University of Hertfordshire UH _OP4RE Online Proctoring for Remote Examination

OP4RE: IO2 - Penetration Test

20180405:02

This document has now been edited to permit access beyond its original restricted commercial use.

University of Hertfordshire
College Lane
Hatfield
Hertfordshire
AL10 9AB

Document Control

Document Properties

Title	OP4RE: IO2 - Penetration Test
Version	20180405:02
Author	Dr. Stilianos Vidalis
Penetration Testers	Dr. Stilianos Vidalis
Reviewer	Prof. Andy Jones
Approver	Prof. Amanda Jefferies
Classification	Confidentiality now removed by agreement with partners

Version Control

Change Description	**Report Version**	**Date of Change**	**Change Author**	**Signature**
Draft Report	20180405:01	5th April 2018	Svidalis	
Final Revision	20180405:02	9th April 2018	AJones	
Final Copy	20180405:03	4th July 2018	AJefferies	
Removal of Confidentiality Restrictions	20180405:04	11th February 2019	A Jefferies	

Contents

Executive Summary

The OP4RE Consortium required a **Grey Box Infrastructure Penetration Test and a WebApp Penetration Test** on their information environment hosting the Proctor Exam platform. The scope was to identify whether students could abuse the platform via a set of scenarios agreed between the test team and the owners of the ProctorExam platform.

The following targets were tested:

1. Pentest.proctorexam.com on IP 35.187.39.177

The Penetration Testing Execution Standard (PTES) was used together with Open Web Application Security Project (OWASP) methodologies as a baseline for undertaking the tests. The attack vectors that were considered were:

- Information leakage
- Unauthorised access
- Denial of service.

Additionally, a use case of a student using virtualisation for bypassing proctoring controls was considered.

The penetration test was conducted on the 29th March 2018. Pending further exploitation activities, the following observations are made:

1. No information is leaking from the environment. Only ports 80 and 443 are open. Redirection and error control are set up appropriately.

2. Denial of service attempts were not successful. There was only a slight degradation of the service at the network level which was not notable at the application level.

3. HTTPS is used for the requests. The Cookie management scheme is appropriate. No unauthorised remote access was achieved.

The use case of a student using virtualisation was discussed with ProctorExam. No feasible technology solution exists to this problem. The proposed solution is using an external camera for monitoring the Point of View of the student.

Test Narrative

The test took place on the 29th March 2018 between 1000 and 1700 UK time. The test was conducted from room LC204, School of Computer Science, University of Hertfordshire. The external IP address of the computers used for the test was: 62.232.253.150.

Footprinting

Footprinting is the technique of gathering information about computer systems and the entities they belong to. This is done by employing various computer security techniques, as:

- DNS queries
- Network enumeration
- Network queries
- Operating system identification
- Organizational queries
- Ping sweeps
- Point of contact queries
- Port Scanning
- Registrar queries (WHOIS queries)
- SNMP queries
- World Wide Web spidering

Targets reported active:

- pentest.proctorexam.com

The SSL certificates were valid and current:

- Ciphers: ECDHE-RSA-AES256-GCM-SHA384
- Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure Server CA

The other servers identified through the footprinting activities were part of the production environment and outside the scope of this test.

In attempting to map the target infrastructure traceroute and hping3 were used. Packets were stopping at hop 14, having been blocked by Google. The target environment was hosted by Google.

Open Source Intelligence (OSINT) tools were not used as they were considered outside the scope of this test.

The web page source code was examined. No issues were identified. Good practice was identified in using HTTPS.

Reconnaissance

ICMP was not blocked. **This control should be considered.**

Nmap scans reported TCP ports 80 and 443 are open. Null, FIN, Xmas scans did not yield any additional information. The Port 80 server header returned ‘nginx 1.13.8’. The SSL certificate as indicated in the footprinting stage is for ProctorExam.com. **The OS prediction was not successful**.

Reverse lookups did not reveal any additional information.

Enumeration

An enumeration is a complete, ordered listing of all the items in a collection. Under the context of a penetration test, it is a process to identify and corroborate with OSINT results domain names, associated networks related to a particular organization and a listing of all of the services offered to and accessible by the world.

Using DIRB, the directory structure of the webserver was mapped. Identified directories were returning a 302 code. This is considered best practice.

```
---- Scanning URL: https://35.187.39.177/ ----
+ https://35.187.39.177/404 (CODE:200|SIZE:1687)
+ https://35.187.39.177/500 (CODE:200|SIZE:1477)
+ https://35.187.39.177/admin (CODE:302|SIZE:101)
+ https://35.187.39.177/admin_ (CODE:302|SIZE:101)
+ https://35.187.39.177/admin_area (CODE:302|SIZE:101)
+ https://35.187.39.177/admin_banner (CODE:302|SIZE:101)
+ https://35.187.39.177/admin_c (CODE:302|SIZE:101)
+ https://35.187.39.177/admin_index (CODE:302|SIZE:101)
+ https://35.187.39.177/admin_interface (CODE:302|SIZE:101)
+ https://35.187.39.177/admin_login (CODE:302|SIZE:101)
+ https://35.187.39.177/admin_logon (CODE:302|SIZE:101)
+ https://35.187.39.177/admin1 (CODE:302|SIZE:101)
+ https://35.187.39.177/admin2 (CODE:302|SIZE:101)
+ https://35.187.39.177/admin3 (CODE:302|SIZE:101)
+ https://35.187.39.177/admin4_account (CODE:302|SIZE:101)
+ https://35.187.39.177/admin4_colon (CODE:302|SIZE:101)
+ https://35.187.39.177/admin-admin (CODE:302|SIZE:101)
+ https://35.187.39.177/admin-console (CODE:302|SIZE:101)
+ https://35.187.39.177/admincontrol (CODE:302|SIZE:101)
+ https://35.187.39.177/admincp (CODE:302|SIZE:101)
+ https://35.187.39.177/adminhelp (CODE:302|SIZE:101)
+ https://35.187.39.177/admin-interface (CODE:302|SIZE:101)
+ https://35.187.39.177/administer (CODE:302|SIZE:101)
+ https://35.187.39.177/administr8 (CODE:302|SIZE:101)
+ https://35.187.39.177/administracion (CODE:302|SIZE:101)
+ https://35.187.39.177/administrador (CODE:302|SIZE:101)
+ https://35.187.39.177/administrat (CODE:302|SIZE:101)
+ https://35.187.39.177/administratie (CODE:302|SIZE:101)
+ https://35.187.39.177/administration (CODE:302|SIZE:101)
+ https://35.187.39.177/administrator (CODE:302|SIZE:101)
+ https://35.187.39.177/administratoraccounts (CODE:302|SIZE:101)
+ https://35.187.39.177/administrators (CODE:302|SIZE:101)
+ https://35.187.39.177/administrivia (CODE:302|SIZE:101)
+ https://35.187.39.177/adminlogin (CODE:302|SIZE:101)
+ https://35.187.39.177/adminlogon (CODE:302|SIZE:101)
+ https://35.187.39.177/adminpanel (CODE:302|SIZE:101)
+ https://35.187.39.177/adminpro (CODE:302|SIZE:101)
+ https://35.187.39.177/admins (CODE:302|SIZE:101)
+ https://35.187.39.177/adminsessions (CODE:302|SIZE:101)
+ https://35.187.39.177/adminsql (CODE:302|SIZE:101)
+ https://35.187.39.177/admintools (CODE:302|SIZE:101)
+ https://35.187.39.177/backoffice (CODE:302|SIZE:101)
+ https://35.187.39.177/browser (CODE:200|SIZE:1522)
+ https://35.187.39.177/docs (CODE:200|SIZE:88697)
+ https://35.187.39.177/favicon.ico (CODE:200|SIZE:24838)
+ https://35.187.39.177/robots.txt (CODE:200|SIZE:202)
+ https://35.187.39.177/version (CODE:200|SIZE:57)

-----------------
END_TIME: Thu Mar 29 11:11:38 2018
```

Nikto and Spartan did not yield any additional notable results with the exception of no ALLOW or Public Header in Options for the http-methods.

Very good error control, not returning 404 codes. This is considered best practice, not allowing for information leakage.

The following directories were also discovered:

```
https://35.187.39.177/images
https://35.187.39.177/scripts
https://35.187.39.177/cgi-bin
https://35.187.39.177/docs/stylesheets/bundled
https://35.187.39.177/docs/stylesheets
https://35.187.39.177/docs
https://35.187.39.177/docs/1.0
https://35.187.39.177/docs/1.0/attachments
https://35.187.39.177/docs/1.0/documents
https://35.187.39.177/docs/1.0/exams
https://35.187.39.177/docs/1.0/institutes
https://35.187.39.177/docs/1.0/users
https://35.187.39.177/docs/javascripts/bundled
https://35.187.39.177/docs/javascripts
https://35.187.39.177/img
```

Vulnerability Identification

General

Vulnerability research on the web server version did not yield any notable results. Automated vulnerability scanning using OpenVAS was also negative. There is a potential local privilege escalation (CVE-201601247) but this is not an issue as it would first require remote access.

By communicating with the server manually, it was possible to map the authentication schema using BURP. POST is used. Packet interception is considered outside the scope so no issues with the request type.

The POST and GET requests were examined. **The ‘max-age’ cookie attribute was set to 0.** This is considered to be best practice.

The site uses SSL and the Strict-Transport-Security HTTP header is not defined.

No other notable issue was identified.

Exploitation

Web Server

A number of different directory traversal methods were tried. **Redirection works and is set up appropriately. No information is leaked.**

Bruteforcing using HYDRA was allowed and did not result in a blacklisting of the attack IP address. This control should be considered.

Denial of Service - Flooding

An attempt was made to flood the target network using HPING3. There was a slight delay in the response time but the load balancer was more than adequate. No DDOS was attempted.

```
64 bytes from 35.187.39.177: icmp_seq=119 ttl=46 time=13.1 ms
64 bytes from 35.187.39.177: icmp_seq=120 ttl=46 time=13.1 ms
64 bytes from 35.187.39.177: icmp_seq=121 ttl=46 time=13.0 ms
64 bytes from 35.187.39.177: icmp_seq=122 ttl=46 time=13.1 ms
64 bytes from 35.187.39.177: icmp_seq=123 ttl=46 time=13.2 ms
64 bytes from 35.187.39.177: icmp_seq=124 ttl=46 time=13.0 ms
64 bytes from 35.187.39.177: icmp_seq=125 ttl=46 time=13.2 ms
64 bytes from 35.187.39.177: icmp_seq=126 ttl=46 time=13.0 ms
64 bytes from 35.187.39.177: icmp_seq=127 ttl=46 time=13.1 ms
64 bytes from 35.187.39.177: icmp_seq=132 ttl=46 time=230 ms
64 bytes from 35.187.39.177: icmp_seq=139 ttl=46 time=231 ms
64 bytes from 35.187.39.177: icmp_seq=142 ttl=46 time=230 ms
64 bytes from 35.187.39.177: icmp_seq=145 ttl=46 time=230 ms
64 bytes from 35.187.39.177: icmp_seq=147 ttl=46 time=231 ms
64 bytes from 35.187.39.177: icmp_seq=149 ttl=46 time=230 ms
64 bytes from 35.187.39.177: icmp_seq=153 ttl=46 time=231 ms
64 bytes from 35.187.39.177: icmp_seq=154 ttl=46 time=230 ms
64 bytes from 35.187.39.177: icmp_seq=157 ttl=46 time=244 ms
64 bytes from 35.187.39.177: icmp_seq=162 ttl=46 time=230 ms
64 bytes from 35.187.39.177: icmp_seq=166 ttl=46 time=231 ms
64 bytes from 35.187.39.177: icmp_seq=172 ttl=46 time=230 ms
64 bytes from 35.187.39.177: icmp_seq=173 ttl=46 time=252 ms
64 bytes from 35.187.39.177: icmp_seq=175 ttl=46 time=254 ms
64 bytes from 35.187.39.177: icmp_seq=185 ttl=46 time=290 ms
64 bytes from 35.187.39.177: icmp_seq=189 ttl=46 time=307 ms
64 bytes from 35.187.39.177: icmp_seq=190 ttl=46 time=232 ms
64 bytes from 35.187.39.177: icmp_seq=194 ttl=46 time=231 ms
64 bytes from 35.187.39.177: icmp_seq=195 ttl=46 time=316 ms
64 bytes from 35.187.39.177: icmp_seq=196 ttl=46 time=231 ms
64 bytes from 35.187.39.177: icmp_seq=200 ttl=46 time=230 ms
64 bytes from 35.187.39.177: icmp_seq=201 ttl=46 time=331 ms
64 bytes from 35.187.39.177: icmp_seq=203 ttl=46 time=342 ms
64 bytes from 35.187.39.177: icmp_seq=205 ttl=46 time=340 ms
64 bytes from 35.187.39.177: icmp_seq=211 ttl=46 time=372 ms
64 bytes from 35.187.39.177: icmp_seq=216 ttl=46 time=231 ms
64 bytes from 35.187.39.177: icmp_seq=228 ttl=46 time=231 ms
64 bytes from 35.187.39.177: icmp_seq=230 ttl=46 time=232 ms
64 bytes from 35.187.39.177: icmp_seq=237 ttl=46 time=453 ms
64 bytes from 35.187.39.177: icmp_seq=242 ttl=46 time=231 ms
64 bytes from 35.187.39.177: icmp_seq=260 ttl=46 time=232 ms
64 bytes from 35.187.39.177: icmp_seq=264 ttl=46 time=13.1 ms
64 bytes from 35.187.39.177: icmp_seq=265 ttl=46 time=13.1 ms
64 bytes from 35.187.39.177: icmp_seq=266 ttl=46 time=13.0 ms
64 bytes from 35.187.39.177: icmp_seq=267 ttl=46 time=13.2 ms
64 bytes from 35.187.39.177: icmp_seq=268 ttl=46 time=13.1 ms
64 bytes from 35.187.39.177: icmp_seq=269 ttl=46 time=13.0 ms
```