機密扱い

ID: AAA-BBBB-CCCC

株式会社********* 御中

脆弱性診断報告書

本報告書は、御社Webサイト「www.badstore.net」内Webアプリケーションの脆弱性を診断した結果をまとめ、
ご報告するものです。
内容には、脆弱性情報、および一部に機密に値する情報が含まれていますので、本報告書の管理・取り扱いには
細心の注意を払っていただきますようお願いいたします。

2017.10.26

フォームズ株式会社

開発部(仮)　K

機密扱い

目次

1 はじめに

1.1 診断の目的

企業のWebサイトやシステム上の弱点(脆弱性)を狙った、インターネットを通じての不正アクセス攻撃が、
年々その脅威を増している。
直近の例としては、交通機関や銀行などのインフラ施設のシステムに侵入し使用不能な状態に陥らせるなど
したうえで身代金(Ransom)を要求するランサムウェアの一種「WannaCry」が猛威を振るったことや、
Webアプリケーションフレームワークとして広く利用されている「Apache Struts 2」に脆弱性が
見つかり、この脆弱性を狙った攻撃によって情報漏洩の被害が多数発生したことなどが挙げられる。

インターネットを介した情報のやり取りが高度化する中、堅牢なWebシステムの構築が求められている。
そのためには、構成要素に対する正しい認識と対処が不可欠である。　しかし、OSやサーバなどのシステムソフトウェアや、データベースなどのミドルウェアの脆弱性情報が
公的機関から発表されることが多いのに対し、Webアプリケーション自体の脆弱性は開発する企業側で
調査し、正しく理解する必要がある。

本診断は、開発部Kのセキュリティ研修として行うものであり、脆弱性の発見と対処指針の策定を行い、
本報告書に結果をまとめ成果物として提出することを目的とする。

1.2 本報告書の取り扱い

本報告書は、セキュリティ研修の一環として、開発部Kが脆弱性発見練習用Webアプリケーション
「BadStore.net」の脆弱性を調査した結果を、エグゼクティブ・サマリー(経営層向け報告書)として
まとめたものである。
練習用の資料ではあるが、実際に攻撃を行った結果を掲載しているため、他のWebアプリケーションや
サイトでの悪用を固く禁ずる。

本資料の利用に関し、利用者もしくは第三者に損害が生じた場合であっても、本資料の利用が自己責任で
行われることを鑑み、弊社は刑事責任および民事責任の一切を負わないものとする。

2 診断内容

2.1 診断日程

日程

- 2017年9月27日 ~ 2017年10月16日

時間帯

- 9:30 ~ 18:30

2.2 診断対象

対象URL

- http://www.badstore.net/ 以下全ページ
- https://www.badstore.net/ 以下全ページ

対象ドメイン

- badstore.net

IPアドレス

- 192.168.11.16

サービス名

- 練習用Webアプリケーション「BadStore.net」

2.3 診断環境

- 仮想環境構築ソフト : Oracle VirtualBox
- ホストOS : Windows 10 Home
- ゲストOS : BadStore_212(Linux version 2.4.21)
- サーバ : Apache 1.3.28
- 脆弱性自動診断ソフト : OWASP Zed Attack Proxy
- 脆弱性手動診断ソフト : PortSwigger Burp Suite
- ブラウザ : Google Chrome, Mozilla FireFox

2.4 実施者

- K.S(フォームズ株式会社 開発部(仮))

2.5 診断項目

診断項目を以下に列挙する。

攻撃区分	攻撃名称
不正コマンド実行	SQLインジェクション
	OSコマンドインジェクション
	クロスサイトスクリプティング(XSS)
情報開示	ディレクトリトラバーサル
	ディレクトリリスティング (強制ブラウズ)
	公開不要の機能・ファイル・ ディレクトリの存在
	エラーメッセージによる 情報の露出
	HTTPS不備
	HTTPS利用時のCookieの Secure属性不備
認証不備	脆弱なパスワードポリシ
	ログアウト不備
	過度な認証試行(ブルートフォース) への対策不備
	パスワードリセット不備
認可不備	認可制御不備
セッション管理不備	Cookieの HttpOnly属性不備
	推測可能なセッションID

3 診断結果概要

3.1 総合評価

I : 深刻な脆弱性が存在

※総合評価について

本報告書では、診断結果詳細、および付録Aに記載の脆弱性危険度レベル、個数に応じて下記の表のように評価している。

評価	基準
S (Safe)	**脆弱性の検出はなし**
L (Low)	**危険度Lowの脆弱性が検出**
M (Medium)	**危険度Mediumの脆弱性が検出**
H (High)	**危険度Highの脆弱性が検出**
D (Dangerous)	**危険度Highの脆弱性が複数検出**
I (Immediately)	**危険度Immediatelyの脆弱性が検出**

3.2 検出された脆弱性

3.2.1 クライアントサイドからの攻撃

区分	名称	危険度	個数
不正コマンド実行	SQLインジェクション	Immidiately	4
	OSコマンドインジェクション	High	1
	クロスサイトスクリプティング(XSS)	High	1
情報開示	ディレクトリトラバーサル	Medium	1
	ディレクトリリスティング (強制ブラウズ)	Medium	1

3.2.2 サーバ設定等の不備

区分	名称	危険度
情報開示	公開不要の機能・ファイル・ ディレクトリの存在	Medium
	エラーメッセージによる 情報の露出	High
	HTTPS不備	Medium
	HTTPS利用時のCookieの Secure属性不備	Medium
認証不備	脆弱なパスワードポリシ	High
	ログアウト不備	Medium
	過度な認証試行(ブルートフォース) への対策不備	Medium
	パスワードリセット不備	Medium
セッション管理不備	Cookieの HttpOnly属性不備	Medium
	推測可能なセッションID	Medium

3.3 総評

今回の診断の結果、当該サイトにおいては、パラメータのチェック漏れや入力値のサニタイジング(無害化)が実施されていないことに起因する、危険度の高い脆弱性が多数存在することが確認された。
特に顕著であった脆弱性として、SQLインジェクションやコマンドインジェクション等が挙げられる。

ログイン時に使用された場合、パスワード等の入力を回避してアカウントに侵入、個人情報の漏洩やデータ改ざん、他アカウントへの不正アクセスなどの被害につながるおそれがある。

また、一部ページにおいてエラー発生時にSQL構文、サーバのバージョン等詳細な情報を表示してしまう箇所が見受けられた。これらの情報からSQLインジェクション等、他の脆弱性との組み合わせによって被害の拡大を引き起こす可能性がある。

その他、パスワードそのものが脆弱なものが使用される、ログアウト機能がないなど、設計自体の問題も数多く見受けられた。

いずれの脆弱性についても本報告書を参考に十分な対策を行っていただければ幸いである。

4 診断結果詳細
A クライアントサイド

4.A.1 不正なコマンドの実行

4.A.1.1 SQLインジェクション

1. **危険度**
   Immediately : **緊急**

2. CWE (Common Weakness Enumeration : **共通脆弱性タイプ一覧**)
   CWE-89「SQLコマンドに含まれる特殊文字列の不適切な不活化**」**

3. **脆弱性発生状況**

- **発生個所**

No.	URL	パラメータ
1	http://www.badstore.net/cgi-bin/badstore.cgi?searchquery=	BODY : searchquery URL : searchquery
2	http://www.badstore.net/cgi-bin/badstore.cgi?action=myaccount	BODY : email
3	http://www.badstore.net/cgi-bin/badstore.cgi?action=loginregister	BODY : email
4	https://www.badstore.net/cgi-bin/badstore.cgi?action=supplierlogin	BODY : email

機密扱い

- **解説**

  ここではNo.3について解説する。
  パラメータ'email'に以下のように値を設定し送信する。

  ```
  email=admin'--
  ※ "--" の後に半角スペースを1つ置く。
  ```

  その結果、以下の画面のように、不正にアカウントにログインすることができた。

  本脆弱性は、入力された文字列に含まれる、SQL上の処理に関連する文字列の無効化や、取得された内容の検査を実施しない、または不完全に行うことによって発生する脆弱性である。
  本脆弱性を利用することにより、通常ユーザ側からアクセスできないデータベースからの情報の取得や、不正ログインを行うことが可能になる。

4. **本脆弱性による脅威**
   本脆弱性により、管理者権限への不正ログイン、ユーザ情報の不正取得・書き換えなどが行われ、特に管理者権限にアクセスされた場合には売り上げ情報確認、パスワード初期化など、ほぼ全てのデータにアクセスされる可能性がある。

5. **本脆弱性への対策**
   SQL文を、文字列の直接組み立てによって構成するのではなく、プレースホルダ、バインド機構を使用し、あらかじめ実行可能なSQL文を組み立てる方式にする。
   バージョンが古いなどの事由からそれらの対策が困難な場合は、実行結果に含まれる値をチェックし、不正な文字列が含まれている、もしくは型が合わなければエラー処理やサニタイジング (無害化) を行う、という方式でもよい。

機密扱い

4.A.1.2 OSコマンドインジェクション

1. **危険度**
   High : **重要**

2. CWE
   CWE-78「OSコマンドに含まれる特殊文字列の不適切な不活化」

3. **脆弱性発生状況**

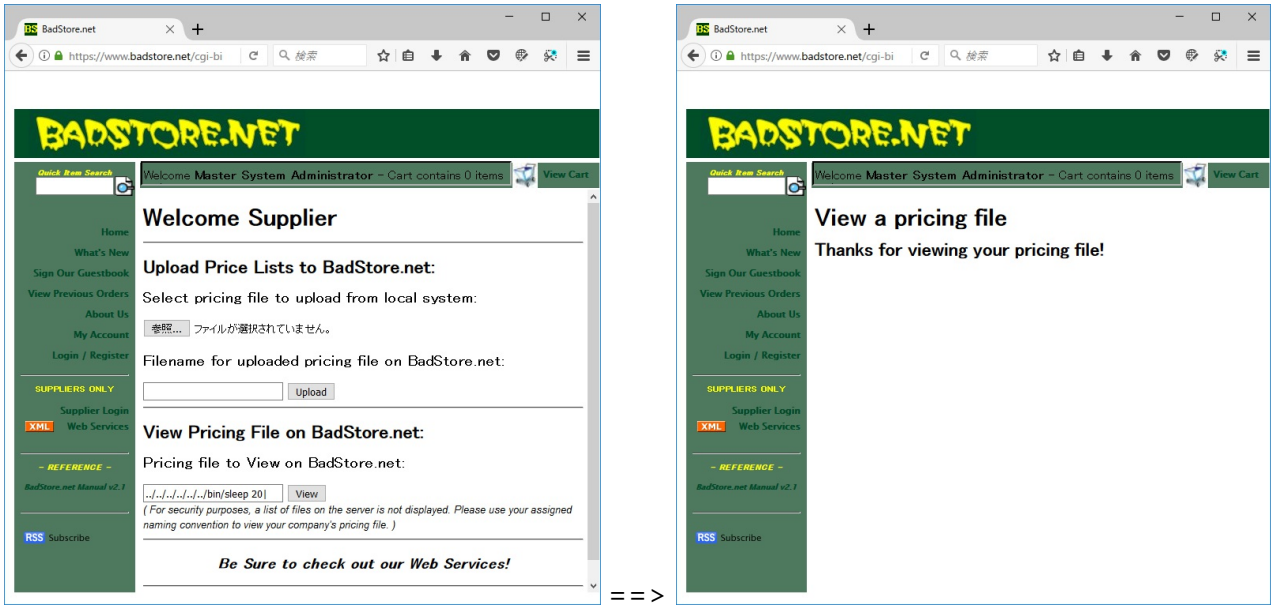
- **発生個所**

No.	URL	パラメータ
1	https://www.badstore.net/cgi-bin/badstore.cgi?action=supplierportal	BODY : viewfilename

- **解説**
  パラメータ'viewfilename'**に以下のように値を設定し送信する。**

```
../../../../../../bin/sleep 20|
```

この場合は、レスポンスが20**秒遅れて返ってくる。**



本脆弱性は、攻撃者がOSへの直接アクセス権をもたないWebアプリケーション等の環境において、入力文字列の検査を実施しない、もしくは不完全に行うことによって発生し、攻撃者によって予期しないOS上のコマンドを実行されるおそれがある。
プロセスの権限を適切に設定していない場合、本脆弱性の利用により、上位権限で使用可能なコマンドを使用した攻撃が外部から行われ、ユーザ権限の変更や設定ファイルの窃視など、被害が拡大する可能性がある。

4. 本脆弱性による脅威
   本Webアプリケーション上では、システムのシャットダウンや、データ消去等に係るコマンドは実行できなかったものの、ホスト名やIPアドレスの設定を閲覧したり、レスポンスを遅らせるといったコマンドを実行することができた。
   本脆弱性では、権限設定が不適切な場合、システムのシャットダウンやファイル消去、内部設定ファイルの閲覧等が行われ、サービスへの直接的な被害が発生する可能性がある。

5. 本脆弱性への対策
   入力文字列のエスケープ (無効化) や、サーバ側での入力文字列の検査、あるいは直接OS上のコマンドを呼び出す関数を使用しないファイルの呼び出し方法を用いる。
   システムの関係でOSコマンドの呼び出しが必要な場合は、シェル(OSとユーザの間にあるコマンド実行機構)を経由せずにコマンドを呼び出す関数を使用する。

4.A.1.3 クロスサイトスクリプティング(Cross(X) Site Scripting : XSS)

1. **危険度**
   High : **重要**

2. CWE
   CWE-79「Webページ生成中入力値の不適切な不活化」

3. **脆弱性発生状況**

- **発生個所**

No.	URL	パラメータ
1	http://www.badstore.net/cgi-bin/badstore.cgi?action=guestbook	BODY : name BODY : email BODY : comments
2	https://www.badstore.net/cgi-bin/badstore.cgi?action=supplierportal	BODY : viewfilename

機密扱い

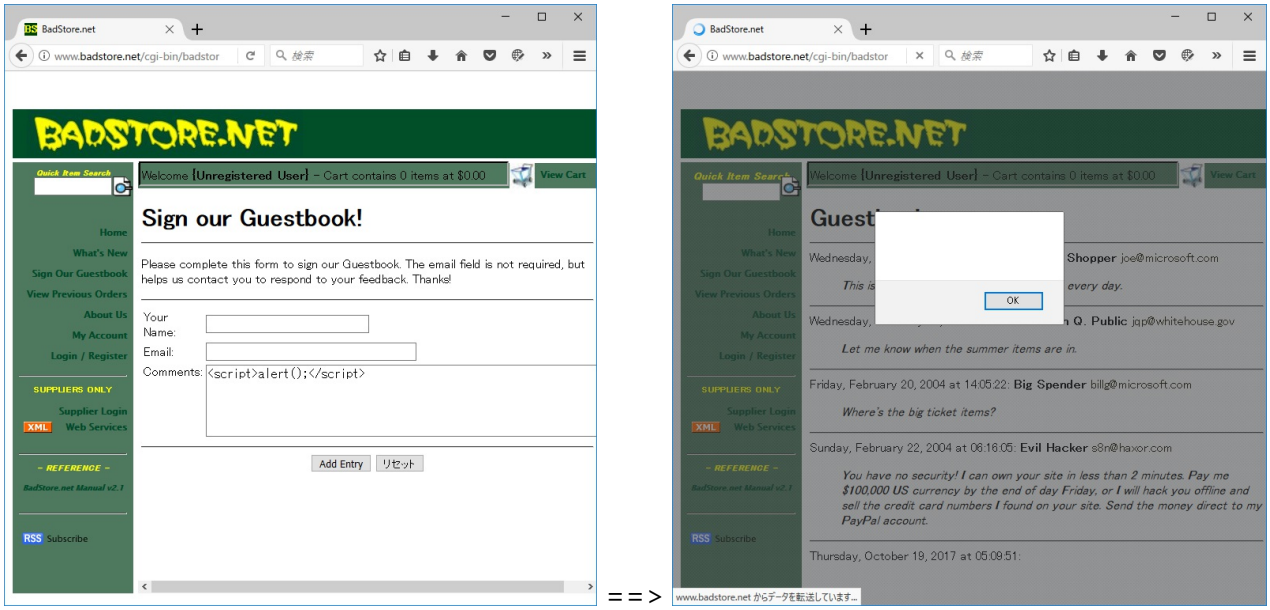
- **解説**

  ・No.1について

  パラメータ'name','email','comments'**のいずれかに以下のように値を設定し送信する。**

```
name=%3Cscript%3Ealert%28%29%3B%3C%2Fscript%3E
email=%3Cscript%3Ealert%28%29%3B%3C%2Fscript%3E
comments=%3Cscript%3Ealert%28%29%3B%3C%2Fscript%3E
%3Cscript%3Ealert%28%29%3B%3C%2Fscript%3E : <script>alert();</script>
```

この例では、以下のようにアラートが表示される。



・No.2について

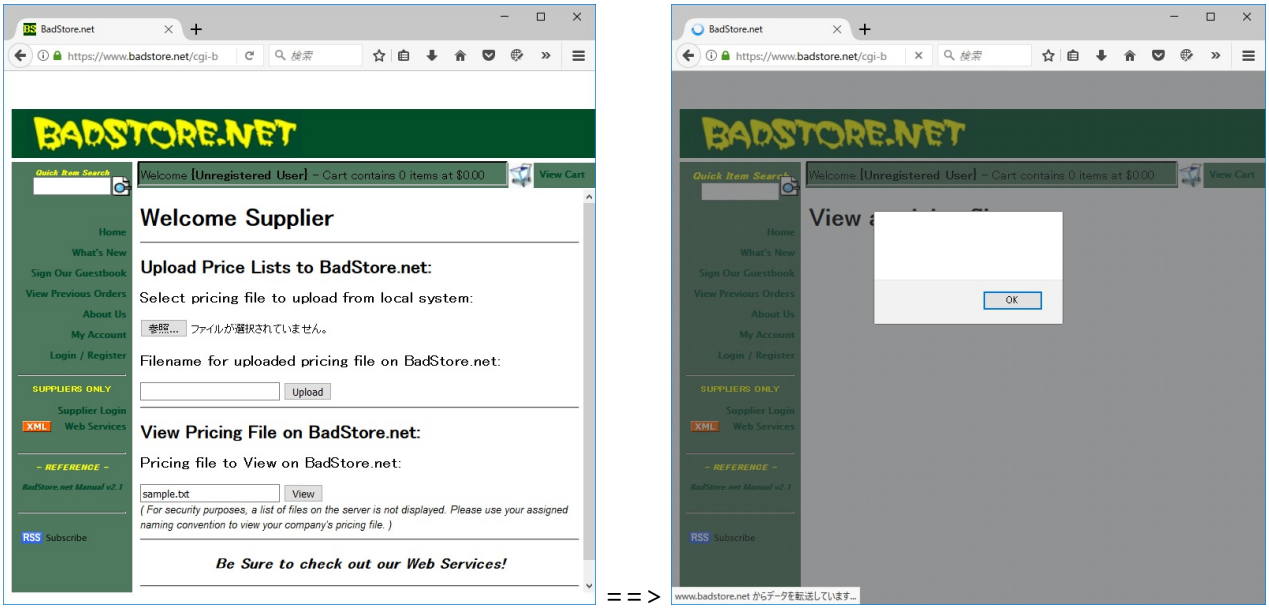
当該ページ内にあるファイルアップロード機能を利用し、以下の内容を記述した'sample.txt'**ファイルをアップロードする。**

```
<script>alert();</script>
```

アップロード後、再度当該ページにログインし、パラメータ'viewfilename'**に以下の値を設定し送信する。**

```
sample.txt
```

この例においても、以下のようにアラートが表示される。



4. 本脆弱性による脅威

本脆弱性により、予期しないページへの遷移や、クッキー値の窃取、偽のフォームによるフィッシングなど、Webアプリケーションの機能を悪用して他の利用者に被害を与えることが可能になる。
例として、掲示板などコメントが表示されるページでは、コメント中にスクリプトが埋め込まれた場合、当該ページを見ただけでスクリプトによる被害が発生してしまい、信用を大きく損なうことになる。

5. 本脆弱性への対策

HTMLの特殊文字列をエスケープ(無効化)し、そのうえで入力値の検証や、クッキーにスクリプトでアクセスできないようにするHttpOnly属性を設定する方法が効果的である。
また、文字エンコードの差異を利用したXSSも存在するため、HTTPレスポンスにエンコーディングを明示することで、ブラウザ-Webアプリケーション間のエンコード差異を抑えるのも有効である。

4.A.2 情報開示

4.A.2.1 ディレクトリトラバーサル (パストラバーサル)

1. 危険度
   Medium：警告

2. CWE
   CWE-22「アクセス制限されたディレクトリを参照するパス名の不適切な制限」

3. 脆弱性発生状況

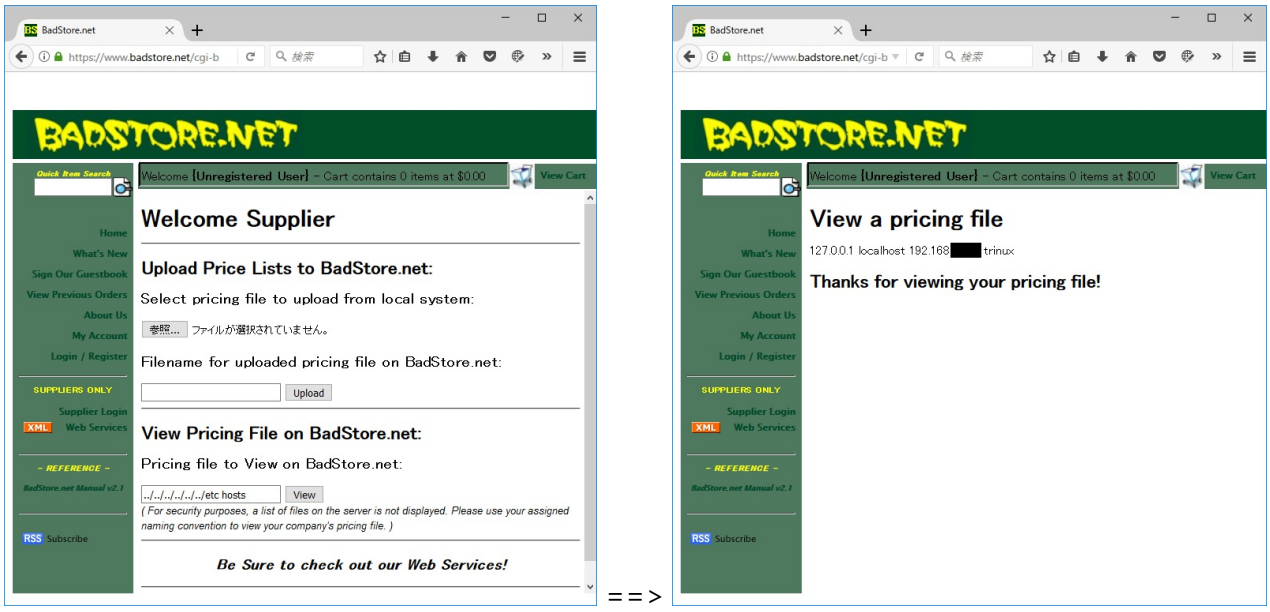
- 発生個所

No.	URL	パラメータ
1	https://www.badstore.net/cgi-bin/badstore.cgi?action=supplierportal	

- 解説
  パラメータ'viewfilename'に以下のように値を設定し送信する。

```
../../../../../../etc/hosts
```

この例では、以下のようにホスト名やIPアドレスの設定が表示される。



4. 本脆弱性による脅威
   外部からのアクセス権限のないファイルやフォルダにアクセスされ、サーバの設定情報やパスワードといった情報を盗み見られるおそれがある。また、それらの情報をもとにサーバに不正にログインされるなど攻撃を受ける可能性がある。

5. 本脆弱性への対策
   パス名の入力文字列をチェックし、ファイル名以外の特殊文字列が入っている場合には処理を必ず失敗させる、上位のフォルダや指定された形式以外のファイルへの外部からのアクセスを制限する、などの方法がある。

機密扱い

4.A.2.2 ディレクトリリスティング | インデクシング

1. **危険度**
   Medium : **警告**

2. CWE
   CWE-548「ディレクトリリスト化による情報の曝露」

3. **脆弱性発生状況**

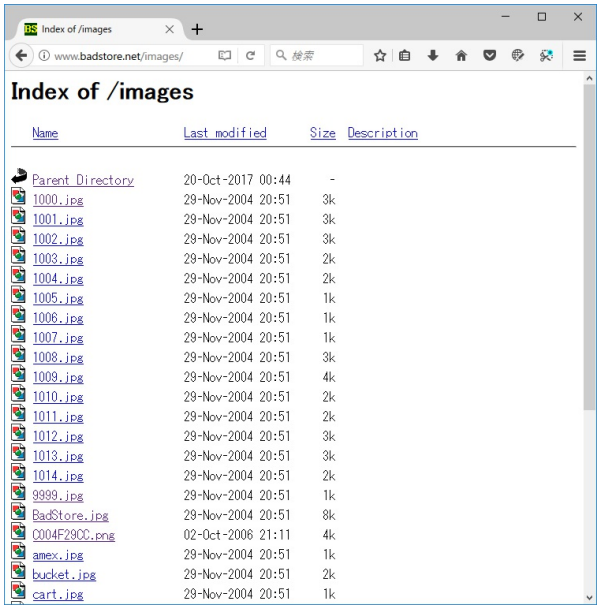
- **発生個所**

No.	URL	パラメータ
1	http://www.badstore.net/images/	-
2	http://www.badstore.net/ws/	-

- **解説**
  以下のURLを直接入力する。

```
http://www.badstore.net/images/
```

この例では、以下のようにフォルダの中身が表示される。



機密扱い

4. **本脆弱性による脅威**
   本脆弱性により、通常は直接アクセスできないファイルを閲覧される可能性がある。
   また、仮に機密情報を含むファイルが置かれている場合は情報漏洩に

5. **本脆弱性への対策**
   本脆弱性は、サーバーの設定に起因する脆弱性であるため、設定ファイルの内容を編集することで抑制できる。
   具体的な対策例を下記に示す。

   'httpd.conf'**ファイルを編集し以下の内容を追記する。**

```
Alias /images/ "/usr/local/apache/htdocs/images"

<Directory "/usr/local/apache/htdocs/images">
    Option FollowSymLinks Multiviews
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
```

   追記後、httpd**を再起動する。**

B サーバ設定等の不備

4.B.1 情報開示

4.B.1.1 公開不要の機能・ファイル・ディレクトリの存在

1. 危険度
   Medium：警告

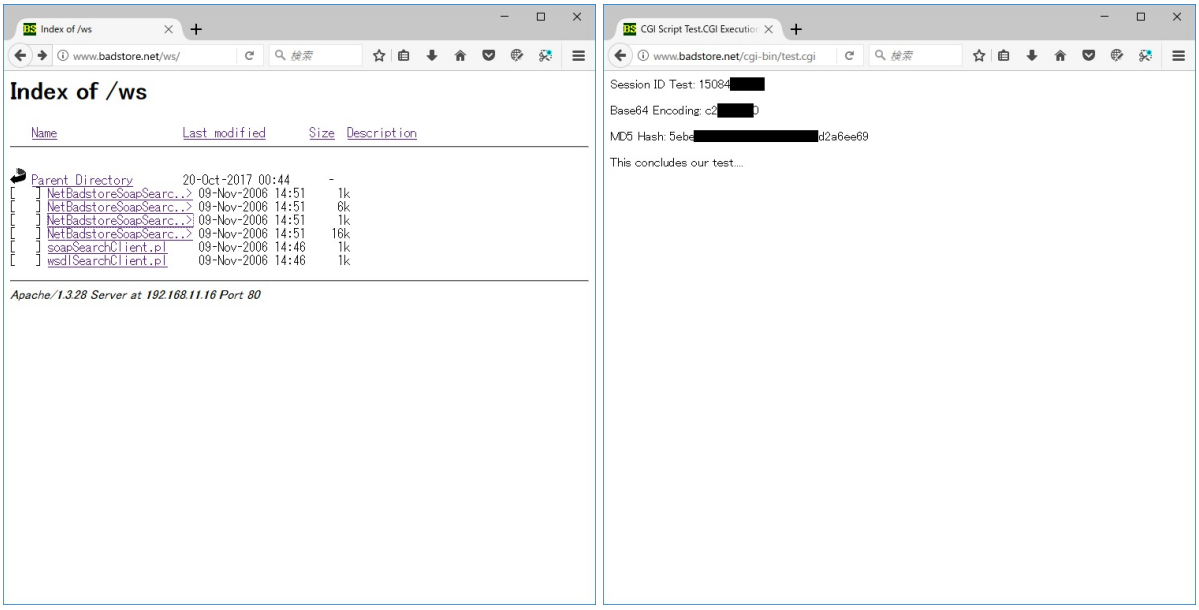
2. CWE
   CWE-200「情報開示」

3. 脆弱性発生状況

- 発生個所

No.	URL,パス	パラメータ
	1	http://www.badstore.net/ws/
	2	/usr/local/apache/cgi-bin/badstore.old
	3	/usr/local/apache/cgi-bin/test.cgi

- 解説
  古いバージョンのファイルや、接続テスト用にセッションID等を出力するファイル、データベースの検索に使用していると思われるjavaやperlのファイルを発見した。
  OSコマンドインジェクションやセッションの乗っ取りなどに悪用されるおそれがあるため、速やかな削除が必要である。



左：http://www.badstore.net/ws/
右：http://www.badstore.net/cgi-bin/test.cgi

機密扱い

4.B.1.2 エラーメッセージによる情報の露出

1. **危険度**
   High : **重要**

2. CWE
   CWE-209「エラーメッセージを通じた情報の露出」

3. **脆弱性発生状況**

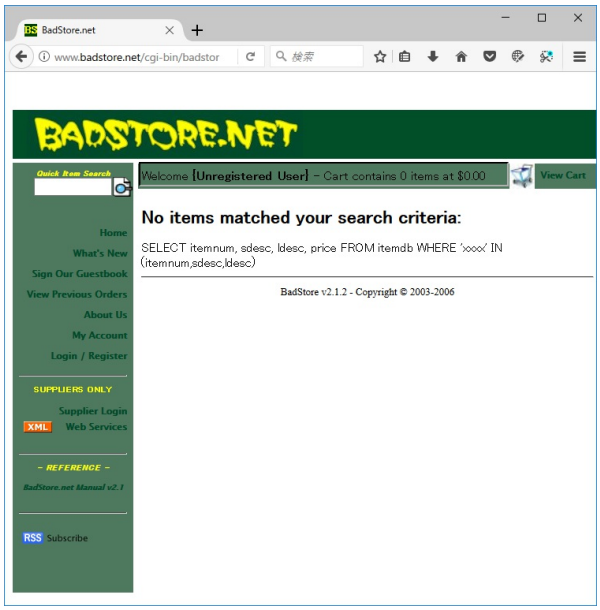
- **発生個所**

No.	URL,パス	パラメータ
1		http://www.badstore.net/cgi-bin/badstore.cgi?searchquery=&action=qsearch

- **解説**
  ・パターン1
  以下の値 (存在しない商品番号) をsearchqueryに入力し送信する。

```
xxxx
```

結果は以下の通りになる。



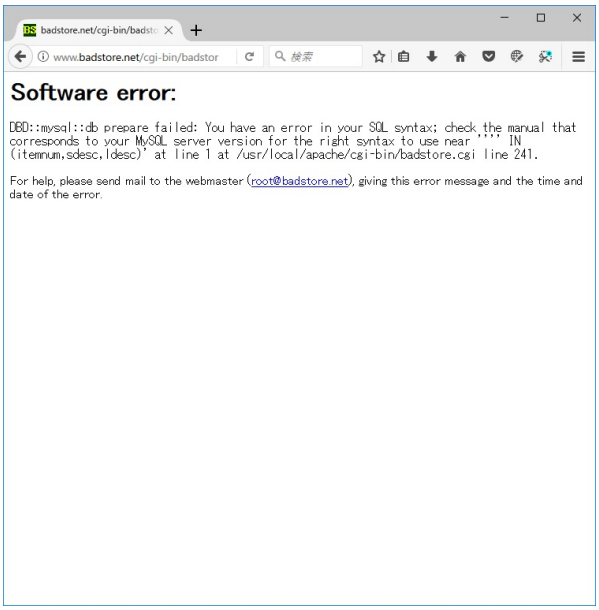
データベース中に商品が存在しない旨のエラーメッセージであるが、処理に使用していると思われるSQL文まで出力している。

機密扱い

・パターン2

コンマ (') をsearchqueryに入力し送信する。

結果は以下の通りになる。



入力文字列をそのままSQL文に組み込んでおり、不完全なSQL文が作られることでソフトウェアエラーが発生している。
また、適切にエラーをハンドリングできていないため、ファイルパスやエラー行の情報など、詳細なエラーまで
出力されている。

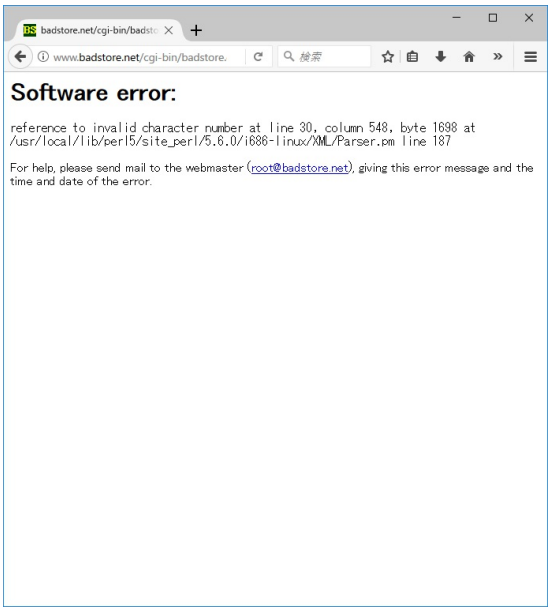
機密扱い

・パターン3

BurpSuiteのRepeaterなどを用いてsearchqueryに以下の値を入力し送信する。

```
%02 等の特殊文字
```

結果は以下の通りになる。



特殊文字を入力されることで、Parserで解釈不能になることによってソフトウェアエラーが発生している。
また、エラーのハンドリングが適切でないため、ファイルパス等の詳細な情報までエラーメッセージとして
出力されている。

いずれのパターンにおいてもエラーを適切にハンドルできておらず、詳細なメッセージを出力している。
こうして出力された内容がSQLインジェクションやOSインジェクションに用いられるおそれがある。

4. 本脆弱性への対策

   本脆弱性は、エラーを適切にハンドルしていないため、詳細部分を隠蔽できていないことにより発生している。
   エラーを検知した場合には、エラーが発生した旨のみをユーザに通知し、詳細なエラーはログに記録するなど
   外部から詳細を確認できないようにしたほうがよい。

4.B.2 設定・設計の不備

4.B.2.1 HTTPS不備

1. 危険度
   Medium：警告

2. CWE
   CWE-522「不十分な資格情報の保護」

3. 脆弱性発生状況

- 発生個所

No.	URL	パラメータ
1	http://www.badstore.net/cgi-bin/badstore.cgi?action=loginregister	
2	https://www.badstore.net/cgi-bin/badstore.cgi?action=supplierlogin	

- 解説

・No.1について

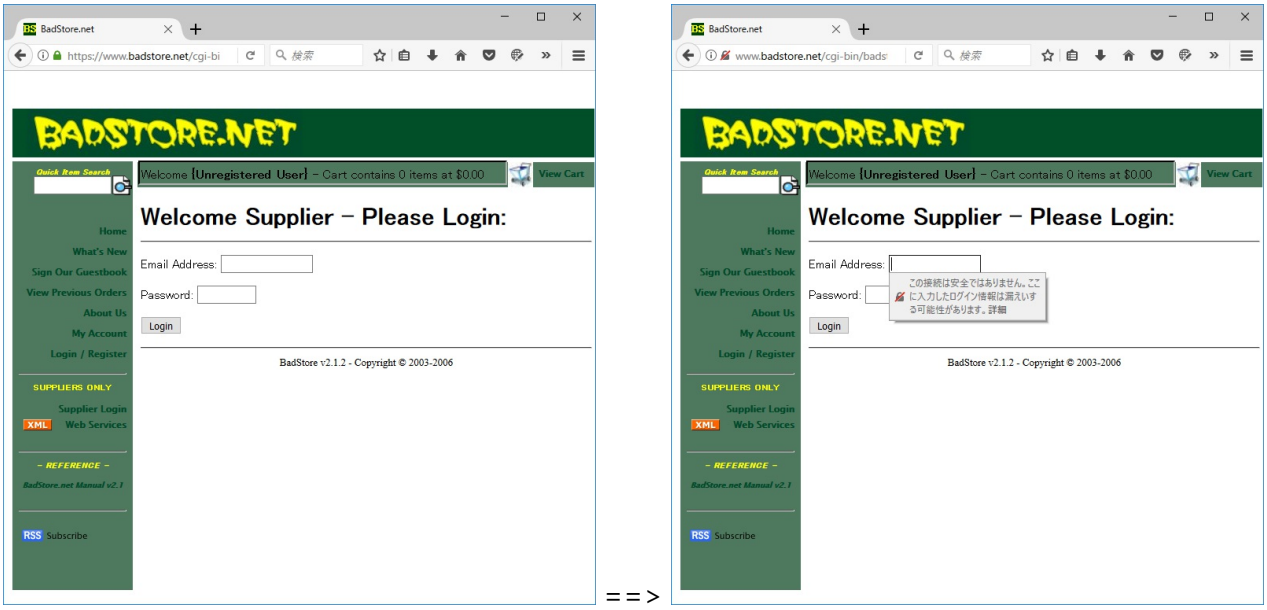
本ページは、ユーザログイン画面であるが、HTTPSによる保護がなされていないため、メールアドレスやパスワード等は全て平文での受け渡しとなる。

平文での通信のため、盗聴や改竄にあうおそれがある。また、大半のブラウザにおいて、図のような警告が出る。

機密扱い

・No.2について

本ページは、業者専用のログインページとなっている。
アクセスした際にはHTTPSによる保護が行われているが、URLの "https" を "http" に変えることができるため、
こちらも平文での通信が可能となっている。
フィッシングメール等によりhttpから始まるアドレスにアクセスさせられることで、メールアドレスやパスワードを
盗聴、改竄されるおそれがある。



= = >

左 : HTTPS , **右** : HTTP **で通信**

4. **本脆弱性への対策**

HTTPSでの通信が必要なページでは、HTTPSから始まるURLにリダイレクトさせるなど、HTTPでの通信をさせないようにする。

機密扱い

4.B.2.2 HTTPS利用時のCookieのSecure属性不備

1. 危険度
   Medium：警告

2. CWE
   CWE-614「HTTPSセッションにおける機微CookieのSecure属性不備」

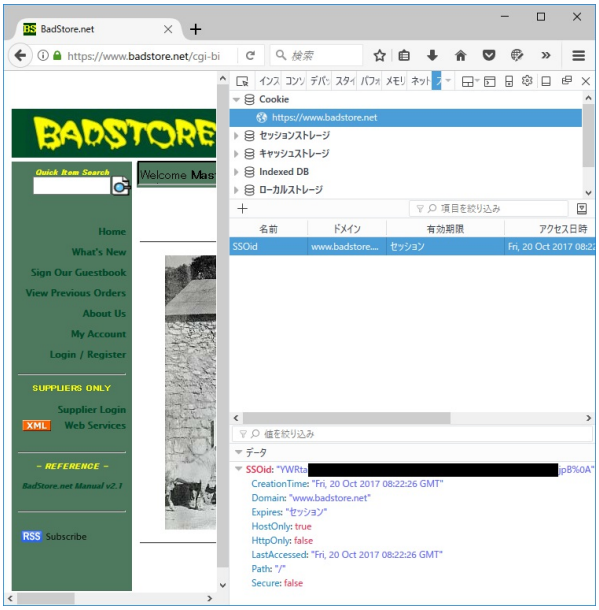
3. 脆弱性発生状況

- 発生個所

No.	URL	パラメータ
1	https://www.badstore.net/cgi-bin/badstore.cgi?action=loginresister	

- 解説

ユーザログイン画面のURLをhttpsにしてアクセスし、ログイン処理を行う。
F12キー等でCookie情報を閲覧すると、"Secure" の値が "false (偽)" となっている。



CookieのSecure属性が有効でない場合、罠サイト等によりHTTPS通信の途上でHTTP通信をさせられる攻撃にあった場合、リクエスト中のCookieを盗聴されるおそれがある。
盗聴されたCookieはセッションハイジャック (乗っ取り) に利用され、なりすまし等の被害を引き起こすおそれがある。

機密扱い

4. **本脆弱性への対策**

   badstore.cgiに以下のようにコードを書き足す。

```
### Set SSO Cookie ###
    ~
    print "Set-Cookie: $cartcookie; secure\n";
    ~                                ^^^^^^ "secure" を付け足す
```

4.B.2.3 脆弱なパスワードポリシ

1. 危険度
   High : 警告

2. CWE
   CWE-521「脆弱なパスワード要求」

3. 脆弱性発生状況

- 発生個所

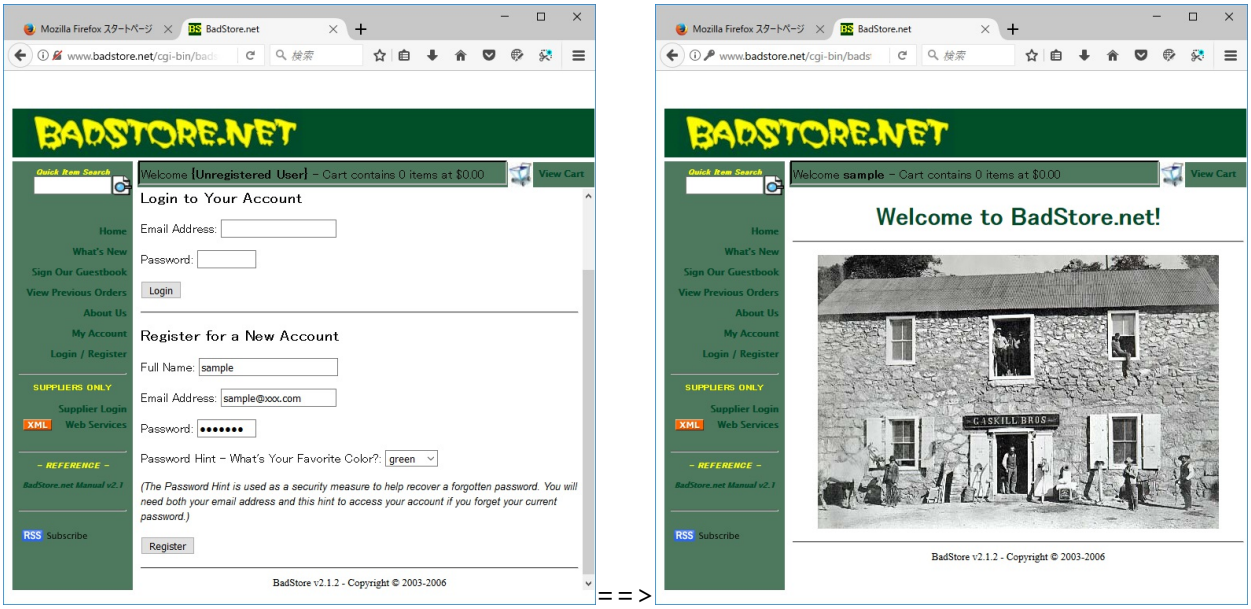
No.	URL	パラメータ
1	http://www.badstore.net/cgi-bin/badstore.cgi?action=loginregister	

- 解説

ユーザログイン画面からユーザ登録処理を行う。
ユーザ名、Eメールアドレスを入力したあと、パスワードを次のように入力し、登録ボタンをクリックする。

```
welcome
```

結果は以下のように、アカウントの作成に成功する。
脆弱なパスワードを使用している場合、パスワード辞書攻撃等で突破されやすくなり、不正ログインされてしまうおそれがある。



4. 本脆弱性への対策

パスワード登録時に文字種と文字列長をチェックし、英大文字、英小文字、数字を全て含めた8文字以上の文字列でない場合は再度パスワードを入力させるようにする。

なお、文字種と文字列長によるパスワードの個数は以下の表のようになる。

文字種	4	5	6	7	8
	数字単体	1万	10万	100万	1000万
	英小文字単体・英大文字単体	45万	1188万	3億	80億
	英小+数字・英大+数字	167万	6046万	21億	783億
	英数字	1477万	9.1億	568億	3.5兆

4.B.2.4 ログアウト不備

1. 危険度
   Medium：警告

2. CWE
   CWE-613「不十分なセッションの無効化」

3. 脆弱性発生状況

- 発生個所

No.	URL	パラメータ
1	https://www.badstore.net/ 以下	

- 解説
  全画面にログアウト用のリンクやボタンがなく、ブラウザを閉じる以外にログアウトする手段がない。
  そのためユーザはセッションIDを明示的に破棄することができない。また、一般ユーザのログインがHTTP
  で行われることにより、セッションIDを盗聴されるおそれがあり、セッションハイジャック等に悪用される
  おそれがある。

4. 本脆弱性への対策
   ログアウト機能を実装し、ログアウト処理の際にセッションIDをデータベースから削除するようにする。

4.B.2.5 過度な認証試行 (ブルートフォース) への対策不備

1. 危険度
   Medium：警告

2. CWE
   CWE-307「過度な認証試行への不適切な制限」

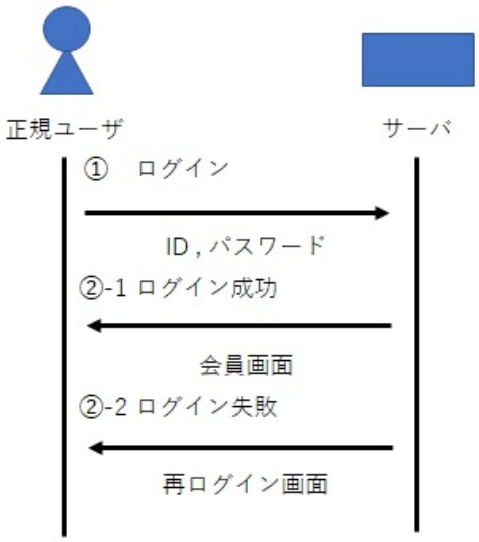
3. 脆弱性発生状況

- 発生個所

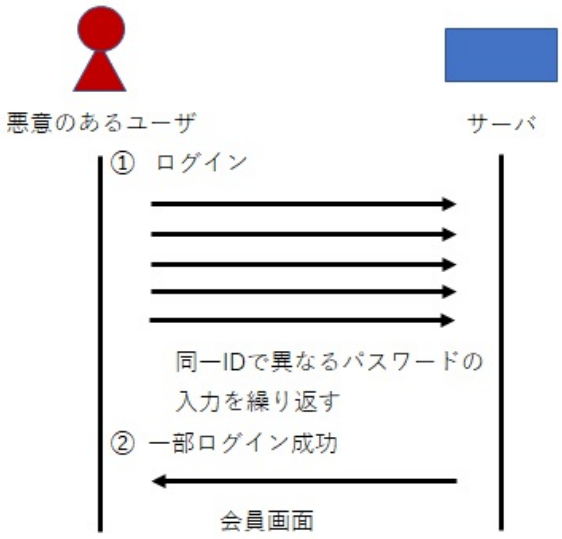
No.	URL	パラメータ
1	http://www.badstore.net/cgi-bin/badstore.cgi?action=loginregister	
2	https://www.badstore.net/cgi-bin/badstore.cgi?action=supplierlogin	

- 解説
  パスワードもしくはメールアドレスの入力を間違った場合、その場で再度入力させるようにするべきであるが、入力に失敗するたびに再度ログイン画面にアクセスする必要があり、非常に使い勝手が悪くなっている。
  また、10回以上メールアドレスやパスワードの入力を間違った場合は、ロックアウト処理 (一定期間ログインできない状態にすること) を行うべきであるが、本ページではそのような処理がなされていないため、
  ツール等でランダムに値を入力され続けた場合、ログインが成功するおそれがある。

正規のログイン



悪意のあるログイン



4. 本脆弱性への対策
   同一メールアドレスでのログイン試行が10回程度失敗した場合、当該アカウントを一定期間停止する処置をとる。
   ただし期間を長くしすぎると正規ユーザが困惑するおそれががあるため、長くても1日程度に留めること。

4.B.2.6 パスワードリセット不備

1. 危険度
   Medium：警告

2. CWE
   CWE-620「検証されないパスワードの変更」

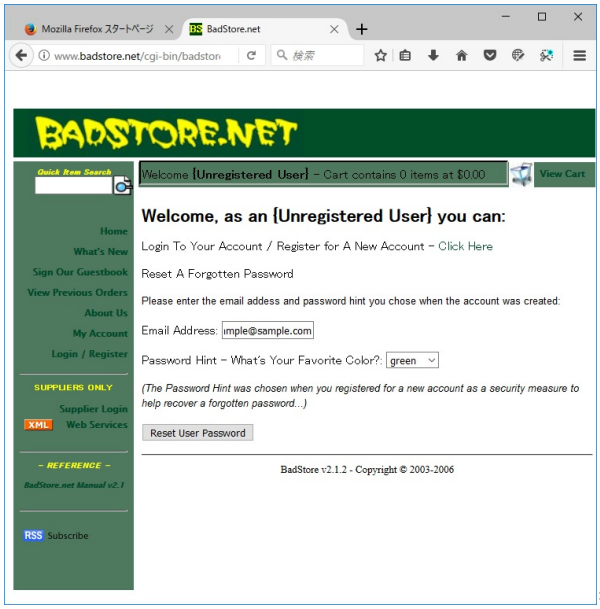
3. 脆弱性発生状況

- 発生個所

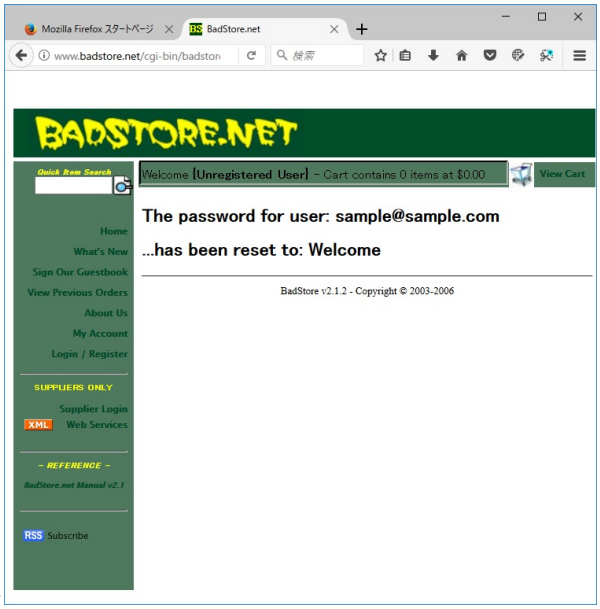
No.	URL	パラメータ
1	http://www.badstore.net/cgi-bin/badstore.cgi?action=myaccount	
2	http://www.badstore.net/cgi-bin/badstore.cgi?action=loginregister	

- 解説

No.1のページでパスワードの初期化を行うことができるが、パスワードは一律で"Welcome"という文字列に初期化される。No.2のページでログインを行う際には、この初期化されたパスワードがそのまま使用可能になっている。
このままパスワードを変更せずに利用を続けるユーザがいた場合、パスワードは一律で"Welcome"で初期化されているため、悪意あるユーザが他ユーザのメールアドレスを入手している場合、そのメールアドレスで不正にログインされるおそれがある。
また、秘密の質問の回答が選択式になっているため、同一メールアドレスで初期化を最大で選択肢の数だけ試行すれば、他アカウントのパスワードであっても初期化することができ、こちらも不正ログインされるおそれがある。



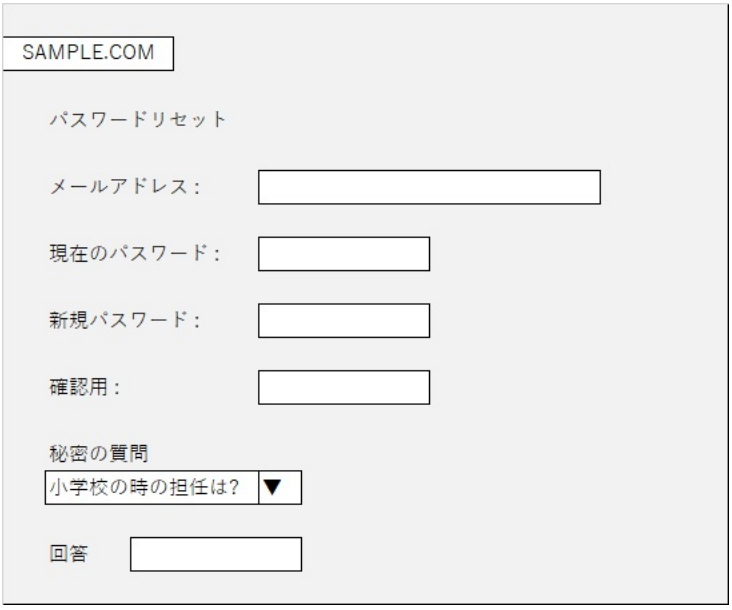
= = >



4. 本脆弱性への対策

パスワードをリセットした際には、必ずユーザにメールで通知すること (不正なリセットに対する対策)

パスワードリセットを行った後の初回ログイン時に、パスワード変更画面を出してユーザにパスワードを変更させる。なお、パスワード変更の際には、先述のパスワードポリシ強化策に則ったパスワードを入力させるよう、文字種や文字列長のチェックを行うこと。
また、初期化の際に指定する秘密の質問については、質問内容は選択式、回答はテキストでの入力にすること。



機密扱い

4.B.2.7 CookieのHttpOnly属性不備

1. **危険度**
   Medium：**警告**

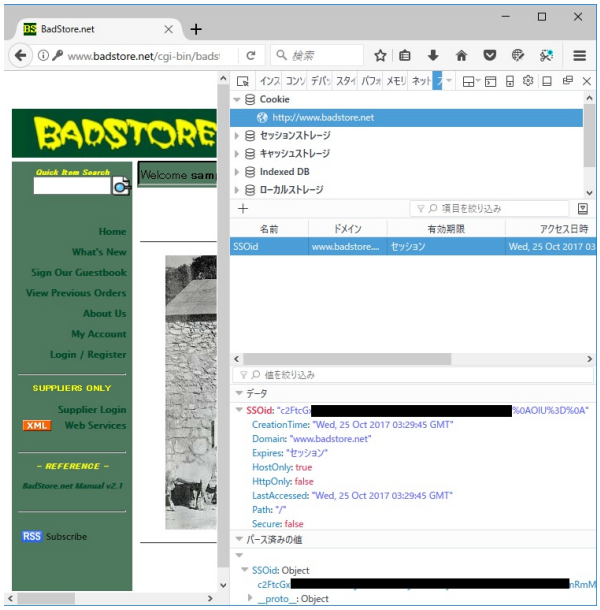
2. CWE
   CWE-1004「HttpOnlyタグのない機微Cookie」

3. **脆弱性発生状況**

- **発生個所**

No.	URL	パラメータ
1	http://www.badstore.net/ 以下	

- **解説**
  ログインページ (http://badstore.net/badstore.cgi?action=loginregister) からログイン後、ブラウザの開発者ツールをF12キーなどで開き、クッキーの内容を確認する。



「HttpOnly:」の項を見ると、値が「false (偽)」となっているため、HttpOnly属性が無効になっていることが分かる。
この属性は、JavaScriptからのクッキーの読出しを禁止するために付与される属性であり、この属性が無効になっていると、XSSによりセッションIDが盗まれるおそれがある。

機密扱い

4. **本脆弱性への対策**

   badstore.cgiに以下のようにコードを書き足す。

```
### Set SSO Cookie ###
    ~
    print "Set-Cookie: $cartcookie; HttpOnly\n";
    ~                                ^^^^^^^^  "HttpOnly" を付け足す
```

機密扱い

4.B.2.8 推測可能なセッションID

1. **危険度**
   Medium：**警告**

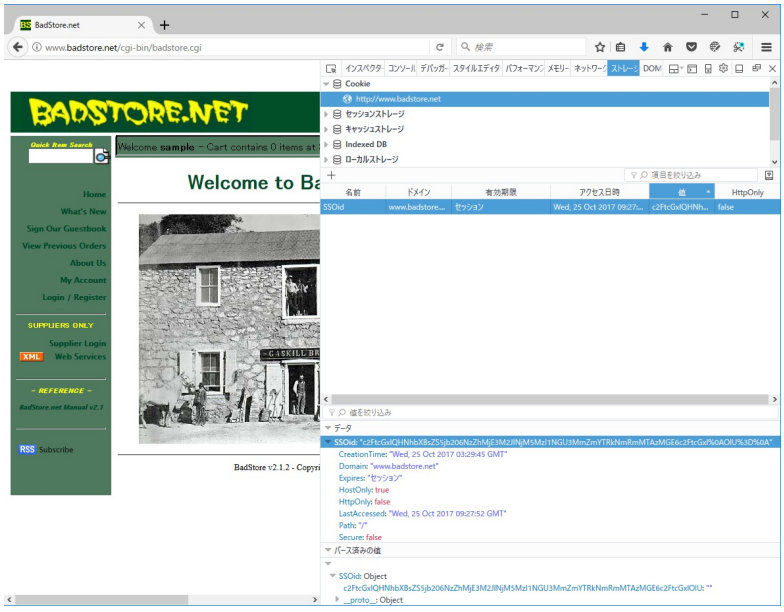
2. CWE
   CWE-334「狭小なランダム値域」

3. **脆弱性発生状況**

- **発生個所**

No.	URL	パラメータ
1	http://www.badstore.nte/ **以下**	

- **解説**
  ログイン後、ブラウザの開発者ツールをF12キーなどで開き、クッキーの内容を確認する。



「SSOid」の項を見るとクッキー値が表示されているが、この値を詳しく調べてみる。

```
c2FtcGxlQHNhbXBsZS5jb206NzZhMjE3M2JlNjM5MZl1NGU3MmZmYTRkNmRmMTAzMGE
62FtcGxl%0AOlU%3D%0A
```

機密扱い

一見すると複雑な文字列に見えるが、これを診断ツールのデコーダ (解読) 機能を用いて解読すると、

```
sample@sample.com:76a2173be6393254e72ffa4d6df1030a:sample:U

* "%0A" は改行、"%3D" は '=' を表すエスケープ表記であるため、それぞれ
  通常の文字に置き換えてデコードを行っている。
```

メールアドレスやユーザ名らしき文字列などが ':' 区切りで入っている文字列であると分かる。

また、別のユーザ (sample1) としてログイン後、同様にクッキーの内容を確認しデコードしてみると、

```
sample1@sample.com:51cb61ce9da718a931d5b0dbfe4240be:sample1:U
```

先のユーザ "sample" のものと同様の文字列を得ることができた。
':' で区切られた2番目の文字列を比較してみると、

```
sample  : 76a2173be6393254e72ffa4d6df1030a
sample1 : 51cb61ce9da718a931d5b0dbfe4240be
```

両者とも 0~9,a~f からなる固定長の文字列であることが分かる。
ユーザ "sample" のパスワードは "passwd" , "sample1" のパスワードは "okcorral" と設定しているため、
これらの文字列を、MD5というアルゴリズムを用いてハッシュ (暗号化) した値を求め、比較してみる。

```
"passwd"   -> 76a2173be6393254e72ffa4d6df1030a
sample     :  76a2173be6393254e72ffa4d6df1030a

"okcorral" -> 51cb61ce9da718a931d5b0dbfe4240be
sample1    :  51cb61ce9da718a931d5b0dbfe4240be
```

この結果から、SSOidに設定されているセッションIDが、メールアドレスやパスワードからなる文字列で
ことが判明した。

このように、第三者に推測されうる不適切な生成方法でセッションIDを生成していると、セッション
ハイジャック (セッションの乗っ取り) 等の被害に遭う可能性がある。

4. 本脆弱性への対策

セッションIDを生成する際に、安全性の高い乱数を生成する機構 (暗号論的疑似乱数生成器) を用いて生成された乱数を組み合わせて生成する。
また、ユーザIDやパスワードはセッションIDとは別途安全な方法 (HTTPSを用いて盗聴不能にするなど) で送信し、必ず内容をサーバ側でチェックするようにする。

5 注意事項

5.1 HTTPS通信について

アカウント情報等の重要な情報を、HTTP通信で送信してしまうと、情報が暗号化されないため、通信経路上で攻撃者に盗聴されるおそれがある。
そのため、重要な情報の通信を行う際には、HTTPS (HTTP over SSL/TLS)通信の利用を推奨する。

HTTPSの実装については以下の点に留意すること。

1. HTTP通信の制限
   HTTPS通信を行うページでは、必ずHTTPSで通信するように、HTTPからHTTPSへの自動リダイレクト等の設定を行うこと。
   攻撃者によりHTTPでの通信に誘導された場合に、データが盗聴される危険性を未然に防ぐことができる。

2. CookieのSecure属性
   HTTPS通信を利用するページ内でセッション(ログイン等の状態)の管理を行いたい場合には、Cookie(セッションを管理するプロトコル、もしくはブラウザに一時的に保存される情報)の「Secure」属性を有効にする。
   この設定を行い当該CookieをHTTPS通信以外で送信させないことで、セッションIDの盗聴を防ぐことができる。

3. セッションID
   HTTPページとHTTPSページにまたがってセッション管理を行う際には、前者にSecure属性を付与しないCookieを使用し、後者にSecure属性を付与したCookieを使用すること。
   (HTTP通信ではSecure属性付きCookieを利用できないため)

5.2 ブラウザ側の対応

現在、GoogleChrome,InternetExplorerをはじめとした主要ブラウザのほとんどでHTTPS通信が可能である。
なお、Chromeに関しては、10月17日リリースのバージョン62において、HTTPSを使用していない一部ページにアクセスすると、「安全でない(HTTPSでない)」旨の表示がURL欄に出現するようになった。

5.3 SSL/TLS

HTTPSにおける通信の暗号化を行っているプロトコルを、SSL (Secure Socket Layer) 、もしくは
TLS (Transport Layer Security) という。
TLSはSSLを元に開発されたプロトコルであり、最新バージョンは1.2となっている。
なお、SSLについてはバージョン3が2014年まで使われていたが、「POODLE」という仕様上の脆弱性が発見されたため、現在はほとんどのサーバがSSLからTLSへと移行している。
また、TLSについては、現在バージョン1.3がIETF (Internet Engineering Task Force) にて検討されている。

付録

A 共通脆弱性評価システム (CVSSv3 : Common Vulnerability Scoring System version 3)

本報告書においては、CVSSv3による脆弱性の評価値、および脆弱性のレベル区分を元に危険度を評価している。

以下の表はIPA「共通脆弱性評価システムCVSS v3概説」より引用

深刻度	スコア
緊急	9.0~10.0
重要	7.0~8.9
警告	4.0~6.9
注意	0.1~3.9
なし	0

スコアは、攻撃の容易さ (攻撃容易性)、システムが受ける影響 (影響度)、影響の及ぶ範囲 (スコープ)などを基準と比較した値を以下の数式にかけて算出する。

スコープ変更 (影響が直接関連のないアプリケーションや機能などに及ぶ) なし

```
スコア = ((影響度 + 攻撃容易性),10 のうち最小値) を切り上げ
```

スコープ変更あり

```
スコア = ((1.08*(影響度 + 攻撃容易性), 10 のうち最小値) を切り上げ
```

B 参考文献

著者,タイトル	URL/出版元,発行年
上野 宣 「Webセキュリティ担当者のための 脆弱性診断スタートガイド」	翔泳社 , 2016
徳丸 浩 「体系的に学ぶ 安全なWebアプリケーションの作り方」	ソフトバンククリエイティブ , 2011
IPA 「共通脆弱性評価システム(CVSSv3) 概説」	https://www.ipa.go.jp /security/vuln/CVSSv3.html , 2015
上野 宣 「Webアプリケーション 脆弱性診断ガイドライン(第1.0版)」	https://github.com/ueno1000 /WebAppPentestGuidelines/blob/master /WebAppPentestGuidelines.pdf , 2017
Symantec 「ウェブアプリケーション 脆弱性診断報告書」	https://www.symantec.com/content/ja/jp /enterprise/other_resources /webapp_or_report_sample.pdf , 不詳
Computer Security Technology Limited 「Web Application Security Assessment Report」	https://www.cstl.com/CST/Penetration-Test /CST-Web-Application-Testing-Report.pdf , 2012

C 参考ページ

タイトル	URL
JVN iPedia 脆弱性対策情報データベース	http://jvndb.jvn.jp/
CWE Common Weakness Enumeration	https://cwe.mitre.org/index.html
Weblio 英和辞典・和英辞典	http://ejje.weblio.jp/
英辞郎 on the WEB:アルク	http://eow.alc.co.jp/
とほほのCookie入門	http://www.tohoho-web.com/wwwcook.htm
Markdown記法 チートシート - Qiita	https://qiita.com/Qiita/items/c686397e4a0f4f11683d

機密扱い

D 使用ツール

作成者	名称	URL
OWASP	OWASP Zed Attack Proxy	https://github.com/zaproxy/zaproxy/releases/download/2.6.0/ZAP_2_6_0_windows.exe
PortSwigger Web Security	Burp Suite	https://portswigger.net/burp/releases/download?product=free&version=1.7.27&type=windowsx64
不詳	BadStore.net	**テキスト記載のため省略**