

Hackmiami P0wn OFF 2014
by Alex Laplume [@ac3x0r](#), Rod Soto [@rodsoto](#), James Ball [@revhattrick](#),
Alexander Heid [@alexheid](#)

www.HackMiami.com [@hackmiami](#)

The security industry is in a very exciting moment of growth and expansion. As a result of this growth and expansion, there has been significant development of security software products that bring the promise of providing “One click” and at times, “All in One” solutions. These solutions range in price from the very affordable for all to the enterprise budgets only.

Regardless of the price point or advertised features, end users only expect one thing. The expectation is the ability to find as many exploitable vulnerabilities with the least configuration changes or adjustments in the fastest amount of time. Users should not need certifications or extensive training to be able to do their jobs with automated software products. Furthermore, even knowing how to use the product at times is not enough to maintain a consistent security posture, since it is known among both security professionals and attackers that certain products will result in a rate high on false positives and negatives, or have shortcomings in features such as validation of findings, reporting functions, or cross-tool interoperability.

The purpose of the HackMiami P0wn OFF has always been very simple. We seek to answer several questions that are common pain points within the information security community:

- How far and accurate can a standard operator or user go by using automated vulnerability scanning tools in their defaults, template, pre-configured settings?
- Are vendors misrepresenting or stretching their advertised features?
- How much customization is needed for usable results?
- Are there alternative products that can be used by single consultants or junior information security professionals with less acquisition power but still be able to complete their jobs?
- Are there new products with innovative features?

HackMiami researchers have been pursuing answers to these questions since the year 2010 and providing our findings to the information security for review. The audience is very technical, and the criteria is clearly communicated to vendors and audience prior to the event.

It is important for vendors to receive real feedback from real users and it is important for the community to separate in between artificially built marketing hype and the real results of a vulnerability assessments on client networks and applications.

In this year's HackMiami P0wn OFF, automated web application vulnerability scanners were revisited by Alex Laplume ([@ac3x0r](#)) and Greg Hannis ([@gregtampa](#)). The application scanners were tested against common content management systems (CMS) and pre configured vulnerable web applications. The 2014 Web Application P0wn OFF was a live event that took place at the [HackMiami 2014 Hackers Conference](#) in Miami Beach Florida.

2014 HackMiami Web Application P0wn OFF Criteria:

- Ease of Interface and Installation
- Accuracy of Vulnerability Detection
- Granularity of Reporting
- Overall Quality

The scans consisted of a single pre-authentication scan, and a single post-authentication scan against each user level of a vulnerable web application. Rating scores were on a scale of 1 (lowest) to 5 (highest).

The Targets

The targeted hosts were preconfigured and validated with a series of web application vulnerabilities, and all scanners were tested against the same pre configured vulnerable applications. These applications were virtual machines with snapshots. These snapshots were re initiated after each scanning application was finished. The scans were also performed twice, first without authentication (pre-authentication) then with authentication (post-authentication).

List of targets

- PHP Vulnerable web application
- JSP Vulnerable web application
- .NET Vulnerable web application

Vulnerabilities tested

- XXS (Cross Site Scripting)
- SQLi (SQL injection)
- Blind SQLi (Blind SQL injection)
- Directory Traversal
- CSRF (Cross Site Request Forgery)
- Command Injection
- File Inclusion (LFI/RFI) Local and Remote
- Bad HTTP Methods
- Application Errors
- Directory Listing
- Informational

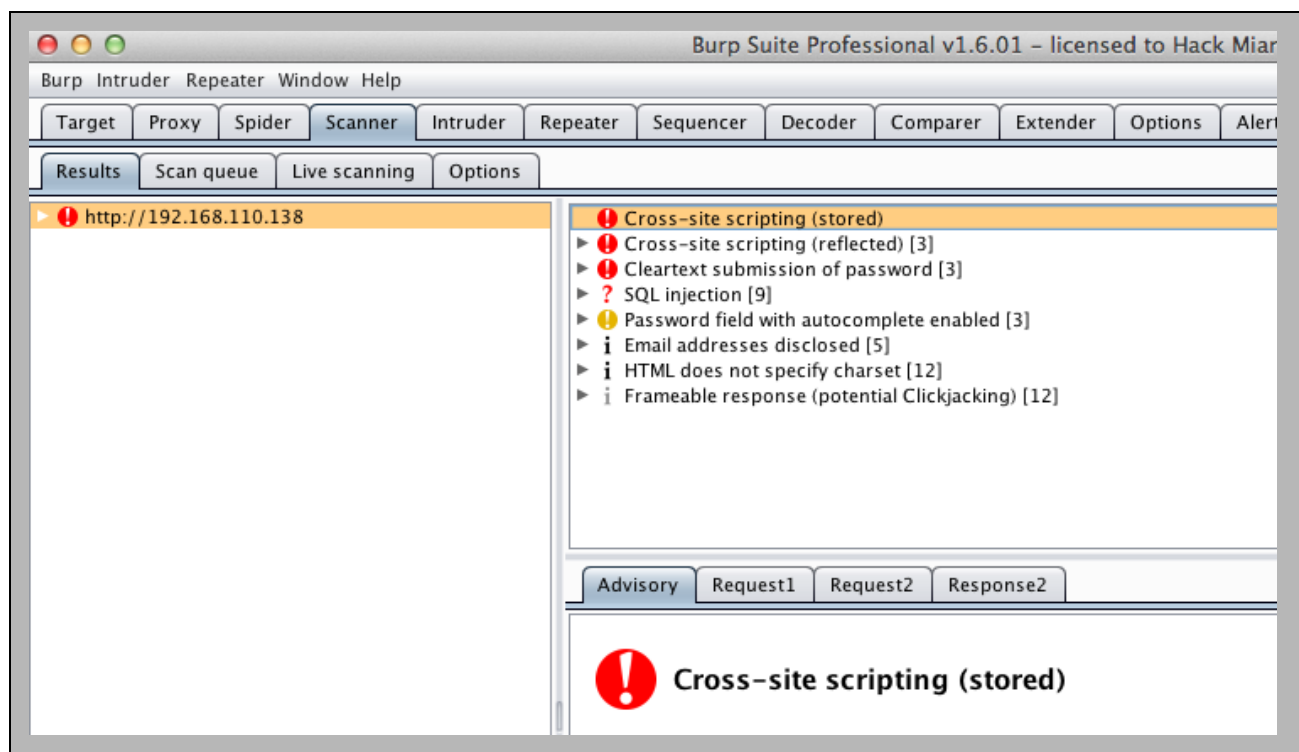
The selection of these vulnerabilities was based on Hackmiami field experience and OWASP TOP 10, which is a known criteria for the most important web application security flaws. More information about OWASP TOP 10*. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Burp Suite – 1.6.01

Interface and Installation

Burp is an easy to use cross platform web scanner written in Java which means no installation required. Since it uses Java its very easy to consume lots of machine resources when running multiple automated scans, so be careful there. The user interface is easy to use and navigate. The tool is broken up in to tabs, in each of these tabs is where different features of the tool can be accessed. Burp has options for automated and manual web application auditing, useful for different phases of a penetration test. Overall for the easy of use, portability and large feature-set Burp suite gets a 4/5

Vulnerability Detection



Burp has options for scanning, crawling, and discovering content on websites. With the Active Scanner you get web application scans of pages that have been crawled or discovered with the content discovery tool. With the Passive scanner Burp will audit the web application while you browse the site. The Proxy feature of Burp is yet another great addition. This tool can be used to intercept requests and tamper them or send them to one of the other many tools.

Burp was able to detect the critical vulnerabilities in our test web applications with ease and false positives could be weeded out quickly. Burp Suite gets a 5/5

Reporting

Burp has still not implemented a feature for exporting the report as a PDF, but does offer options to generate HTML reports from results in the scanner tab. Overall feels like the reporting side of Burp Suite is clear and concise, but maybe too simple. For this, Burp Suite gets a 3/5

Overall

Burp Suite is a great, feature rich web application scanner. It's portability, ease of use, and great automated/manual approach makes it flexible for all parts of a test. For these reasons, Burp Suite gets a 4.5/5

Netsparker – 3.2

Interface and Installation

Netsparker is a Windows application with a very easy and straightforward installation. While running scans and browsing through the features of Netsparker, I noticed little to no sluggishness which was awesome! All of Netsparker's options can be displayed on the screen by simply clicking a check under the view option. Netsparker also has a schedule scan option which makes it convenient for doing scans while being out and about completing important errands. Since Netsparker has a very straightforward interface, was easy to use and navigate, and wasn't sluggish while in use Netsparker gets a 4.5/5

Vulnerability Detection

Netsparker gets right to what needs to be done, scanning and vulnerability detection. Netsparker finished scanning the target web applications with speed and very little system resource usage. The best thing about Netsparker that I noticed was that it stays true to its claims of being false positive free. It has wealth of information including links about the vulnerabilities discovered. Since Netsparker was able to discover and display information on critical vulnerabilities found in the web applications used without false positives Netsparker gets a 5/5

Reporting

Netsparker has a wealth of information displayed in the Vulnerability tab, as if that wasn't enough Netsparker also has an option for Reporting where it will generate different types of reports such as PCI Compliance, OWASP Top Ten, and even Comparison Reports. Netsparker has a huge amount of information and easy report generating options for this Netsparker gets a 4/5

Overall

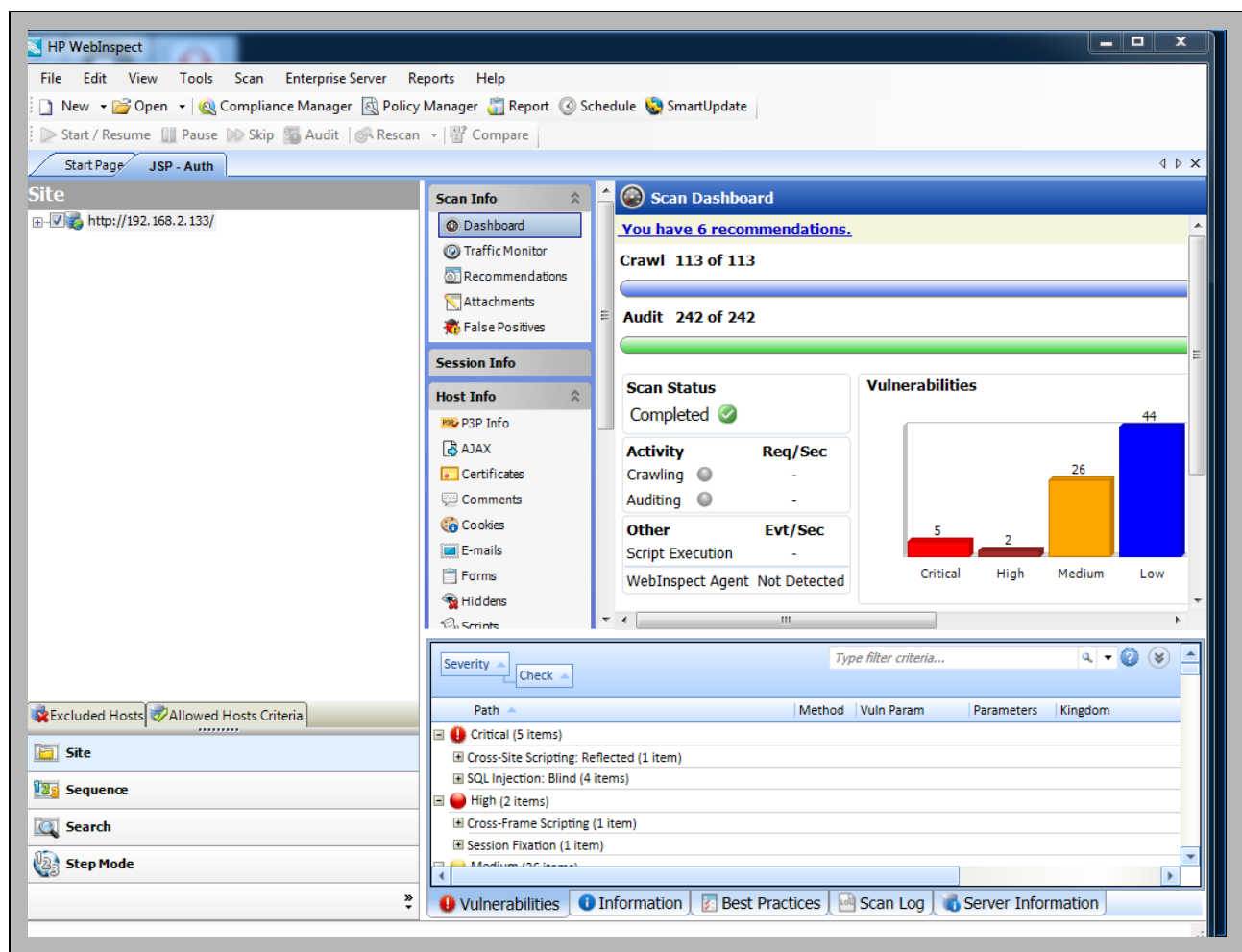
Netsparker was a great tool to use and test with: scheduled scans, easy to use interface, and false positive free application scanning gives this tools score a 4.5/5

HP WebInspect – 10.20.666.10

Interface and Installation

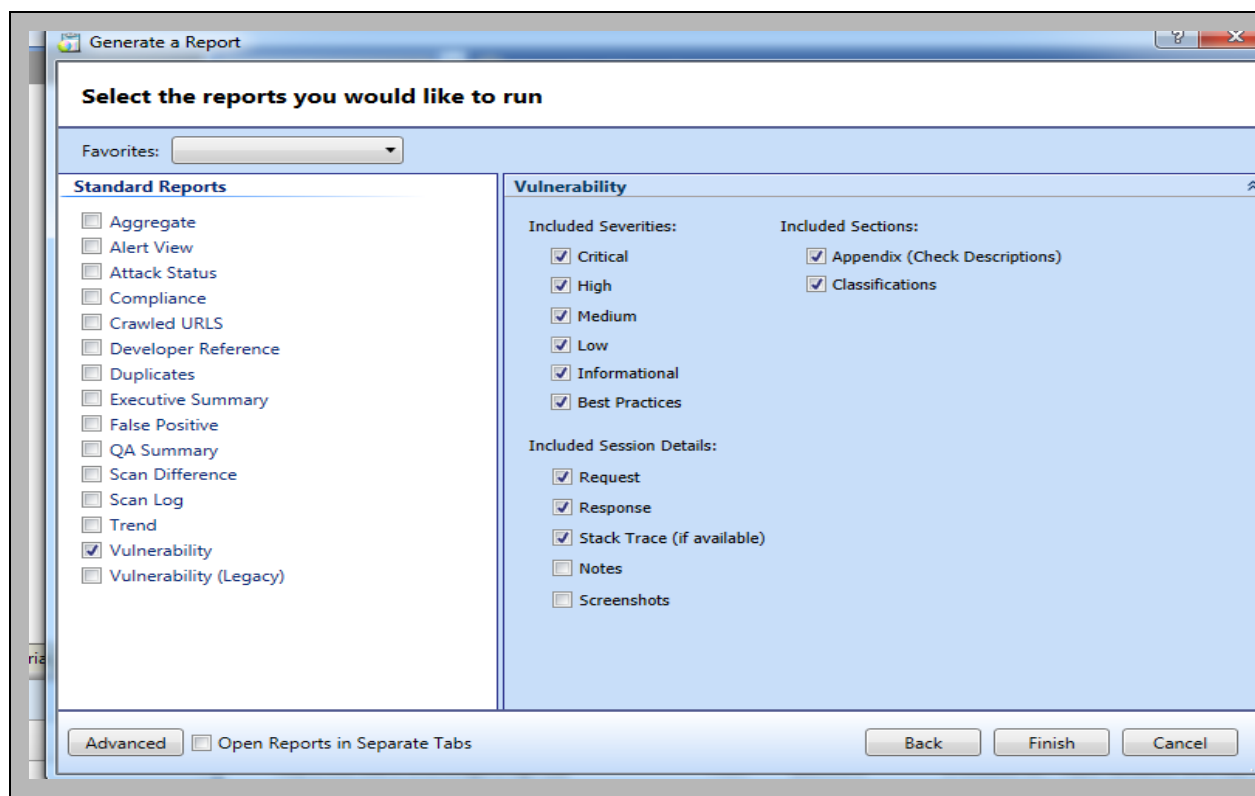
HP WebInspect's interface was a robust tool with the most features that I've tested. Therefore, the interface had a bit of a higher learning curve. HP WebInspect is a Windows tool that requires the installation of SQL Server so be ready for that. HP WebInspect is meant for huge enterprise scanning and vulnerability detection so that limits the portability of this particular tool. I should also mention that this tool uses a great deal of resources so, be prepared to use appropriate hardware. Once you look past all that the tool has an option for everything you could want on a web application scanner. Since HP WebInspect has a bit harder of a learning curve, is quite resource intensive, and is not very portable, HP WebInspect gets a 3.5

Vulnerability Detection



HP WebInspect was the most thorough when it came to vulnerability detection. The Scans took very long to complete as the tool will crawl and audit if the option is selected. HP WebInspect gave very detailed reports detailing the vulnerabilities and possible remediation solutions which was helpful. HP WebInspect did however have the most false positives of the tools in this test. HP WebInspect also has great tools for exploiting the vulnerabilities once discovered to show full proof of vulnerability. Since HP WebInspect was able to catch the critical vulnerabilities, gives tons of information on found vulnerabilities, and has impressive exploitation tools HP WebInspect gets a 5/5

Reporting



HP WebInspect really took the cake with regard to reporting in this years test. HP WebInspect has lots of options for generating reports. Hp WebInspect will allow you to choose which data format you want results in, use a wizards to generate custom reports, or use predefined templates to generate reports in. Since HP WebInspect has the most varied feature-set with regard to reporting HP WebInspect gets a 5/5

Overall

HP WebInspect is an amazing over the top web application scanning and reporting tool. HP WebInspect is great for huge organizations to keep up with their security posture. For great detection, reporting, but limited portability HP WebInspect gets a 4/5

Conclusion

Due to the prolific amount of web applications vulnerabilities and configuration flaws that are possible is crucial for businesses and organizations in order to operate with the least possible amount of risk. Security professionals must drive the probing, testing and verification of possible vulnerabilities before malicious actors have a chance to do the same. The tools outlined in this report provide great amounts of information that can drive the hardening and defense of organization's web applications.

It is also important to separate fact from hype and provide security professionals with tools that can help them streamline their vulnerability assessments and penetration tests. The need for real threat intelligence is even critical following the disclosure of three (3) major vulnerabilities during 2014, such as Heartbleed, [Shellshock](#) and [POODLE](#). The fluid state of vulnerability discovery and exploitation will drive the use and improvement of security like the ones reviewed in this report. Furthermore, the will also fuel the development of attack tools used by malicious actors in the wild.

The tools used by security professionals for vulnerability detection must be easy to install, easy to use, easy to update, portable, and with have the ability to generate precise and meaningful reports. These features will allow for quick detection and remediation of any potential problems before they take place.

Addendum

Results by vulnerable application and scanning tool

Burp Suite – 1.6.01			
PHP Vulnerable Web App (Unauthenticated)			
Vulnerability	Matches	False Positives	False Negatives
XXS	3	0	0
SQLI	2	0	0
Blind SQLI	0	0	0
Directory Traversal	2	0	0
CSRF	0	0	0
Command Injection	1	0	0
File Inclusion	1	0	0
Bad HTTP Methods	0	0	0
App Errors	0	0	0
Directory Listing	1	0	0
Informational	5	0	0

PHP Vulnerable Web App (Authenticated)			
Vulnerability	Matches	False Positives	False Negatives
XXS	3	0	0
SQLI	2	0	0
Blind SQLI	0	0	0
Directory Traversal	2	0	0
CSRF	0	0	0
Command Injection	1	0	0
File Inclusion	1	0	0
Bad HTTP Methods	2	1	0
App Errors	0	0	0
Directory Listing	2	0	0
Informational	10	2	0

JSP Vulnerable Web App (Unauthenticated)			
Vulnerability	Matches	False Positives	False Negatives
XXS	1	0	0
SQLI	0	0	0
Blind SQLI	2	1	0
Directory Traversal	0	0	0
CSRF	0	0	0
Command Injection	0	0	0
File Inclusion	0	0	0
Bad HTTP Methods	0	0	0
App Errors	0	0	0
Directory Listing	0	0	0
Informational	37	5	0

JSP Vulnerable Web App (Authenticated)			
Vulnerability	Matches	False Positives	False Negatives
XXS	4	0	0
SQLI	0	0	0
Blind SQLI	4	2	0
Directory Traversal	0	0	0
CSRF	0	0	0
Command Injection	0	0	0
File Inclusion	0	0	0
Bad HTTP Methods	0	0	0
App Errors	0	0	0
Directory Listing	0	0	0
Informational	32	2	0

.NET Vulnerable Web App (Unauthenticated)			
Vulnerability	Matches	False Positives	False Negatives
XXS	1	0	0
SQLI	0	0	0
Blind SQLI	0	0	0
Directory Traversal	0	0	0
CSRF	0	0	0
Command Injection	0	0	0
File Inclusion	0	0	0
Bad HTTP Methods	2	0	0
App Errors	0	0	0
Directory Listing	0	0	0
Informational	2	0	0

.NET Vulnerable Web App (Authenticated)			
Vulnerability	Matches	False Positives	False Negatives
XXS	56	6	0
SQLI	4	0	0
Blind SQLI	0	0	0
Directory Traversal	0	0	0
CSRF	0	0	0
Command Injection	1	0	0
File Inclusion	1	0	0
Bad HTTP Methods	0	0	0
App Errors	0	0	0
Directory Listing	0	0	0
Informational	36	4	0

Netsparker – 3.2			
PHP Vulnerable Web App (Unauthenticated)			
Vulnerability	Matches	False Positives	False Negatives
XXS	2	0	0
SQLI	1	0	0
Blind SQLI	0	0	0
Directory Traversal	2	0	0
CSRF	0	0	0
Command Injection	0	0	0
File Inclusion	0	0	1
Bad HTTP Methods	1	0	0
App Errors	0	0	0
Directory Listing	2	0	0
Informational	15	0	0

PHP Vulnerable Web App (Authenticated)			
Vulnerability	Matches	False Positives	False Negatives
XXS	3	0	0
SQLI	1	0	1
Blind SQLI	0	0	0
Directory Traversal	2	0	0
CSRF	0	0	0
Command Injection	0	0	1
File Inclusion	1	0	0
Bad HTTP Methods	2	0	0
App Errors	10	0	0
Directory Listing	2	0	0
Informational	23	0	0

JSP Vulnerable Web App (Unauthenticated)			
Vulnerability	Matches	False Positives	False Negatives
XXS	1	0	0
SQLI	0	0	0
Blind SQLI	2	0	0
Directory Traversal	0	0	0
CSRF	0	0	0
Command Injection	0	0	0
File Inclusion	0	0	0
Bad HTTP Methods	0	0	0
App Errors	5	0	0
Directory Listing	0	0	0
Informational	31	0	0

JSP Vulnerable Web App (Authenticated)			
Vulnerability	Matches	False Positives	False Negatives
XXS	2	0	0
SQLI	0	0	0
Blind SQLI	2	0	0
Directory Traversal	0	0	0
CSRF	0	0	0
Command Injection	0	0	0
File Inclusion	0	0	0
Bad HTTP Methods	1	0	0
App Errors	12	0	0
Directory Listing	0	0	0
Informational	22	0	0

.NET Vulnerable Web App (Unauthenticated)			
Vulnerability	Matches	False Positives	False Negatives
XXS	1	0	0
SQLI	0	0	0
Blind SQLI	0	0	0
Directory Traversal	0	0	0
CSRF	0	0	0
Command Injection	0	0	0
File Inclusion	0	0	0
Bad HTTP Methods	0	0	0
App Errors	0	0	0
Directory Listing	0	0	0
Informational	3	0	0

.NET Vulnerable Web App (Authenticated)			
Vulnerability	Matches	False Positives	False Negatives
XXS	22	0	0
SQLI	4	0	0
Blind SQLI	0	0	0
Directory Traversal	0	0	0
CSRF	1	0	0
Command Injection	1	0	0
File Inclusion	2	0	0
Bad HTTP Methods	1	0	0
App Errors	2	0	0
Directory Listing	0	0	0
Informational	17	0	0

HP WebInspect – 10.20.666.10			
PHP Vulnerable Web App (Unauthenticated)			
Vulnerability	Matches	False Positives	False Negatives
XXS	5	2	0
SQLI	1	0	0
Blind SQLI	2	1	0
Directory Traversal	2	1	0
CSRF	0	0	0
Command Injection	0	0	0
File Inclusion	3	2	0
Bad HTTP Methods	1	0	0
App Errors	1	0	0
Directory Listing	2	0	0
Informational	13	0	0

PHP Vulnerable Web App (Authenticated)			
Vulnerability	Matches	False Positives	False Negatives
XXS	5	2	0
SQLI	1	0	0
Blind SQLI	2	1	0
Directory Traversal	2	0	0
CSRF	2	0	0
Command Injection	1	0	0
File Inclusion	3	2	0
Bad HTTP Methods	2	0	0
App Errors	2	0	0
Directory Listing	2	0	0
Informational	56	0	0

JSP Vulnerable Web App (Unauthenticated)			
Vulnerability	Matches	False Positives	False Negatives
XXS	1	0	0
SQLI	0	0	0
Blind SQLI	4	2	0
Directory Traversal	0	0	0
CSRF	0	0	0
Command Injection	0	0	0
File Inclusion	0	0	0
Bad HTTP Methods	0	0	0
App Errors	10	0	0
Directory Listing	0	0	0
Informational	25	0	0

JSP Vulnerable Web App (Authenticated)			
Vulnerability	Matches	False Positives	False Negatives
XXS	1	0	0
SQLI	0	0	0
Blind SQLI	4	2	0
Directory Traversal	0	0	0
CSRF	2	0	0
Command Injection	0	0	0
File Inclusion	0	0	0
Bad HTTP Methods	0	0	0
App Errors	20	4	0
Directory Listing	0	0	0
Informational	45	3	0

.NET Vulnerable Web App (Unauthenticated)			
Vulnerability	Matches	False Positives	False Negatives
XXS	1	0	0
SQLI	0	0	0
Blind SQLI	0	0	0
Directory Traversal	0	0	0
CSRF	0	0	0
Command Injection	0	0	0
File Inclusion	0	0	0
Bad HTTP Methods	0	0	0
App Errors	0	0	0
Directory Listing	0	0	0
Informational	1	0	0

.NET Vulnerable Web App (Authenticated)			
Vulnerability	Matches	False Positives	False Negatives
XXS	16	3	0
SQLI	16	3	0
Blind SQLI	2	1	0
Directory Traversal	0	0	0
CSRF	0	0	0
Command Injection	0	0	1
File Inclusion	1	0	0
Bad HTTP Methods	0	0	0
App Errors	16	0	0
Directory Listing	1	0	0
Informational	11	0	0