



Advanced Web Attacks and Exploitation

Offensive Security

Copyright © 2019 Offsec Services Ltd. All rights reserved — No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distant learning, in any form or by any means such as any information storage, transmission or retrieval system, without prior written permission from the author.

Table of Contents

0	Introduction.....	9
0.1	About the AWAE Course.....	9
0.2	Our Approach.....	11
0.3	Obtaining Support.....	12
0.4	Legal.....	13
0.5	Offensive Security AWAE Labs.....	13
0.5.1	General Information	13
0.5.2	Lab Restrictions	13
0.5.3	Forewarning and Lab Behaviour.....	13
0.5.4	Control Panel	14
0.6	Backups	14
1	Tools & Methodologies.....	15
1.1	Web Traffic Inspection.....	15
1.1.1	BurpSuite Proxy.....	16
1.1.2	BurpSuite Scope.....	21
1.1.3	BurpSuite Repeater and Comparer	24
1.1.4	BurpSuite Decoder.....	28
1.1.5	Exercise.....	30
1.2	Interacting with Web Listeners with Python.....	30
1.2.1	Exercise.....	35
1.3	Source Code Recovery.....	35
1.3.1	Managed .NET Code.....	35
1.3.2	Decompiling Java classes	44
1.3.3	Exercise.....	48
1.3.4	Source Code Analysis	48
2	Atmail Mail Server Appliance: from XSS to RCE.....	50
2.1	Overview	50
2.2	Getting Started	50
2.3	Atmail Vulnerability Discovery.....	50
2.3.1	Exercise.....	56
2.4	Session Hijacking.....	57

2.4.1	Exercise.....	61
2.5	Session Riding.....	62
2.5.1	The Attack	62
2.5.2	Minimizing the Request.....	63
2.5.3	Developing the Session Riding JavaScript Payload.....	65
2.5.4	Exercise.....	68
2.5.5	Extra Mile.....	68
2.6	Gaining Remote Code Execution	69
2.6.1	Overview	69
2.6.2	Vulnerability Description.....	71
2.6.3	The addattachmentAction Vulnerability Analysis	71
2.6.4	The globalsaveAction Vulnerability Analysis.....	77
2.6.5	Exercise.....	83
2.6.6	addattachmentAction Vulnerability Trigger.....	84
2.6.7	Exercise.....	85
2.6.8	Extra Mile.....	85
2.7	Summary	85
3	ATutor Authentication Bypass and RCE	86
3.1	Overview	86
3.2	Getting Started	86
3.2.1	Setting Up the Environment.....	86
3.3	Initial Vulnerability Discovery.....	89
3.3.1	Exercise.....	99
3.4	A Brief Review of Blind SQL Injections.....	100
3.5	Digging Deeper	101
3.5.1	When \$addslashes Are Not	101
3.5.2	Improper Use of Parameterization.....	103
3.6	Data Exfiltration.....	105
3.6.1	Comparing HTML Responses.....	105
3.6.2	MySQL Version Extraction	109
3.6.3	Exercise.....	112
3.6.4	Extra mile.....	112

3.7	Subverting the ATutor Authentication	112
3.7.1	Exercise.....	118
3.7.2	Extra Mile.....	119
3.8	Authentication Gone Bad.....	119
3.8.1	Exercise.....	120
3.8.2	Extra Mile.....	121
3.9	Bypassing File Upload Restrictions.....	121
3.9.1	Exercise.....	130
3.10	Gaining Remote Code Execution	130
3.10.1	Escaping the Jail.....	130
3.10.2	Disclosing the Web Root	132
3.10.3	Finding Writable Directories.....	133
3.10.4	Bypassing File Extension Filter	134
3.10.5	Exercise.....	136
3.10.6	Extra Mile.....	136
3.11	Summary	136
4	ATutor LMS Type Juggling Vulnerability.....	138
4.1	Overview	138
4.2	Getting Started	138
4.3	PHP Loose and Strict Comparisons.....	138
4.4	PHP String Conversion to Numbers.....	141
4.4.1	Exercise.....	143
4.5	Vulnerability Discovery.....	143
4.6	Attacking the Loose Comparison	146
4.6.1	Magic Hashes.....	146
4.6.2	ATutor and the Magic E-Mail address	147
4.6.3	Exercise.....	153
4.6.4	Extra Mile.....	153
4.7	Summary	153
5	ManageEngine Applications Manager AMUserResourcesSyncServlet SQL Injection RCE..	154
5.1	Overview	154
5.2	Getting Started	154

5.3	Vulnerability Discovery.....	154
5.3.1	Servlet Mappings	155
5.3.2	Source Code Recovery.....	156
5.3.3	Analyzing the Source Code.....	158
5.3.4	Enabling Database Logging.....	164
5.3.5	Triggering the Vulnerability.....	167
5.3.6	Exercise.....	170
5.4	Bypassing Character Restrictions.....	170
5.4.1	Using CHR and String Concatenation.....	172
5.4.2	It Makes Lexical Sense	173
5.5	Blind Bats.....	173
5.5.1	Exercise.....	174
5.6	Accessing the File System.....	175
5.6.1	Exercise.....	177
5.6.2	Reverse Shell Via Copy To	177
5.6.3	Exercise.....	183
5.6.4	Extra Mile.....	184
5.7	PostgreSQL Extensions	184
5.7.1	Build Environment.....	184
5.7.2	Testing the Extension	187
5.7.3	Loading the Extension from a Remote Location.....	188
5.7.4	Exercise.....	189
5.8	UDF Reverse Shell.....	189
5.8.1	Exercise.....	192
5.9	More Shells!!!.....	192
5.9.1	PostgreSQL Large Objects.....	192
5.9.2	Large Object Reverse Shell	196
5.9.3	Exercise.....	198
5.9.4	Extra Mile.....	198
5.10	Summary	198
6	Bassmaster NodeJS Arbitrary JavaScript Injection Vulnerability.....	199
6.1	Overview	199

6.2	Getting Started	199
6.3	The Bassmaster Plugin.....	199
6.4	Vulnerability Discovery.....	200
6.5	Triggering the Vulnerability	209
6.6	Obtaining a Reverse Shell.....	211
6.6.1	Exercise.....	215
6.6.2	Extramile.....	215
6.7	Summary	215
7	DotNetNuke Cookie Deserialization RCE	216
7.1	Overview	216
7.2	Getting Started	216
7.3	Introduction.....	216
7.4	Serialization Basics.....	217
7.4.1	XmlSerializer Limitations.....	217
7.4.2	Basic XmlSerializer Example	217
7.4.3	Exercise.....	221
7.4.4	Expanded XmlSerializer Example	221
7.4.5	Exercise.....	226
7.4.6	Watch your Type dude.....	226
7.4.7	Exercise.....	228
7.5	DotNetNuke Vulnerability Analysis.....	229
7.5.1	Vulnerability Overview.....	229
7.5.2	Debugging DotNetNuke.....	232
7.5.3	Exercise.....	239
7.5.4	How Did We Get Here.....	239
7.6	Payload Options	243
7.6.1	FileSystemUtils PullFile Method	243
7.6.2	ObjectDataProvider Class	244
7.6.3	Example Use of the ObjectDataProvider Instance	248
7.6.4	Exercise.....	252
7.6.5	Serialization of the ObjectDataProvider	252
7.6.6	Enter The Dragon (ExpandedWrapper Class).....	256



- 7.6.7 Exercise..... 261
- 7.7 Putting It All Together 261
 - 7.7.1 Exercise..... 265
- 7.8 ysoserial.net..... 266
 - 7.8.1 .Net Extra Mile 266
 - 7.8.2 Java Extra Mile 266
- 7.9 Summary 266