**Data Science**

**Project Proposal**

**Proposed by:**

**Sharef Mustafa & Loai Abdallatif**

Date : Feb 20, 2017

**Introduction**

Web Sites security is a major concern these days, even though many security controls are applied, still there will be always new types of attacks.

Traditional security controls ( IPS, WAF, Apache Hardening, etc…) depends on predefined attack signatures which been inspected in limited time window.

In this project, we are going to investigate the logs of three security controls applied on one website in order to reveal attack types that are not detected by the current controls.

**Context**

The Datasets that we are going to analyze from three sources which are:

1. Intrusion prevention system(IPS) firewall
2. Web Application Firewall (WAF)
3. Apache Web Server.

The above three sources contain data collected for the period Jan 04, 2017 till Feb 19, 2017.

**Content**

Each row of the logs in the three data sets corresponds to one http request, and each row has its own time stamp.

**Methodology**

In our project, we will investigate the relationship between the source Address, http request URL, and Request Timestamp among the three data sets in order to distinguish the legitimate requests and isolate other requests for further analyses specially if these isolated requests passed through existing security controls.

**Sample**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | Feb 19, 2017, 3:00:20 PM |  | HTTP 200 - Ok | <142>Feb 19 15:00:20 www.jawwal.ps httpd: 188.161.179.210 217.66.226.69 - - [19/Feb/2017:15:00:20 +0200] "GET /jawwal\_scripts/css/New\_layout.css HTTP/1.1" 200 80 644 | | Feb 19, 2017, 3:00:20 PM |  | HTTP 403 - Forbidden | <142>Feb 19 15:00:20 www.jawwal.ps httpd: 82.205.49.254 217.66.226.69 - - [19/Feb/2017:15:00:20 +0200] "GET /web\_files/home\_bg/ HTTP/1.1" 403 80 220 | | Feb 19, 2017, 3:00:20 PM |  | HTTP 304 - Not Modified | <142>Feb 19 15:00:20 www.jawwal.ps httpd: 213.244.116.31 217.66.226.69 - - [19/Feb/2017:15:00:20 +0200] "GET /web\_files/all\_files\_and\_images/880-125.jpg HTTP/1.1" 304 80 - | | Feb 19, 2017, 3:00:20 PM |  | HTTP 200 - Ok | <142>Feb 19 15:00:20 www.jawwal.ps httpd: 188.161.179.139 217.66.226.69 - - [19/Feb/2017:15:00:20 +0200] "GET /jawwal\_scripts/images/BGs/megaMenu-h2\_bg.png HTTP/1.1" 200 80 167 | | Feb 19, 2017, 3:00:21 PM |  | HTTP 200 - Ok | <142>Feb 19 15:00:21 www.jawwal.ps httpd: 217.66.226.251 217.66.226.69 - - [19/Feb/2017:15:00:21 +0200] "GET /" 200 80 18498 | | Feb 19, 2017, 3:00:21 PM |  | HTTP 200 - Ok | <142>Feb 19 15:00:21 www.jawwal.ps httpd: 188.161.179.139 217.66.226.69 - - [19/Feb/2017:15:00:21 +0200] "GET /jawwal\_scripts/images/BGs/megaMenu-li\_bg.png HTTP/1.1" 200 80 147 | | Feb 19, 2017, 3:00:21 PM |  | HTTP 404 - Not Found | <142>Feb 19 15:00:21 www.jawwal.ps httpd: 46.253.89.249 217.66.226.69 - - [19/Feb/2017:15:00:21 +0200] "GET /jawwal\_scripts/tabs\_scripts/images/ui-bg\_flat\_75\_ffffff\_40x100.png HTTP/1.1" 404 80 264 | | Feb 19, 2017, 3:00:21 PM |  | HTTP 404 - Not Found | <142>Feb 19 15:00:21 www.jawwal.ps httpd: 46.253.89.249 217.66.226.69 - - [19/Feb/2017:15:00:21 +0200] "GET /jawwal\_scripts/tabs\_scripts/images/ui-bg\_glass\_75\_e6e6e6\_1x400.png HTTP/1.1" 404 80 264 | | Feb 19, 2017, 3:00:21 PM |  | HTTP 404 - Not Found | <142>Feb 19 15:00:21 www.jawwal.ps httpd: 46.253.89.249 217.66.226.69 - - [19/Feb/2017:15:00:21 +0200] "GET /jawwal\_scripts/tabs\_scripts/images/ui-icons\_454545\_256x240.png HTTP/1.1" 404 80 260 | | Feb 19, 2017, 3:00:21 PM |  | HTTP 200 - Ok | <142>Feb 19 15:00:21 www.jawwal.ps httpd: 188.161.179.210 217.66.226.69 - - [19/Feb/2017:15:00:21 +0200] "GET /jawwal\_scripts/css/New\_header10.css HTTP/1.1" 200 80 3347 | |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |