2020 WEB APPLICATION SECURITY FOR RETAIL & ECOMMERCE

Attack Surface Analysis and Benchmark Study for Top Online Retailers
In a year which we saw a global pandemic leading to a 30% surge in online shopping and exponential growth in cyber security threats for enterprises, our team felt there was no better time but to take a deeper look and analyze the web application attack surface for 20 of the biggest retailers in Europe and the US. Using our innovative Attack Surface Discovery tool - Scout, to provide in-depth data analysis of potential application security flaws and a true picture of the attack surface posed to the top retail businesses in the world. Offering vital context for security professionals working in online retail to refine their cybersecurity program and tooling to successfully combat cybercrime against their business.

Online retail security professionals are becoming more challenged than ever to detect where they’re most vulnerable and how a potential breach may stem from within their increasingly complex digital ecosystem – it’s like finding a needle in a haystack. We help retail organizations quickly discover the digital footprint of their live applications (including ‘staging’ or ‘production’ URLs) as often they are in the dark about how many publicly exposed web apps are out there and the true extent of their attack surface. See detailed methodology on page 10.

In this report we have outlined the results of our 2020 web application security analysis for the top 20 retailers (Deloitte’s Global Powers of Retailing Report 2019) in the US and EU* to highlight the most common attack vectors affecting the sector through aggregated risk scoring to compare and benchmark the risk levels. Enabling security folks to take the right steps to mitigate imminent web application threats affecting their retail business and cyber security hygiene today.

Key report findings:

- **US retailers have a larger attack surface** with an average risk exposure score of 35.1 (out of 42.33) vs an average score of 30.8 for EU retailers
- **US retailers run 3,357 web applications over 401 domains**, with 8% of them considered as suspect (e.g. test environment) and 22% of them running on old components containing known vulnerabilities
- **EU retailers run 2,799 applications over 509 domains**, with 4% considered as suspect (e.g. test environment) and 27% of them are running on old components containing known vulnerabilities
- **Security mechanisms (95); active content (93.3) and degree of distribution (81.5)** are the average top three attack vectors identified across US and EU retailers
- **90% of the top 10 EU retailers are running outdated jQuery vs 50% for US retail**
- Other common issues detected include authentication and insecure servers

---

*EU analysis includes the United Kingdom*
WEB APPLICATION RISK IS A CRITICAL ISSUE THAT NEEDS ADDRESSING

With web applications accounting for 43% of data breaches in 2019, this research brings this to the top of the boardroom agenda in 2020 and digs deeper into the overall retail attack surface - taking a magnifying glass and critical view into the potential risks of the web applications that we all know and shop with regularly.

Using our multi-layered attack surface discovery model, we found US retailers to have a larger attack surface with an average risk exposure score of 35.1 and 30.8 for EU retailers, out of the maximum score of 42.33. This is a worrying trend, as we all know the larger the attack surface, the more likely it is for bad actors to find holes in security defenses and execute potential exploits.

Web application security is a well-known issue faced by organizations worldwide due to the sheer volume of applications they own (the majority they don’t even know exist). How these applications have been built and its makeup can often add an additional threat element to this puzzle. That’s why it is important to understand the key attack vectors hackers use to spot entry points during reconnaissance and work back from there to level the playing field between defenders (your security team) and attackers. Identifying what you own and how this can be targeted by hackers cannot be based on guess work.

From a security perspective, you want to ensure your organization’s web application attack surface is kept at a minimum. The rather high risk scores discovered in our research highlights the need for US and EU retail security professionals to do more to protect their applications, especially if they are business critical and revenue generating, by performing regular pen tests and continuous vulnerability assessments to ensure no backdoors exist.
In the US, we found 3,357 publicly exposed web applications running over 401 domains among the top retailers, with 8% of them considered as suspect and 22% of them running on old components. In the EU, we discovered 2,799 applications running over 509 domains, with 4% considered as suspect and 27% of them running on old components containing known vulnerabilities. ‘Suspect’ are often test environments that have been left online, intentionally or unintentionally, providing a potential backdoor for bad actors to access the production database.

Overall, we found US retailers more up to date than EU retailers in the use of modern application technologies, however with new technology adoption they are twice more likely than their EU counterparts in running shadow IT which creates more open doors and potential risks for US retailers to be attacked.
WHAT EVERY RETAILER SHOULD KNOW ABOUT THEIR ATTACK SURFACE

So, what can retail security professionals learn from this? Our risk score is calculated by evaluating the top retailers’ web applications against the seven most common attack vectors (from 1-100) that hackers would use during reconnaissance.

Hackers are masters of reconnaissance and will go to great lengths to identify a target by looking at how many pages there are per application, if there is outdated software in the architecture and what CMS and associated vulnerabilities it’s built on. All these combined elements pose a threat if managed incorrectly and it only takes a small misstep to give them a foothold into your system and create a catastrophic data breach. Therefore, its crucial to use an attack surface discovery tool like Scout to pinpoint your exposure and apply the right security controls in the right places for maximum protection.
From our research we can see security mechanisms comes out on top with a risk exposure score of >99, active content is a close second place (>97) and degree of distribution (>85) is the third top attack vector affecting online retailers in the US and EU.

In this attack surface spider map you can see the average weightings of the top attack vectors from our research, enabling security professionals to better understand where a hacker can find the open pathways and ensuring you have the right security defenses and budgets assigned.
1. Security mechanism (SM)

Our tool found security mechanism the single biggest attack surface exposure amongst the 7 attack vectors for both US and EU retailers. For retailers using a HTTP website, without encryption, and not restricting access to those adversaries trying to get into unsecured parts of a site, including unsecured redirection, this will increase the attack surface by potentially exposing to bad actors as the data is sent unencrypted, in plain text, for anyone to read, which can lead to credential stuffing.

2. Active content (ACT)

In the second place, we have seen (in some cases applications scoring 100/100) JavaScript and ActiveX controls are commonly used for ecommerce applications with a large product range, with many pages using various active content technologies to display dynamic product information for greater customer experience. In the US we found on the whole more modern technologies are being used compared to the EU, and hence include more active components and scripts. This leaves more doors open for a hacker to insert malicious scripts, and if this goes unnoticed can lead to Magecart attacks and credit card skimming. So although they can help provide a better customer experience, it increases the risk of script-based attacks.

3. Degree of distribution (DOD)

A higher risk exposure score for degree of distribution is common within retail applications, as they tend to have a large number of pages due to the volume of products on sale for customers to purchase. However this directly increases the attack surface as the more pages there are, the harder it is to keep on top of the security hygiene of every single page on every domain, the input vectors and fields, and where the pages are linking internally and externally, giving bad actors more pathways and vulnerabilities to enter or exploit.
OTHER COMMON ATTACK VECTORS AFFECTING RETAILERS

Authentication is essential for ecommerce sites as it verifies the identity of the user and determines whether they can gain access to restricted areas of the application based on assigned user roles and privileges. With online fraud on the rise due to the surge in online shopping during the pandemic, hackers are looking to drive successful Account Takeover fraud (ATO) attacks. We found 90% of US retail web applications with authentication mechanisms vs 20% in the EU. Authentication on your application takes place when a customer checks out or updates the contents on the app and is key for retailers to keep unauthorized users out.

But the presence of authentication mechanisms could also be a breeding ground for vulnerabilities, like weak password standards and brute-force attacks. Therefore, it’s advisable to keep only the necessary authentication required to minimize the attack surface.

In addition, we also found up to 90% of EU retailers and 50% US retailers to be running outdated jQuery versions. By using an older version, it’ll open the retailer up to exploitable vulnerabilities in jQuery’s like cross site scripting (XXS) attacks. Web applications running on components which are out of date are more likely to be vulnerable and could include bugs and increases the likelihood for a variety of application attacks.

In our research we also found retailers using a variety of outdated servers to run their applications from Amazon S3 to older versions of the Apache Server, meaning they’re at risk of Apache bugs granting hackers access to your shared hosting environment. Therefore it’s critical for retailers to ensure their servers are kept up to date with the latest upgrade, close down servers no longer in use, to prevent web servers from being compromised through denial of service (DoS) attacks. We have also discovered the use of outdated components and servers, including Microsoft IIS (version 8.5) containing known vulnerabilities, making it easy for attackers to carry out privilege escalation or perform HTTP request smuggling attacks.

How the application is built and developed is an indicator for our Scout tool to analyze how vulnerable you are as the file directories used to build your website and development technologies like PHP generators which are commonly used in ‘out of the box’ applications CMS and ecommerce (Drupal, WordPress and Magento) can carry vulnerabilities like the recent WordPress breaches show and prove how important it is to ensure these are kept up to date.
MEETING THE RETAIL APPLICATION SECURITY CHALLENGE

Our research shows the complexity of modern-day retail applications and how debunking the attack surface can help security professionals to focus on their biggest risks.

Best practice for securing your web applications

The dynamic nature of retail applications mean security must be continuous. Outpost24’s Application Security Program (ASP) is designed to help customers take a proactive view of their internet facing applications through continuous Discovery, Scoring, Alignment, Assessment and Reporting for successful integration with their application development workflow to fit your business needs and risk criticality levels.

- **Discovery.** Helping organizations uncover what applications they own that are externally accessible and visible to threat actors.
- **Scoring.** Provides an attack surface score for each of the discovered applications against the 7 most common attack vectors.
- **Alignment.** Aligning discovered applications against their business criticality and application development lifecycle and zooming in on the high risk areas for further investigation.
- **Assessment.** Systematically onboard problem applications for either a one-off assessment (e.g. manual testing), or continuous (DAST scanning).
- **Reporting.** Real time insights guiding organizations on the steps they need to take to reduce web application risks.

This best practice process creates an application repository CMDB, gathering the pertinent information for each application, along with the attack surface score and other information from the discovery, scoring and assessment phases of the program to ensure you have visibility of your entire digital facing ecosystem. Retailers can use the data and intelligence built up over time to better understand their risks and apply effective remediation as their attack surface evolves, hence improving their application security accordingly and in a continuous process.

Talk to us
Methodology for Web Application Discovery and Attack Surface Analysis

We help retailers locate suspected applications based on the common seven web attack vectors (page 5) and providing a risk exposure score to guide their remediation effort. Outpost24 Scout, a web application discovery and attack surface assessment tool, uses the following set of processes and techniques to simulate a web application reconnaissance, just like a threat actor would do. Starting with information gathering to discover the potential weakness and entry points.

The 7 Steps during RECONNAISSANCE

- **R1:** Gather information
- **R2:** Determine the range (domain)
- **R3:** Identify active web applications
- **R4:** Discover open doors and entry points (7 vectors)
- **R5:** Fingerprint the web app (score)
- **R6:** Uncover components behind those doors (components detection)
- **R7:** Map the apps (crawl)

Outpost24 uses multiple discovery techniques to assess a Web Application against the seven vectors by crawling publicly available domains and application components to determine the attack surface with a spider chart and risk rating (1 to 42.3).

- **V1:** Security Mechanisms (SM) - How the traffic between users and the application is secured i.e is there authentication in place?
- **V2:** Page Creation Method (PCM) - This depends on the code the web app has been developed in. Developing websites with insecure code or using outdated versions increases the risks of potential vulnerabilities.
- **V3:** Degree of Distribution (DOD) - The more pages you have, the more risks there are, all pages must be identified, and vulnerabilities uncovered at all levels.
- **V4:** Authentication (AUTH) - This is the process of verifying the identity of an individual accessing your application. Access to certain actions or pages can be restricted using user levels set up by the administrator and critical to keeping the bad guys out.
- **V5:** Input Vectors (IV) - The attack surface increases with the number of different input fields you have on a web application which can lead to a range of XSS attack.
- **V6:** Active Content (ACT) - When an application runs scripts the content becomes active, and depending on the way those scripts have been implemented, the attack surface could increase if a website has been developed using several active content technologies.
- **V7:** Cookies (CS) - Cookies are essential for real time application security, by monitoring session activity and ensuring anyone who sends requests to your website are allowed access and keep hackers away from unauthorized areas.

The attack surface is an indication of the risk level. For example, we may have identified an application with missing SSL encryption (active application on port 80 rather than the more secure 443 port). The scan can also detect whether the application is running on out of date components which hasn’t been hardened and poses a potential threat. The tool simply provides a spotlight on the areas that could lead to potential vulnerabilities and exposure (not a full vulnerability assessment report), helping security leaders prioritize what’s most urgent for further investigation, whether it’s through pen testing or application security scanning. More information can be found here.
Top retailers analyzed

For EU

1. Schwarz Group (Germany)
2. Aldi (Germany)
3. Tesco (UK)
4. Ahold Delhaize (Netherlands)
5. Edeka Group (Germany)
6. Auchan (France)
7. Rewe Combine (Germany)
8. E. Leclerc (France)
9. Casino Guichard-Perrachon (France)
10. IKEA (Sweden)

For US

1. Walmart
2. Costco
3. Amazon US
4. The Kroger
5. Walgreens Boots Alliance
6. The Home Depot
7. CVS Health Corporation
8. Target
9. Lowe's
10. Albertsons Companies

Based on Deloitte Global Powers of Retailing 2019

This retail attack surface analysis was conducted between July to September 2020 using our Attack Surface Discovery tool - Scout and is based on the US and EU retailers in the Deloitte Global Powers of Retailing Report 2019.

All information collected or assets scanned are available from the public domain. At no point unauthorized access was used. All data is presented in an aggregated manner to ensure individual retailer performance and scoring remain anonymous. If any of the named retailers would like to request a full disclosure of our findings in this research please contact info@outpost24.com
ABOUT US AND CONCLUSION

As hackers become even more relentless and we see data breaches and fines increasing, it’s never been more essential for businesses, especially in the retail space, who manage details for thousands of shoppers and their personal information (PII) to maintain visibility of their online attack surface to mitigate against harmful cyber risks more proactively and effectively. Scout helps by providing a true picture of your current attack surface and enables you to direct your time and resources correctly to deal with the real threats effecting your online business. Protecting your digital ecosystem in the long term as one breach can lead to irreparable brand damage and financial loss – this isn’t just an issue for CISO’s but for the entire retail business to understand to support business growth.

Whether you’re at risk of cross site scripting, by running out of date software or credential stuffing from lack of encryption we’ll find it, even if you don’t have visibility of all the applications you own. As shown in this report our Scout tool uses in-depth, multiple discovery techniques used by hackers during reconnaissance to provide the most accurate risk score of US and EU retail web apps taking away the guess work of assessing your entire application landscape. Allowing you more time to focus on what matters most by providing a complete blueprint of your web app security posture so you can apply the right security controls to the right places and optimize protection.

Request your full web app assessment

---

**Outpost24 Europe Headquarters**
Skeppsbrokajen 8
SE-371 33 Karlskrona,
Sweden
Phone: +46 455 612 300
info@outpost24.com

**Outpost24 US Headquarters**
35, S Washington St.
Suite 308
Naperville, IL 60540
Phone: +1 (630) 352 2283