دانشگاه شهید بهشتی

دانشکده مهندسی و علوم کامپیوتر

گزارش پروژه پایانی درس امنیت شبکه های کامپیوتری

بررسی مقاله پژوهشی با عنوان «سیاست امنیتی پیچیده؟ تحلیل طولی استقرار سیاست های امنیت محتوا (CSP)» اثر سباستین راث و همکاران

نگارش

سهیل ضیائی قهنویه

استاد

دکتر مقصود عباسپور

تیر ماه ۱۴۰۰

چکیده

در این گزارش، مقاله پژوهشی با عنوان «سیاست امنیتی پیچیده؟ تحلیل طولی استقرار سیاست های امنیت محتوا[1] اثر سباستین راث و همکاران مورد مطالعه و بررسی قرار گرفته و ضمن انعکاس نکات کلیدی، نقاط قوت و ضعف آن در پایان جمع بندی شده است. در مقاله مذکور پس از معرفی سیاست های امنیت محتوا (CSP) به عنوان راهکاری برای دفع حملات تزریق کد، با جمع آوری و تحلیل داده های حدود ۱۰ هزار نمونه از وب سایت های پر بازدید در طول سال های ۲۰۱۲ تا ۲۰۱۸، سیر به کارگیری این سیاست ها در وب با سه کاربرد اصلی محدود سازی محتوا، الزام به ارتباط امن، و محدود سازی استفاده در فریم مورد مطالعه و تحقیق قرار گرفته است. یافته های این مقاله به همراه تحقیق میدانی و نظر سنجی از مدیران وب سایت های مورد مطالعه، چالش اصلی استقرار سیاست های امنیت محتوا را پیچیدگی پیاده سازی آن ها از دید توسعه دهندگان و مدیران وب سایت ها معرفی می کند.

کلیدواژه‌ها

سیاست های امنیت محتوا، تزریق کد، محدود سازی محتوا، الزام به ارتباط امن، محدود سازی استفاده در فریم

[1] Complex Security Policy? A Longitudinal Analysis of Deployed Content Security Policies

فهرست نوشتار

بخش اول: مقدمه

معرفی مقاله

در این گزارش، مقاله پژوهشی مرجع [1] مورد مطالعه و بررسی قرار گرفته است. مقاله مذکور با عنوان «سیاست امنیتی پیچیده؟ تحلیل طولی استقرار سیاست های امنیت محتوا» با هدف بررسی علل عدم پذیرش و استقرار گسترده سیاست های امنیت محتوا[۲]- که از این پس با عنوان CSP از آن یاد می کنیم - داده های حدود ۱۰ هزار نمونه از وب سایت های پر بازدید در طول سال های ۲۰۱۲ تا ۲۰۱۸ را جمع آوری و تحلیل نموده است. همچنین در کنار تحلیل روند استقرار CSP در طول زمان، نظرسنجی ای از مدیران و توسعه دهندگان وب سایت های مذکور به عمل آمده است که در نهایت پیچیدگی استفاده از این مکانیزم را به عنوان علت اصلی عدم پذیرش آن معرفی می نماید.

معرفی سیاست های امنیت محتوا (CSP)

سیاست های امنیت محتوا، یکی از استانداردهای امنیتی وب است که در قالب سرآیند پاسخ HTTP[۳] با نام content-security-policy سیاست هایی را جهت به کارگیری محتوای ارائه شده از سرور به مرورگرها تجویز می کند. برخلاف سایر مکانیزم های امنیتی که تعداد محدودی گزینه های پیکربندی دارند، CSP به توسعه دهندگان وب اجازه می دهد تا سیاست های پیچیده و مبتنی بر لیست سفید را برای تعیین دقیق منابع قابل اعتماد برای طیف گسترده ای از محتوا از جمله جاوا اسکریپت، تصاویر، پلاگین ها، و فونت ها تنظیم کنند.

ساختار گزارش

در ادامه این گزارش نتایج مطالعه دقیق مقاله شامل: تشریح صورت مسئله، تشریح راه حل، و در نهایت بحث و نقد این مقاله ارائه می گردد.

---

۲ Content Security Policy (CSP)

۳ Response Header

بخش دوم: تشریح صورت مسئله مقاله

صورت مسئله

استفاده از CSP به دلیل امکانات گسترده امنیتی که در اختیار توسعه دهندگان وب قرار می دهد، گزینه مناسبی برای جلوگیری از بسیاری از حملات وب به شمار می آید، ولی نویسندگان مقاله بنا بر مطالعات پیشین بر این باورند که پذیرش این مکانیزم و استقرار آن بسیار کمتر از حد انتظار بوده است. به همین منظور، نویسندگان مقاله تلاش کرده اند ضمن جمع آوری داده ها و تحلیل روند به کار گیری CSP در طول زمان و انجام مطالعات میدانی از طریق مکاتبه و نظرسنجی علت این عدم پذیرش و استقرار را ارائه نمایند.

اهمیت مسئله

یکی از انگیزه های اولیه طراحی CSP مقابله با حملات تزریق کد (XSS)[۴] بوده است. در این گونه حملات، پس از برقراری ارتباط مرورگر قربانی با یک سرور وب سایت، کد های مهاجم به نحوی در پاسخ سرور به مرورگر تزریق و در سیستم قربانی اجرا می شود که امنیت و محرمانگی اطلاعات آن را به خطر می اندازد. با استفاده از CSP، با محدود سازی منابع قابل اعتماد محتوا از جمله منابع کدها و اسکریپت ها از حملات XSS جلوگیری به عمل می آید. هرچند راهکارهای دیگری برای جلوگیری از حمله مذکور ارائه شده است ولی پیکربندی متمرکز CSP از طریق دستورات استاندارد متنوع از مزیت های آن به شمار می آید. تلاش ها و هزینه های بسیاری برای طراحی و پیاده سازی این مکانیزم به کار بسته شده است و همچنین مرورگرهای مختلف برای پشتیبانی از این راهکار استاندارد هزینه های زیادی صرف کرده اند؛ به همین دلیل، ریشه یابی علت عدم استقرار آن از اهمیت بالایی برخوردار است.

[۴] Cross Site Scripting (XSS)

بخش سوم: تشریح راه حل مقاله

روش پژوهش

بر خلاف مقالات دیگر که به بررسی میزان آسیب پذیری CSP پرداخته شده، در این مقاله مجموعه داده ای از میزان و نحوه به کار گیری CSP در طول زمان ساخته شده و بر اساس آن تحلیل های مختلفی از روند کاربرد این مکانیزم در وب ارائه گردیده است. بخشی از تحلیل های ارائه شده، توسط مکاتبه و نظرسنجی مورد ارزیابی قرار گرفته و در قالب نتایج جمع بندی شده است.

ساخت مجموعه داده

از آن جا که پشتیبانی مرورگرها از CSP تقریبا در ۲۰۱۲ کامل شده، مقاله تمرکز خود را بر بازه زمانی سال های ۲۰۱۲ تا ۲۰۱۸ قرار داده است. در بازه زمانی مذکور، برای هر ماه لیستی از ۵۰ هزار وب سایت پربازدید بر اساس اطلاعات Alexa استخراج شده و پس از اشتراک گیری و امتیاز دهی، در نهایت ۱۰ هزار وب سایت با امتیاز بالاتر جهت ساخت مجموعه داده انتخاب شده است. پس از آن آرشیو CSP از سرآیند های هر یک از وب سایت های مذکور برای هر روز در بازه زمانی مذکور از Internet Archive به نشانی https://archive.org/ استخراج شده است. به ازای روزهایی که آرشیو وجود نداشته، CSP روز قبلی (به صورت بازگشتی) جایگزین شده که به نظر می رسد تأثیر به سزایی در روش پژوهش نداشته باشد. در نهایت مجموعه داده CSP های سایت های پربازدید بازه زمانی پژوهش شامل فقط زمان های تغییر CSP تشکیل داده شده است که در نشانی https://archive-csp.github.io موجود است.

اعتبارسنجی مجموعه داده

مقاله ضمن معرفی روش استخراج داده ها و تشکیل مجموعه داده، به دو دلیل زیر اعتبار این مجموعه را خالی از اشکال نمی دانسته و سعی در رفع ابهامات در این زمینه داشته است:

۱- داده های آرشیوی نادرست: به دلیل عدم شفافیت تأثیر نحوه آرشیو اطلاعات وب سایت های مختلف در Internet Archive داده های جمع آوری شده با منبع دیگری با عنوان Common Crawl به نشانی http://commoncrawl.org کنترل و با توجه به کشف منشأ مغایرت های بین دو منبع، تا حد زیادی از اعتبار مجموعه داده اصلی اطمینان حاصل شده است.

۲- به کار گیری CSP در قالب Meta Tag: یکی دیگر از روش های پیاده سازی CSP، درج دستورات در Meta Tag به جای سرآیند HTTP معرفی شده است. Meta Tag ها در Internet Archive به دلیل پرهیز از تداخل حذف می شوند و این نگرانی وجود دارد که بررسی پیاده سازی تنها از طریق بررسی سرآیند content-security-policy ممکن است دقیق و صحیح نباشد. بررسی و مقایسه Meta Tag ها و سرآیند های HTTP و مشاهده مغایرت جزئی در آخرین وضعیت هر یک از وب سایت های مورد پژوهش به نویسندگان مقاله این اطمینان را داده است که بررسی سرآیندها به تنهایی می تواند تا حد بسیار زیادی معادل بررسی پیاده سازی CSP باشد.

روش تحلیل داده ها

برای تحلیل و بررسی پیرامون به کار گیری CSP، سه مورد کاربرد مد نظر قرار گرفته است:

۱- محدود سازی محتوا[۵] مورد کاربرد اصلی CSP که در برگیرنده دستورات script-src و default-src می باشد.

۲- الزام به ارتباط امن[۶] در برگیرنده دستورات upgrade-insecure-requests، block-all-mixed-content و لیست سفید از منابعی که فقط HTTPS باشند.

۳- محدود سازی استفاده در فریم[۷] در برگیرنده دستور frame-ancestors

برای هر یک از سه مورد کاربرد فوق سه روند زیر در وب سایت های مورد پژوهش در بازه زمانی مذکور، بررسی شده و توجیهات منطقی برای این روندها ارائه شده است:

۱- شروع به کارگیری CSP

۲- تغییرات به کارگیری CSP

۳- پایان به کارگیری CSP

با استفاده از داده های تاریخی جمع آوری شده، در کنار تحلیل روندهای فوق، تحلیلی از میزان امنیت وب سایت ها بعد از به کارگیری CSP در موارد کاربرد مذکور هم انجام شده است؛ با این هدف که شاید بخشی از دلایل عدم تمایل یا انصراف توسعه دهندگان وب از به کارگیری این مکانیزم، عدم رفع آسیب پذیری های امنیتی به واسطه پیاده سازی ناقص یا نادرست آن بوده باشد.

روش ارزیابی

نویسندگان مقاله برای تأیید تحلیل های استخراج شده از روند تغییرات به کارگیری CSP به ویژه در مورد کاربرد سوم، اقدام به

---

[۵] Script Content Restriction

[۶] TLS Enforcement

[۷] Framing Control

مکاتبه با متولیان وب سایت های مورد پژوهش نموده اند و پاسخ های دریافت شده از طرف توسعه دهندگان و مدیران وب سایت ها در کنار تحلیل داده های تاریخی به شکل دهی یافته های مقاله انجامیده است.

نتایج

یکی از دستاوردهای مقاله، ثبت روند مورد کاربرد های دیگر برای به کارگیری CSP عنوان شده است، با این توضیح که هرچند انگیزه اولیه طراحی CSP کاهش آسیب پذیری در برابر حملات تزریق کد بوده است، ولی در طول زمان برای دیگر موارد کاربرد از جمله الزام به ارتباط امن و محدودسازی استفاده در فریم هم به کار رفته است.

یکی دیگر از دستاوردهای مقاله مستندسازی چالش هایی است که توسعه دهندگان وب در پیاده سازی CSP با آن ها مواجه بوده اند. از جمله اینکه امن ترین CSP ها هم به واسطه غلط املایی[۸] و نیز عدم به روزرسانی دامنه های منقضی شده در لیست سفید در معرض تهدید قرار می گیرند.

به نظر می رسد به کارگیری CSP در مورد کاربرد اصلی محدودسازی محتوا آینده موفقی نداشته باشد؛ به علاوه هرچند به موارد کاربرد الزام به ارتباط امن و محدودسازی استفاده در فریم رشد داشته اند ولی هنوز هم به حد مورد انتظار نرسیده اند.

یافته های نظرسنجی نشان می دهد که CSP به خاطر پیچیدگی های پیاده سازی مورد کاربرد اصلی خود (محدود سازی محتوا) شهرت نه چندان مطلوبی کسب کرده، به گونه ای که توسعه دهنگان وب را از دیگر موارد کاربرد هم منصرف نموده است و در مجموع باعث شده CSP جایگاه اصلی خود در بهبود امنیت وب را از دست بدهد.

---

[۸] Typo

بخش چهارم: بحث و نقد مقاله

نقاط قوت

به عنوان یکی از نقاط قوت این مقاله، می توان از حل نسبتاً قابل قبول صورت مسأله که بررسی علت عدم اقبال توسعه دهندگان وب به استفاده از CSP در تقویت امنیت وب می باشد نام برد. صورت مسأله با مطالعه اقدامات پژوهشی پیشین در این زمینه مورد توجه نویسندگان قرار گرفته است و توانسته روش پژوهشی شامل ساخت و ارزیابی مجموعه داده، و تعریف نکات حائز اهمیت برای تحلیل این مجموعه را هدفمند به پیش ببرد.

همچنین ضمن آماده سازی مقدمات قابل قبولی از پیشینه مباحث مورد پژوهش، به بخش زیادی از نقاط ابهام و نگرانی هایی که ممکن است از شیوه پژوهش در ذهن مخاطبین متبادر گردد، پاسخ های قابل قبول کیفی و کمی به همراه آمار ارائه شده است.

نقاط ضعف

هرچند در یکی از موارد کاربرد CSP (بحث محدودسازی فریم) سعی شده است از مکاتبه و نظرسنجی به عنوان ارزیابی نتایج حاصله استفاده شود، ولی یکی از بزرگترین نقاط ضعف این مقاله عدم تعریف معیار ارزیابی و به صورت کلی عدم ارزیابی مدون و هدفمند نتایج می باشد. به این ترتیب اکثر یافته های مقاله بدون قابلیت ارزیابی، صرفا منعکس کننده تحلیل و استنباط شخصی نویسندگان است. در صورتی که نظرسنجی از توسعه دهندگان وب به عنوان معیار ارزیابی یافته های این مقاله در نظر گرفته شود، پیشنهاد می شود به عنوان یکی از کارهای آتی این نظر سنجی در تمام یافته های مقاله اجرا شود.

یکی دیگر از ایرادات وارده به مقاله، ارائه ناقص مجموعه داده مورد بحث می باشد؛ مجموعه داده ثبت شده در نشانی https://archive-csp.github.io صرفا شامل اطلاعات تاریخچه سرآیندهای حدود ۱۲۰۰ وب سایت می باشد، در صورتی که دامنه پژوهش در مقاله ۱۰ هزار وب سایت اعلام شده است و در متن توضیحی در خصوص علت این مغایرت به چشم نمی خورد. این ضعف باعث می شود پیاده سازی و صحت سنجی بخشی از نتایج امکان پذیر نباشد.

مراجع

[1] S. Roth, T. Barron, S. Calzavara, N. Nikiforakis and B. Stock, "Complex Security Policy? A Longitudinal Analysis of Deployed Content Security Policies," in *Network and Distributed Systems Security (NDSS) Symposium*, San Diego, 2020.