Machine Learning for Application Security Professionals

Talal Albacha
@talal_basha1982
Talal.basha@owasp.org
Mission

• Our mission is to **make software security visible**, so that individuals and organizations worldwide can make informed decisions about true software security risks.
## Our Purpose & Our Core Values

**Our Purpose**: The OWASP Foundation will be the thriving global community that drives visibility and evolution in the safety and security of the world’s software.

<table>
<thead>
<tr>
<th>Core Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPEN</td>
<td>Everything at OWASP is radically transparent from our finances to our code.</td>
</tr>
<tr>
<td>INNOVATION</td>
<td>OWASP encourages and supports innovation/experiments for solutions to software security challenges.</td>
</tr>
<tr>
<td>GLOBAL</td>
<td>Anyone around the world is encouraged to participate in the OWASP community.</td>
</tr>
<tr>
<td>INTEGRITY</td>
<td>OWASP is an honest and truthful, vendor agnostic, global community.</td>
</tr>
</tbody>
</table>
The OWASP Flagship designation is given to projects that have demonstrated strategic value to OWASP and application security as a whole. After a major review process [More info here](#) the following projects are considered to be flagship candidate projects. These project have been evaluated more deeply to confirm their flagship status:

**Tools [Health Check January 2017] [edit source]**
- OWASP Zed Attack Proxy
- OWASP Web Testing Environment Project
- OWASP OWTF
- OWASP Dependency Check
- OWASP Security Shepherd

**Code [Health Check January 2017] [edit source]**
- OWASP ModSecurity Core Rule Set Project
- OWASP CSRFGuard Project
- OWASP AppSensor Project

**Documentation [Health Check January 2017] [edit source]**
- OWASP Application Security Verification Standard Project
- OWASP Software Assurance Maturity Model (SAMM)
- OWASP AppSensor Project
- OWASP Top Ten Project
- OWASPTesting Project
The OWASP Top 5 Machine Learning Risks

The idea is to build the required resources which help software security community to understand the emerging technology of machine learning and how it is related to security. Warn them about the risk associated with using ML, and discuss the defending strategies.

Presentation

TBD

Project Leader

TBD

OUTCOMES

Guidelines for some usage of machine learning techniques

N/A

Synopsis and Takeaways

- Create common datasets with the purpose of testing and validating the security of machine learning algorithms
  - How to prepare a dataset for use in ML projects
  - Discuss the importance of having well-prepared datasets

- Create a working group to work on tools and guidance
  - How to check if a dataset is noise-free (not compromised)
  - Review of algorithms implementations

- Use ML techniques in the current tools provided by OWASP (e.g., use ML to reduce false positives in ZAP scanning output)

Quick Download

[edit | edit source]

TBD

News and Events

TBD

In Print

[edit | edit source]

TBD

Back to list of all Outcomes

Original Working Session content: Machine Learning and Security
The power of machine learning reaches data management

With so much to gain from computers helping us with front-end processing in apps and services, it's no surprise that machine learning is rapidly moving to the backroom of data centers. How this transformational technology is helping enterprises overcome storage sprawl and intelligently manage their data.

Fraud Prevention, Robo-Advisory Services, and Credit Scoring Transformed Through Machine Learning

Speed and precision enable financial services to meet challenges related to time and cost, finds Frost & Sullivan's Digital Transformation team.

Google parent backs machine-learning cancer treatment

Alphabet venture capital arm takes part in Gritstone $93m fundraising round.

How machine learning could help to improve climate forecasts

Apple’s ‘Neural Engine’ Infuses the iPhone With AI Smarts

Face-reading AI will be able to detect your politics and IQ, professor says.
Would this remind you of any recent RCE...
\[ CL = \left( \frac{CI}{CD} \right)^2 \]
Supporting human decision

Automating decisions
By Experience ;)

How did you reach to this decision?

We need root cause analysis

We need Audit Trail
Counting false positives only is not accurate

Correctly Classified Instances     83 %
Incorrectly Classified Instances   17 %

=== Detailed Accuracy By Class ===

<table>
<thead>
<tr>
<th>TP Rate</th>
<th>FP Rate</th>
<th>ROC Area</th>
<th>PRC Area</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.909</td>
<td>0.324</td>
<td>0.897</td>
<td>0.950</td>
<td>fraud</td>
</tr>
<tr>
<td>0.676</td>
<td>0.091</td>
<td>0.897</td>
<td>0.790</td>
<td>not_fraud</td>
</tr>
</tbody>
</table>

Weighted Avg. 0.830 0.244 0.897 0.896

---

**Condition**

(As determined by "Gold standard")

<table>
<thead>
<tr>
<th>Condition positive</th>
<th>Condition negative</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Test outcome</strong></td>
<td><strong>True positive</strong></td>
</tr>
<tr>
<td>Test outcome positive</td>
<td></td>
</tr>
<tr>
<td>Test outcome negative</td>
<td>False negative (Type II error)</td>
</tr>
</tbody>
</table>

**Precision** = $\frac{\Sigma \text{True positive}}{\Sigma \text{Test outcome positive}}$

**Negative predictive value** = $\frac{\Sigma \text{True negative}}{\Sigma \text{Test outcome negative}}$

**Sensitivity** = $\frac{\Sigma \text{True positive}}{\Sigma \text{Condition positive}}$

**Specificity** = $\frac{\Sigma \text{True negative}}{\Sigma \text{Condition negative}}$

**Accuracy**
Hype or Reality? Stealing Machine Learning Models via Prediction APIs

by atakancetinsoy on September 30, 2016

Wired magazine just published an article with the interesting title How to Steal an AI, where the author explores the topic of reverse engineering Machine Learning algorithms based on a recently published academic paper: Stealing Machine Learning Models via Prediction APIs.
Adversarial training
Thank you