2023/04/3

A02:Cryptographic Failures

菅田大輔

目次

- A04:Cryptographic failuresとは
- 対策
- OWASP juice shopにおける実践
- Nested Easter egg
- エンコードの見分け方

A04:Cryptographic failuresとは

- 概要

暗号化技術を不適切に使用、または使用しないことにより、重要な情報の漏洩を引き起こすこと（かつてのカテゴリ名は「機微な情報の露出」だった）

対応するCWE数	最大発生率	平均発生率	加重平均（攻撃の難易度）	加重平均（攻撃による影響）	最大網羅率	平均網羅率
29	46.44%	4.49%	7.29	6.81	79.33%	34.85%

用語集

・CWEs Mapped(カテゴリにあたるCWEの数): Top10チームがカテゴリー にマッピングしたCWEの数です。

・Incidence Rate(発生率): 発生率とは、当年に機関によってテストされた 母集団のうち、カテゴリにマップされたCWEに脆弱なアプリケーションの 割合を示します。

・(Testing) Coverage(テスト)網羅範囲: カテゴリにマップされたCWEに対 して、機関がテストできたアプリケーションの範囲。

・Weighted Exploit(重み付けされた悪用性): CVEに割り当てられている CVSSv2およびCVSSv3スコアの悪用性サブスコアを正規化し、10ptのス ケールで表示したものです。

・Weighted Impact(重み付けされた影響度): CVEに割り当てられている CVSSv2およびCVSSv3スコアの影響サブスコアを正規化し、10ptのスケー ルで表示したものです。

A04:Cryptographic failuresとは

- 具体例

1. 古いまたは脆弱な暗号アルゴリズムやプロトコルを初期設定のまま、または古いコードで使っていないか。(→Nested Easteregg)
2. MD5やSHA1といった非推奨のハッシュ関数が使用されていないか。また暗号学的ハッシュ関数が必要とされる場合において、暗号学的でないハッシュ関数が使用されていないか。
3. どんなデータであれ平文で送信していないか。これは、HTTP、SMTP、FTPといったSTARTTLSのようなTLS upgradesのプロトコルを使っている場合に該当する。外部インターネットへのトラフィックは危険である。また、ロードバランサー、Webサーバー、バックエンドシステムなどの内部の通信もすべて確認すること。

用語

- MD5、SHA-1

MD5（Message Digest 5）、SHA-1は、データのメッセージダイジェストを生成するためのハッシュ関数の一種。つまり、任意の長さのデータを入力として受け取り、固定長のメッセージダイジェストを出力する。共にセキュリティ上の問題が発見されている。

- STARTTLS

STARTTLSは、プレーンテキストの通信プロトコル（例えばSMTPやPOP3）を、セキュアなTLS通信にアップグレードするための方法の一つ。STARTTLSは、TLSが使用できない古いメールサーバーやクライアントでのセキュリティ向上に役立ちますが、最近のセキュリティ要件を満たすためにはTLSを直接使用することが推奨されている。

- ロードバランサー

ロードバランサー（Load Balancer）は、ネットワークトラフィックを分散して、システムの負荷分散や冗長性の向上を実現するための装置やソフトウェアです。ロードバランサーは、クライアントからのリクエストを複数のサーバーに分散させることにより、単一のサーバーに集中する負荷を分散することができます。

対策

1. 最新の暗号強度の高い標準アルゴリズム、プロトコル、暗号鍵を実装しているか確認する。そして適切に暗号鍵を管理する。
2. 前方秘匿性(FS)を有効にしたTLS、サーバーサイドによる暗号スイートの優先度決定、セキュアパラメータなどのセキュアなプロトコルで、通信経路上のすべてのデータを暗号化する。HTTP Strict Transport Security (HSTS)のようなディレクティブで暗号化を強制する。
3. FTPやSMTPといったレガシーなプロトコルを機密データの伝送に使用しない。
4. アプリケーションごとに処理するデータ、保存するデータ、送信するデータを分類する。そして、どのデータがプライバシー関連の法律・規則の要件に該当するか、またどのデータがビジネス上必要なデータか判定する。

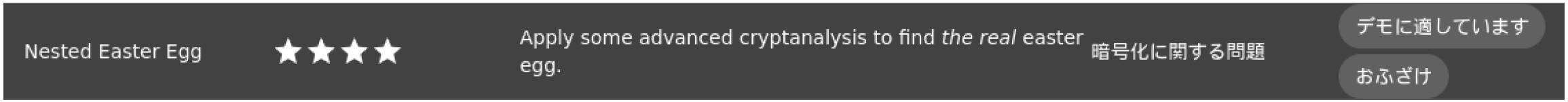
OWASP juice shop における実践

- Nested Easter Egg

Apply some advanced cryptanalysis to find the real easter egg

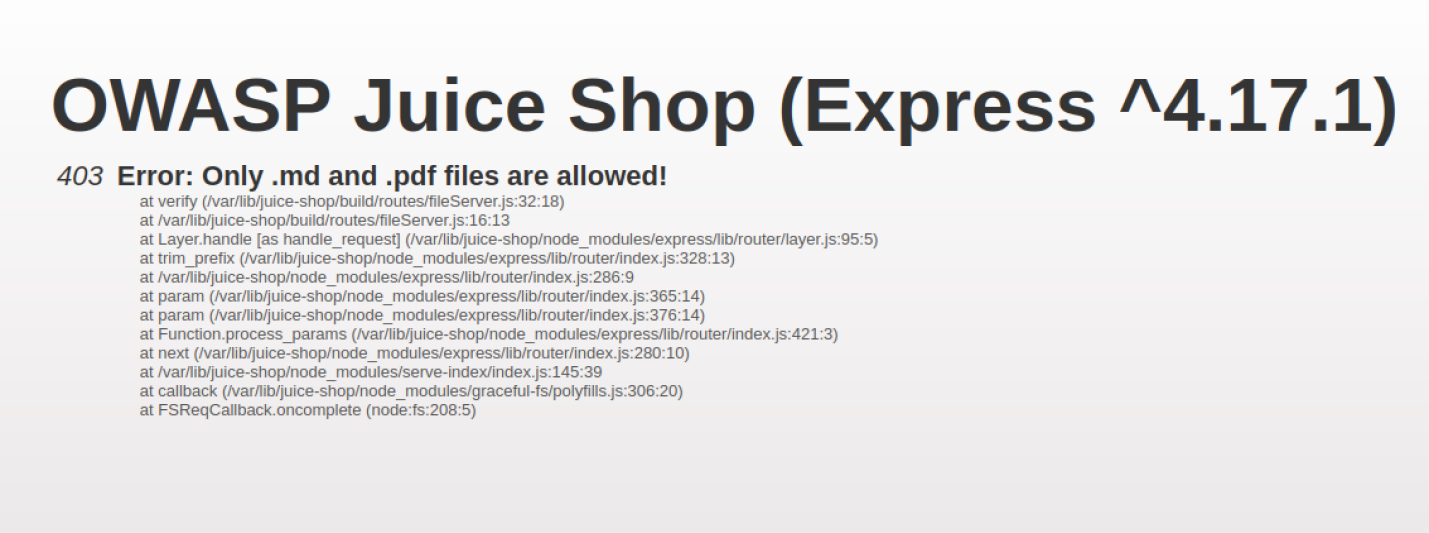
- 概要

Eastere.gg.mdにある暗号化されたメッセージを頼りにeaster eggを見つける。メッセージをBase64でdecodeすると、URLらしきものに復元されるので、それをさらにROT-13で復元するとiイースターエッグのURLが手に入る



Nested Easter Egg

0. 前準備として、Easter Eggのありかが示されている eastere.gg.mdを入手する。そのために、忘れられたバックアップファイルのあるhttp://localhost:42000/ftpにアクセスする。
ここで、eastere.ggを発見し、ダウンロードしようとする
が、.mdか.pdfしかダウンロードできないと拒否されてしまう。



Nested Easter Egg

0. ここで、Null Injectionを行う。アドレスの末尾に%00.mdをつければ、%00以下が認識されないが、拡張子がmdファイルとなるのでダウンロードが可能になる。ここで、%はURL用にエンコードすると%25になることに注意する。

```
"Congratulations, you found the easter egg!"
- The incredibly funny developers

...

...

...

Oh' wait, this isn't an easter egg at all! It's just a boring text file!
The real easter egg can be found here:

L2d1ci9xcmlmL25lci9mYi9zaGFhbC9ndXJsL3V2cS9uYS9ybmZncmUvcnR0L2p2Z3V2YS9ndX
Ivcm5mZ3JlL3J0dA==

Good luck, egg hunter!
```

Nested Easter Egg

Base64:
Base64は、データを64種類の文字で構成されるテキスト形式に変換するためのエンコーディング方式です。これは、電子メールやHTTPなどのプロトコルで、バイナリデータをテキスト形式で送信する場合に使用されます。

1. L2d1ci9xcmlmL25lci9mYi9zaGFhbC9ndXJsL3V2cS9uYS9ybmZncmUvcnR0L2p2Z3V2YS9ndXIvcm5mZ3JlL3J0dA==

   をよく見てみると、

   ・英数字が多い

   ・末尾に=がある

   ・行頭に長さを表す文字がない

   ため、Base64によってエンコードされていることがわかる。

   実際にこれをデコードすると、

/gur/qrif/ner/fb/shaal/gurl/uvq/na/rnfgre/rtt/jvguva/gur/rnfgre/rtt

   となる。

参考：各種エンコードの見分け方

代表的なエンコードの方法は3種類であり、
・UUEncode
・Base64
・yEnc
UUEncodeの特徴
・「begin 3桁の数字 ファイル名」の行から始まる
・「M」から始まる行が続く
・「end」で終わる
があげられる。
Base64の特徴
・MIMEヘッダがついている（エンコード方式としてbase64と書いてあることがほとんど）
・UUEnoceに比べて記号が少なく、英数字が多い
・行頭に長さを表す文字がない
yEncの特徴
・「=ybegin」で始まる
・データがバイナリであり、制御コードなどがそのまま本文に現れる
・「=yend」で終わる
があげられる

http://www.artin.nu/newsgroup/encode.html

Nested Easter Egg

ROT13：
ROT13（Rotate by 13）は、シンプルな暗号化手法の1つで、アルファベットの文字を13文字ずらすことによってテキストを暗号化する。

2.
/gur/qrif/ner/fb/shaal/gurl/uvq/na/rnfgre/rtt/jvguva/gur/rnfgre/rtt

をよく見てみると、gurやrttといった文字が繰り返されているとわかる。そのことから、これがROT13によって暗号化された文字列だと気づく。これを元に戻してやると、目的のURL

http://localhost:3000/the/devs/are/so/funny/they/hid/an/easter/egg/within/the/easter/egg

を得る。