5ZA-01

特殊文字に着目したWebアプリケーション攻撃検知手法

清水 大貴† 小高 知宏† 黒岩 丈介† 諏訪 いずみ† 白井 治彦‡
† 福井大学工学研究科 ‡ 福井大学工学部

1. はじめに

近年, インターネットの普及に伴い,web アプリケーションの利用者が増加している. そのため, データベースに格納されている個人情報を脅威から守るために管理を徹底する必要がある. web アプリケーションを対象とした外部からの攻撃 (XSS,SQL インジェクション等) の対策として WAF(Web Application Firewall) が挙げられ実際に運用されている.

先行研究では外部からの入力データである HTTP リクエストに対して特徴抽出を行い, 生成した特徴ベクトルを用いて攻撃検知を試みている [1][2]. 本研究では,HTTP リクエストの特殊文字に着目し, 攻撃と正常入力に対して特徴抽出を行う. また, 生成された特徴ベクトルを機械学習アルゴリズムを用いて分類を行う.

2. Webアプリケーション

Web アプリケーションとは, ブラウザから利用可能なアプリケーションサービスのことである. クライアントとサーバ間で HTTP 通信を利用してデータの送受信を行っている.

HTTP 通信はステートレスな通信であり, クライアントサーバ間で HTTP メッセージの送受信を行う. クライアントからサーバへの HTTP メッセージは HTTP リクエストとであり, リクエスト内部はヘッダとボディで構成されている. 主に, 利用者からの入力は HTTP リクエストのヘッダ部分に現れる.

Web アプリケーションへの攻撃は様々あり, ここでは代表的な攻撃手法を表 1 に挙げる. 表 1 の攻撃手法はいずれも Web アプリケーションを標的としている. 主な被害として,Cookie 値の漏洩, データベース内の個人情報流出など様々である.

表 1 では, 各攻撃手法に出現する特殊文字の入力を示したものである. これらの攻撃手法は入力スクリプトに特殊文字が含まれている. そのため,HTTP リクエストのヘッダ部分に表 1 の特殊文字が現れる場合, 攻撃を受けている可能性がある. そこで, 本研究では出現する特殊文字に着目した特徴量抽出を 4 章で述べる.

表 1: 各攻撃手法に出現する特殊文字

攻撃名	特殊文字
XSS(Cross-Site-Scripting)	< > = ・ ;
SQLI(SQL-Injection)	’ sp +
DT(Directory-Traversal)	/ ・ \

3. 機械学習アルゴリズム

本章では, 実験で使用した機械学習アルゴリズムである SVM,Random Forest ついて, 概要を述べる

3.1 Support Vector Machine

SVM は 2 クラスパターン識別器を構成する手法である. カーネル法による SVM では決定関数 $\hat{f}(x)$ は以下の式で定式化されている.

$$\hat{f}(x) = sgn(\sum_{v} \alpha_i y_i K(x_i, x) + b) \quad (1)$$

ここで,x は入力ベクトル,y は予測値,$K(x_i, x)$ はカーネル関数,α はラグランジュ乗数,b はバイアスパラメータである.

SVM は分類境界と最も近いデータとの距離 (マージン) を最大化することで, 汎化誤差が最小になるような分類境界を求める.

3.2 Random Forest

Random Forest は複数の決定木による集団学習による機械学習アルゴリズムの一つである. 学習データからランダムに抽出した要素を用いて複数の決定木で構成され, 各決定木の分類結果から最終的な出力をする手法である.

Random Forest において, 目的関数 $IG(D_p, f)$ は以下の式で定義される.

$$IG(D_p, f) = I(D_p) - \sum_{i=1}^{m} \frac{N_i}{N_p} I(D_i) \quad (2)$$

ここで,D_p は親のデータ,N はノード,i は参照しているデータ,m は分割ノード数,I は不純度である. 決定木の分類条件は $IG(D_p, f)$ を最大になるようにすることである.

Web application attack detection method based on special characters
†Daiki Shimizu †Tomohiro Odaka †Josuke Kuroiwa ‡Izumi Suwa ‡Haruhiko Shirai
†Graduate School of Engineering, University of Fukui
‡Faculty of Engineering, University of Fukui

Copyright ©2019 Information Processing Society of Japan.
All Rights Reserved.

4. 特徴量抽出方法

特殊文字に着目して, 次の 2 種類を特殊量抽出手法とする.

4.1 手法 1

攻撃, 正常入力内の入力パラメータの有無 (x_1), 特殊文字の有無 (x_2), 特殊記号 (表 2) の出現回数 ($x_3 \sim x_{35}$) から生成した 35 次元の特徴ベクトル.

入力パラメータの有無は, パラメータが存在する場合 1, 存在しない場合は 0 とし,2 進数とする. その後 10 進数に変換する. 特殊文字の有無は, 入力パラメータ内に表 2 に示してある特殊文字が存在しない場合 1, 存在しない場合 0 として, 同様に 10 進数に変換する. 図 1 のリクエストの変換を行うと表 3 のようになる.

4.2 手法 2

攻撃, 正常入力内の入力パラメータの有無 (x_1), 各入力パラメータに含まれている特殊文字の出現回数 ($x_2 \sim x_n$) から生成した特徴ベクトル. 次元数は入力パラメータの数により異なる. 入力パラメータの有無は手法 1 と同様である.

5. 実験方法

本実験では, 機械学習アルゴリズムとして Random Forest,SVM を用いる. 実行環境として,Python の機械学習ライブラリである scikit learn を使用する.

実験を行うにあたり,HTTP リクエストは [3] より入手した. このリクエストは,web サイトへの正常な HTTP リクエストと攻撃 HTTP リクエストを公開しており, 入力パラメタが 5 個の正常入力 1000 個, 攻撃入力 1000 をデータ 1, 入力パラメタが 13 個の正常入力 1000 個, 攻撃入力 1000 をデータ 2 を本実験のデータセットとする. ここで, 抽出した HTTP リクエストは GET メソッドのみとしている. また, 訓練データとテストデータとして 7:3 で分割を行った.

評価を行うにあたって,SVM と Random Forest の評価項目として, 正解率, 適合率, 再現率,F 値を用いる.

6. 結果

特殊文字に着目した特徴量における手法 1 の分類結果を図 1 に示す. 今回の実験では,SVM はパラメタとしてデータ 1 では C=0.1, γ =1.0, データ 2 では C=10.0, γ =0.1 とした. また,Random Forest はパラメタとしてデータ 1, データ 2 ともに決定木の数 30, 深さ最大 4 とした. 手法 2 の分類結果に関して当日発表する.

表 4 より, データ 1 に関して SVM,Random forest 両方とも高い精度であったが, データ 2 に関しては, データ 1 の結果と異なり精度が下がってしまった.

7. 考察・まとめ

今回の実験では, 各機械学習アルゴリズムにおいて,HTTP リクエストの入力パラメタ内の特殊文字に着目した 2 種類の特徴量抽出手法を用いて精度がどの程度あるか検証を行った. 結果より, 手法 1 の場合少ない入力パラメータであるなら、十分な分離が可能であると考えられる. また, データ 2 の精度の低さはパラメタが 13 個あり, 内容として特殊文字を含むメールアドレス等が含まれているためと考えられる.

表 2: 特殊文字一覧

sp	!	“	#	$	%	&	’	(	)	*
+	,	-	·	/	:	;	<	=	>	?
@	[	\	]	^	_	‘	{	|	}	~

parameter1 = dog & parameter3 = /cat/<dog >

図 1: リクエスト例

表 3: 生成した特徴ベクトル

x_1	x_2	$\cdots$	x_{16}	$\cdots$	x_{19}	$\cdots$	x_{21}	$\cdots$
		$\cdots$	/	$\cdots$	<	$\cdots$	>	$\cdots$
5	6	$\cdots$	2	$\cdots$	1	$\cdots$	1	$\cdots$

表 4: 分類結果 (手法 1)

	SVM		Random Forest	
	data1	data2	data1	data2
Accuracy	0.997	0.888	0.998	0.903
Precision	0.993	0.928	1.000	0.940
Recall	1.000	0.836	0.997	0.853
F-measure	0.997	0.879	0.998	0.894

参考文献

[1] 清水大貴 小高知宏 黒岩丈介 白井治彦 諏訪いずみ, Web アプリケーションの攻撃検知における機械学習手法の比較, 電気関係学会北陸支部連合大会, E-18, 2018.

[2] 伊波靖 高良富夫, サポートベクタマシンを用いた WAF への異常検知機能の実装と評価, 情報処理学会論文誌コンピューティングシステム, Vol.7(1), pp.1-13, 2014.

[3] HTTP DATA SET CSIC 2010 http://www.isi.csic.es/dataset/

Copyright ©2019 Information Processing Society of Japan.
All Rights Reserved.