
ID 6319940 - <a href="https://screendoor.dobt.co:443/sign_in">https://screendoor.dobt.co:443/sign_in</a>

## 6.5.1 Hidden Form Value

## Info

None

OWASP Top 10: None

PCI 3.0: None

### Summary

While preventing display of information on the web page itself, the information submitted via hidden form fields is easily accessible, and could give an attacker valuable information that would prove helpful in escalating his attack methodology. Recommendations include not relying on hidden form fields as a security solution for any area of the web application that contains sensitive information or access to privileged functionality such as remote site administration functionality.

### Explanation

The greatest danger from exploitation of a hidden form field design vulnerability is that the attacker will gain information that will help in orchestrating a far more dangerous attack.

### Execution

Any attacker could bypass a hidden form field security solution by viewing the source code of that particular page.

### Recommendation

Do not rely on hidden form fields as a method of passing sensitive information or maintaining session state. One workable bypass is to encrypt the hidden values in a form, and then decrypt them when that information is to be utilized by a database operation or a script. From a security standpoint, the best method of temporarily storing information required by different forms is to utilize a session cookie.

Whether hidden or not, if your site utilizes values submitted via a form to construct database queries, do not make the assumption that the data is non-malicious. Instead, utilize the following recommendations to sanitize user supplied input.

- Stringently define the data type (for instance, a string, an alphanumeric character, etc) that the application will accept.
- Use what is good instead of what is bad.
- Validate input for improper characters.
- Do not display error messages to the end user that provide information (such as table names) that could be utilized in orchestrating an attack.
- Define the allowed set of characters. For instance, if a field is to receive a number, only let that field accept numbers.
- Define the maximum and minimum data lengths for what the application will accept.
- Specify acceptable numeric ranges for input.

### Instances

#### Hidden Form Value

#### Info

##### Location

ID 6319942 - <https://screendoor.dobt.co:443/account/settings>

## 6.5.2 Possible Authentication Misconfiguration (WWW-Authenticate)

Info

None

OWASP Top 10: None

PCI 3.0: None

### Summary

The web server sent a 401 "Authorization Required" status code with a response that did not contain a WWW-Authenticate HTTP header. This means the server is asking for authentication, but the browser is not prompting for authentication because of the missing WWW-Authenticate header. Recommendations include reviewing the web pages to determine if they should be protected via authentication, and correct the web server or application configuration to correct the problem by setting the 401 "Authorization Required" status code or by removing the WWW-Authenticate header.

### Explanation

To prompt for user authentication, a web server must send a 401 "Authorization Required" status code, along with a WWW-Authenticate HTTP header. This could mean portions of the web site are available that should require authentication, or this may simply be a misconfiguration at the application or web server level.

### Recommendation

#### For Security Operations:

Review the web pages to determine if they should be protected via authentication, and correct the web server or application configuration to correct the problem by sending a WWW-Authenticate header or by changing the 401 "Authorization Required" status code to a different status.

#### For Development:

Review the web pages to determine if they should be protected via authentication, and correct the web server or application configuration to correct the problem by sending a WWW-Authenticate header or by changing the 401 "Authorization Required" status code to a different status.

#### For QA:

Review the web pages to determine if they should be protected via authentication, and correct the web server or application configuration to correct the problem by sending a WWW-Authenticate header or by changing the 401 "Authorization Required" status code to a different status.

### References

#### RFC-2616

[Section 10.4.2: 401 Unauthorized](#)

[Section 14.47: WWW-Authenticate](#)

### Instances

#### Possible Authentication Misconfiguration (WWW-Authenticate)

Info

##### Location

ID 6319937 - [https://screendoor.dobt.co:443/dobt\\_hooks/session](https://screendoor.dobt.co:443/dobt_hooks/session)

# 6.5.3 Possible File Upload Capability

Info

None  
OWASP Top 10: None  
PCI 3.0: None

## Summary

An indicator of file upload capability was found. File upload capability allows a web user to send a file from his or her computer to the webserver. If the web application that receives the file does not carefully examine it for malicious content, an attacker may be able to use file uploads to execute arbitrary commands on the server. Recommendations include adopting a strict file upload policy that prevents malicious material from being uploaded via sanitization and filtering.

## Explanation

The exact implications depend upon the nature of the files an attacker would be able to upload. Implications range from unauthorized content publishing to aid in phishing attacks, all the way to full compromise of the web server.

## Recommendation

**For Security Operations:**  
This check is part of unknown application testing. Unknown application testing seeks to uncover new vulnerabilities in both custom and commercial software. Because of this, there are no specific patches or descriptions for this issue. If there is no apparent file upload capability on the page, this check may be safely ignored. You can instruct the scanner to ignore this vulnerability by right-clicking the vulnerability node on the displayed results tree and click "Ignore Vulnerability."

**For QA:**  
This issue will need to be resolved in the production code. Notify the appropriate developer of this issue.

**For Development:**  
Ensure that the following steps are taken to sanitize the file being received:

- Limit the types of files that can be uploaded. For instance, on an image upload page, any file other than a .jpg should be refused.
- Ensure that the web user has no control whatsoever over the name and location of the uploaded file on the server.
- Never use the name that the user assigns it.
- Never derive the filename from the web user's username or session ID.
- Do not place the file in a directory accessible by web users. It is preferable for this location to be outside of the webroot.
- Ensure that strict permissions are set on both the uploaded file and the directory it is located in.
- Do not allow execute permissions on uploaded files. If possible, deny all permission for all users but the web application user.
- Verify that the uploaded file contains appropriate content. For instance, an uploaded JPEG should have a standard JPEG file header.

## Instances

Possible File Upload Capability	Info
Location	
ID 6319946 - <a href="https://screendoor.dobt.co:443/hp-scan/12345/admin/imports/new">https://screendoor.dobt.co:443/hp-scan/12345/admin/imports/new</a>	

# Request and Response

Below is an enumeration of all dynamic issues with their request and response sections.

## 7.1.1 ID 6319938 - Weak SSL Protocol - TLS v1.0

High

https://screendoor.dobt.co:443/account/projects

### Request

```
GET /account/projects HTTP/1.1
Referer: https://screendoor.dobt.co/
Accept: */*
Accept-Encoding: gzip, deflate
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Host: screendoor.dobt.co
Connection: Keep-Alive
X-WIPP: AscVersion=10.40.323.10
X-Scan-Memo: Category="Crawl"; SID="EF265B3659ACBE5D86773BA424312004"; PSID="C7AF1EE59487CE1089CBF7B4154EF6BB";
SessionType="Crawl"; CrawlType="HTML"; AttackType="None"; OriginatingEngineID="00000000-0000-0000-0000-000000000000";
ThreadId="107"; ThreadType="CrawlBreadthFirstDBReader";
X-RequestManager-Memo: StateID="21"; sc="1"; ID="1122adfd-abd6-4233-be3b-2e676b130350";
X-Request-Memo: ID="bf0b5087-37f6-42df-8f0f-0f78d5934b02"; sc="1"; ThreadID="40";
Cookie: CustomCookie=WebInspect106897ZX235B8F34E2EC46F59AD23433063D90B6YD581;secure_reme
mber_token_production=M16Q_zy9Y-Qaz7Dyzt-z; screendoor_session=K252b2RGQm1OU3JOO
UppUmVQQVvYUEQxWctSUU1CeDgraGFSWEpVWlFb2RSMT0tJkt3eVdZWDFCTnI1NHZ0NGtGRDFVTCtEc
kV2b1FKQkRUaU81UDgzWTQ2Qm5YmNuWlJMS5S5c0YxRlBQTDJHRWt3a2VqY0ZXL3V4cW0vSlZTcUFZM
3lKQ2J65j1JSTNUWnBHQ0YyTl16OTZQOGNlc2VxenhhkRDQ5R2NlbXN6VWVhXalNoZlE0TFV0UDU1T0tBL
SlhZlFKMETuelY2UFdMMytWZndwWElnPT0%3D--044472f39a14467cb99b0b2db4950c6fad4cdbfa
```

### Response

```
HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
Content-Type: text/html; charset=utf-8
Date: Sat, 08 Aug 2015 04:33:36 GMT
ETag: W/"86cde519b77b90209785f1b447b85cbf"
Server: nginx + Phusion Passenger 5.0.10
Content-Length: 15454
Set-Cookie: _screendoor_session=VnVZNjllaTI2S1lMdmFXOHdwUi96Ti9RemdYa3U2WUd4TjRzTDVrdWU0Rmdz
cUpMSzBXRjIyY3VlU05Td3lnRGhnWkpKVGP2cDFrcUpNK3BGbE1QaG1MaFhQWStUS3FaWGF5dS9OYlZl
V2FUZDNUVXl5WUkvZ21GaStCdkpMc1pUjFZY3NtQ0s1NzR5aUdNamZBQ2dxbnJ3dXYlVXBjdG1BOFg5
OGxrZXJ5aGdQQWJpcUctEK2k4emViR3ZPN0ZBLSl0SnFZSzlzcVhXZGkzQkZCVUprBbGJBPT0%
3D--48421999c8bfcdccc6adfed91b8789a0386797b4; path=/; HttpOnly
Status: 200 OK
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Powered-By: Phusion Passenger Enterprise 5.0.10
X-Powered-By: cloud66
X-Request-Id: 2a26ba42-e482-4c3e-90a4-15cf714fa363
X-Runtime: 0.073504
X-XSS-Protection: 1; mode=block
Connection: keep-alive

<!doctype html><html><head>
<script type="text/javascript">window.NREUM||(NREUM={});NREUM.info={"beacon":"bam.
nr-data.net","errorBeacon":"bam.nr-data.net","licenseKey":"037a027bf3","applicat
ionID":"6297642","transactionName":"dwtcTBBcD1lQQU0EAVcLR1YWHBNdWlKHbHZH","queue
Time":0,"applicationTime":73,"agent":"js-agent.newrelic.com/nr-686.min.
js"}</script>
<script type="text/javascript">window.NREUM||(NREUM={}),(function(e,n,t){fun
ction r(t){if(!n[t]){var o=n[t]={};e[t][0].call(o.exports,function(n){var o=e[t][1][n];return
r(o,o,n)},o,o.exports)}return n[t].exports;if("function"==typeof __nr_require)return __nr_require;for(var
o=0;o<t.length;o++){r(t[o]);}return r}({QJf3ax:[function(e,n){function t(e){function
n(n,t,a){e&&(n,t,a),a||((a={})).for(var u=c(n),f=u.length,s=i(a,o,r),p=0;f>p;p++)u[p].apply(s,t);return s}function
a(e,n){f[e]=c(e).concat(n)}function c(e){return f[e]||[]}function u(){return t(n)}var
f={};return{on:a,emit:n,create:u,listeners:c,_events:f}}function r(){return{}}var
o="nr@context",i=e("gos");n.exports=t({}),{gos:"7eSDFh"}},ee:[function(e,n){n.
exports=e("QJf3ax")},{}],3:[function(e,n){function t(e){return function(){r(e,[(new
Date).getTime()].concat(i(arguments)))}}var r=e("handle"),o=e(1),i=e(2);"undefined"==typeof
window.newrelic&&(newrelic=window.NREUM);var
a=["setPageViewName","addPageAction","setCustomAttribute","finished","addTrace
","inlineHit","noticeError"];o(n,function(e,n){window.NREUM[n]=t("api-"+n)}),n.
exports=window.NREUM},{1:12,2:13,handle:"D5DuLP"}],gos:[function(e,n){n.
exports=e("7eSDFh")},{}],7eSDFh:[function(e,n,t){function t(e,n,t){if(r.call(e,n))return e[n];var
o=t();if(Object.defineProperty&&Object.keys)try{return
Object.defineProperty(e,n,{value:o,writable:!0,enumerable:!1}),o}catch(i){}retur
n e[n]=o,o}var r=Object.prototype.hasOwnProperty;n.exports=t},{}],D5DuLP:[function(e,n){functio
n t(e,n,t){return r.listeners(e).length?r.emit(e,n,t):void(r.q&&(r.q[e]||(r.q[e]=[]),r.q[e].
push(n)))}var r=e("ee").create();n.exports=t,t.ee=r,r.q={},{ee:"QJf3ax"}],handle:[function(e,
```

```

n){n.exports=e("D5DuLP"),{}},XL7HBI:[function(e,n){function t(e){var n=typeof
e;return!e||"object"!==n&&"function"!==n?-1:e===window?0:i(e,o,function(){return
r++})}var r=1,o="nr@id",i=e("qos");n.exports=t},{qos:"7eSDFh"},id:[function(e,n){n.
exports=e("XL7HBI")},{}],G9z0B1:[function(e,n){function t(){var
e=d.info+NRREUM.info,n=f.getElementsByTagName("script")[0];if(e&&e.licenseKey&
&e.applicationID&&n){c(p,function(n,t){n in e||e[n]=t});var
t="https"===s.split(":")[0]||e.sslForHttp;d.proto=t?"https://":"http://",a("mark
",[{"onload",i()}]);var r=f.createElement("script");r.src=d.proto+e.agent.n.parentNode.insertBefore(r,n)
}}function r(){"complete"===f.readyState&&o()}function o(){a("mark",[{"domContent",i()}])}function i(){return(new
Date).getTime()}var a=e("handle"),c=e(1),u=window,f=u.document;e(2);var
s=(""+location).split("?")[0],p={beacon:"bam.nr-data.net",errorBeacon:
"bam.nr-data.net",agent:"js-agent.newrelic.com/nr-686.min.js"},d=n.exports={offs
et:i(),origin:s,features:{}};f.addEventListener?(f.addEventListener("DOMContentL
oaded",o,!1),u.addEventListener("load",t,!1)):f.attachEvent("onreadystatechange
",r),u.attachEvent("onload",t),a("mark",[{"firstbyte",i()}]),{1:12,2:3,handle:
"D5DuLP"},loader:[function(e,n){n.exports=e("G9z0B1")},{}],12:[function(e,n){fu
nction t(e,n){var t=[],o="",i=0;for(o in e)r.call(e,o)&&(t[i]=n(o,e[o]),i+=1);return t}var
r=Object.prototype.hasOwnProperty,n.exports=t},{},13:[function(e,n){function t(e,n,t){n||(n=0),"undefined"===typeof
t&&(t=e.length);for(var r=-1,o=t-n||0,i=Array(0>o?0:o);++r<o;)i[r]=e[n+r];return
i}n.exports=t},{},{}],["G9z0B1"]];</script><title>Your projects - Screendoor</title><script>var App =
{"DEFAULT_LAT_LNG":["40.77,-73.98"],"user_id":"7670","is_dobt_admin":false,"js":
{"advanced_search":["/d3bt6306j428ad.cloudfront.net/assets/advanced_search-e09af
03ffb2dd9f4bab25d6116871425cc27d728a88e69d966a38eb9922031e3.js"],"at_mentions":
"/d3bt6306j428ad.cloudfront.net/assets/at_mentions-1d3e89344d3fb82c16dee141196e
0ed2c14392b69cccefe4a719348c33bad114.js"],"copy_to_clipboard":["/d3bt6306j428ad.
cloudfront.net/assets/copy_to_clipboard-8c44a5ffa4b6e7863c8120642ecc23ea7a041944
d31c59f146007065b70bb361.js"],"datetime_picker":["/d3bt6306j428ad.cloudfront.
net/assets/datetime_picker-1e19bd6377eeabe5dcfa4fdcf6a249c33495ad496a06264ee3c5b
91393cae78f.js"],"esignature":["/d3bt6306j428ad.cloudfront.net/assets/esignature-
3488cd05237a0a7a16bb62d5f08e23ea95c29025510eadc0d8c5f2755e64a273.js"],"form_build
er":["/d3bt6306j428ad.cloudfront.net/assets/form_builder-309a3be4961360272ceef6e
903ab6e247895f4ce9cc9baee9d9e851c9ed1df83.js"],"maps":["/d3bt6306j428ad.
cloudfront.net/assets/maps-61c1862ece8acd3f7d14037e3a059838bc58a21271d63edb19235
9aa41988149.js"],"wysiwyg":["/d3bt6306j428ad.cloudfront.net/assets/wysiwyg-4af684
3b7cd5e668bbdc22ef4fc3650f7cf5d294fc8d4532celdea8cc67aef16.js"],"import_wizard":
"/d3bt6306j428ad.cloudfront.net/assets/import_wizard-06affecb30f34bb68de14b432a
7b52e7f744a4eafda7a3f96e1030c9a328a3bc.js"}];</script><link rel="stylesheet" media="all"
href="/d3bt6306j428ad.cloudfront.net/assets/application-070a10a8796c0c29a8928c9
8d49b6232b657079f0f0892628d164a745ab18cd9.css" data-turbolinks-track="true" /><link rel="icon" type="image/png"
href="/apple-touch-icon-precomposed.png" /><script
src="//ajax.googleapis.com/ajax/libs/jquery/1.11.1/jquery.min.js"></script>
<script>window.jQuery || document.write('<script src="//non_digest_assets/jquery.js"><\script>')</script><script
src="//use.typekit.net/ckbldps.js"></script><script>try{Typekit.load();
}catch(e)}</script><script src="//d3bt6306j428ad.cloudfront.net/assets/application-939e20a6c4eb570799c55553
5c4351232f39ddf45c682f0c4068524b005fc50c.js" data-turbolinks-track="true"
crossorigin="anonymous"></script><script>App.assetsLoaded || alert('There was an error loading assets and Screendoor
might not function properly. Try disabling any ad-blocking software, or contact us at
support@dobt.co.');

```

[illegible]



## 7.2.1 ID 6319945 - SSL Cookie Not Used

Medium

https://screendoor.dobt.co:443/

### Request

```
GET / HTTP/1.1
Host: screendoor.dobt.co
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://dashboard.dobt.co/sign_in?app_id=5&payload=[%221658bcfe549e1aee203508719c89a0e2c7a22f27%22,%7B%22state%22:%7B%22redirect%22:%22https://screendoor.dobt.co/%22%7D%7D]
Pragma: no-cache
Cookie: ajs_user_id=null; ajs_group_id=null; ajs_anonymous_id=%226f7e1237-94e1-4772-aa4b-b84efe0ef3aa%22; mp_3bb656b8f64677ca9a920cdd2eeledd5_mixpanel=%7B%22distinct_id%22%3A%20%2214f0b9543d5127-05d595623bd9988-43514336-19b940-14f0b9543d6d6%22%2C%22%24initial_referrer%22%3A%20%22%24direct%22%2C%22%24initial_referring_domain%22%3A%20%22%24direct%22%7D; _ga=GAl.2.1413980223.1439008376; _gat=1; secure_remember_token_production=M16Q_zy9Y-Qaz7Dyzt-z; _screendoor_session=R0VVtmk2amZhaythOFMxOFJlbVV4ZDVVSWMzVkvXaXk1VG1wc2lZd3pEZEJyekxQeFE5bzdDNU10RGJlZWRYalVoK3JCVMjTa2NWN1FXblp1WlFBdHRmOU1vZDJ2QVpoNjlocHk2bGg2UVh0SXV3Q1c0WF1MaEc4VEJDT21TQTRKbUJkN0V3NGxwb2JwNDhVSFJ5SENXZVhtVVBQV29yYWJPTmxsMlR6Z28wPS0tQUgreE0wL2pDcXM3T2tVNEVGmKx4QT09--ea71185b0e7788d9f2b11cbbb99e3f7c19cf4ff6
Connection: keep-alive
X-WIPP: AscVersion=10.40.323.10
X-Scan-Memo: Category="Crawl.EventMacro.Startup"; SID="00000000000000000000000000000000"; SessionType="StartMacro"; CrawlType="None";
X-RequestManager-Memo: Category="EventMacro.Login"; MacroName="LoginMacro";
X-Request-Memo: ID="34f64119-4951-4a29-be9e-449b97677ead"; ThreadId="44";
```

### Response

```
HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
Content-Type: text/html; charset=utf-8
Date: Sat, 08 Aug 2015 04:32:59 GMT
ETag: W/"e4152bfdc9d49e000clea8f8fc4f5c8d"
Server: nginx + Phusion Passenger 5.0.10
Content-Length: 14187
Set-Cookie: _screendoor_session=eXdWc09ZV0dvSmNGaWFTRONNR3lGTnNadVVrd1pYaHJDcDFBckJSTHFJczdcRFNLRDlPU0hzCThvc1hsUGxmR2JZcWZSZSFVfVWVNUUdtOHVzSW04R0paYWQ5UDZNSmNSdjJNZERUWwdHYkdHSUZHNnFXNUVUVWxyT3VobzdGUHh3UWtJZkd4VlF4VmNsTXQwUHRqamxvY1pXRUFON3BYZy9lNXNOaEdkZms2Q1pTWU12QzZ4M3FjaEF5aU9peHBodko3VEVBcUtyc2F1YzhBd2huTk0TXh2UEpBQ1FveVgyZW8vYThpMGdNUlJ0L3pxSFhtWmJWcDF0bGF1WjVpcWM2a1ByT2RlPVxluYW1uS3pBWKVKNHc9PS0tMlJlTUVJlMFJONFNsZ2hGQmV5RGp4QT09--d99c8cc005df521b1d895116fc7032edf4c3a83f; path=/; HttpOnly
Status: 200 OK
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Powered-By: Phusion Passenger Enterprise 5.0.10
X-Powered-By: cloud66
```

## 7.3.1 ID 6319947 - Form Validation Disabled

Low

https://screendoor.dobt.co:443/account/settings

### Request

```
GET /account/settings HTTP/1.1
Referer: https://screendoor.dobt.co/
Accept: */*
Accept-Encoding: gzip, deflate
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Host: screendoor.dobt.co
Connection: Keep-Alive
X-WIPP: AscVersion=10.40.323.10
X-Scan-Memo: Category="Crawl"; SID="F956FCDD2C46A857E84B14F9A97849D5"; PSID="C7AF1EE59487CE1089CBF7B4154EF6BB";
SessionType="Crawl"; CrawlType="HTML"; AttackType="None"; OriginatingEngineID="00000000-0000-0000-0000-000000000000";
ThreadId="107"; ThreadType="CrawlBreadthFirstDBReader";
X-RequestManager-Memo: StateID="21"; sc="1"; ID="4db247cd-acc-4906-af06-8676d189b53f";
X-Request-Memo: ID="2af9a359-374a-4b9c-8a6b-4bc5959d39b5"; sc="1"; ThreadID="40";
Cookie: CustomCookie=WebInspect106897ZX235B8F34E2EC46F59AD23433063D90B6YD581;secure_reme
mber_token_production=M16Q_zy9Y-Qaz7Dyzt-z;_screendoor_session=aS9JWjdMYmlwVlp4b
XdxTU82QSSyMEpBdnNwRWVBZkdLbEl1MTVqNTQzV250L2dqamdT0FLYjVZbTIwTGhibmV2R0NEOEhsc
klQL3I5dFVDZncza2lX0svckowOElqTFpYRUg5NGxvZkQ5Q05GcGJGcGtsdDN6RG12dn11bDJRcUVaV
CtRdFd2MENnVk50TEhjenpxcFByaENGamJlM00zOEc2VUorSWk4SUh5SzRqK2hk22FJdnVjU1FYnJm1L
SlESkl1WFBJRURkOU00Ud3QvenNkMFRnPT0%3D--6d623486800c9f9c34927553f1f378848bff944a;
browserupdateorg=pause
```

### Response

```
HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
Content-Type: text/html; charset=utf-8
Date: Sat, 08 Aug 2015 04:33:48 GMT
ETag: W/"85a06ec8085817671730855760cbd692"
Server: nginx + Phusion Passenger 5.0.10
Content-Length: 16205
Set-Cookie: _screendoor_session=cHZEkeGJubWdLeVdKaW1sd2U1VEwzbUJiZFRJc0ppakpPY3BjbExvdxHNNYlNR
eWtCM2VXLONGRExdk45cldBUDY0eHkzWHpVcXJkMD1PRUJWcHVdWE8xMULZVTRFWXNTWXZuOG8zVDVC
Y3oxaTZzeXRWZHNWUjZHZUlpwklCS3liZUpTaH1EdTdHwkhleENETG9EbXdsdG9laUpYK0U5bWl6SEcy
cXoweHRYczVrcjhjN0xBalQrcEtoSPhpYTJxLSlWk5pRnhralBkOXhBYUNCMM0L05BPT0%
3D--59968d3337296e8446e335ce837deaa8bea9c05b; path=/; HttpOnly
Status: 200 OK
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Powered-By: Phusion Passenger Enterprise 5.0.10
X-Powered-By: cloud66
X-Request-Id: c00c2fd8-317d-4728-bda0-f971f1f88a55
X-Runtime: 0.085326
X-XSS-Protection: 1; mode=block
Connection: keep-alive

<!doctype html><html><head>
<script type="text/javascript">window.NREUM||(NREUM={});NREUM.info={"beacon":"bam.
nr-data.net","errorBeacon":"bam.nr-data.net","licenseKey":"037a027bf3","applicat
ionID":"6297642","transactionName":"dwtcTBBcD1lQUU0EAVcLR1YWHBBUQUcLCwVH","queue
Time":0,"applicationTime":76,"agent":"js-agent.newrelic.com/nr-686.min.
js"}</script>
<script type="text/javascript">window.NREUM||(NREUM={});__nr_require=function(e,n,t){fun
ction r(t){if(!n[t]){var o=n[t]={exports:{}};e[t][0].call(o.exports,function(n){var o=e[t][1][n];return
r(o?o:n)},o,o.exports)}return n[t].exports}if(["function"]==typeof __nr_require)return __nr_require;for(var
o=0;o<t.length;o++){r(t[o]);return r}({QJf3ax:[function(e,n){function t(e){function
n(n,t,a){e&&e(n,t,a),a||((a={}));for(var u=c(n),f=u.length,s=i(a,o,r),p=0;p<f;p++)u[p].apply(s,t);return s}function
a(e,n){f[e]=c(e).concat(n)}function c(e){return f[e]||[]}}function u(){return t(n)}var
f=[];return{on:a,emit:n,create:u,listeners:c,_events:f}}function r(){return{}}var
o="nr@context",i=e("gos");n.exports=t(),{gos:"7eSDFh"}},ee:[function(e,n){n.
exports=e("QJf3ax")},{}],3:[function(e,n){function t(e){return function(){r(e,[new
Date).getTime().concat(i(arguments))}}var r=e("handle"),o=e(1),i=e(2);"undefined"===typeof
window.newrelic&&(newrelic=window.NREUM);var
a=["setPageViewName","addPageAction","setCustomAttribute","finished","addToTrace
","inlineHit","noticeError"];o(a,function(e,n){window.NREUM[n]=t("api-"+n)}),n.
exports=window.NREUM},{1:12,2:13,handle:"D5DuLP"}],gos:[function(e,n){n.
exports=e("7eSDFh")},{}],7eSDFh:[function(e,n){function t(e,n,t){if(r.call(e,n))return e[n];var
o=t();if(Object.defineProperty&&Object.keys)try{return
Object.defineProperty(e,n,{value:o,writable:!0,enumerable:!1}),o}catch(i){return
n e[n]=o,o}var r=Object.prototype.hasOwnProperty;n.exports=t(),{}},D5DuLP:[function(e,n){functio
n t(e,n,t){return r.listeners(e).length?r.emit(e,n,t):void(r.q&&(r.q[e]||r.q[e]=[]),r.q[e].
push(n))}var r=e("ee").create();n.exports=t,t.tee=r,r.q={},ee:"QJf3ax"},handle:[function(e,
n){n.exports=e("D5DuLP")},{}],XL7HBI:[function(e,n){function t(e){var n=typeof
e;return!e||"object"!==n&&"function"!==n?-1:e===window?0:i(e,o,function){return
r++})}var r=1,o="nr@id",i=e("gos");n.exports=t(),{gos:"7eSDFh"},id:[function(e,n){n.
exports=e("XL7HBI")},{}],G9z0Bl:[function(e,n){function t(){var
e=d.info=NREUM.info,n=f.getElementsByTagName("script")[0];if(e&&e.licenseKey&
e.applicationID&&n){c(p,function(n,t){n in e||e[n]=t});var
t="https"===s.split(":")[0]||e.sslForHttp;d.proto=t?"https://":"http://",a("mark
",[["onload",i()]);var r=f.createElement("script");r.src=d.proto+e.agent,n.parentNode.insertBefore(r,n)
}}function r(){["complete"===f.readyState&&o]}function o(){a("mark",["domContentLoaded",i()])}function i(){return(new
```

```

Date).getTime())var a=e("handle"),c=e(1),u=window,f=u.document;e(2);var
s=(""+location).split("?")[0],p={beacon:"bam.nr-data.net",errorBeacon:
"bam.nr-data.net",agent:"js-agent.newrelic.com/nr-686.min.js"},d=n.exports={offs
et:i(),origin:s,features:{}};f.addEventListener((f.addEventListener("DOMContentL
oaded",o,!1),u.addEventListener("load",t,!1)):(f.attachEvent("onreadystatechange
",r),u.attachEvent("onload",t)),a("mark",["firstbyte",i()]),{1:12,2:3,handle:
"D5DuLP"}],loader:[function(e,n){n.exports=e("G9z0B1")},{},12:[function(e,n){fu
nction t(e,n){var t=[],o="",i=0;for(o in e)r.call(e,o)&&(t[i]=n(o,e[o]),i+=1);return t}var
r=Object.prototype.hasOwnProperty;n.exports=t},{},13:[function(e,n){function t(e,n,t){n||(n=0),"undefined"===typeof
t&&(t=e?e.length:0);for(var r=-1,o=t-n||0,i=Array(0>o?0:o);++r<o;)i[r]=e[n+r];return
i}n.exports=t},{},{}],["G9z0B1"]];</script><title>Notification settings - Screendoor</title><script>var App =
{"DEFAULT_LAT_LNG":{"40.77,-73.98"},"user_id":7670,"is_dobt_admin":false,"js":
{"advanced_search":"//d3bt6306j428ad.cloudfront.net/assets/advanced_search-e09af
03ffb2dd9f4bab25d6116871425cc27d728a88e69d966a38eb9922031e3.js","at_mentions":
"//d3bt6306j428ad.cloudfront.net/assets/at_mentions-1d3e89344d3fb82c16dee141196e
0ed2c14392b69cccefe4a719348c33bad114.js","copy_to_clipboard":"//d3bt6306j428ad.
cloudfront.net/assets/copy_to_clipboard-8c44a5ffa4b6e7863c8120642ecc23ea7a041944
d31c59f146007065b70bb361.js"},"datetime_picker":"//d3bt6306j428ad.cloudfront.
net/assets/datetime_picker-1e19bd6377eeabe5dcfa4fdcf6a249c33495ad496a06264ee3c5b
91393cae78f.js"},"signature":"//d3bt6306j428ad.cloudfront.net/assets/esignature-
3488cd05237a0a7a16bb62d5f08e23ea95c29025510eadc0d8c5f2755e64a273.js"},"form_build
er":"//d3bt6306j428ad.cloudfront.net/assets/form_builder-309a3be4961360272ceef6e
903ab6e247895f4ce9cc9baee9d9e851c9ed1df83.js"},"maps":"//d3bt6306j428ad.
cloudfront.net/assets/maps-61c1862ece8acd3f7d14037e3a059838bc58a21271d63edb19235
9aa41988149.js"},"wysiwyg":"//d3bt6306j428ad.cloudfront.net/assets/wysiwyg-4af684
3b7cd5e668bbdc22ef4fc3650f7cf5d294fc8d4532celdea8cc67aef16.js"},"import_wizard":
"//d3bt6306j428ad.cloudfront.net/assets/import_wizard-06affecb30f34bb68de14b432a
7b52e7f744a4eafda7a3f96e1030c9a328a3bc.js"}];</script><link rel="stylesheet" media="all"
href="//d3bt6306j428ad.cloudfront.net/assets/application-070a10a8796c0c29a8928c9
8d49b6232b657079f0f0892628d164a745ab18cd9.css" data-turbolinks-track="true" /><link rel="icon" type="image/png"
href="/apple-touch-icon-precomposed.png" /><script
src="//ajax.googleapis.com/ajax/libs/jquery/1.11.1/jquery.min.js"></script>
<script>window.jQuery || document.write('<script src="/non_digest_assets/jquery.js"></script>')</script><script
src="//use.typekit.net/ckblpds.js"></script><script>try{Typekit.load();
}catch(e){}</script><script src="//d3bt6306j428ad.cloudfront.net/assets/application-939e20a6c4eb570799c55553
5c4351232f39ddf45c682f0c4068524b005fc50c.js" data-turbolinks-track="true"
crossorigin="anonymous"></script><script>App.assetsLoaded || alert('There was an error loading assets and Screendoor
might not function properly. Try disabling any ad-blocking software, or contact us at
support@dobt.co.');

```

## 7.3.2 ID 6319939 - Missing HTTP Strict-Transport-Security Header

Low

https://screendoor.dobt.co:443/

### Request

```
GET / HTTP/1.1
Host: screendoor.dobt.co
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://dashboard.dobt.co/sign_in?app_id=5&payload=[%221658bcfe549e1aee203508719c89a0e2c7a22f27%22,%7B%22state%22:%7B%22redirect%22:%22https://screendoor.dobt.co/%22%7D%7D]
Pragma: no-cache
Cookie:ajs_user_id=null;ajs_group_id=null;ajs_anonymous_id=%226f7e1237-94e1-4772-aa4b-b84efe0ef3aa%22;mp_3bb656b8f64677ca9a920cdd2eeledd5_mixpanel=%7B%22distinct_id%22%3A%20%2214f0b9543d5127-05d595623bd9988-43514336-19b940-14f0b9543d6d6%22%2C%22%24initial_referrer%22%3A%20%22%24direct%22%2C%22%24initial_referring_domain%22%3A%20%22%24direct%22%7D;_ga=GAL.2.1413980223.1439008376;_gat=1;secure_remember_token_production=M16Q_zy9Y-Qaz7Dyzt-z;_screendoor_session=R0VVtmk2amZhaythOFMxOFJlBVV4ZDVVSWmzVkvXaXk1VG1wc2lZd3pEZEJyekxQeFE5bzdDNU10RGJlZWRYalVoK3JCVMjTa2NWN1FXblp1WlFBdHRmOU1vZDJ2QVpoNjlicHk2bGg2UVh0SXV3QlclOWFlMaEc4VEJDT2lTQTRKbUJkN0V3NGxbw2JwNDhVSFJ5SENxZVhtVVBQV29yYWJPTmxsMlR6Z28wPS0tQUGreE0wL2pDcXM3T2tVNEVGmKx4QT09--ea71185b0e7788d9f2b11cbbb99e3f7c19cf4ff6
Connection: keep-alive
X-WIPP: AscVersion=10.40.323.10
X-Scan-Memo: Category="Crawl.EventMacro.Startup"; SID="00000000000000000000000000000000"; SessionType="StartMacro"; CrawlType="None";
X-RequestManager-Memo: Category="EventMacro.Login"; MacroName="LoginMacro";
X-Request-Memo: ID="34f64119-4951-4a29-be9e-449b97677ead"; ThreadId="44";
```

### Response

```
HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
Content-Type: text/html; charset=utf-8
Date: Sat, 08 Aug 2015 04:32:59 GMT
ETag: W/"e4152bfcd9d49e000clea8f8fc4f5c8d"
Server: nginx + Phusion Passenger 5.0.10
Content-Length: 14187
Set-Cookie:_screendoor_session=eXdWc09ZV0dvSmNgawFTR0NNR3lGTnNadVVrdlpYaHJDcDFBckJSTHFJczd0RFNLRLDlPU0hZcThvc1hsUGxmR2JzcWZSZFVfVWVNUdOtOHVzSW04R0paYWQ5UDZSNsmSndjJNZERUWwdHYkdHSUZHNnFXNUVUVWxyT3VobzdGUHp3UWtJZkd4VlF4VmNsTXQwUHRqamxvYlpxRUFON3BYZy9lNXNQaEdkZms2QlplTWU12QzZAM3FjaEF5aU9peHB0dKo3VEVBcUtyc2F1YzhBd2huTkD0TXh2UEpBQ1FveVgyZW8vYThpMGdNULJ0L3pxSFhtWmJwCDF0bGFlWjVpcWMW2a1ByT2RVPXluYWl3pBwKVKNHc9PS0tM1JlTUJlMFJONFNzS2hGQmV5RGp4QT09--d99c8cc005df521b1d895116fc7032edf4c3a83f;
path=/; HttpOnly
Status: 200 OK
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Powered-By: Phusion Passenger Enterprise 5.0.10
X-Powered-By: cloud66
X-Request-Id: 74d75823-86c1-41b1-ad61-4159a7e40622
X-Runtime: 0.159650
X-XSS-Protection: 1; mode=block
Connection: keep-alive

<!doctype html><html><head>
<script type="text/javascript">window.NREUM||(NREUM={});NREUM.info={"beacon":"bam.nr-data.net","errorBeacon":"bam.nr-data.net","licenseKey":"037a027bf3","applicationID":"6297642","transactionName":"dwtcTBBcD1lQQU0NDVkBHVEMVwZJ","queueTime":0,"applicationTime":159,"agent":"js-agent.newrelic.com/nr-686.min.js"}</script>
<script type="text/javascript">window.NREUM||(NREUM={},__nr_require=function(e,n,t){function r(t){if(!n[t]){var o=n[t]={exports:{}};e[t][0].call(o.exports,function(n){var o=e[t][1][n];return r(o?o:n),o,o.exports)}return n[t].exports}if("function"!==typeof __nr_require)return __nr_require;for(var o=0;o<t.length;o++){return r(t[o]);return r}({QJf3ax:[function(e,n){function t(e){function n(n,t,a){e&&(n,t,a),a||((a={}));for(var u=c(n),f=u.length,s=i(a,o,r),p=0;p<f;p++)u[p].apply(s,t);return s}function a(e,n){f[e]=c(e).concat(n)}function c(e){return f[e]||[]}function u(i){return t(n)}var f={};return t(n);a,emit:n.create,u,listeners:c,_events:f}function r(t){return t}var o="nr@context",i=e("gos");n.exports=t(),{gos:"7eSDFh"},ee:[function(e,n){n.exports=e("QJf3ax")},{}],3:[function(e,n){function t(e){return function(){r(e,[new Date).getTime().concat(i(arguments))}}var r=e("handle"),o=e(1),i=e(2);"undefined"!==typeof window.newrelic&&(newrelic=window.NREUM);var a=["setPageViewName","addPageAction","setCustomAttribute","finished","addToTrace","inlineHit","noticeError"];o(a,function(e,n){window.NREUM[n]=t("api-"+n)}),n.exports=window.NREUM},{1:12,2:13,handle:"D5DuLP"}],gos:[function(e,n){n.exports=e("7eSDFh")},{}],"7eSDFh":[function(e,n){function t(e,n,t){if(r.call(e,n))return e[n];var o=t;if(Object.defineProperty(e,n,{value:o,writable:!0,enumerable:!1}),o.catch(i)){return n e[n]=o,o}var r=Object.prototype.hasOwnProperty,n.exports=t},{},D5DuLP:[function(e,n){function t(e,n,t){return r.listeners(e).length?r.emit(e,n,t):void(r.q&&(r.q[e]||r.q[e]=[]),r.q[e].push(n))}var r=e("ee").create();n.exports=t,t.rr=r,r.q={},ee:"QJf3ax"},handle:[function(e,n){n.exports=e("D5DuLP")},{}],XL7HBI:[function(e,n){function t(e){var n=typeof
```

```
e;return!e||"object"!==n&&"function"!==n?-1:e===window?0:i(e,o,function(){return
r++})}var r=1,o="nr@id",i=e("gos");n.exports=t},{gos:"7eSDFh"}],id:[function(e,n){n.
exports=e("XL7HBI")},{},G9z0B1:[function(e,n){function t(){var
e=d.info=NREUM.info,n=f.getElementsByTagName("script")[0];if(e&&e.licenseKey&
&e.applicationID&&n){c(p,function(n,t){n in e||(e[n]=t)});var
t="https"===s.split("://")[0]||e.sslForHttp;d.proto=t?"https://":"http://",a("mark
",[ "onload",i()]);var r=f.createElement("script");r.src=d.proto+e.agent,n.parentNode.insertBefore(r,n)
}function r(){ "complete"===f.readyState&&o()function o(){a("mark",[ "DOMContentLoaded",i()])}function i(){return(new
Date).getTime()}var a=e("handle"),c=e(1),u=window,f=u.document;e(2);var
s=(""+location).split("?")[0],p={beacon:"bam.nr-data.net",errorBeacon:
"bam.nr-data.net",agent:"js-agent.newrelic.com/nr-686.min.js"},d=n.exports={offs
et:i(),origin:s,features:{}};f.addEventListener?(f.addEventListener("DOMContentLoaded
loaded",o,!1),u.addEventListener("load",t,!1)):(f.attachEvent("onreadystatechange
",r),u.attachEvent("onload",t)),a("mark",[ "firstbyte",i()]),{1:12,2:3,handle:
"D5DuLP"}},loader:{function(e,n){n.exports=e("G9z0B1")},{},12:[function(e,n){fu
nction t(e,n){var t=[],o="",i=0;for(o in e)r.call(e,o)&&(t[i]=n(o,e[o]),i+=1);return t}var
r=Object.prototype.hasOwnProperty,n.exports=t},{},13:[function(e,n){function t(e,n,t){n||(n=0),"undefined"===typeof
t&&(t=e.p.length-1);for(var r=-1,o=t-1|0,i=Array(0>o?0:o);++r<o;)i[r]=e[n+r];return
i;n.exports=t},{},14:[function(e,n){n.exports=e("G9z0B1")}]</script><title>Screendoor</title><
script>var App = {"DEFAULT_LAT_LNG":{"40.77,-73.98"},"user_id":7670,"is_dobt_admin":false,"js":
{"advanced_search":"//d3bt6306j428ad.cloudfront.net/assets/advanced_search-e09af
03ffb2dd9f4bab25d6116871425cc27d728a88e69d966a38eb9922031e3.js"},"at_mentions":
"//d3bt6306j428ad.cloudfront.net/assets/at_mentions-1d3e89344d3fb82c16dee141196e
0ed2c14392b69cccefe4a719348c33bad114.js"},"copy_to_clipboard":"//d3bt6306j428ad.
cloudfront.net/assets/copy_to_clipboard-8c44a5ffa4b6e7863c8120642ecc23ea7a041944
d31c59f146007065b70bb361.js"},"datetime_picker":"//d3bt6306j428ad.cloudfront.
net/assets/datetime_picker-1e19bd6377eeabe5dcfa4fdcf6a249c33495ad496a06264ee3c5b
91393cae78f.js"},"signature":"//d3bt6306j428ad.cloudfront.net/assets/esignature-
3488cd05237a0a7a16bb62d5f08e23ea95c29025510eadc0d8c5f2755e64a273.js"},"form_bu
ilder":"//d3bt6306j428ad.cloudfront.net/assets/form_builder-309a3be4961360272ceef6e
903ab6e247895f4ce9cc9baee9d9e851c9ed1df83.js"},"maps":"//d3bt6306j428ad.
cloudfront.net/assets/maps-61c1862ece8acd3f7d14037e3a059838bc58a21271d63edb19235
9aa41988149.js"},"wysiwyg":"//d3bt6306j428ad.cloudfront.net/assets/wysiwyg-4af684
3b7cd5e668bbdc22ef4fc3650f7cf5d294fc8d4532celdea8cc67aef16.js"},"import_wizard":
"//d3bt6306j428ad.cloudfront.net/assets/import_wizard-06affecb30f34bb68d14b432a
7b52e7f744a4eafda7a3f96e1030c9a328a3bc.js"}];</script><link rel="stylesheet" media="all"
href="//d3bt6306j428ad.cloudfront.net/assets/application-070a10a8796c0c29a8928c9
8d49b6232b657079f0f0892628d164a745abl8cd9.css" data-turbolinks-track="true" /><link rel="icon" type="image/png"
href="/apple-touch-icon-precomposed.png" /><script
src="//ajax.googleapis.com/ajax/libs/jquery/1.11.1/jquery.min.js"></script>
<script>window.jQuery || document.write('<script src="/non_digest_assets/jquery.js"></script>')</script><script
src="//use.typekit.net/cckblpds.js"></script><script>try{Typekit.load();
}catch(e){}</script><script src="//d3bt6306j428ad.cloudfront.net/assets/application-939e20a6c4eb570799c55553
5c4351232f39ddf45c682f0c4068524b005fc50c.js" data-turbolinks-track="true"
crossorigin="anonymous"></script><script>App.assetsLoaded || alert("There was an error loading assets and Screendoor
might not function properly. Try disabling any ad-blocking software, or contact us at
support@dobt.co.");</script><script>!function(){var
analytics=window.analytics=window.analytics||[];if(!analytics.initialize)if(anal
ytics.invoked)window.console.error&&console.error("Segment snippet included
twice.");else{analytics.invoked=!0;analytics.methods=["trackSubmit","trackClick"
,"trackLink","trackForm","pageview","identify","group","track","ready","alias","
page","once","off","on"];analytics.factory=function(t){return function(){var
e=Array.prototype.slice.call(arguments);e.unshift(t);analytics.push(e);
return analytics}};for(var t=0;t<analytics.methods.length;t++){var
e=analytics.methods[t];analytics[e]=analytics.factory(e)}analytics.load=function
(t){var e=document.createElement("script");e.type="text/javascript";e.async=!0;
e.src=("https"===document.location.protocol?"https://":"http://")+cdn.
segment.com/analytics.js/v1/"+t+"/analytics.min.js";var
n=document.getElementsByTagName("script")[0];n.parentNode.insertBefore(e,n);
analytics.SNIPPET_VERSION="3.0.1";}}();</script><script>var $buoop = {}; $buoop.ol = window.onload;
window.onload=function(){ try {if ($buoop.ol) $buoop.ol();}catch (e) {} var e = document.createElement("script");
e.setAttribute("type", "text/javascript"); e.setAttribute("src", " //browser-update.org/update.js");
document.body.appendChild(e); }</script><script
src="//d2wy8f7a9ursnm.cloudfront.net/bugsnag-2.min.js"></script><script>
Bugsnag.apiKey = "09151347cb529da47dfbb0998088d790"; Bugsnag.user = { id: 8893 }; Bugsnag.releaseStage =
"production";</script><meta name="viewport" content="width=device-width, initial-scale=1.0" /><meta name="csrf-param"
content="authenticity_token" />
<meta name="csrf-token" content="XktPao2CsBPCBPct4OuBlcVndGx5RhkzwlUR9OeZWcrB2hAOW4HxIZz4NnRNSEhK7XQwPN
d38haWREr5JFVtQ==" /><!--[if lt IE 9]><script src="//d2yxxgjkbbvnhdt.cloudfront.net/dist/shim.js"></script><![endif]>-->
</head><body class="home-index" data-page-key="home-index"><a class="visuallyhidden focusable" id="skip"
href="#start_of_content">Skip to content</a><header class="banner"><nav class="navbar navbar_sticky"><div
class="container"><div class="navbar_header"><a class="navbar_brand" href="/" data-no-turbolink></a><a class="navbar_toggle"><i class="fa fa-reorder"></i></a></div><div
class="navbar_content_wrapper"><div class="navbar_content navbar_content_primary"><ul><li><a href="/"
data-no-turbolink><i class="fa fa-home"></i> Home</a></li><li><a href="/hp-scan"><i class="fa fa-building-o"></i>
Your organization</a></li></ul></div><div class="navbar_content navbar_content_secondary"><ul><li class="dropdown
dropdown_navbar js_nav_search_dropdown"><a class="js_nav_search_btn" title="Search" href="#"><span
class="navbar_full_i"><i class="fa fa-search navbar_icon"></i></span><span
class="navbar_collapsed_i">Search</span></a><div class="navbar_search_form js_nav_search_form" style="display:
none;"><input class="js_nav_search_input" type="text" placeholder="Search" /></div><div class="dropdown_menu
js_nav_search_loading"><ul class="dropdown_body"><li class="dropdown_loading js_help_dropdown_target"><span><i
class="fa fa-refresh fa-spin"></i></span></li></ul></div><li class="dropdown_dropdown_navbar"><a
data-toggle="dropdown" title="Help" class="js-help-dropdown" href="#"><span class="navbar_full_i"><i class="fa
fa-question-circle navbar_icon"></i></span><span class="navbar_collapsed_i">Help</span></a><div class="dropdown_menu"
role="menu"><h3>Help</h3><ul class="dropdown_body"><li class="dropdown_loading js_help_dropdown_target"><span><i
class="fa fa-refresh fa-spin"></i></span></li><li class="divider"></li><li><a href="mailto:support@dobt.co"><span
class="fa fa-envelope"></i></span></li></ul></div><div class="dropdown_dropdown_navbar"><a href="#"
data-toggle="dropdown" data-partial-href="/notifications/dropdown"
data-partial-replace="#notificationsDropdownContent" title="Notifications" class="js-notification-dropdown"><span
```

```
<class="navbar_full_i"><i class="fa fa-bolt navbar_icon"></i></span><span  
class="navbar_collapsed_i">Notifications</span><script type='text/javascript'  
data-sync-id='8c7427abdf14ea4580ada3f717df7fe58bf25d6-start'> Sync.onReady(function(){ var partial = new  
Sync.Partial({ name: 'unread_notification_badge', resourceName: 'user', resourceId: '7670', authToken:  
'8c7427abdf14ea4580ada3f717df7fe58bf25d6', channelUpdate: '8c7427abdf14ea4580ada3f717df7fe58bf25d6-update',  
channelDestroy: '8c7427abdf14ea4580ada3f717df7fe58bf25d6-destroy', selectorStart:  
'8c7427abdf14ea4580ada3f717df7fe58bf25d6-start', selectorEnd: '8c7427abdf14ea4580ada3f717df7fe58bf25d6-end',  
refresh: false }); partial.subscribe(); }); </script><script type='text/javascript'  
data-sync-id='8c7427abdf14ea4580ada3f717df7fe58bf25d6-end'> </script></a><div class="dropdown_menu"  
role="menu"><h3>Notifications</h3><ul class="dropdown_body" id="notificationsDropdownContent"><li  
class="dropdown_loading"><span><i class="fa fa-refresh fa-spin"></i></span></li></ul></div></li><li class="dropdown  
dropdown_navbar"><a class="js_projects_nav_dropdown" data-toggle="dropdown" data-partial-href="/projects/dropdown"  
data-partial-replace="#projectsDropdownContent" title="Projects" href="#"><span class="navbar_full_i"><i class="fa  
fa-file-text navbar_icon"></i></span><span class="navbar_collapsed_i">Projects</span></a><div class="dropdown_menu"  
role="menu"><h3>Projects</h3><ul class="dropdown_body"><li class="dropdown_loading"  
id="projectsDropdownContent"><span><i class="fa fa-refresh fa-spin"></i></span></li><li class="divider"></li><li><a  
class="drop_sng" href="/projects/new">New </a></li><li class="divider"></li><li class="all"><a  
href="/account/projects"><span class="dropdown_navbar">All </span></li><li></li><li><div class="dropdown  
dropdown_navbar"><a data-toggle="dropdown" title="You" href="#"></a><div class="dropdown_menu" role="menu"><h3>HP  
Scan</h3><ul class="dropdown_body"><li><a href="/account/settings">Your settings</li><li><a  
href="/settings/api_keys">Organization settings</li><li class="divider"></li><li><a  
href="https://dashboard.dobt.co/account/app_id=5&payload={%221658bcfe549elae  
e203508719c89a0e2c7a22f27%22,%7B%22state%22:%7B%22redirect%22:%22https:  
//screenoor.dobt.co/%22%7D%7D}>Your account</a></li><li><a  
href="https://dashboard.dobt.co/sign_out?app_id=5&payload={%221658bcfe549ela  
ee203508719c89a0e2c7a22f27%22,%7B%22state%22:%7B%22redirect%22:%22https:  
//screenoor.dobt.co/%22%7D%7D}" data-method="delete">Sign  
out</a></li></ul></div></li></ul></div></div></div></div></div></div><div id="start_of_content"></div><div  
class="container container_single" id="main"><div class="page_header"><h2>Welcome, HP Scan!</h2></div><div  
class="grid"><div class="item"><div class="margin_bd"><div class="blank_slate"><i class="fa fa-file-text  
></i></div><h4>You don't have any projects</h4><a class="button primary" href="/projects/new">Create your first  
project</a></div></div></div></div></div></div></div></div></div></div></div><div class="footer_inner"><span>Screendoor is an  
application by <a href='http://www.dobt.co' target='_blank'>The Department of Better Technology</a>.</span><ul><li><a  
href="http://status.dobt.co" target="_blank">Service Status</a></li><li><a href="https://dashboard.dobt.co/terms"  
target="_blank">Legal</a></li><li><a href="http://help.dobt.co" target="_blank">Get Help</a></li><li><a  
href="mailto:support@dobt.co">Contact Us</a></li></ul></div></div></div><!--[if lt IE 9]><script  
src="//d2yxxgjkbbvnhd.cloudfront.net/dist/polyfills.js"></script><!endif-->  
<script src="https://d3dy5mtp8yhk7.cloudfront.net/2.2/pusher.min.js"  
data-turbolinks-eval=false"></script><script>analytics.page().analytics.  
alias("8893");</script></body></html>
```

**Low**

Request

Response

This report contains HP CONFIDENTIAL information, including but not limited to HP's analysis, techniques for analysis and recommendations. This report may not be made public, used for competitive or consulting purposes or used outside of the recipient.

### 7.3.4 ID 6319943 - Set-Cookie does not use HTTPOnly Keyword

Low

https://screendoor.dobt.co:443/hp-scan/12345/admin/collaborators?direction=asc  
&sort=user\_name

#### Request

```
GET /hp-scan/12345/admin/collaborators?direction=asc&sort=user_name HTTP/1.1
Referer: https://screendoor.dobt.co/hp-scan/12345/admin/collaborators?direction=asc&
sort=user_name
Host: screendoor.dobt.co
Accept: text/html, application/xhtml+xml, application/xml
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-XHR-Referer: https://screendoor.dobt.co/hp-scan/12345/admin/collaborators?direction=asc&
sort=user_name
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Connection: Keep-Alive
X-WIPP: AscVersion=10.40.323.10
X-Scan-Memo: Category="Crawl"; SID="CEE3494723589C4B91C3C1840F39BE63"; PSID="B67E8C8B9A1E2B0DD794DDF850E50E33";
SessionType="Crawl"; CrawlType="AJAXInclude"; AttackType="None";
OriginatingEngineID="00000000-0000-0000-0000-000000000000"; ThreadId="185"; ThreadType="JScriptEvent";
X-RequestManager-Memo: StateID="41"; sc="1"; ID="09bd4ed1-34be-454c-a175-dae0bd97d9ad";
X-Request-Memo: ID="82471973-48c1-48d8-8fe0-7bd1943598ae"; sc="1"; ThreadId="185";
Cookie: CustomCookie=WebInspect106897ZX235B8F34E2EC46F59AD23433063D90B6YD581;secure_reme
mber_token_production=M16Q_zy9Y-Qaz7Dyzt-z; screendoor_session=cHBVdVVGbTVCSUI4K
01NZklPS3cwRmthQXpucWVBNE9qOHWNWkdPNHlxR0JhOWQyQmRLQWRITURlUWE1Rk1PVWVmNXJPTnpIa
EJISFBVTFWURXyWVWNieUJiUWM4SWJQUlJ5YXVhUGVHk3QxRGtLWXlBMloyaHdDOFJJYN2o3dVREVW55a
DM0ZU9UdFZqK2c4ZUFjbG5yaVVQeHhrendpVY3pqBTBUN3YwVE8vM05nNU5QV04valpWYmloL3IvVm9PL
S1lMzdFeFpHRjlmekpxOTk2a20yeVVBPT0%3D--b9cc4b2eb3049c658dfe3aba6d706bc3091f4052;
browserupdateorg=pause;request_method=POST
```

#### Response

```
HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
Content-Type: text/html; charset=utf-8
Date: Sat, 08 Aug 2015 04:42:19 GMT
ETag: W/"7090539fe4eba60edc2acd96d7c18f32"
Server: nginx + Phusion Passenger 5.0.10
Content-Length: 30272
Set-Cookie: _screendoor_session=ZmxoR2RCR3ZsYldhM1VuNHZ6d2lhSWwvTTBDbVJHVlgyUUxkUmw4cG8rQXB0
eFFlejQ4UC9PZlVUeVV6eVZhZUFjbWhrcTlzQS9vcWhyVzFCM1lEWWVHQTlGbXBObk1VaWdORzVscEdp
Ylp1NElDZkslalF2MlJjbzRkNU9SK1Jwa3RldXBocENTallvRHRZSnRXbzc5R1VhZWg5ZDdlVGNzRGx5
OW9nVExrZDNaRjJoU2lBZlQ0SVBTOFR4RDY5LS15b1BTK0lPUzUwOEdkRnc1OGVyaEt3PT0%
3D--2f832b49170012646b01cb9efd3b99cf4f15bced; path=/; HttpOnly
Set-Cookie: request_method=; path=/; max-age=0; expires=Thu, 01 Jan 1970 00:00:00 -0000
Status: 200 OK
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Powered-By: Phusion Passenger Enterprise 5.0.10
X-Powered-By: cloud66
```



## 7.4.1 ID 6319944 - Form Auto Complete Active

## Best Practice

https://screendoor.dobt.co:443/account/projects

### Request

```
GET /account/projects HTTP/1.1
Referer: https://screendoor.dobt.co/
Accept: */*
Accept-Encoding: gzip, deflate
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Host: screendoor.dobt.co
Connection: Keep-Alive
X-WIPP: AscVersion=10.40.323.10
X-Scan-Memo: Category="Crawl"; SID="EF265B3659ACBE5D86773BA424312004"; PSID="C7AF1EE59487CE1089CBF7B4154EF6BB";
SessionType="Crawl"; CrawlType="HTML"; AttackType="None"; OriginatingEngineID="00000000-0000-0000-0000-000000000000";
ThreadId="107"; ThreadType="CrawlBreadthFirstDBReader";
X-RequestManager-Memo: StateID="21"; sc="1"; ID="1122adfd-abd6-4233-be3b-2e676b130350";
X-Request-Memo: ID="bf0b5087-37f6-42df-8f0f-0f78d5934b02"; sc="1"; ThreadID="40";
Cookie: CustomCookie=WebInspect106897ZX235B8F34E2EC46F59AD23433063D90B6YD581;secure_reme
mber_token_production=M16Q_zy9Y-Qaz7Dyzt-z;_screendoor_session=K252b2RGQm1OU3JOO
UppUmVQQVvYUEQxWctSUULCeDgraGFSWExPVWlFb2RSM0tJTk3eVdZWDFCTnI1NHZONGtGRDFVTCtEc
kV2b1FKQkRUAu81UDgzWTQ2Qm5YmNmUw1JMSs5c0YxRlBQTDJHRWt3a2VqY0ZXL3V4cW0vSlZTcUFZM
3lKQ2J6Qj1JSTNUWnBHQ0YyTl16OTZQOGNlc2VxenhhkRDQ5R2NlbXN6VWVhXa1NoZlE0TFV0UDU1T0tBL
SlhZlFKMETue1Y2UFdMMYtWZndwWElnPT0%3D--044472f39a14467cb99b0b2db4950c6fad4cdbfa
```

### Response

```
HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
Content-Type: text/html; charset=utf-8
Date: Sat, 08 Aug 2015 04:33:36 GMT
ETag: W/"86cde519b77b90209785f1b447b85cbf"
Server: nginx + Phusion Passenger 5.0.10
Content-Length: 15454
Set-Cookie: _screendoor_session=VnVZnj1laTI2S1lMdmFXOHdwUi96T9RemdYa3U2WUD4TjRzTDVrdWU0Rmdz
cUpMSzBXRjIyY3V1U05Td3lnRGhnWkpKVGP2cDFrcUpNK3BGBE1QaG1MaFhQWStUS3FaWGF5dS9OYlZH
V2FUZDNUVXl5WUkvZ2lGaStCdkpMc1pUjFZY3NtQ0s1NzR5aUdNamZBQ2dxbnJ3dXYlVXBjJdG1BOFG5
OGxrZXJ5aGdQQWJpcUtEK2k4emVir3ZPN0ZBLSloSnFZS3licVhXZGkzQkZCVUpRbGJBPT0%
3D--48421999c8bfcdccc6adfed91b8789a0386797b4; path=/; HttpOnly
Status: 200 OK
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Powered-By: Phusion Passenger Enterprise 5.0.10
X-Powered-By: cloud66
X-Request-Id: 2a26ba42-e482-4c3e-90a4-15cf714fa363
X-Runtime: 0.073504
X-XSS-Protection: 1; mode=block
Connection: keep-alive

<!doctype html><html><head>
<script type="text/javascript">window.NREUM||(NREUM={});NREUM.info={"beacon":"bam.
nr-data.net","errorBeacon":"bam.nr-data.net","licenseKey":"037a027bf3","applicat
ionID":"6297642","transactionName":"dwctTBBcD1lQQU0EAVcLRlYWHBNDWlkHBhZH","queue
Time":0,"applicationTime":73,"agent":"js-agent.newrelic.com/nr-686.min.
js"}</script>
<script type="text/javascript">window.NREUM||(NREUM={}),__nr_require=function(e,n,t){fun
ction r(t){if(!n[t]){var o=n[t]={exports:{}};e[t][0].call(o.exports,function(n){var o=e[t][1][n];return
r(o?o:n)},o,o.exports)}return n[t].exports}if("function"==typeof __nr_require)return __nr_require;for(var
o=0;o<t.length;o++){r(t[o]);return r}({QJf3ax:[function(e,n){function t(e){function
n(n,t,a){e&&e(n,t,a),a||((a={});for(var u=c(n),f=u.length,s=i(a,o,r),p=0;p<f;p++)u[p].apply(s,t);return s}function
a(e,n){f[e]=c(e).concat(n)}function c(e){return f[e]||[]}function u(){return t(n)}var
f=[];return{on:a,emit:n,create:u,listeners:c,_events:f}}function r(){return{}}var
o="nr@context",i=e("gos");n.exports=t({},{gos:"7eSDFh"}),ee:[function(e,n){n.
exports=e("QJf3ax")},{},3:[function(e,n){function t(e){return function(){r(e,[new
Date).getTime().concat(i(arguments))}}var r=e("handle"),o=e(1),i=e(2);"undefined"==typeof
window.newrelic&&(newrelic=window.NREUM);var
a=["setPageViewName","addPageAction","setCustomAttribute","finished","addToTrace
","inlineHit","noticeError"];o(a,function(e,n){window.NREUM[n]=t("api-"+n)}),n.
exports=window.NREUM},{1:12,2:13,handle:"D5DuLP"}],gos:[function(e,n){n.
exports=e("7eSDFh")},{},7eSDFh:[function(e,n){function t(e,n,t){if(r.call(e,n))return e[n];var
o=t();if(Object.defineProperty&&Object.keys)try{return
Object.defineProperty(e,n,{value:o,writable:!0,enumerable:!1}),o}catch(i){return
n[e]=o}var r=Object.prototype.hasOwnProperty;n.exports=t},{},D5DuLP:[function(e,n){functio
n t(e,n,t){return r.listeners(e).length?r.emit(e,n,t):void(r.q&&(r.q[e]||r.q[e]=[]),r.q[e].
push(n))}var r=e("ee").create();n.exports=t,t.ee=r,r.q={},{ee:"QJf3ax"}],handle:[function(e,
n){n.exports=e("D5DuLP")},{},XL7HBI:[function(e,n){function t(e){var n=typeof
e;return!e||"object"!=n&&"function"!=n?-1:e===window?0:i(e,o,function(){return
r+1})}var r=1,o="nr@id",i=e("gos");n.exports=t},{gos:"7eSDFh"}],id:[function(e,n){n.
exports=e("XL7HBI")},{},G9z0B1:[function(e,n){function t(){var
e=d.info=NREUM.info,n=f.getElementsByTagName("script")[0];if(e&&e.licenseKey&
&e.applicationID&&n){c(p,function(n,t){n in e||e[n]=t)};var
t="https"==s.split("://")[0]||e.sslForHttp;d.proto=t?"https://":"http://",a("mark
","onload",i());var r=f.createElement("script");r.src=d.proto+e.agent.n.parentNode.insertBefore(r,n)
}}function r(){"complete"===f.readyState&&o()}function o(){a("mark",["domContentLoaded",i()])}function i(){return(new
Date).getTime()}var a=e("handle"),c=e(1),u=window,f=u.document;e(2);var
```

```

s=("+location).split("?")[0],p={beacon:"bam.nr-data.net",errorBeacon:
"bam.nr-data.net",agent:"js-agent.newrelic.com/nr-686.min.js"},d=n.exports={offs
et:i(),origin:s,features:{}};f.addEventListener(f.addEventListener("DOMContentL
oaded",o,!1),u.addEventListener("load",t,!1)):f.attachEvent("onreadystatechange
",r),u.attachEvent("onload",t)),a("mark",[{"firstbyte",i()}]),{1:12,2:3,handle:
"D5DuLP"}},loader:{function(e,n){n.exports=e("G9z0Bl")}},{}},12:[function(e,n){fu
nction t(e,n){var t=[],o="",i=0;for(o in e)r.call(e,o)&&(t[i]=n(o,e[o]),i+=1);return t}var
r=Object.prototype.hasOwnProperty;n.exports=t},{}},13:[function(e,n){function t(e,n,t){n||(n=0),"undefined"===typeof
t&&(t=e.length);for(var r=-1,o=t-1|0,i=Array(0>o?0:o);++r<o;)i[r]=e[n+r];return
i}n.exports=t},{}},{},"G9z0Bl"])/</script><title>Your projects - Screendoor</title><script>var App =
{"DEFAULT_LAT_LNG":[40.77,-73.98],"user_id":7670,"is_dobt_admin":false,"js":
{"advanced_search":"//d3bt6306j428ad.cloudfront.net/assets/advanced_search-e09af
03ffb2dd9f4bab25d6116871425cc27d728a88e69d966a38eb9922031e3.js","at_mentions":
"/d3bt6306j428ad.cloudfront.net/assets/at_mentions-1d3e89344d3fb82c16dee141196e
0ed2c14392b69cccefe4a719348c33bad114.js","copy_to_clipboard":"//d3bt6306j428ad.
cloudfront.net/assets/copy_to_clipboard-8c44a5ffa4b6e7863c8120642ecc23ea7a041944
d31c59f146007065b70bb361.js","datetime_picker":"//d3bt6306j428ad.cloudfront.
net/assets/datetime_picker-1e19bd6377eeabe5dcfa4fdcf6a249c33495ad496a06264ee3c5b
91393cae78f.js","esignature":"//d3bt6306j428ad.cloudfront.net/assets/esignature-
3488cd05237a0a7a16bb62d5f08e23ea95c29025510eadc0d8c5f2755e64a273.js","form_build
er":"//d3bt6306j428ad.cloudfront.net/assets/form_builder-309a3be4961360272ceef6e
903ab6e247895f4ce9cc9baee9d9e851c9ed1df83.js","maps":"//d3bt6306j428ad.
cloudfront.net/assets/maps-61c1862ece8acd3f7d14037e3a059838bc58a21271d63edb19235
9aa41988149.js","wysiwyg":"//d3bt6306j428ad.cloudfront.net/assets/wysiwyg-4af684
3b7cd5e668bbdc22ef4fc3650f7cf5d294fc8d4532celdea8cc67aef16.js","import_wizard":
"/d3bt6306j428ad.cloudfront.net/assets/import_wizard-06affecb30f34bb68del4b432a
7b52e7f744a4eafda7a3f96e1030c9a328a3bc.js"};"/</script><link rel="stylesheet" media="all"
href="//d3bt6306j428ad.cloudfront.net/assets/application-070a10a8796c0c29a8928c9
8d49b6232b657079f0f0892628d164a745abl8cd9.css" data-turbolinks-track="true" /><link rel="icon" type="image/png"
href="//apple-touch-icon-precomposed.png" /><script
src="//ajax.googleapis.com/ajax/libs/jquery/1.11.1/jquery.min.js"></script>
<script>window.jQuery || document.write('<script src="//non_digest_assets/jquery.js"></script>')</script><script
src="//use.typekit.net/ckbldps.js"></script><script>try{Typekit.load();
}catch(e){}</script><script src="//d3bt6306j428ad.cloudfront.net/assets/application-939e20a6c4eb570799c55553
5c4351232f39ddf45c682f0c4068524b005fc50c.js" data-turbolinks-track="true"
crossorigin="anonymous"></script><script>App.assetsLoaded || alert('There was an error loading assets and Screendoor
might not function properly. Try disabling any ad-blocking software, or contact us at
support@dobt.co.');

```

## 7.4.2 ID 6319948 - Possible Insecure Cryptographic Hash (MD Family)

Best Practice

https://screendoor.dobt.co:443/

### Request

```
GET / HTTP/1.1
Host: screendoor.dobt.co
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://dashboard.dobt.co/sign_in?app_id=5&payload=[%221658bcfe549e1aee203508719c89a0e2c7a22f27%22,%7B%22state%22:%7B%22redirect%22:%22https://screendoor.dobt.co/%22%7D%7D]
Pragma: no-cache
Cookie:ajs_user_id=null;ajs_group_id=null;ajs_anonymous_id=%226f7e1237-94e1-4772-aa4b-b84efe0ef3aa%22;mp_3bb656b8f64677ca9a920cdd2ee1edd5_mixpanel=%7B%22distinct_id%22%3A%20%2214f0b9543d5127-05d595623bd9988-43514336-19b940-14f0b9543d6d6%22%2C%22%24initial_referrer%22%3A%20%22%24direct%22%2C%22%24initial_referring_domain%22%3A%20%22%24direct%22%7D;_ga=GAL.2.1413980223.1439008376;_gat=1;secure_remember_token_production=M16Q_zy9Y-Qaz7Dyzt-z;_screendoor_session=R0VVtMk2amZhaythOFMxOFJlbVV4ZDVVSWMzVkvXaXk1VG1wc2l2d3pEZEJyekxQeFE5bzdDNu1ORGJ1ZWRYalVoK3JCvMjTa2NWN1FXblp1WlFBdHRmOU1vZDJ2QVpONjlocHk2bGg2UVhOSXV3Qlc0WF1MaEc4VEJDT21TQTRkbUJkN0V3NGxbw2JwNDhVSFJ5SENxZVhtVVBQV29yYWJPTmxsMlR6Z28wPS0tQUgreE0wL2pDcXM3T2tVNEVGMkx4QT09--ea71185b0e7788d9f2b11cbbb99e3f7c19cf4ff6
Connection: keep-alive
X-WIPP: AscVersion=10.40.323.10
X-Scan-Memo: Category="Crawl.EventMacro.Startup"; SID="00000000000000000000000000000000"; SessionType="StartMacro"; CrawlType="None";
X-RequestManager-Memo: Category="EventMacro.Login"; MacroName="LoginMacro";
X-Request-Memo: ID="34f64119-4951-4a29-be9e-449b97677ead"; ThreadId="44";
```

### Response

```
HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
Content-Type: text/html; charset=utf-8
Date: Sat, 08 Aug 2015 04:32:59 GMT
ETag: W/"e4152bfdc9d49e000c1ea8f8fc4f5c8d"
Server: nginx + Phusion Passenger 5.0.10
Content-Length: 14187
Set-Cookie: _screendoor_session=eXdwC09ZV0dvSmNGaWFR0NNR3lGTnNadVVrdlpYahJdCkDFBckJSTHFJczdORFNLRLDlPU0hZcThvclhsUGxmR2JZcWZSZFVFWVNUUdtOHVzSW04R0paYWQ5UDZNSmNSdjJNZERUWwdHYkdHSUZHNnFXNUVUVWYxT3VobzdGUHp3UWtJZkd4VlF4VmNsTXQwUHRqamxvY1pXRUFON3BYZy9lNXNQaEdkZms2QlpTWU12QzZ4M3FjaEF5aU9peHB0dKo3VEVBcUtyc2F1YzhBd2huTk0TXh2UEpBQlFveVgyZW8yYThpMGdNUlJ0L3pxSFhtWmJWcDF0bGFFWjVpcWM2a1ByT2RVPVx1uYW1uS3pBwkVKNhc9PS0tMlJlTUJlMFJONFNsZ2hGQmVSRGp4QT09--d99c8cc005df521b1d895116fc7032edf4c3a83f; path=/; HttpOnly
Status: 200 OK
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Powered-By: Phusion Passenger Enterprise 5.0.10
X-Powered-By: cloud66
X-Request-Id: 74d75823-86c1-41b1-ad61-4159a7e40622
X-Runtime: 0.159650
X-XSS-Protection: 1; mode=block
Connection: keep-alive

<!doctype html><html><head>
<script type="text/javascript">window.NREUM||(NREUM={});NREUM.info={"beacon":"bam.nr-data.net","errorBeacon":"bam.nr-data.net","licenseKey":"037a027bf3","applicationID":"6297642","transactionName":"dwtcTBBcD1lQUU0NDVkBHVEMVwZJ","queueTime":0,"applicationTime":159,"agent":"js-agent.newrelic.com/nr-686.min.js"}</script>
<script type="text/javascript">window.NREUM||(NREUM={}),(function(){function t(e,n,t){function r(t){if(!n[t]){var o=n[t]={exports:{}};e[t][0].call(o.exports,function(n){var o=e[t][1][n];return r(o?o:n),o,o.exports)}return n[t].exports}if("function"==typeof __nr_require)return __nr_require;for(var o=0;o<t.length;o++){r(t[o]);return r}([function(e,n){function t(e){function n(n,t,a){e&&e(n,t,a),a||((a={}));for(var u=c(n),f=u.length,s=i(a,o,r),p=0;p<f;p++)u[p].apply(s,t);return s}function a(e,n){f[e]=c(e).concat(n)}function c(e){return f[e]||[]}function u(i){return t(n,i)}var f={},return function(a,emit:n,create:u,listeners:c,_events:f){function r(){return f}var o="nr@context",i=e("gos");n.exports=t(),{gos:"7eSDFh"},ee:[function(e,n){n.exports=e("QJf3ax")},{}],3:[function(e,n){function t(e){return function(){r(e,[(new Date).getTime()].concat(i(arguments)))}}var r=e("handle"),o=e(1),i=e(2);"undefined"!==typeof window.newrelic&&(newrelic=window.NREUM);var a=["setPageViewName","addPageAction","setCustomAttribute","finished","addToTrace","inlineHit","noticeError"];o(a,function(e,n){window.NREUM[n]=t("api-"+n)}),n.exports=window.NREUM},{1:12,2:13,handle:"D5DuLP"}],gos:[function(e,n){n.exports=e("7eSDFh")},{}],7eSDFh:[function(e,n){function t(e,n,t){if(r.call(e,n))return e[n];var o=t();if(Object.defineProperty&&Object.keys)try{return Object.defineProperty(e,n,{value:o,writable:!0,enumerable:!1}),o}catch(i){return n e[n]=o,o}var r=Object.prototype.hasOwnProperty;n.exports=t},{}],D5DuLP:[function(e,n){function t(e,n,t){return r.listeners(e).length?r.emit(e,n,t):void(r.q&&(r.q[e]||(r.q[e]=[]),r.q[e].
```

```

push(n))}var r=e("ee").create();n.exports=t,t.ee=r,r.q={},{ee:"QJf3ax"},handle:[function(e,
n){n.exports=e("D5DuLP")},{},{XL7HBI:[function(e,n){function t(e){var n=typeof
e;return!e||"object"!==n&&"function"!==n?-1:e===window?0:i(e,o,function(){return
r++})}var r=1,o="nruid",i=e("gos");n.exports=t},{gos:"7eSDFh"}],id:[function(e,n){n.
exports=e("XL7HBI")},{},{G9z0B1:[function(e,n){function t(){var
e=d.info=NRUM.info,n=f.getElementsByTagName("script")[0];if(e&&e.licenseKey&
&e.applicationID&&n){c(p,function(n,t){n in e||e[n]=t});var
t="https"===s.split(":")[0]||e.sslForHttp;d.proto=t?"https://":"http://",a("mark
",[{"onload",i()}]);var r=f.createElement("script");r.src=d.proto+e.agent.n.parentNode.insertBefore(r,n)
}}function r(){"complete"===f.readyState&&o()}function o(){a("mark",["domContentLoaded
",i()])}function i(){return(new
Date).getTime()}var a=e("handle"),c=e(1),u=window,f=u.document;e(2);var
s=(""+location).split("?")[0],p={beacon:"bam.nr-data.net",errorBeacon:
"bam.nr-data.net",agent:"js-agent.newrelic.com/nr-686.min.js"},d=n.exports={offs
et:i(),origin:s,features:{}};f.addEventListener?(f.addEventListener("DOMContentLoaded
",o,!1),u.addEventListener("load",t,!1)):(f.attachEvent("onreadystatechange
",r),u.attachEvent("onload",t)),a("mark",["firstbyte",i()]),{1:12,2:3,handle:
"D5DuLP"}},loader:[function(e,n){n.exports=e("G9z0B1")},{},{12:[function(e,n){fu
nction t(e,n){var t=[],o="";i=0;for(o in e)r.call(e,o)&&(t[i]=n(o,e[o])),i+=1;return t}var
r=Object.prototype.hasOwnProperty;n.exports=t},{},{13:[function(e,n){function t(e,n,t){n||(n=0),"undefined"===typeof
t&&(t=e.length?0):for(var r=-1,o=t-n|0,i=Array(0>o?0:o);++r<o){i[r]=e[n+r];return
i}n.exports=t},{},{},{G9z0B1}]}</script><title>Screendoor</title><
script>var App = { "DEFAULT_LAT_LNG": [40.77, -73.98], "user_id": 7670, "is_dobt_admin": false, "js":
{ "advanced_search": "/d3bt6306j428ad.cloudfront.net/assets/advanced_search-e09af
03ffb2dd9f4bab25d6116871425cc27d728a88e69d966a38eb9922031e3.js", "at_mentions":
"/d3bt6306j428ad.cloudfront.net/assets/at_mentions-1d3e89344d3fb82c16dee141196e
0ed2c14392b69cccefe4a719348c33bad114.js", "copy_to_clipboard": "/d3bt6306j428ad.
cloudfront.net/assets/copy_to_clipboard-8c44a5ffa4b6e7863c8120642ecc23ea7a041944
d31c59f146007065b70bb361.js", "datetime_picker": "/d3bt6306j428ad.cloudfront.
net/assets/datetime_picker-1e19bd6377eeabe5dcfa4f6cf6a249c33495ad496a06264ee3c5b
91393cae78f.js", "esignature": "/d3bt6306j428ad.cloudfront.net/assets/esignature-
3488cd05237a0a7a16bb62d5f08e23ea95c29025510eadc0d8c5f2755e64a273.js", "form_build
er": "/d3bt6306j428ad.cloudfront.net/assets/form_builder-309a3be4961360272ceef6e
903ab6e247895f4ce9cc9baee9d9e851c9ed1df83.js", "maps": "/d3bt6306j428ad.
cloudfront.net/assets/maps-61c1862ece8acd3f7d14037e3a059838bc58a21271d63edb19235
9aa41988149.js", "wysiwyg": "/d3bt6306j428ad.cloudfront.net/assets/wysiwyg-4af684
3b7cd5e668bbdc22ef4fc3650f7cf5d294fcd8d4532celdea8cc67aef16.js", "import_wizard":
"/d3bt6306j428ad.cloudfront.net/assets/import_wizard-06affecb30f34bb68de14b432a
7b52e7f744a4eafda7a3f96e1030c9a328a3bc.js"} }</script><link rel="stylesheet" media="all"
href="/d3bt6306j428ad.cloudfront.net/assets/application-070a10a8796c0c29a8928c9
8d49b6232b657079f0f0892628d164a745abl8cd9.css" data-turbolinks-track="true" /><link rel="icon" type="image/png"
href="/apple-touch-icon-precomposed.png" /><script
src="//ajax.googleapis.com/ajax/libs/jquery/1.11.1/jquery.min.js"></script>
<script>window.jQuery || document.write('<script src="/non_digest_assets/jquery.js"></script>')</script><script
src="//use.typekit.net/ckbldps.js"></script><script>try{Typekit.load();
}catch(e)}</script><script src="/d3bt6306j428ad.cloudfront.net/assets/application-939e20a6c4eb570799c55553
5c4351232f39ddf45c682f0c4068524b005fc50c.js" data-turbolinks-track="true"
crossorigin="anonymous"></script><script>App.assetsLoaded || alert('There was an error loading assets and Screendoor
might not function properly. Try disabling any ad-blocking software, or contact us at
support@dobt.co.')

```

## 7.4.3 ID 6319941 - Possible Insecure Cryptographic Hash (SHA-0/SHA-1)

Best Practice

https://screendoor.dobt.co:443/

### Request

```
GET / HTTP/1.1
Host: screendoor.dobt.co
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://dashboard.dobt.co/sign_in?app_id=5&payload=[%221658bcfe549e1aee203508719c89a0e2c7a22f27%22,%7B%22state%22:%7B%22redirect%22:%22https://screendoor.dobt.co/%22%7D%7D]
Pragma: no-cache
Cookie:ajs_user_id=null;ajs_group_id=null;ajs_anonymous_id=%226f7e1237-94e1-4772-aa4b-b84efe0ef3aa%22;mp_3bb656b8f64677ca9a920cdd2ee1edd5_mixpanel=%7B%22distinct_id%22%3A%20%2214f0b9543d5127-05d595623bd9988-43514336-19b940-14f0b9543d6d6%22%2C%22%24initial_referrer%22%3A%20%22%24direct%22%2C%22%24initial_referring_domain%22%3A%20%22%24direct%22%7D;_ga=GA1.2.1413980223.1439008376;_gat=1;secure_remember_token_production=M16Q_zy9Y-Qaz7Dyzt-z;_screendoor_session=R0VVVtmk2amZhaythOFMxOFJlbVV4ZDVVSWMzVkvXaXk1VG1wc2lzd3pEZEJyekxQeFE5bzdDNu1ORGJ1ZWRYalVoK3JCvMjTa2NWN1FXblp1WlFBdHRmOU1vZDJZQVpONjlocHk2bGg2UVhOSXV3Qlc0WF1MaEc4VEJDT21TQTRkbUJkN0V3NGxwb2JwNDhVSFJ5SENxZVhtVVBQV29yYWJPTmxsMlR6Z28wPS0tQUgreE0wL2pDcXM3T2tVNEVGMkx4QT09--ea71185b0e7788d9f2b11cbbb99e3f7c19cf4ff6
Connection: keep-alive
X-WIPP: AscVersion=10.40.323.10
X-Scan-Memo: Category="Crawl.EventMacro.Startup"; SID="00000000000000000000000000000000"; SessionType="StartMacro"; CrawlType="None";
X-RequestManager-Memo: Category="EventMacro.Login"; MacroName="LoginMacro";
X-Request-Memo: ID="34f64119-4951-4a29-be9e-449b97677ead"; ThreadId="44";
```

### Response

```
HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
Content-Type: text/html; charset=utf-8
Date: Sat, 08 Aug 2015 04:32:59 GMT
ETag: W/"e4152bfdc9d49e000c1ea8f8fc4f5c8d"
Server: nginx + Phusion Passenger 5.0.10
Content-Length: 14187
Set-Cookie:_screendoor_session=eXdwC09ZV0dvSmNGaWFR0NNR3lGTnNadVVrdlpYahJdCkDFBckJSTHFJczdORFNLRLDlPU0hZcThvclhsUGxmR2JZcWZSZFVFWVNUUdtOHVzSW04R0paYWQ5UDZNSmNSdjJNZERUWwdHYkdHSUZHNnFXNUVUVWYxT3VobzdGUHp3UWtJZkd4VlF4VmNsTXQwUHRqamxvY1pXRUFON3BYZy9lNXNQaEdkZms2QlpTWU12QzZ4M3FjaEF5aU9peHB0dko3VEVBcUtYc2F1YzhBd2huTk0TXh2UEpBQlFveVgyZW8yYThpMGdNULJ0L3pxSFhtWmJWcDF0bGF1WjVpcWM2a1ByT2RVPXluYW1uS3pBwkVKNHc9PS0tMlJlTUJlMFJONFnsZ2hGQmVSRGp4QT09--d99c8cc005df521b1d895116fc7032edf4c3a83f;
path=/; HttpOnly
Status: 200 OK
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Powered-By: Phusion Passenger Enterprise 5.0.10
X-Powered-By: cloud66
X-Request-Id: 74d75823-86c1-41b1-ad61-4159a7e40622
X-Runtime: 0.159650
X-XSS-Protection: 1; mode=block
Connection: keep-alive

<!doctype html><html><head>
<script type="text/javascript">window.NREUM||(NREUM={});NREUM.info={"beacon":"bam.nr-data.net","errorBeacon":"bam.nr-data.net","licenseKey":"037a027bf3","applicationID":"6297642","transactionName":"dwtcTBBcD1lQUU0NDVkBHVEMVwZJ","queueTime":0,"applicationTime":159,"agent":"js-agent.newrelic.com/nr-686.min.js"}</script>
<script type="text/javascript">window.NREUM||(NREUM={}),(function(){function t(e,n,t){function r(t){if(!n[t]){var o=n[t]={exports:{}};e[t][0].call(o.exports,function(n){var o=e[t][1][n];return r(o?o:n),o,o.exports)}return n[t].exports}if("function"==typeof __nr_require)return __nr_require;for(var o=0;o<t.length;o++){r(t[o]);return r}([function(e,n){function t(e){function n(n,t,a){e&&e(n,t,a),a||((a={}));for(var u=c(n),f=u.length,s=i(a,o,r),p=0;p<f;p++)u[p].apply(s,t);return s}function a(e,n){f[e]=c(e).concat(n)}function c(e){return f[e]||[]}function u(i){return t(n)}var f={},return function r(){var o="nr@context",i=e("gos");n.exports=t(),{gos:"7eSDFh"}},ee:[function(e,n){n.exports=e("QJf3ax")},{}],3:[function(e,n){function t(e){return function(){}(r(e,[(new Date).getTime()].concat(i(arguments))))}var r=e("handle"),o=e(1),i=e(2);"undefined"!==typeof window.newrelic&&(newrelic=window.NREUM);var a=["setPageViewName","addPageAction","setCustomAttribute","finished","addToTrace","inlineHit","noticeError"];o(a,function(e,n){window.NREUM[n]=t("api-"+n)}),n.exports=window.NREUM},{1:12,2:13,handle:"D5DuLP"}],gos:[function(e,n){n.exports=e("7eSDFh")},{}],7eSDFh:[function(e,n){function t(e,n,t){if(r.call(e,n))return e[n];var o=t();if(Object.defineProperty&&Object.keys)try{return Object.defineProperty(e,n,{value:o,writable:!0,enumerable:!1}),o}catch(i){return n e[n]=o,o}var r=Object.prototype.hasOwnProperty;n.exports=t},{}],D5DuLP:[function(e,n){function t(e,n,t){return r.listeners(e).length?r.emit(e,n,t):void(r.q&&(r.q[e]||(r.q[e]=[]),r.q[e].
```

```

push(n))}var r=e("ee").create();n.exports=t,t.ee=r,r.q={},{ee:"QJf3ax"}},handle:[function(e,
n){n.exports=e("D5DuLP")},{},{XL7HBI:[function(e,n){function t(e){var n=typeof
e;return!e||"object"!==n&&"function"!==n?-1:e===window?0:i(e,o,function(){return
r++})}var r=1,o="nr@id",i=e("gos");n.exports=t},{gos:"7eSDFh"}],id:[function(e,n){n.
exports=e("XL7HBI")},{},{G9z0B1:[function(e,n){function t(){var
e=d.info=NRUM.info,n=f.getElementsByTagName("script")[0];if(e&&e.licenseKey&
&e.applicationID&&n){c(p,function(n,t){n in e||(e[n]=t)});var
t="https"===s.split(":")[0]||e.sslForHttp;d.proto=t?"https://":"http://",a("mark
",[{"onload",i()}]);var r=f.createElement("script");r.src=d.proto+e.agent.n.parentNode.insertBefore(r,n)
}}function r(){"complete"===f.readyState&&o()}function o(){a("mark",["domContentLoaded
",i()])}function i(){return(new
Date).getTime()}var a=e("handle"),c=e(1),u=window,f=u.document;e(2);var
s=(""+location).split("?")[0],p={beacon:"bam.nr-data.net",errorBeacon:
"bam.nr-data.net",agent:"js-agent.newrelic.com/nr-686.min.js"},d=n.exports={offs
et:i(),origin:s,features:{}};f.addEventListener?(f.addEventListener("DOMContentLoaded
",o,!1),u.addEventListener("load",t,!1)):(f.attachEvent("onreadystatechange
",r),u.attachEvent("onload",t)),a("mark",["firstbyte",i()]),{1:12,2:3,handle:
"D5DuLP"}},loader:[function(e,n){n.exports=e("G9z0B1")},{},{12:[function(e,n){fu
nction t(e,n){var t=[],o="";i=0;for(o in e)r.call(e,o)&&(t[i]=n(o,e[o])),i+=1;return t}var
r=Object.prototype.hasOwnProperty;n.exports=t},{},{13:[function(e,n){function t(e,n,t){n||(n=0),"undefined"===typeof
t&&(t=e.length?0):for(var r=-1,o=t-n|0,i=Array(0>o?0:o);++r<o;)i[r]=e[n+r];return
i}n.exports=t},{},{},{G9z0B1}]}</script><title>Screendoor</title><
script>var App = {"DEFAULT_LAT_LNG":[40.77,-73.98],"user_id":7670,"is_dobt_admin":false,"js":
{"advanced_search":"//d3bt6306j428ad.cloudfront.net/assets/advanced_search-e09af
03ffb2dd9f4bab25d6116871425cc27d728a88e69d966a38eb9922031e3.js","at_mentions":
"//d3bt6306j428ad.cloudfront.net/assets/at_mentions-1d3e89344d3fb82c16dee141196e
0ed2c14392b69cccefe4a719348c33bad114.js","copy_to_clipboard":"//d3bt6306j428ad.
cloudfront.net/assets/copy_to_clipboard-8c44a5ffa4b6e7863c8120642ecc23ea7a041944
d31c59f146007065b70bb361.js","datetime_picker":"//d3bt6306j428ad.cloudfront.
net/assets/datetime_picker-1e19bd6377eeabe5dcfa4f6cf6a249c33495ad496a06264ee3c5b
91393cae78f.js","esignature":"//d3bt6306j428ad.cloudfront.net/assets/esignature-
3488cd05237a0a7a16bb62d5f08e23ea95c29025510eadc0d8c5f2755e64a273.js","form_build
er":"//d3bt6306j428ad.cloudfront.net/assets/form_builder-309a3be4961360272ceef6e
903ab6e247895f4ce9cc9baee9d9e851c9ed1df83.js","maps":"//d3bt6306j428ad.
cloudfront.net/assets/maps-61c1862ece8acd3f7d14037e3a059838bc58a21271d63edb19235
9aa41988149.js","wysiwyg":"//d3bt6306j428ad.cloudfront.net/assets/wysiwyg-4af684
3b7cd5e668bbdc22ef4fc3650f7cf5d294fcd8d4532celdea8cc67aef16.js","import_wizard":
"//d3bt6306j428ad.cloudfront.net/assets/import_wizard-06affecb30f34bb68de14b432a
7b52e7f744a4eafda7a3f96e1030c9a328a3bc.js"}]}</script><link rel="stylesheet" media="all"
href="//d3bt6306j428ad.cloudfront.net/assets/application-070a10a8796c0c29a8928c9
8d49b6232b657079f0f0892628d164a745abl8cd9.css" data-turbolinks-track="true" /><link rel="icon" type="image/png"
href="/apple-touch-icon-precomposed.png" /><script
src="//ajax.googleapis.com/ajax/libs/jquery/1.11.1/jquery.min.js"></script>
<script>window.jQuery || document.write('<script src="/non_digest_assets/jquery.js"></script>')</script><script
src="//use.typekit.net/ckbldps.js"></script><script>try{Typekit.load();
}catch(e)}</script><script src="//d3bt6306j428ad.cloudfront.net/assets/application-939e20a6c4eb570799c55553
5c4351232f39ddf45c682f0c4068524b005fc50c.js" data-turbolinks-track="true"
crossorigin="anonymous"></script><script>App.assetsLoaded || alert('There was an error loading assets and Screendoor
might not function properly. Try disabling any ad-blocking software, or contact us at
support@dobt.co.');

```

## 7.4.4 ID 6319940 - Privacy Policy Not Present

## Best Practice

https://screendoor.dobt.co:443/sign\_in

### Request

```
GET /sign_in HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Host: screendoor.dobt.co
Connection: Keep-Alive
X-WIPP: AscVersion=10.40.323.10
X-Scan-Memo: Category="Crawl"; SID="6B1EDC68B075F63DDE5E5AFEFCB13A3A"; SessionType="ExternalAddedToCrawl";
CrawlType="None"; AttackType="None"; OriginatingEngineID="00000000-0000-0000-0000-000000000000"; ThreadId="64";
ThreadType="CrawlBreadthFirstDBReader";
X-RequestManager-Memo: StateID="21"; sc="1"; ID="e2d043ec-60fd-48c9-b949-9869e7a39057";
X-Request-Memo: ID="ef9857f0-ad6c-4ab6-aec9-768fb937774c"; sc="1"; ThreadId="40";
Cookie: CustomCookie=WebInspect106897ZX235B8F34E2EC46F59AD23433063D90B6YD581;secure_reme
mber_token_production=M16Q_zy9Y-Qaz7Dyzt-z;_screendoor_session=YUd3dC81V3pCdE9kY
1R1bXNvazJKZldOcWVRWI3eJZhd3JCRXI2bENlcXlpMzhJRFQ4MWZzNS96M3VNWm5Oai9JbXFhUW9ka
mdPSWxpVv1GbzRuTVB3WHZqShh3cWJmeVorTEVhRlVMWwXFDShGUZfZuZu3dkSddOandVSDAvSVVGMXpza
CtCc28wbFFST2M1YjYra2F4Rk85VWRSTfJSQU1zWWRXRHByTFdiWkdjVvUwR1ZlRmtSWHhVenF4dDhIQ
2lsZUFxXWc4cms5c1VjS3NrnVJrZ2U2ZGJmZW1HWTZkS2h4dldsQ2s3UDVOSDBaay9naE1TVHpwK0NaW
mkrYVhoMnBUNUVTVGhnbWc2RkF1UFEzVE9PS0tUGI5SWZTcnErelJoZlNGYmFWbmVtdz09--1f03e8e
dec440248c4fe2681657756591a503193
```

### Response

```
HTTP/1.1 302 Found
Cache-Control: no-cache
Content-Type: text/html; charset=utf-8
Date: Sat, 08 Aug 2015 04:33:31 GMT
Location: https://dashboard.dobt.co/sign_in?app_id=5&payload=[%221658bcfe549e1aee203508719
c89a0e2c7a22f27%22,%7B%22state%22:%7B%22redirect%22:%22https://screendoor.
dobt.co/%22%7D%7D]
Server: nginx + Phusion Passenger 5.0.10
Set-Cookie: _screendoor_session=Z2ViZmlsa0pueHlpK1dRUTljZ2xwMXlUSHdBeGJGb09wQmVzRFIzalBlSnFT
VvhZSEJ3eR5cFJzRSt2dJVDQ2xVSUVvL2Y3SEhBandSL1ZzTjFZbkNYVEdyQz1WalU1ckhBOFJaTzRK
SzdVRFVxbGQ5THZQOWhYUkYrQUJnMWRYSdhwVUpvZzZQMkJoN0tsVUE0amFmTE94TW52Y2Rwd2MybEt1
SXpjddZCWHoyOTdiUXpTSdRydHpvTjBiRUNTWExnSlcwWGRYRkhNQjVvR0hiU3FJRmJrZ1Fua012ZmV4
MDZlT3RGQ01DUGJVCm82ZmlieE5RdnlaOHRLMGswNUowbHBDbCWJNSThQa0pkdWxuN1oyeCtVWHhmY3l6
WjIvYzVvQTRsKzhvVDQ9LS1sS2cvU0FKYjFvTmdOTGNuU1YxRTVnPT0%3D--0941e8e70014ad929221
788cf11dddl60af12ab; path=/; HttpOnly
Status: 302 Found
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Powered-By: Phusion Passenger Enterprise 5.0.10
X-Powered-By: cloud66
X-Request-Id: 740a8498-f364-4a08-ace3-c566473a2d5e
X-Runtime: 0.006477
X-XSS-Protection: 1; mode=block
Content-Length: 242
Connection: keep-alive

<html><body>You are being <a href="https://dashboard.dobt.co/sign_in?app_id=5&payload=[%221658bcfe549e1ae
e203508719c89a0e2c7a22f27%22,%7B%22state%22:%7B%22redirect%22:%22https:
//screendoor.dobt.co/%22%7D%7D]">redirected</a>.</body></html>
```



## 7.5.1 ID 6319942 - Hidden Form Value

Info

https://screendoor.dobt.co:443/account/settings

### Request

```
GET /account/settings HTTP/1.1
Referer: https://screendoor.dobt.co/
Accept: */*
Accept-Encoding: gzip, deflate
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Host: screendoor.dobt.co
Connection: Keep-Alive
X-WIPP: AscVersion=10.40.323.10
X-Scan-Memo: Category="Crawl"; SID="F956FCDD2C46A857E84B14F9A97849D5"; PSID="C7AF1EE59487CE1089CBF7B4154EF6BB";
SessionType="Crawl"; CrawlType="HTML"; AttackType="None"; OriginatingEngineID="00000000-0000-0000-0000-000000000000";
ThreadId="107"; ThreadType="CrawlBreadthFirstDBReader";
X-RequestManager-Memo: StateID="21"; sc="1"; ID="4db247cd-acc-4906-af06-8676d189b53f";
X-Request-Memo: ID="2af9a359-374a-4b9c-8a6b-4bc5959d39b5"; sc="1"; ThreadID="40";
Cookie: CustomCookie=WebInspect106897ZX235B8F34E2EC46F59AD23433063D90B6YD581;secure_reme
mber_token_production=M16Q_zy9Y-Qaz7Dyzt-z;_screendoor_session=aS9JWjdMYmlwVlp4b
XdxTU82QSSyMEpBdnNwRWVBZkdLbEl1MTVqNTQzV250L2dqamdT0FLYjVZbTIwTGhibmV2R0NEOEhsc
klQL3I5dFVDZncza2lX0svckowOElqTFpYRUg5NGxvZkQ5Q05GcGJGcGtsdDN6RG12dn11bDJRcUVaV
CtRdFd2MENnVks50TEhjenpxcFBYaENGamJlM00zOEc2VUorSWk4SUh5SzRqK2hkC2FJdnVjU1FYnJm1L
SlESkl1WFBJRURkOU0tUd3QvenNkMFRnPT03D--6d623486800c9f9c34927553f1f378848bff944a;
browserupdateorg=pause
```

### Response

```
HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
Content-Type: text/html; charset=utf-8
Date: Sat, 08 Aug 2015 04:33:48 GMT
ETag: W/"85a06ec8085817671730855760cbd692"
Server: nginx + Phusion Passenger 5.0.10
Content-Length: 16205
Set-Cookie: _screendoor_session=cHZeKjGubWdLeVdKaW1Sd2U1VEWzbUJiZFRJc0ppakpPY3BjbExvdxHNNYlNR
eWtCM2VLONGRExXdk45cldBUDY0eHkzWHpVXkxMD1PRUJWcHVdWE8xMULZVTRFWXNTWXZuOG8zVDVC
Y3oxaTZzeXRWZHNWUjZHZUlpWk1CS3liZUpTaH1EdTdHwkhleENETG9EbXdsG9laUpYK0U5bW16SEcy
cXoweHRYczVrcjhjN0xBalQrcEtoSPhpYTJxLS1wRk5pRnhralBkOXhBYUNCMM0L05BPT0%
3D--59968d3337296e8446e335ce837deaa8bea9c05b; path=/; HttpOnly
Status: 200 OK
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Powered-By: Phusion Passenger Enterprise 5.0.10
X-Powered-By: cloud66
X-Request-Id: c00c2fd8-317d-4728-bda0-f971f1f88a55
X-Runtime: 0.085326
X-XSS-Protection: 1; mode=block
Connection: keep-alive

<!doctype html><html><head>
<script type="text/javascript">window.NREUM||(NREUM={});NREUM.info={"beacon":"bam.
nr-data.net","errorBeacon":"bam.nr-data.net","licenseKey":"037a027bf3","applicat
ionID":"6297642","transactionName":"dwtcTBBcD1lQQU0EAVcLR1YWHBBUQUcLCwVH","queue
Time":0,"applicationTime":76,"agent":"js-agent.newrelic.com/nr-686.min.
js"}</script>
<script type="text/javascript">window.NREUM||(NREUM={});__nr_require=function(e,n,t){fun
ction r(t){if(!n[t]){var o=n[t]={exports:{}};e[t][0].call(o.exports,function(n){var o=e[t][1][n];return
r(o?o:n)},o,o.exports)}return n[t].exports}if(["function"]==typeof __nr_require)return __nr_require;for(var
o=0;o<t.length;o++){r(t[o]);return r}({QJf3ax:[function(e,n){function t(e){function
n(n,t,a){e&&e(n,t,a),a||((a={}));for(var u=c(n),f=u.length,s=i(a,o,r),p=0;p<f;p++)u[p].apply(s,t);return s}function
a(e,n){f[e]=c(e).concat(n)}function c(e){return f[e]||[]}}function u(){return t(n)}var
f=[];return{on:a,emit:n,create:u,listeners:c,_events:f}}function r(){return{}}var
o="nr@context",i=e("gos");n.exports=t(),{gos:"7eSDFh"},ee:[function(e,n){n.
exports=e("QJf3ax"),{},{},3:[function(e,n){function t(e){return function(){r(e,[new
Date].getTime()).concat(i(arguments))}}var r=e("handle"),o=e(1),i=e(2);"undefined"==typeof
window.newrelic&&(newrelic=window.NREUM);var
a=["setPageViewName","addPageAction","setCustomAttribute","finished","addToTrace
","inlineHit","noticeError"];o(a,function(e,n){window.NREUM[n]=t("api-"+n)}),n.
exports=window.NREUM},{1:12,2:13,handle:"D5DuLP"}],gos:[function(e,n){n.
exports=e("7eSDFh"),{},{},7eSDFh:[function(e,n){function t(e,n,t){if(r.call(e,n))return e[n];var
o=t();if(Object.defineProperty&&Object.keys)try{return
Object.defineProperty(e,n,{value:o,writable:!0,enumerable:!1}),o}catch(i){return
n e[n]=o,o}var r=Object.prototype.hasOwnProperty;n.exports=t(),{},{},D5DuLP:[function(e,n){functio
n t(e,n,t){return r.listeners(e).length?r.emit(e,n,t):void(r.q&&(r.q[e]||r.q[e]=[]),r.q[e].
push(n))}var r=e("ee").create();n.exports=t,t.tee=r,r.q={},{},ee:"QJf3ax"},handle:[function(e,
n){n.exports=e("D5DuLP"),{},{},XL7HBI:[function(e,n){function t(e){var n=typeof
e;return!e||"object"!=n&&"function"!=n?-1:e===window?0:i(e,o,function){return
r++})}var r=1,o="nr@id",i=e("gos");n.exports=t(),{gos:"7eSDFh"},id:[function(e,n){n.
exports=e("XL7HBI"),{},{},G9z0Bl:[function(e,n){function t(){var
e=d.info=NREUM.info,n=getElementsByName("script")[0];if(e&&e.licenseKey&
e.applicationID&&n){c(p,function(n,t){n in e||e[n]=t});var
t="https"==s.split(":")[0]||e.sslForHttp;d.proto=t?"https://":"http://",a("mark
",[["onload",i()]);var r=f.createElement("script");r.src=d.proto+e.agent,n.parentNode.insertBefore(r,n)
}}function r(){if("complete"===f.readyState&&o)}function o(){a("mark",["domContentLoaded",i()])}function i(){return(new
```



```

Date).getTime())var a=e("handle"),c=e(1),u=window,f=u.document;e(2);var
s=(""+location).split("?")[0],p={beacon:"bam.nr-data.net",errorBeacon:
"bam.nr-data.net",agent:"js-agent.newrelic.com/nr-686.min.js"},d=n.exports={offs
et:i(),origin:s,features:{}};f.addEventListener((f.addEventListener("DOMContentL
oaded",o,!1),u.addEventListener("load",t,!1)):(f.attachEvent("onreadystatechange
",r),u.attachEvent("onload",t)),a("mark",["firstbyte",i()]),{1:12,2:3,handle:
"D5DuLP"}],loader:[function(e,n){n.exports=e("G9z0B1")},{},12:[function(e,n){fu
nction t(e,n){var t=[],o="",i=0;for(o in e)r.call(e,o)&&(t[i]=n(o,e[o]),i+=1);return t}var
r=Object.prototype.hasOwnProperty;n.exports=t},{},13:[function(e,n){function t(e,n,t){n||(n=0),"undefined"===typeof
t&&(t=e?e.length:0);for(var r=-1,o=t-n||0,i=Array(0>o?0:o);++r<o;)i[r]=e[n+r];return
i}n.exports=t},{},{}],["G9z0B1"]];</script><title>Notification settings - Screendoor</title><script>var App =
{"DEFAULT_LAT_LNG":{"40.77,-73.98"},"user_id":7670,"is_dobt_admin":false,"js":
{"advanced_search":"//d3bt6306j428ad.cloudfront.net/assets/advanced_search-e09af
03ffb2dd9f4bab25d6116871425cc27d728a88e69d966a38eb9922031e3.js","at_mentions":
"//d3bt6306j428ad.cloudfront.net/assets/at_mentions-1d3e89344d3fb82c16dee141196e
0ed2c14392b69cccefe4a719348c33bad114.js","copy_to_clipboard":"//d3bt6306j428ad.
cloudfront.net/assets/copy_to_clipboard-8c44a5ffa4b6e7863c8120642ecc23ea7a041944
d31c59f146007065b70bb361.js"},"datetime_picker":"//d3bt6306j428ad.cloudfront.
net/assets/datetime_picker-1e19bd6377eeabe5dcfa4fdcf6a249c33495ad496a06264ee3c5b
91393cae78f.js"},"signature":"//d3bt6306j428ad.cloudfront.net/assets/esignature-
3488cd05237a0a7a16bb62d5f08e23ea95c29025510eadc0d8c5f2755e64a273.js"},"form_build
er":"//d3bt6306j428ad.cloudfront.net/assets/form_builder-309a3be4961360272ceef6e
903ab6e247895f4ce9cc9baee9d9e851c9ed1df83.js"},"maps":"//d3bt6306j428ad.
cloudfront.net/assets/maps-61c1862ece8acd3f7d14037e3a059838bc58a21271d63edb19235
9aa41988149.js"},"wysiwyg":"//d3bt6306j428ad.cloudfront.net/assets/wysiwyg-4af684
3b7cd5e668bbdc22ef4fc3650f7cf5d294fc8d4532celdea8cc67aef16.js"},"import_wizard":
"//d3bt6306j428ad.cloudfront.net/assets/import_wizard-06affecb30f34bb68de14b432a
7b52e7f744a4eafda7a3f96e1030c9a328a3bc.js"}];</script><link rel="stylesheet" media="all"
href="//d3bt6306j428ad.cloudfront.net/assets/application-070a10a8796c0c29a8928c9
8d49b6232b657079f0f0892628d164a745abl8cd9.css" data-turbolinks-track="true" /><link rel="icon" type="image/png"
href="/apple-touch-icon-precomposed.png" /><script
src="//ajax.googleapis.com/ajax/libs/jquery/1.11.1/jquery.min.js"></script>
<script>window.jQuery || document.write('<script src="/non_digest_assets/jquery.js"></script>')</script><script
src="//use.typekit.net/ckblbps.js"></script><script>try{Typekit.load();
}catch(e)}</script><script src="//d3bt6306j428ad.cloudfront.net/assets/application-939e20a6c4eb570799c55553
5c4351232f39ddf45c682f0c4068524b005fc50c.js" data-turbolinks-track="true"
crossorigin="anonymous"></script><script>App.assetsLoaded || alert('There was an error loading assets and Screendoor
might not function properly. Try disabling any ad-blocking software, or contact us at
support@dobt.co.');

```

## 7.5.2 ID 6319937 - Possible Authentication Misconfiguration (WWW-Authenticate)

Info

https://screendoor.dobt.co:443/dobt\_hooks/session

### Request

```
GET /dobt_hooks/session HTTP/1.1
Referer: https://screendoor.dobt.co/dobt_hooks/session?payload=[%2224a2f1e394a28901d943bf0c8e524d8e5a7f1cda%22,%7B%22verification_token%22:%22QKs7uVmaw6YqoDiz_HsK9qUt5w%22,%22state%22:%7B%22redirect%22:%22https://screendoor.dobt.co/%22%7D%7D]
Accept: */*
Accept-Encoding: gzip, deflate
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Host: screendoor.dobt.co
Connection: Keep-Alive
X-WIPP: AscVersion=10.40.323.10
X-Scan-Memo: Category="Audit.Attack"; SID="83BB18E093344C4CBCCB86E2A531BCB1"; PSID="769287543E1CEFE4B1476C06CEF7BB80";
SessionType="PathTruncation"; CrawlType="None"; AttackType="None";
OriginatingEngineID="398bfe9e-1b77-4458-9691-603eea06e341"; AttackSequence="0"; AttackParamDesc="";
AttackParamIndex="0"; AttackParamSubIndex="0"; CheckID="0"; Engine="Path+Truncation"; Retry="False";
SmartMode="AllChecks"; ThreadID="22"; ThreadType="AuditorStateRequestorPool";
X-RequestManager-Memo: StateID="21"; sc="1"; ID="0c89778c-7986-40f1-b0e5-ca5c1534d7d8";
X-Request-Memo: ID="d2c0cc1e-5bd2-4d02-a633-f241b58bc51a"; sc="1"; ThreadID="40";
Cookie: CustomCookie=WebInspect106897ZX235B8F34E2EC46F59AD23433063D90B6YD581;secure_reme
mber_token_production=M16Q_zy9Y-Qaz7Dyzt-z;_screendoor_session=YWR3a2lyZ2R4aUpGW
Wl3bU5SSldEQU5HWGN2SjZwZTJqZFlPM1pVWlhGb0ZYTkh0U2RwMkswL3grdTRFeFlCaStQL3o1QThoM
3o5RE5ydTN1THUyOEpuMXI1U1hubm93dzdXMGNrMlNDbG45MFBqOW9qRkRIZDU2MDJrSzNudU0wdmowe
Eply2cvQ0QlaEs5QjBYOGpyeVBEU1RFTHppdG1NUDZxMmNWVGpwejJHamZ0TE9xSUxvZ0JFcjBKOEZmL
S0relhhYUVVND1Bci9vT3FqZk9pcVBBPT0%3D--669857f30c57ccd0865284b6b6f7a9c6a98ce033
```

### Response

```
HTTP/1.1 401 Unauthorized
Cache-Control: no-cache
Content-Type: text/html
Date: Sat, 08 Aug 2015 04:33:32 GMT
Server: nginx + Phusion Passenger 5.0.10
Content-Length: 5
```

... Starting at line 12 ...

```
X-Request-Id: fab77388-c537-4d5e-a1e1-fc098e54871b
X-Runtime: 0.006016
X-XSS-Protection: 1; mode=block
Connection: keep-alive
```

0

## 7.5.3 ID 6319946 - Possible File Upload Capability

Info

https://screendoor.dobt.co:443/hp-scan/12345/admin/imports/new

### Request

```
GET /hp-scan/12345/admin/imports/new HTTP/1.1
Referer: https://screendoor.dobt.co/hp-scan/12345/admin/responses
Accept: */*
Accept-Encoding: gzip, deflate
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Host: screendoor.dobt.co
Connection: Keep-Alive
X-WIPP: AscVersion=10.40.323.10
X-Scan-Memo: Category="Crawl"; SID="A4637F4C1343A01F2F8B2C17D6F4D201"; PSID="8CDF9AAE22117896809084539DAD43E7";
SessionType="Crawl"; CrawlType="HTML"; AttackType="None"; OriginatingEngineID="00000000-0000-0000-0000-000000000000";
ThreadId="148"; ThreadType="CrawlBreadthFirstDBReader";
X-RequestManager-Memo: StateID="21"; sc="1"; ID="62e94e28-421f-456a-b4b2-7eaa793ac314";
X-Request-Memo: ID="9db940e0-a21b-4ad3-aa02-1cf129b8f2bf"; sc="1"; ThreadID="40";
Cookie: CustomCookie=WebInspect106897ZX235B8F34E2EC46F59AD23433063D90B6YD581; screendoor
_session=UX14SzhBZ11PbVpFZnhqblNsUkpOendNK1NBA2paaThjZHZRdmslclZHVXRjVTBLYktGR29
xcmc4b20vWkhVRmdqT21WRGRwbDJYsmlMSTJRRzFleUtKZEhScmdGaXhSdKJCem1HUNDHeDhNbZVFRzV
XZHVkQ0MvRHY4ZkNEVUZCeE9PTepkM1RnQ29DbGtEbWNTSjkzcytlSm1RTmtkOVpYeUxGaS84VnNEUmI
rW1VlaVBpRFA1NHZ0WGVHZZHprLSOxRzI4WXRpL1RLNjBWC3p5eDNiM01BPT0%3D--db96aaeda93ae59
68d661e878825bdc5f4944e3f;secure_remember_token_production=M16Q_zy9Y-Qaz7Dyzt-z;
browserupdateorg=pause
```

### Response

```
HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
Content-Type: text/html; charset=utf-8
Date: Sat, 08 Aug 2015 04:37:08 GMT
ETag: W/"7c645fb6d0bea282c047d4945e052f5b"
Server: nginx + Phusion Passenger 5.0.10
Content-Length: 18234
Set-Cookie: _screendoor_session=RGZyVFNZOFkra3gxRjk0MHRvViswY2tEcTlDZ2FCUER6di84a2c3TUZ3Rmh6
QlJ4T0NSczEveG5mRnpobWxjd1FzSXNUK1hpN1kvdGlacnE2MUTHSjVGeFZHaWlvY1l5NGdUSXFGWQZ
Sld0b09zWFltTaitjZmdHcVvYRzhMmdFdlpRc0hUc3F2d3NHalNsNldVMHlqeUI0VU1jR0J5VVZMkZx
bjFjOTESYnN4dEYwT3pwSlRrOXA0engxU3RsLSlMU3lQRS9xTUX0RjBLYVp0dVRkUHRRT0%
3D--6f4d09197e431f2e6ff7c70d486b8e39d808db72; path=/; HttpOnly
Status: 200 OK
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Powered-By: Phusion Passenger Enterprise 5.0.10
X-Powered-By: cloud66
X-Request-Id: a7cf2cle-1a75-4c2e-alec-8c29289c93cd
X-Runtime: 1.229004
X-XSS-Protection: 1; mode=block
Connection: keep-alive

<!doctype html><html><head>
<script type="text/javascript">window.NREUM||(NREUM={});NREUM.info={"beacon":"bam.
nr-data.net","errorBeacon":"bam.nr-data.net","licenseKey":"037a027bf3","applicat
ionID":"6297642","transactionName":"dwtcTBBcD1lQUU0VEFsOV1sWbAJVWFoMShBRF0JXDEAG
blxeEqoQQBcdVqde","queueTime":0,"applicationTime":1228,"agent":"js-agent.
newrelic.com/nr-686.min.js"}</script>
<script type="text/javascript">window.NREUM||(NREUM={});__nr_require=function(e,n,t){fun
ction r(t){if(!n[t]){var o=n[t]={exports:{};e[t][0].call(o.exports,function(n){var o=e[t][1][n];return
r(o?o:n)},o,o.exports)}return n[t].exports}if("function"==typeof __nr_require)return __nr_require;for(var
o=0;o<t.length;o++){r(t[o]);return r}({QJf3ax:[function(e,n){function t(e){function
n(n,t,a){e&&e(n,t,a),a||((a={}));for(var u=c(n),f=u.length,s=i(a,o,r),p=0;p<f;p++)u[p].apply(s,t);return s}function
a(e,n){f[e]=c(e).concat(n)}function c(e){return f[e]||[]}}function u(){return t(n)}var
f=[];return{on:a,emit:n,create:u,listeners:c,_events:f}}function r(){return{}}var
o="nr@context",i=e("gos");n.exports=t(),{gos:"7eSDFh"},ee:[function(e,n){n.
exports=e("QJf3ax")},{}],3:[function(e,n){function t(e){function n(function(){}r(e,[new
Date].getTime()).concat(i(arguments)))}var r=e("handle"),o=e(1),i=e(2);"undefined"==typeof
window.newrelic&&(newrelic=window.NREUM);var
a=["setPageViewName","addPageAction","setCustomAttribute","finished","addToTrace
","inlineHit","noticeError"];o(a,function(e,n){window.NREUM[n]=t("api-"+n)}),n.
exports=window.NREUM},{1:12,2:13,handle:"D5DuLP"}],gos:[function(e,n){n.
exports=e("7eSDFh")},{}],7eSDFh:[function(e,n){function t(e,n,t){if(r.call(e,n))return e[n];var
o=t();if(Object.defineProperty&&Object.keys)try{return
Object.defineProperty(e,n,{value:o,writable:!0,enumerable:!1}),o}catch(i){return
n e[n]=o,o}var r=Object.prototype.hasOwnProperty;n.exports=t(),{}],D5DuLP:[function(e,n){functio
n t(e,n,t){return r.listeners(e).length?r.emit(e,n,t):void(r.q&&(r.q[e]||r.q[e]=[]),r.q[e].
push(n))}var r=e("ee").create();n.exports=t,t.tee=r,r.q={},ee:["QJf3ax"],handle:[function(e,
n){n.exports=e("D5DuLP")},{}],XL7HBI:[function(e,n){function t(e){var n=typeof
e;return!e||"object"!=n&&"function"!=n?-1:e===window?0:i(e,o,function(){}return
r++)}var r=1,o="nr@id",i=e("gos");n.exports=t(),{gos:"7eSDFh"},id:[function(e,n){n.
exports=e("XL7HBI")},{}],G9z0Bl:[function(e,n){function t(){var
e=d.info=NREUM.info,n=e.createElement("script");if(e&&e.licenseKey&
e.applicationID&&n){c(p,function(n,t){n in e||e[n]=t});var
t="https"==s.split(":")[0]||e.sslForHttp;d.proto=t?"https://":"http://",a("mark
",[["onload",i()]);var r=f.createElement("script");r.src=d.proto+e.agent,n.parentNode.insertBefore(r,n)
}}function r(){if("complete"===f.readyState&&o)}function o(){a("mark",[["domContentLoaded",i()]])}function i(){return(new
```

```






Date).getTime())var a=e("handle"),c=e(1),u=window,f=u.document;e(2);var
s=(""+location).split("?")[0],p={beacon:"bam.nr-data.net",errorBeacon:
"bam.nr-data.net",agent:"js-agent.newrelic.com/nr-686.min.js"},d=n.exports={offs
et:i(),origin:s,features:{}};f.addEventListener?(f.addEventListener("DOMContentL
oaded",o,!1),u.addEventListener("load",t,!1)):(f.attachEvent("onreadystatechange
",r),u.attachEvent("onload",t)),a("mark",["firstbyte",i()]),{1:12,2:3,handle:
"D5DuLP"}},loader:[function(e,n){n.exports=e("G9z0B1")},{}],12:[function(e,n){fu
nction t(e,n){var t=[],o="",i=0;for(o in e)r.call(e,o)&&(t[i]=n(o,e[o]),i+=1);return t}var
r=Object.prototype.hasOwnProperty;n.exports=t},{}],13:[function(e,n){function t(e,n,t){n||(n=0),"undefined"===typeof
t&&(t=e?e.length:0);for(var r=-1,o=t-n||0,i=Array(0>o?0:o);++r<o;)i[r]=e[n+r];return
i}n.exports=t},{}],{}],["G9z0B1"]];</script><title>Import responses - Screendoor</title><script>var App =
{"DEFAULT_LAT_LNG":{"40.77,-73.98"},"user_id":7670,"is_dobt_admin":false,"js":
{"advanced_search":"//d3bt6306j428ad.cloudfront.net/assets/advanced_search-e09af
03ffb2dd9f4bab25d6116871425cc27d728a88e69d966a38eb9922031e3.js","at_mentions":
"//d3bt6306j428ad.cloudfront.net/assets/at_mentions-1d3e89344d3fb82c16dee141196e
0ed2c14392b69cccefe4a719348c33bad114.js","copy_to_clipboard":"//d3bt6306j428ad.
cloudfront.net/assets/copy_to_clipboard-8c44a5ffa4b6e7863c8120642ecc23ea7a041944
d31c59f146007065b70bb361.js"},"datetime_picker":"//d3bt6306j428ad.cloudfront.
net/assets/datetime_picker-1e19bd6377eeabe5dcfa4fdcf6a249c33495ad496a06264ee3c5b
91393cae78f.js"},"signature":"//d3bt6306j428ad.cloudfront.net/assets/esignature-
3488cd05237a0a7a16bb62d5f08e23ea95c29025510eadc0d8c5f2755e64a273.js"},"form_build
er":"//d3bt6306j428ad.cloudfront.net/assets/form_builder-309a3be4961360272ceef6e
903ab6e247895f4ce9cc9baee9d9e851c9ed1df83.js"},"maps":"//d3bt6306j428ad.
cloudfront.net/assets/maps-61c1862ece8acd3f7d14037e3a059838bc58a21271d63edb19235
9aa41988149.js"},"wysiwyg":"//d3bt6306j428ad.cloudfront.net/assets/wysiwyg-4af684
3b7cd5e668bbdc22ef4fc3650f7cf5d294fc8d4532celdea8cc67aef16.js"},"import_wizard":
"//d3bt6306j428ad.cloudfront.net/assets/import_wizard-06affecb30f34bb68de14b432a
7b52e7f744a4eafda7a3f96e1030c9a328a3bc.js"}];</script><link rel="stylesheet" media="all"
href="//d3bt6306j428ad.cloudfront.net/assets/application-070a10a8796c0c29a8928c9
8d49b6232b657079f0f0892628d164a745ab18cd9.css" data-turbolinks-track="true" /><link rel="icon" type="image/png"
href="/apple-touch-icon-precomposed.png" /><script
src="//ajax.googleapis.com/ajax/libs/jquery/1.11.1/jquery.min.js"></script>
<script>window.jQuery || document.write('<script src="/non_digest_assets/jquery.js"></script>')</script><script
src="//use.typekit.net/ckblpds.js"></script><script>try{Typekit.load();
}catch(e)}</script><script src="//d3bt6306j428ad.cloudfront.net/assets/application-939e20a6c4eb570799c55553
5c4351232f39ddf45c682f0c4068524b005fc50c.js" data-turbolinks-track="true"
crossorigin="anonymous"></script><script>App.assetsLoaded || alert('There was an error loading assets and Screendoor
might not function properly. Try disabling any ad-blocking software, or contact us at
support@dobt.co.');"</script><script>!function(){var
analytics=window.analytics=window.analytics||[];if(!analytics.initialize)if(anal
ytics.invoked)window.console.error&&console.error("Segment snippet included
twice.");else{analytics.invoked=!0;analytics.methods=["trackSubmit","trackClick"
,"trackLink","trackForm","pageview","identify","group","track","ready","alias","
page","once","off","on"];analytics.factory=function(t){return function(){var
e=Array.prototype.slice.call(arguments);e.unshift(t);analytics.push(e);
return analytics}};for(var t=0;t<analytics.methods.length;t++){var
e=analytics.methods[t];analytics[e]=analytics.factory(e)}analytics.load=function
(t){var e=document.createElement("script");e.type="text/javascript";e.async=!0;
e.src=("https:"===document.location.protocol?"https://":"http://")+cdn.
segment.com/analytics.js/v1/"+t+"/analytics.min.js";var
n=document.getElementsByTagName("script")[0];n.parentNode.insertBefore(e,n);
analytics.SNIPPET_VERSION="3.0.1";}}()</script><script>var $buoop = {}; $buoop.ol = window.onload;
window.onload=function(){ try {if ($buoop.ol) $buoop.ol();}catch (e) {} var e = document.createElement("script");
e.setAttribute("type", "text/javascript"); e.setAttribute("src", "//browser-update.org/update.js");
document.body.appendChild(e); }</script><script
src="//d2wy8f7a9ursnm.cloudfront.net/bugsnag-2.min.js"></script><script>
Bugsnag.apiKey = "09151347cb529da47dfbb0998088d790"; Bugsnag.user = { id: 8893 }; Bugsnag.releaseStage =
"production";</script><meta name="viewport" content="width=device-width, initial-scale=1.0" /><meta name="csrf-param"
content="authenticity_token" />

```

# Appendix - Descriptions of Key Terminology

## Security Rating

The Fortify 5-star assessment rating provides information on the likelihood and impact of defects present within an application. A perfect rating within this system would be 5 complete stars indicating that no high impact vulnerabilities were uncovered.

Rating	
	Fortify awards one star to projects that undergo a Fortify security review, which analyzes a project for a variety of software security vulnerabilities.
	Fortify awards two stars to projects that undergo a Fortify security review that identifies no high likelihood / high impact issues. Vulnerabilities that are trivial to exploit and have a high business or technical impact should never exist in business-critical software.
	Fortify awards three stars to projects that undergo a Fortify security review that identifies no low likelihood / high impact issues and meets the requirements needed to receive two stars. Vulnerabilities that have a high impact, even if they are non-trivial to exploit, should never exist in business critical software.
	Fortify awards four stars to projects that undergo a Fortify security review that identifies no high likelihood / low impact issues and meets the requirements for three stars. Vulnerabilities that have a low impact, but are easy to exploit, should be considered carefully as they may pose a greater threat if an attacker exploits many of them as part of a concerted effort or leverages a low impact vulnerability as a stepping stone to mount a high-impact attack.
	Fortify awards five stars to projects that undergo a Fortify security review that identifies no issues.

## Likelihood and Impact

### Likelihood

Likelihood is the probability that a vulnerability will be accurately identified and successfully exploited.

### Impact

Impact is the potential damage an attacker could do to assets by successfully exploiting a vulnerability. This damage can be in the form of, but not limited to, financial loss, compliance violation, loss of brand reputation, and negative publicity.

## Fortify Priority Order

### Critical

Critical-priority issues have high impact and high likelihood. Critical-priority issues are easy to detect and exploit and result in large asset damage. These issues represent the highest security risk to the application. As such, they should be remediated immediately.

SQL Injection is an example of a critical issue.

### High

High-priority issues have high impact and low likelihood. High-priority issues are often difficult to detect and exploit, but can result in large asset damage. These issues represent a high security risk to the application. High priority issues should be remediated in the next scheduled patch release.

## Medium

Medium-priority issues have low impact and high likelihood. Medium-priority issues are easy to detect and exploit, but typically result in small asset damage.

These issues represent a moderate security risk to the application. Medium-priority issues should be remediated in the next scheduled

## Low

Low-priority issues have low impact and low likelihood. Low-priority issues can be difficult to detect and exploit and typically result in small asset damage.

These issues represent a minor security risk to the application. Low priority issues should be remediated as time allows.

## Issue Status

### New

New issues are ones that have been identified for the first time in the most recent analysis of the application.

### Existing

Existing issues are issues that have been found in a previous analysis of the application and are still present in the latest analysis.

### Reopened

Reopened issues have been discovered in a previous analysis of the application but were not present in subsequent analyses. These issues are now present again in the most recent analysis of the application.

## Fortify Remediation Effort

### Major Remediation

Major remediation effort issues must often be addressed at multiple locations to fix the root problem.

### Minor Remediation

Minor remediation effort issues can typically be addressed at the location of the root problem.