IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

JPCERT/CC

プレスリリース
2005 年 1 月 25 日
独立行政法人 情報処理推進機構
有限責任中間法人 JPCERT コーディネーションセンター

ソフトウエア等の脆弱性関連情報に関する届出状況 [2004 年第 4 四半期（10 月～12 月）]

独立行政法人 情報処理推進機構（略称：IPA）及び有限責任中間法人 JPCERT コーディネーションセンター（略称：JPCERT/CC）は、2004 年第 4 四半期（10 月～12 月）の脆弱性関連情報届出状況を、以下のとおり、とりまとめました。

経済産業省告示「ソフトウエア等脆弱性関連情報取扱基準」（平成 16 年経済産業省告示 第 235 号）に基づき、IPA は脆弱性関連情報の届出を受け付け、JPCERT/CC は日本国内の製品開発者などの関連組織との調整を行いました。2004 年第 4 四半期（10 月～12 月）の脆弱性関連情報の届出状況は以下のとおりです。

- ソフトウエア製品の脆弱性関連情報
  届出：13 件（届出受付開始からの累計は 32 件）
  脆弱性公表：8 件（このうち 1 件は、複数製品開発者に影響あるもの）（届出開始からの累計は 11 件）
- ウェブアプリケーションの脆弱性関連情報
  届出：67 件（届出受付開始からの累計は 140 件）
  修正完了：27 件（このうち 17 件は、IPA が修正確認作業を実施）（届出開始からの累計は 37 件）

1. 届出件数

2004 年 10 月 1 日から 12 月 31 日までの IPA への脆弱性関連情報の届出件数は、80 件（ソフトウエア製品に関するもの 13 件、ウェブアプリケーションに関するもの 67 件）であり、届出受付開始（2004 年 7 月 8 日）からの総計は 172 件です。四半期毎の届出状況を表 1-1 に示します。

表 1-1 脆弱性関連情報の期別届出件数の推移

	2004 年 第 3 四半期	2004 年 第 4 四半期	合計
ソフトウエア製品に関する届出	19	13	32
ウェブアプリケーションに関する届出	73	67	140
合計	92	80	172

（1） ソフトウエア製品の脆弱性

ソフトウエア製品の脆弱性については、2004 年第 4 四半期は、新たに公表した脆弱性が 8 件（累計 11 件）、製品開発者により脆弱性ではないと判断されたものが 2 件（累計 3 件）あります。また、問題が発見者のコンピュータ環境によるものであり、脆弱性でないことから、告示で定める届出の対象外としたものが 1 件（累計 4 件）あります。

ソフトウエア製品の脆弱性関連情報の届出の取扱い状況を図 1-1 に示します。

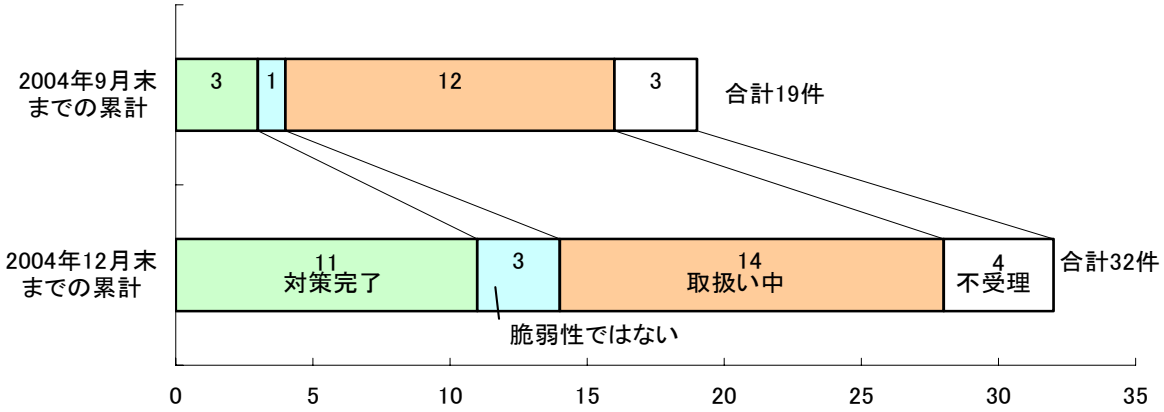

図 1-1 ソフトウエア製品脆弱性関連情報の届出の取扱い状況

(2) ウェブアプリケーションの脆弱性

ウェブアプリケーションの脆弱性については、2004 年第 4 四半期は、新たに修正を完了したものが 27 件(累計 37 件)、ウェブサイト運営者により脆弱性はないと判断されたものが 6 件(累計 11 件)、修正ではなく当該ページの削除により対策されたものが 7 件(累計 7 件)あります。このほか、ウェブサイト運営者と連絡が取れず、取扱いができないものが 10 件(累計 26 件)となりました。

ウェブアプリケーションの脆弱性関連情報の届出の取扱い状況を図 1-2 に示します。

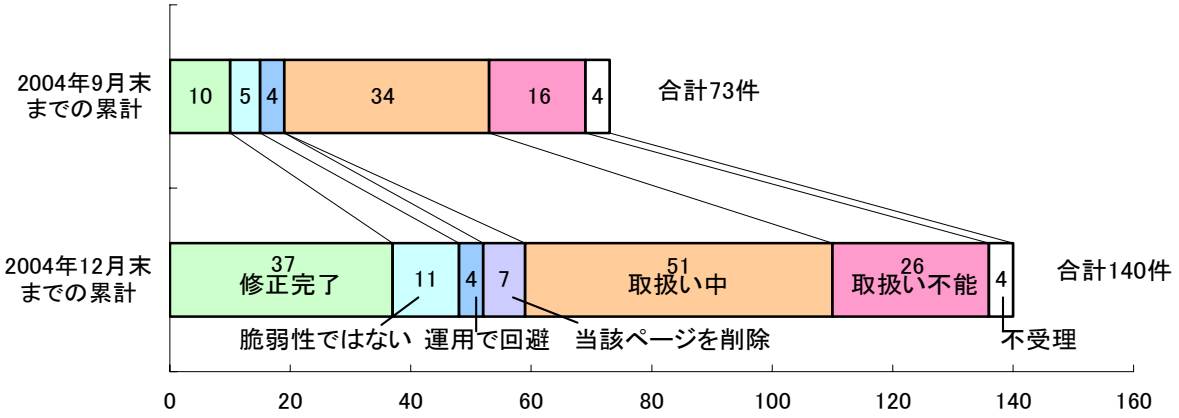

図 1-2 ウェブアプリケーション脆弱性関連情報の届出の取扱い状況

2. ソフトウエア製品の脆弱性関連情報の届出

JPCERT/CC が日本国内の製品開発者と調整を行い、新たに公表した脆弱性については、2004 年第 4 四半期には、23 件となりました。このうち、IPA への届出により手続きを開始した脆弱性は 8 件でした。他の 15 件は、海外 CSIRT[1]から提供された脆弱性情報について、JPCERT/CC が日本国内の製品開発者と調整を行ったものです。

製品開発者の対応状況は、IPA と JPCERT/CC が共同運営している脆弱性対策情報ポータルサイト

[1] Computer Security Incident Response Team の略であり、コンピュータセキュリティに関するインシデント(事故)への対応や調整、サポートをするチームのことです。

JP Vendor status Notes（JVN）において公開しています（URL： http://jvn.jp/ ）。

表 2-1 に、IPA が届出を受け、2004 年第 4 四半期に公表した脆弱性を示します。複数の製品開発者のソフトウエア製品に影響があるものは、DNS[2]キャッシュサーバのリソース消費の 1 件であり、JPCERT/CC が複数の製品開発者に対して調整を行いました。特定製品に関する届出の 7 件のうち、電子メールクライアントソフトウエアの S/MIME（Secure/Multipurpose Internet Mail Extensions）署名検証機能に関する問題が 4 件、検索システムに関するものが 1 件、グループウェアに関するものが 1 件、情報家電のアクセス制御機能に関するものが 1 件ありました。

S/MIME は X.509[3]証明書とデジタル署名を利用することで、電子メールにおけるメールの送信者とメッセージの認証や暗号化、改ざん防止などのセキュリティ機能を提供します。利用者は、S/MIME 機能を持つ電子メールクライアントソフトウエアを使用することで、電子メールにおけるセキュリティを強化できます。現時点では、S/MIME は、一般インターネットユーザにはまだ普及していませんが、企業側のフィッシング詐欺対策として導入されている例もあり、今後、普及が見込まれます。しかしながら、届出にあったような署名検証機能に問題があれば、セキュリティ機能が生かされず、逆に、信頼すべきでないメールを信頼させてしまう危険性があります。

表 2-1　2004 年第 4 四半期に公表された脆弱性

	脆弱性	未対策状態でのセキュリティ上の問題点	JVN 公表日
1	HDD&DVD ビデオレコーダーの認証における脆弱性	HDD&DVD ビデオレコーダーへ認証なしでアクセスできるため、HDD&DVD ビデオレコーダーを外部ネットワークへ接続している場合、オープンプロキシ[4]サーバとして動作し、不正アクセスや嫌がらせなどの踏み台に利用される可能性があります。	2004 年 10 月 15 日
2	DNS キャッシュサーバの TCP SYN_SENT 状態によるリソース消費	インターネット上の住所である IP アドレスとホスト名の名前解決を行う DNS サーバの構成要素の一つである DNS キャッシュサーバにおいて、設定や構成によっては、通信路を確立しようとして待っている状態（SYN_SENT 状態）が複数発生し、このために CPU リソースを多く消費し、DNS キャッシュサーバの反応が悪くなります。	2004 年 10 月 20 日

[2] DNS（Domain Name System）は、インターネット上の住所である IP アドレスとホスト名（例：www.ipa.go.jp）を変換するための仕組みです。

[3] X.509 は、公開鍵を利用して暗号化を行う際の証明書（公開鍵証明書）の規格です。第 3 者機関である認証局が、利用者の情報と公開鍵の対を、認証局の秘密鍵によりデジタル署名した「公開鍵証明書」を発行することで、公開鍵とその所有者を証明します。公開鍵証明書を検証する側では公開鍵証明書の認証局による署名を検証して、公開鍵が正当なものであるかどうか確認することができます。

[4] プロキシは代理という意味であり、インターネットとの接続の際に、セキュリティ確保や Web アクセスの高速化のために設置されるものを指します。通常、内部から外部へのアクセスの際に利用されますが、外部の第三者が利用可能なサーバとして提供されている場合や、意図せず外部から利用可能な状態になっている場合、オープンプロキシと呼ばれ、不正アクセスの際に身元を隠すのに利用されます。

	脆弱性	未対策状態でのセキュリティ上の問題点	JVN 公表日
3	鶴亀メールの S/MIME 署名検証における脆弱性	メールクライアントソフトウエアである「鶴亀メール」の S/MIME 署名検証において、証明書パスおよび証明書の有効期限が検証されない、という問題があります。そのため、メールアドレスを詐称した証明書を使って S/MIME 署名されたメールを受信した際、受信者が詐称メールであることに気づかない可能性があります。	2004 年 10 月 28 日
4	desknet's におけるクロスサイト・スクリプティングの脆弱性	ウェブグループウェアである「desknet's」において、ユーザが悪意のあるスクリプト[5]を含んだ HTML メールやインフォメーション（掲示板に相当する機能）を参照した場合、スクリプトが実行され、Cookie[6]情報（設定によっては ID やパスワードを含む）の漏洩によるなりすましや個人情報の漏洩などが発生する可能性があります。	2004 年 11 月 16 日 （JVN#F88C2C13 の追加情報として公表）
5	Becky! Internet Mail の S/MIME 署名検証における脆弱性	メールクライアントソフトウエアである「Becky! Internet Mail」の S/MIME 署名検証において、証明書パスおよび証明書の有効期限が検証されないという問題があります。そのため、メールアドレスを詐称する証明書を使って S/MIME 署名されたメールを受信した際、受信者が詐称メールであることに気づかない可能性があります。	2004 年 11 月 17 日
6	Shuriken Pro3 の S/MIME 署名検証における脆弱性	メールクライアントソフトウエアである「Shuriken Pro3」の S/MIME 署名検証において、正式な電子署名が施されていれば、From アドレスが署名者アドレスと異なっていても警告を発しないという問題があります。そのため、受信者が詐称メールであることに気づかない可能性があります。	2004 年 11 月 19 日
7	namazu におけるクロスサイト・スクリプティングの脆弱性	日本語全文検索を行うシステムである「namazu」において、検索文字列に、特定の文字を指定することにより、クロスサイト・スクリプティング対策の処理が正しく行われない問題があります。そのため、namazu を使用して検索処理を実現しているウェブサイトにおいて、ページ内容のすり替えや、Cookie 情報の奪取等による個人情報漏洩が発生する可能性があります。	2004 年 12 月 15 日
8	Shuriken Pro3 の S/MIME 署名検証における脆弱性	メールクライアントソフトウエアである「Shuriken Pro3」の S/MIME 署名検証において、電子署名中の証明書の真偽が確認されない、という脆弱性が確認されています。そのため、偽の証明書で電子署名が施されたメールを受信しても、受信者が詐称メールであることに気づかない可能性があります。	2004 年 12 月 21 日

この他に、2005 年 1 月以降に公表されたものとして、LDAP(Lightweight Directory Access Protocol)を実装したソフトウエア製品の更新処理において、入力される文字列の長さを十分に確認していないためにバッファオーバーフローが発生するという問題がありました。

[5] プログラムの一種です。

[6] ウェブサーバが発行し、ウェブブラウザに預ける小さなテキストデータです。いったん Cookie を預かったウェブブラウザは、それを発行したウェブサーバのコンテンツにアクセスする際、預かった Cookie のデータをコンテンツの要求に必ず含めるようになります。ウェブアプリケーションが、どのユーザからのアクセスかを追跡するために Cookie が使われることがあります。その場合、Cookie にはログインの受付番号（場合によってはパスワードそのもの）が格納されるため、Cookie 情報が漏洩するとログイン状態を乗っ取られる（セッションハイジャック攻撃に遭う）、またパスワードが漏洩する危険性があります。

ソフトウエア製品に関する脆弱性関連情報の届出件数の製品種類別の内訳を図 2-1 に示します。

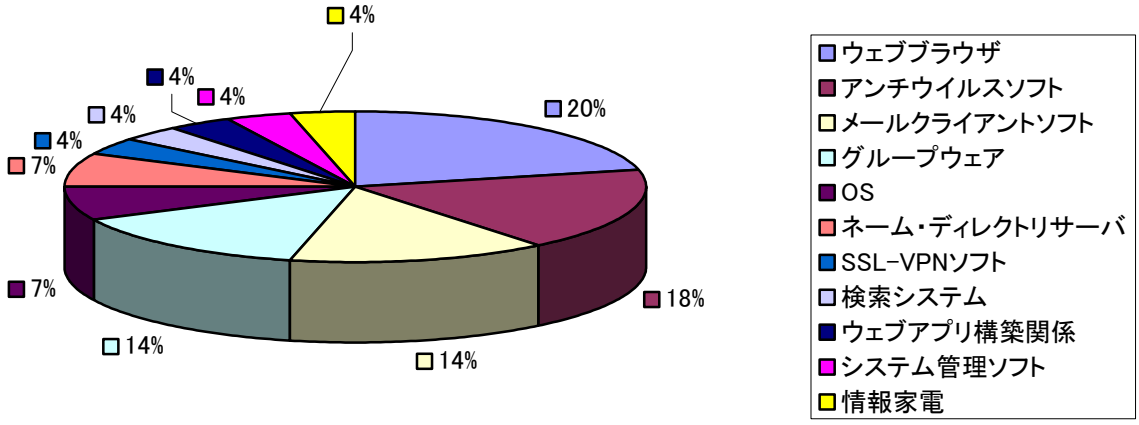

図 2-1　ソフトウエア製品種類別の届出件数の内訳（届出開始から 2004 年 12 月末まで）

3.　ウェブアプリケーションの脆弱性関連情報の届出

ウェブアプリケーションの脆弱性については、2004 年第 4 四半期は、新たに、修正が完了したものが 27 件、ウェブサイト運営者により脆弱性が存在しないと判断されたものが 6 件、修正でなく当該ページの削除により対策されたものが 7 件、合計 40 件の届出の取扱いを終了しました。これにより、届出受付開始時からの、取扱いを終了した届出の累計は 140 件中 59 件になりました。このほか、10 件がウェブサイト運営者と連絡が取れず、取扱いができない状態（取扱い不能）になりました。

2004 年第 4 四半期の届出の特徴としては、システムインテグレータが導入したパッケージソフトウエアに問題があり、複数のウェブサイトに同じ脆弱性が発見、報告された事例が複数ありました。

また、新しい攻撃手法として知られている「HTTP レスポンス分割（HTTP Response Splitting）」に関する届出が数件ありました。これは、悪意ある要求をサーバに送信することで、サーバからの応答を分割させ、応答内容を差し替えるというものです。ユーザが、このような要求をサーバに送信するように仕掛けられた罠のリンクをクリックすると、分割され、差し替えられた形の応答を受信することになります。この問題により、たとえば、プロキシサーバのキャッシュやブラウザのキャッシュの情報が、サーバが本来公開しているものとは別の情報にすり替えられてしまい、その結果、それを見た利用者がフィッシング詐欺の被害に遭う危険性があります。

届出受付開始から 2004 年 12 月末までの届出について、修正された脆弱性の種類別件数および修正に要した日数を表 3-1 に示します。

表 3-1　脆弱性種類別の修正件数および修正に要した日数[7]

脆弱性	件数	修正に要した日数
クロスサイト・スクリプティング（第三者へのスクリプト実行）	25	平均 11 日 （最短：当日、最長：40 日）
パス名パラメータの未チェック（フォーム入力値の操作）	5	平均 13 日 （最短：当日、最長：42 日）
ファイルの誤った公開	2	1 日、21 日
ディレクトリ・トラバーサル（許可されていない範囲へのアクセス）	1	3 日
HTTP レスポンス分割（ウェブサーバ応答内容のすり替え）	1	7 日
SQL インジェクション（データベースへの不正な入力）	1	39 日
セッション管理の不備	1	97 日
メールの第三者中継	1	159 日

届出受付開始から 2004 年 12 月末までに届出られた脆弱性の、種類別内訳を図 3-1 に、脅威別内訳を図 3-2 に示します。

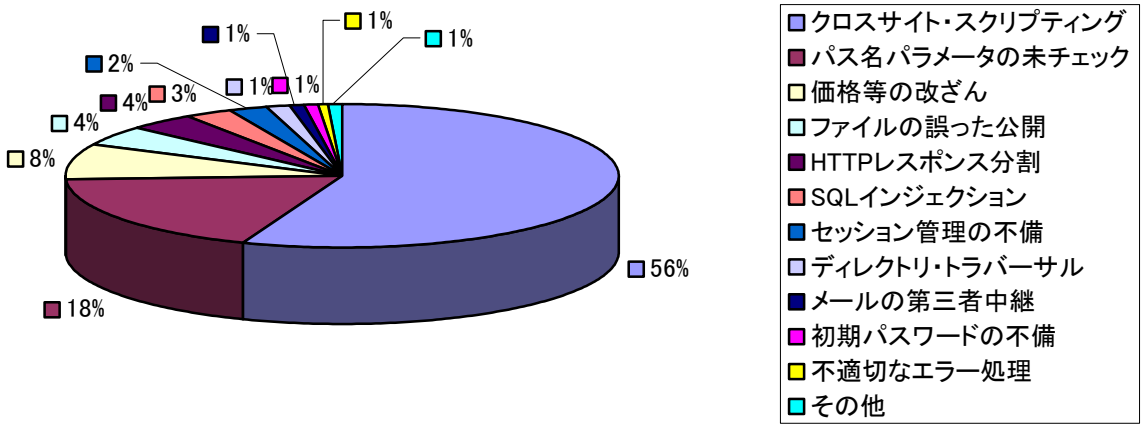

図 3-1　ウェブアプリケーションの脆弱性種類別内訳（届出開始から 2004 年 12 月末まで）

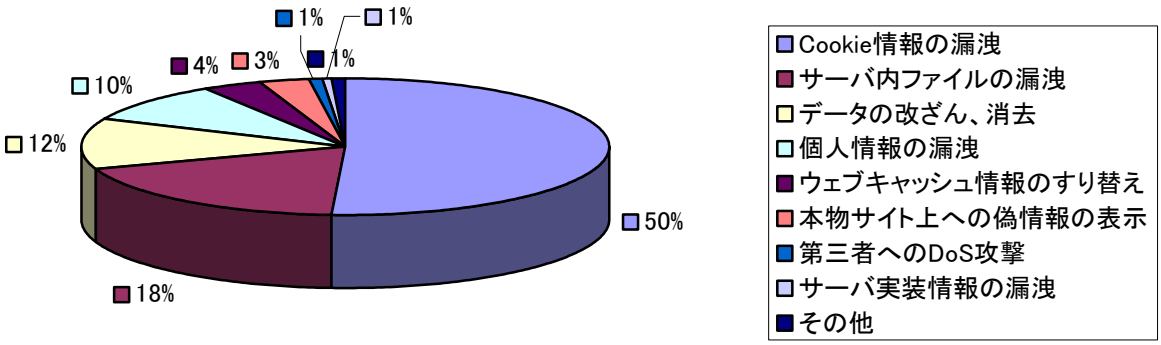

図 3-2　ウェブアプリケーションの脆弱性脅威別内訳（届出開始から 2004 年 12 月末まで）

[7] それぞれの脆弱性の詳しい説明については付録を参照してください。

脆弱性の種類は、依然として「クロスサイト・スクリプティング」が最多となっており、発見者が届出時に想定した脅威別でも、この脆弱性により起こりうる「Cookie 情報の漏洩」が最多となっています。「クロスサイト・スクリプティング」は、Cookie を使用していないサイトであっても、「本物サイト上への偽情報の表示」の攻撃にも利用されうるため、フィッシング詐欺に悪用される可能性があることに注意が必要です。さらに、掲示板等に悪意のあるスクリプトが混入されることによるユーザからの信頼の低下といった影響もありますので注意が必要です。

4. 皆様へのお願い

脆弱性の修正をより強く促進していくため、関係者の皆様に、以下のとおり、ご協力をお願いします。

- ウェブサイト運営者の皆様へ

  クロスサイト・スクリプティング脆弱性に関する届出が依然として多くあります。この脆弱性がフィッシング詐欺に悪用される事例も出てきています。運営しているウェブサイトにおいて、入力フォーム等へのユーザからの入力に対してスクリプトや命令が含まれていないか、また、想定外のパス名が与えられる可能性がないかを十分にチェックし、適切なエスケープ処理を施していることを確認してください。

- 製品開発者の皆様へ

  JPCERT/CC は、ソフトウエア製品の脆弱性関連情報について、整備している「製品開発者リスト」に基づき、一般公表日の調整等を行います。迅速な調整を進められるよう、「製品開発者リスト」への登録にご協力ください（URL：http://www.jpcert.or.jp/）。また、対策情報の公表の際には、利用者が脆弱性を認識し、必要な対策が取れるよう、適切な情報を伝えるようにしてください。

- 脆弱性を発見された皆様へ

  脆弱性を発見した場合は、匿名掲示板などに書き込むことは避け、この届出制度を利用してください。また、届け出た情報は、その脆弱性に関する情報が悪意のある者に利用されることを避けるため、開発者等により対策情報が公表されるまで、公表しないよう、お願いします。

- 一般インターネットユーザの皆様へ

  フィッシング詐欺において、ウェブブラウザの脆弱性を悪用するなど、ウェブサイトの偽装方法の手口が巧妙になってきています。JVN や IPA、JPCERT/CC など、脆弱性情報や対策情報を公表しているウェブサイトを参照し、パッチの適用など、自発的なセキュリティ対策を日ごろから心がけてください。

■ お問い合わせ先
独立行政法人 情報処理推進機構 セキュリティセンター
Tel:03-5978-7527 Fax:03-5978-7518
E-mail: vuln-inq@ipa.go.jp

有限責任中間法人 JPCERTコーディネーションセンター
Tel:03-3518-4600
E-mail: office@jpcert.or.jp

付表 ウェブアプリケーション脆弱性の分類

脆弱性の種類	深刻度	説明	届出において想定された脅威
ファイルの誤った公開	高	一般に公開すべきでないファイルが公開されており、自由に閲覧できる状態になっている	サーバ内ファイルの漏洩 個人情報の漏洩
パス名パラメータの未チェック	高	ユーザからの入力を処理する際のパラメータとして指定されているファイル名を、ユーザが変更し、ウェブサーバ上の任意のディレクトリのファイルを指定できてしまう	サーバ内ファイルの漏洩
ディレクトリ･トラバーサル	高	ウェブサーバ上のディレクトリのアクセス権を超えて、本来許可されている範囲外のディレクトリにアクセスできる	サーバ内ファイルの漏洩
セッション管理の不備	高	セッション管理に、推測可能な情報を使用しているため、他のユーザの情報が容易に推測でき、他のユーザになりすまして、サービスを利用することができる	個人情報の漏洩 権限の無い者によるサービス利用
SQL コマンド･インジェクション	高	入力フォームへ SQL コマンド（データベースへの命令）を入力し、データベース内の情報の閲覧、更新、削除などができる	サーバ内ファイルの漏洩 データの改ざん、消去
クロスサイト･スクリプティング	中	ユーザの Cookie 情報を知らないうちに転送させたり、偽の情報を表示させたりするような罠のリンクをユーザにクリックさせ、個人情報等を盗むことができる	Cookie 情報の漏洩 本物サイト上への偽情報の表示
HTTP レスポンス分割	中	攻撃者がユーザに対し、悪意のある要求をウェブサーバに送信するように仕向けることで、ウェブサーバからの応答を分割させて応答内容をすり替え、ユーザに対して偽のページを表示させることができる	ウェブキャッシュ情報のすり替え
メールの第三者中継	低	他人のメールサーバを用いることで、自分の身元を隠してメールを送信することができる	第三者への DoS 攻撃
初期パスワードの不備	低	認証に使用するために、管理者が発行したユーザ ID や初期パスワードが、単純であり推測が容易である	個人情報の漏洩
不適切なエラー処理	低	表示されるエラーの内容に、一般ユーザには不要な情報が含まれているため、ウェブサイトの実装の詳細や、ファイルやユーザの有無がわかる	サーバ実装情報の開示
価格等の改ざん	低	ショッピングサイトにおいて、価格情報等が利用者側で書き換えられる	データの改ざん