tenable.com

Web Applications Under Attack: Tenable.io and the 2017 Verizon DBIR

7-9 minutes

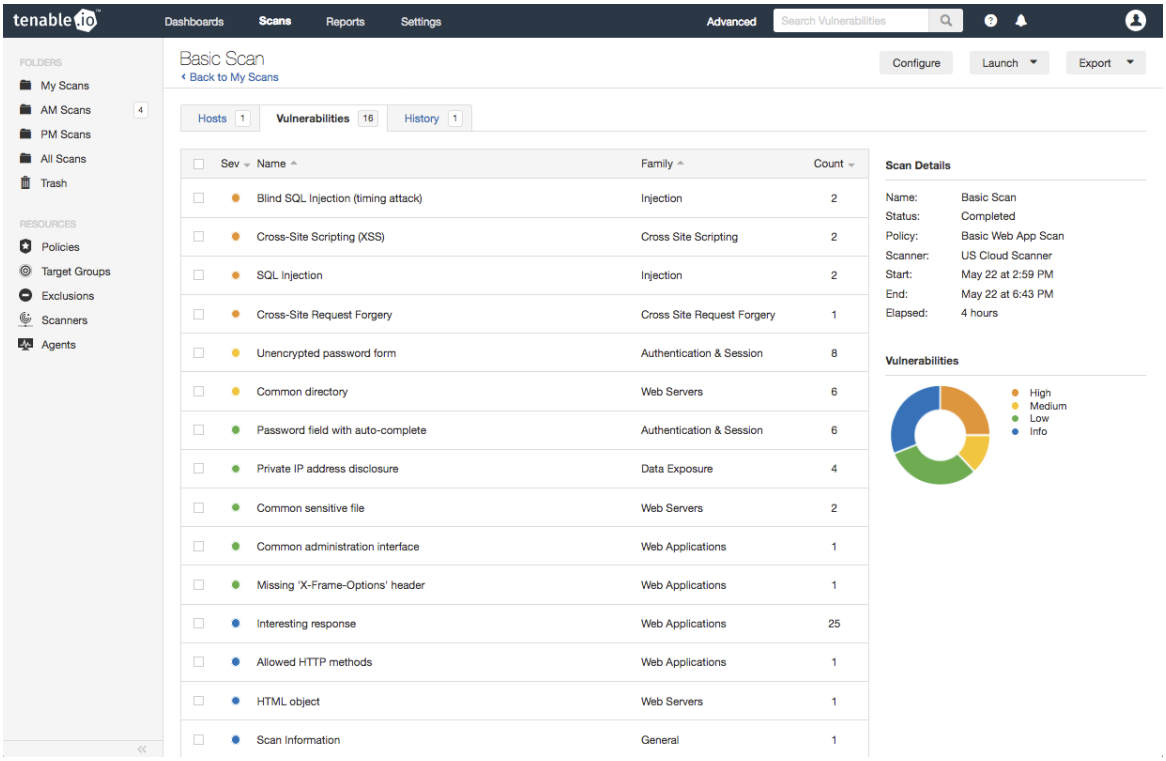
According to the 2017 Verizon Data Breach Investigations Report (DBIR), web applications are under attack even more so than last year (page 57), especially in the financial sector. Primary targets are personal data and credentials: in over half of the reported non-botnet breaches resulting from web application attacks, personal data was compromised. Use of stolen credentials is the top method of hacking web applications, but SQL injection (SQLi) continues to be a dangerous vector (page 58). With enterprises moving more software services to the web, safeguarding the sensitive data handled by web applications is critically important.

“Use of stolen credentials is the top method of hacking web applications”

Tenable.io™ now incorporates Web Application Scanning to help you discover web application vulnerabilities and better protect your data. Tenable.io Web Application Scanning is a new solution from Tenable that offers significant improvements over the existing web application tests provided by the Nessus® scanner. Tenable.io Web Application Scanning is compatible with modern web applications that make heavy use of JavaScript and are built

on HTML5 and AJAX, enabling you to have a more complete picture of the state of your web application security posture. Tenable.io Web Application Scanning offers safe external scanning that ensures production web applications are not disrupted or delayed. The results from a Tenable.io web app scan highlight potential web application problems, offer solution advice, and provide links for more information, including links to the Open Web Application Security Project (OWASP) and the Common Weakness Enumeration (CWE) list of common software security weaknesses.

“Tenable.io Web Application Scanning offers significant improvements over the existing Nessus web application tests”



Stolen information

Attackers can leverage stolen credentials to install software, steal information, and do other nefarious things on your network. While

phishing attacks are the most common way for attackers to obtain credentials, attackers can also obtain credentials and other sensitive information from vulnerable web applications. The DBIR recommends limiting the amount of personal information and credentials stored on web applications and in backend databases (page 58, *Areas of focus*). This recommendation corresponds to security weaknesses A6 (Sensitive Data Exposure) and A5 (Security Misconfiguration) in the OWASP Top Ten, and also to various CWEs, including CWE-200 (Information Exposure).

Tenable.io Web Application Scanning can help you find where sensitive data might be exposed by a web application. While some of the exposed data may not seem particularly sensitive, attackers may be able to make use of the data in subsequent attacks, such as using the information to make phishing attacks seem more genuine. The following is a partial list of the plugins whose results indicate exposed data. You should investigate the results from these and related plugins to determine if any sensitive data is being put at risk, and to take appropriate action.

- **Common Directory** (plugin 98072)
- **Private IP Address Disclosure** (plugin 98077)
- **Email Address Disclosure** (plugin 98078)

Several plugins also highlight website weaknesses that have the potential to expose sensitive data. For example, **Missing 'X-Frame-Options' header** (plugin 98060) detects when the website is at risk for clickjacking, which tricks users into clicking on something different than what they think they're clicking on,

and potentially revealing confidential information. **Unencrypted password form** (plugin 98082) detects when credentials information is not being transmitted securely, potentially revealing the information to anyone sniffing the network traffic.

SQL injection

The DBIR notes (pages 57 and 58) that SQLi is still around, and recommends performing web application scanning and testing to find potential input validation weaknesses. SQLi can be used to dump confidential information from backend databases, and even to modify or delete information within a database. The DBIR recommendation corresponds to the OWASP Top Ten security weakness A1 (Injection) and to CWE-89 (SQL Injection).

Tenable.io Web Application Scanning has several plugins in the injection plugin family that can help you discover SQLi weaknesses in an application, including:

- **SQL Injection** (plugin 98115)
- **NoSQL Injection** (plugin 98116)
- **Blind SQL Injection (timing attack)** (plugin 98118)

The plugin output contains the requests and responses sent to the web application verifying that one or more web pages were vulnerable to SQLi. The solution to SQLi is as it has always been: implementing parameterized queries, aka prepared statements. If you are using third party web applications that are vulnerable to SQLi, upgrade them as soon as possible.

Web application vulnerabilities

This leads to another DBIR recommendation (page 58): consistent patching of content management systems such as WordPress and Drupal, and all their related plugins. This recommendation corresponds to the OWASP Top Ten security weakness A9 (Using Components with Known Vulnerabilities). As with any vulnerabilities, web application and web server vulnerabilities could be – and very likely will be – exploited by attackers to wreak havoc on your network.

Web server vulnerabilities such as outdated versions of Apache or IBM WebSphere can be discovered by doing Nessus scans of your web servers. Monitoring these boxes with the Nessus Network Monitor (formerly PVS™) may also reveal vulnerabilities. Some of these detected vulnerabilities may indicate vulnerabilities in web applications, such as detections of vulnerable versions.

Web application and web server vulnerabilities can also be detected by Tenable.io Web Application Scanning. Various plugins detect misconfigurations and potential vulnerability to attacks such as Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) and code execution. In addition, **Backdoor Detection** (plugin 98097) identifies URLs that contain potential backdoor scripts.

Informational plugins in Tenable.io Web Application Scanning gather additional information about web applications that may be helpful. For example, **Scan Information** (plugin 98000) presents summary information about the scan, such as scan duration, number of requests, and protocols and authentication detected. **Web Application Sitemap** (plugin 98009) provides a hierarchy

of all URLs discovered during the scan, along with the response code and other information for each. **Interesting response** (plugin 98050) notes when a response status code other than 200 (OK) or 404 (Not Found) is returned, which may provide useful insights into the behavior of the web application.

"Tenable.io Web Application Scanning helps you find and fix the top web application attacks noted in the 2017 DBIR"

Tenable.io Web Application Scanning is an important addition to the arsenal of Tenable tools to protect your network. Tenable.io Web Application Scanning helps you find and fix the top web application attacks noted in the 2017 DBIR, enabling you to better secure your web-facing assets, your data and your overall network.

For more information

Tenable.io

- Visit the Tenable.io area of our website
- Start a free Tenable.io Vulnerability Management trial
- Learn about the Tenable.io Web Application Scanning app

2017 Verizon DBIR

- Money, Hackers and Spies: Quick Bytes from Verizon's 2017 DBIR Report
- Back to Basics with the 2017 Verizon DBIR
- Patch or Risk Being Breached: Tenable.io and the Verizon 2017 DBIR

- Blocking and Tackling Unauthorized Access: Tenable.io and the 2017 Verizon DBIR