

۱۲۹۹/۱/۱۱

# مهمترین آسیب‌پذیری‌های وبگاه‌ها

مؤلفین :

یاسر نبهانی

ابراهیم دهقانی

مید. رضا اسماعیلی

عنیرضا بزرگ‌بی

قاسم صبری گل



**NAGHOOS  
PUBLICATION**

عنوان و نام پدیدآور : مهمترین آسیب‌پذیری‌های وبگاه‌ها/ مولف یاسر نبهانی... و [دیگران].  
 مشخصات نشر : تهران: انتشارات ناقوس، ۱۳۹۴.  
 مشخصات ظاهری : ۲۵۸ ص. مصور، جدول.  
 شابک : ۹۷۸-۹۶۴-۳۷۷-۸۲۴-۸ بها : ۱۶۰,۰۰۰ ریال

وضعیت فهرست‌نویسی : فیا  
 یادداشت : مولف یاسر نبهانی، ابراهیم دهقانی، حمیدرضا اسماعیلی، علیرضا بهالگردی، قاسم صفری کلی  
 یادداشت : کتابنامه:  
 موضوع : وبگاه‌ها—تدابیر ایمنی  
 موضوع : ویلاک‌ها—ایران  
 شناسه رده : نبهانی، یاسر، ۱۳۵۹  
 رده بندی کتره : TK۵۱۰۵/۵۹/م۸۳ ۱۳۹۴  
 رده بندی دیویر : ۰۰۰/۸  
 شماره کتابشناسی ملی : ۴۰۰۰۸۳



برای دیدن Online به آدرس زیر مراجعه کنید:

[www.naghoospress.ir](http://www.naghoospress.ir)

انتشارات ناقوس

چاپ اول

نام کتاب : مهمترین آسیب‌پذیری‌های وبگاه‌ها

ناشر : انتشارات ناقوس

مؤلفین : یاسر نبهانی، ابراهیم دهقانی، حمیدرضا اسماعیلی، علیرضا بهالگردی، قاسم صفری کلی

چاپ اول : ۱۳۹۴

تیراژ : ۵۰۰ جلد

چاپ و صحافی : نارنجستان

سرپرست صفحه‌آرا : صدف پورعبدی

قیمت : ۱۶۰,۰۰۰ ریال

شابک : ۹۷۸-۹۶۴-۳۷۷-۸۲۴-۸

ISBN : 978-964-377-824-8

S.M.S : ۳۰۵۰۴۵۲۳۲

کلیه حقوق برای ناشر محفوظ است.  
 تکثیر تمامی این اثر به‌صورت  
 حرفه‌ای، چاپ مجدد، چاپ افست، پلی‌کپی،  
 فتوکپی و انواع دیگر چاپ ممنوع است و  
 پیگرد قانونی دارد.

مرکز پخش: انتشارات ناقوس

۱- خیابان انقلاب-خیابان ۱۲ فروردین- بین وحدت‌نظری و روانمهر- بزرگ‌ترین حقیقت- پلاک ۴

تلفن و فاکس : ۶۶۴۷۸۹۵۸-۶۶۴۷۸۹۵۷

۲- کتابفروشی الباس: خیابان انقلاب، نیش ۱۲ فروردین تلفن: ۶۶۴۰۵۰۸۴

۳- کتابفروشی گلریزان: ضلع جنوب‌شرقی میدان انقلاب، پلاک ۱۱ تلفن: ۶۶۹۷۶۲۳۰

## پیشگفتار

همگام با گسترش شتابان فن آوری اطلاعات در همه حوزه های زندگی بشر، مخاطرات مرتبط با آن نیز در حال افزایش است.

در حوزه فن آوری اطلاعات تا کنون حدود ۷۰ هزار آسیب پذیری به صورت CVE<sup>۱</sup> در وبگاه [cve.mitre.org](http://cve.mitre.org) ثبت گردیده است. در سال نیز حدود ۶ تا ۷ هزار آسیب پذیری جدید ثبت می گردد. بخشی از این آسیب پذیری ها می توانند وبگاه ها را تحت تاثیر قرار داده و در مواردی هم ممکن است خطر آفرین باشند.

هر ساله آسیب پذیری ها جدیدی در حوزه وب منتشر می گردد که امنیت وبگاه ها و برنامه های کاربردی وبی را به خطر می اندازد. ضروری است این آسیب پذیری ها به صورت مداوم و روزآمد، در اختیار مراکز ارزیابی امنیتی و تیم های طراحی و توسعه نرم افزار قرار گیرد. این اطلاعات می توانند هم در انجام ارزیابی ها و هم در تولید امن محصولات نرم افزاری مورد استفاده قرار گیرد.

در این کتاب آسیب پذیری هایی از وبگاه ها که در سال ۲۰۱۴ انتشار یافته، بررسی شده و مواردی که خطر آفرین و قابل تست بوده، مد نظر قرار گرفته است.

بنابر این مولفین تمام آسیب پذیری های ارائه شده در این عملیاتی تست نموده و روش تست هر کدام را در جای خود آورده اند. تعداد آسیب پذیری هایی که با این ویژگی ها انتخاب گردیده به ۱۵۰ مورد می رسد که به همراه توصیف و ارائه راهکارهای پیشگیری از آن آمده است.

در نگاهی گذرا به فهرست آسیب پذیری های استخراج شده، می توان دریافت که چه سامانه هایی در این حوزه بیشتر در معرض آسیب می باشند.

با مطالعه این کتاب خواهید دید بیشتر سامانه های آسیب پذیر، سامانه های متن باز با ریشه php بوده اند. همچنین در می باید با به کار بستن ۱۳ راهکار پیشگیری ارائه شده در انتهای کتاب، می توانید تقریباً از تمامی این آسیب پذیری ها پیشگیری نمایید. این اطلاعات می تواند برای تولید کنندگان و استفاده کنندگان نرم افزار های حوزه وب مفید واقع شود.

امیدواریم با تألیف این کتاب توانسته باشیم گامی هر چند کوچک در جهت ارتقاء امنیت فضای تبادل اطلاعات کشور برداشته باشیم.

در پایان از تمامی خوانندگان گرامی درخواست داریم با ارسال نظرات سازنده خود به آدرس رایانامه [webvul@payanmail.ir](mailto:webvul@payanmail.ir) ما را در این راه یاری رسانند.

۱ CVE مخفف عبارت common vulnerabilities and exposure و استاندارد برای نام های آسیب پذیری امنیت اطلاعات می باشد.

## فهرست مطالب

|    |                                                                                                                  |
|----|------------------------------------------------------------------------------------------------------------------|
| ۱۳ | فصل اول: سامانه های مدیریت محتوا و ایجاد وبگاه                                                                   |
| ۱۴ | ۱.۱. NULL NUKE CMS                                                                                               |
| ۱۴ | ۱.۲. آسیب پذیری تزریق SQL در سامانه مدیریت محتوای NULL NUKE CMS 2.2                                              |
| ۱۶ | ۱.۳. آسیب پذیری CSRF در سامانه مدیریت محتوای NULL NUKE CMS 2.2                                                   |
| ۱۷ | ۱.۴. آسیب پذیری تزریق اسکریپت در سامانه مدیریت محتوای NULL NUKE CMS 2.2                                          |
| ۱۹ | ۱.۵. آسیب پذیری بارگذاری فایل در سامانه مدیریت محتوای NULL NUKE CMS 2.2                                          |
| ۲۰ | ۱.۶. آسیب پذیری حذف فایل ها در سامانه مدیریت محتوای NULL NUKE CMS 2.2                                            |
| ۲۲ | ۱.۷. آسیب پذیری خواندن فایل ها در سامانه مدیریت محتوای NULL NUKE CMS 2.2                                         |
| ۲۳ | ۱.۸. آسیب پذیری تغییر مسیر در سامانه مدیریت محتوای NULL NUKE CMS 2.2                                             |
| ۲۵ | ۲. Wordpress                                                                                                     |
| ۲۶ | ۲.۱. امکان بارگذاری فایل PHP در Wordpress Work-Flow Plugin 1.2.1                                                 |
| ۲۷ | ۲.۲. آسیب پذیری تزریق فایل در Wordpress Theme LineNity 1.20                                                      |
| ۲۸ | ۲.۳. آسیب پذیری CSRF در Wordpress Quick Page/Post Redirect Plugin                                                |
| ۳۰ | ۲.۴. آسیب پذیری تزریق اسکریپت در Wordpress Quick Page/Post Redirect Plugin                                       |
| ۳۲ | ۲.۵. آسیب پذیری CSRF در Wordpress Twitget Plugin                                                                 |
| ۳۳ | ۲.۶. آسیب پذیری CSRF در Wordpress XCloner Plugin 3.1.0                                                           |
| ۳۵ | ۲.۷. حمله تزریق sql در پلاگین CP Multi View Event Calendar نسخه 1.01 از نرم افزار مدیریت محتوای Wordpress        |
| ۳۶ | ۲.۸. آسیب پذیری تزریق sql کور در پلاگین YourMembers از نرم افزار وردپرس                                          |
| ۳۷ | ۲.۹. آسیب پذیری ارسال فایل مخرب در Wordpress Slideshow Gallery نسخه ۱.۴.۶                                        |
| ۳۸ | ۲.۱۰. آسیب پذیری XSS/CSRF در پلاگین Wordpress Login Widget With Shortcode نسخه ۳.۱.۱                             |
| ۴۰ | ۲.۱۱. آسیب پذیری CSRF در پلاگین Bulk Delete Users by Email نسخه ۱.۰ از نرم افزار مدیریت محتوای Wordpress         |
| ۴۲ | ۲.۱۲. آسیب پذیری داتلود فایل در پلاگین Acento Theme از نرم افزار مدیریت محتوای Wordpress                         |
| ۴۳ | ۲.۱۳. آسیب پذیری تزریق SQL پلاگین Participants Database نسخه ۱.۵.۴.۸ از نرم افزار مدیریت محتوای wordpress        |
| ۴۵ | ۲.۱۴. آسیب پذیری ارسال فایل مخرب در پلاگین Wp Symposium نسخه ۱۴.۱۱ از نرم افزار Wordpress                        |
| ۵۰ | ۲.۱۵. آسیب پذیری بارگذاری فایل در پلاگین Wordpress Photo Gallery نسخه ۱.۲.۵ از نرم افزار مدیریت محتوای Wordpress |
| ۵۲ | ۲.۱۶. آسیب پذیری تزریق SQL در پلاگین Document Embedder Google از نرم افزار مدیریت محتوای Wordpress               |
| ۵۴ | ۲.۱۷. آسیب پذیری پیمایش مسیر در DukaPress نسخه ۲.۵.۲                                                             |
| ۵۵ | ۲.۱۸. آسیب پذیری تزریق SQL در پلاگین Cart66 Lite Ecommerce نسخه ۱.۵.۱.۱۷ از نرم افزار مدیریت محتوای Wordpress    |

|    |                                                                                                            |
|----|------------------------------------------------------------------------------------------------------------|
| ۵۷ | ۲۶. آسیب‌پذیری دانلود فایل در پلاگین CodeArt Google MP3 Player از نرم‌افزار مدیریت محتوای WordPress        |
| ۵۸ | ۲۷. آسیب‌پذیری دانلود فایل در WordPress DB Backup Plugin                                                   |
| ۵۹ | ۲۸. آسیب‌پذیری تزریق SQL در پلاگین Symposium نسخه ۱۴.۱۰ از نرم‌افزار مدیریت محتوای WordPress               |
| ۶۰ | ۲۹. تزریق SQL تصدیق شده در افزونه گالری تصاویر Huge-IT 1.0.1 برای سامانه مدیریت محتوای Wordpress           |
| ۶۱ | ۳۰. آسیب‌پذیری قابلیت دانلود دلخواه برای Wordpress                                                         |
| ۶۲ | ۳۱. پلاگین Slideshow Gallery برای Wordpress نسخه ۱.۴.۶ آسیب‌پذیری بازگذاری Shell                           |
| ۶۵ | ۳۲. آسیب‌پذیری File Inclusion محلی در نسخه ۰.۲.۳ پلاگین ShortCode برای Wordpress                           |
| ۶۶ | ۳۳. آسیب‌پذیری SqlInjection در پلاگین AdRotate نسخه ۳.۹.۴ از نرم‌افزار مدیریت محتوای وردپرس                |
| ۶۷ | ۳۴. آسیب‌پذیری Information Exposure در پلاگین VideoWhisper نسخه ۴.۲۷.۳ از نرم‌افزار مدیریت محتوای وردپرس   |
| ۶۸ | ۳۵. آسیب‌پذیری XSS در پلاگین VideoWhisper نسخه ۴.۲۷.۳ از نرم‌افزار مدیریت محتوای وردپرس                    |
| ۷۱ | .....IMPRESS CMS                                                                                           |
| ۷۱ | ۳۶. آسیب‌پذیری حذف فایل دلخواه در ImpressCMS 1.3.5                                                         |
| ۷۳ | ۳۷. آسیب‌پذیری XSS در ImpressCMS 1.3.5                                                                     |
| ۷۵ | .....Joomla                                                                                                |
| ۷۶ | ۳۸. آسیب‌پذیری دانلود فایل در پلاگین Mac Gallery نسخه ۱.۵ از نرم‌افزار مدیریت محتوای Joomla                |
| ۷۷ | ۳۹. آسیب‌پذیری دانلود فایل در پلاگین Face Gallery نسخه ۱.۰ از نرم‌افزار مدیریت محتوای Joomla               |
| ۷۸ | ۴۰. آسیب‌پذیری تزریق SQL در پلاگین Face Gallery نسخه ۱.۰ از نرم‌افزار Joomla                               |
| ۷۹ | ۴۱. آسیب‌پذیری تزریق SQL در پلاگین SpecialForm Maker نسخه ۳.۴ و پایین‌تر از نرم‌افزار مدیریت محتوای Joomla |
| ۸۰ | ۴۲. آسیب‌پذیری تزریق SQL در پلاگین Split Calendar نسخه ۲.۶ و پایین‌تر از نرم‌افزار مدیریت محتوای Joomla    |
| ۸۱ | ۴۳. آسیب‌پذیری SqlInjection در پلاگین Joomla Spider Contacts نسخه ۱.۳.۶ از نرم‌افزار مدیریت محتوای جوملا   |
| ۸۲ | .....Lunar CMS                                                                                             |
| ۸۲ | ۴۴. آسیب‌پذیری اجرای دستور از راه دور در Lunar CMS 3.3                                                     |
| ۸۳ | ۴۵. آسیب‌پذیری (SRF) در Lunar CMS 3.3                                                                      |
| ۸۵ | ۴۶. آسیب‌پذیری تزریق اسکریپت XSS در Lunar CMS 3.3                                                          |
| ۸۶ | .....ZEROCMS                                                                                               |
| ۸۶ | ۴۷. آسیب‌پذیری XSS در ZeroCMS 1.0                                                                          |
| ۸۷ | ۴۸. آسیب‌پذیری تزریق SQL در ZeroCMS 1.0                                                                    |
| ۸۸ | ۴۹. آسیب‌پذیری افزایش سطح دسترسی در ZeroCMS 1.0                                                            |
| ۸۹ | ۵۰. آسیب‌پذیری تزریق SQL در ZeroCMS                                                                        |
| ۹۰ | .....AURACMS                                                                                               |
| ۹۰ | ۵۱. آسیب‌پذیری تزریق XSS در AuraCMS 3.0                                                                    |
| ۹۲ | ۵۲. آسیب‌پذیری نمایش لیست دایرکتوری‌ها در AuraCMS 3.0                                                      |
| ۹۳ | .....BLOOFox CMS                                                                                           |
| ۹۳ | ۵۳. آسیب‌پذیری تزریق SQL در bloofox CMS 0.5.0                                                              |
| ۹۴ | ۵۴. آسیب‌پذیری CSRF در bloofox CMS 0.5.0                                                                   |
| ۹۵ | ۵۵. آسیب‌پذیری تزریق فایل محلی در bloofox CMS 0.5.0                                                        |
| ۹۶ | ۵۶. تزریق SQL در سامانه مدیریت محتوای Drupal Core <= 7.32                                                  |

|     |                                                                                          |
|-----|------------------------------------------------------------------------------------------|
| ۹۸  | ۵۷. آسیب‌پذیری اجرای دستور از راه دور در ApPHP MicroBlog 1.0.1                           |
| ۹۹  | ۵۸. بدست آوردن کاربر Admin در No-CMS 0.6.6 rev 1                                         |
| ۱۰۰ | ۵۹. آسیب‌پذیری تزریق اسکریپت در CMS Made Simple 1.11.10                                  |
| ۱۰۲ | ۶۰. آسیب‌پذیری تزریق اسکریپت در GetSimple CMS 3.3.1                                      |
| ۱۰۳ | ۶۱. وارد کردن فایل از راه دور در CMSimple 4.4.4.2                                        |
| ۱۰۴ | ۶۲. آسیب‌پذیری CSRF در Microweber CMS 0.93                                               |
| ۱۰۶ | ۶۳. آسیب‌پذیری تغییر مسیر در ASP-Nuke 2.0.7                                              |
| ۱۰۷ | ۶۴. آسیب‌پذیری افشای اطلاعات حساس در Kentico CMS 7.0.75                                  |
| ۱۰۸ | ۶۵. آسیب‌پذیری تزریق اسکریپت XSS در Ilch CMS 2.0                                         |
| ۱۰۹ | ۶۶. آسیب‌پذیری اجرای دستور از راه دور در SkyBlueCanvas CMS 1.1 r248-03                   |
| ۱۱۱ | ۶۷. آسیب‌پذیری تزریق SQL در iTechClassifieds 3.03.057                                    |
| ۱۱۲ | ۶۸. آسیب‌پذیری LFI در نرم‌افزار LittleSite 0.1                                           |
| ۱۱۳ | ۶۹. آسیب‌پذیری LFI در نرم‌افزار متن باز OsClass نسخه ۳.۴.۷                               |
| ۱۱۴ | ۷۰. آسیب‌پذیری بارگذاری در Frog CMS 0.9.5                                                |
| ۱۱۵ | ۷۱. آسیب‌پذیری تزریق SQL در Pligg 2.۰                                                    |
| ۱۱۶ | ۷۲. آسیب‌پذیری XSS در Simple Planet 0.1                                                  |
| ۱۱۸ | ۷۳. آسیب‌پذیری CSRF در نرم‌افزار مدیریت محتوا Snowfox                                    |
| ۱۲۰ | ۷۴. تزریق SQL در پلاگین Verify Email Before Registration از نرم‌افزار vBulletin نسخه 4.x |
| ۱۲۲ | <b>..... PARALLELS PLESK SITEBUILDER</b>                                                 |
| ۱۲۲ | ۷۵. عبور از صفحه هویت‌سنجی در Parallels Plesk Sitebuilder نسخه 9.5                       |
| ۱۲۳ | ۷۶. ارسال فایل مخرب در Parallels Plesk Sitebuilder نسخه 9.5                              |
| ۱۲۴ | ۷۷. آسیب‌پذیری دایرکتوری در Parallels Plesk Sitebuilder نسخه 9.5                         |
| ۱۲۵ | ۷۸. آسیب‌پذیری XSS در Parallels Plesk Sitebuilder نسخه ۹.۵                               |
| ۱۲۶ | <b>..... CODIAD</b>                                                                      |
| ۱۲۶ | ۷۹. آسیب‌پذیری XSS در نرم‌افزار Codiad نسخه 2.4.3                                        |
| ۱۲۷ | ۸۰. آسیب‌پذیری LFI در نرم‌افزار Codiad نسخه 2.4.3                                        |
| ۱۲۸ | ۸۱. امکان نصب مجدد کاربر Admin در Bonetire 0.7.1                                         |
| ۱۲۹ | <b>فصل دوم: سامانه‌های مدیریت ارتباط با مشتریان .....</b>                                |
| ۱۳۰ | ۸۲. تزریق SQL در kitForm CRM Extension 0.43                                              |
| ۱۳۱ | ۸۳. آسیب‌پذیری وارد کردن فایل محلی در Vtiger CRM 5.4.0, 6.0 RC, 6.0.0 GA                 |
| ۱۳۲ | ۸۴. آسیب‌پذیری XSS در Zurmo CRM                                                          |
| ۱۳۳ | <b>..... OPENSUPPORTS</b>                                                                |
| ۱۳۳ | ۸۵. آسیب‌پذیری عبور از احراز هویت در OpenSupports 2.x                                    |
| ۱۳۴ | ۸۶. آسیب‌پذیری CSRF در OpenSupports 2.x                                                  |
| ۱۳۶ | ۸۷. آسیب‌پذیری تزریق SQL در OpenSupports 2.0                                             |
| ۱۳۸ | ۸۸. آسیب‌پذیری تزریق SQL در نرم‌افزار PHP Ticket System نسخه Beta 1                      |

۸۹. بدست آوردن اطلاعات اعتبارسنجی در 8.3.5 Web Service (CWS) و Technician Web Access (TWA) از نرم افزار TeamHelpdesk

Customer

۱۳۹

۱۴۱..... فصل سوم: سامانه های تجارت الکترونیک و فروشگاه ساز

۱۴۲..... PHPJABBERS

۱۴۲..... ۸۹. آسیب پذیری XSS در PHPJabbers Pet Listing Script 1.0

۱۴۵..... ۸۸. آسیب پذیری CSRF در PHPJabbers Pet Listing Script 1.0

۱۴۷..... ۸۷. آسیب پذیری CSRF در PHPJabbers Property Listing Script 2.0

۱۴۹..... ۹۳. آسیب پذیری XSS در PHPJabbers Vacation Packages Listing 2.0

۱۵۲..... ۸۴. آسیب پذیری CSRF در PHPJabbers Vacation Packages Listing

۱۵۴..... ۹۵. آسیب پذیری افشای فایل محلی در PHPJabbers Vacation Packages Listing 2.0

۱۵۵..... ۹۶. آسیب پذیری XSS در PHPJabbers Hotel Booking System 3.0

۱۵۷..... ۸۷. آسیب پذیری CSRF در PHPJabbers Hotel Booking System 3.0

۱۵۹..... ۸۸. آسیب پذیری افشای فایل محلی در PHPJabbers Hotel Booking System 3.0

۱۶۰..... ۹۹. آسیب پذیری XSS در PHPJabbers Vacation Rental Script 3.0

۱۶۲..... ۱۰۰. آسیب پذیری CSRF در PHPJabbers Vacation Rental Script 3.0

۱۶۴..... ۱۰۱. آسیب پذیری افشای فایل محلی در PHPJabbers Vacation Rental Script 3.0

۱۶۵..... ۱۰۲. آسیب پذیری XSS در PHPJabbers Job Listing Script

۱۶۸..... ۱۰۳. آسیب پذیری CSRF در PHPJabbers Job Listing Script

۱۷۰..... ۱۰۴. آسیب پذیری CSRF در PHPJabbers Classifieds Script 2.0

۱۷۲..... ۱۰۵. آسیب پذیری تزریق SQL در نرم افزار TomatoCart نسخه ۱.۵.۳

۱۷۳..... ۱۰۶. آسیب پذیری CSRF در نرم افزار Zen Cart نسخه ۱.۵.۳

۱۷۴..... ۱۰۷. آسیب پذیری XSS در Cart Engine نسخه ۲.۰

۱۷۶..... ۱۰۸. آسیب پذیری تزریق SQL در OpenCart نسخه 1.5.6.1

۱۷۷..... ۱۰۹. آسیب پذیری Session Fixation در CubeCart 5.2.8

۱۷۹..... فصل چهارم: افزونه های جانبی طراحی وب

۱۸۰..... LUXCAL

۱۸۰..... ۱۱۰. آسیب پذیری تزریق SQL در LuxCal 3.2.2

۱۸۳..... PLOGGER

۱۸۳..... ۱۱۲. آسیب پذیری تزریق اسکریپت XSS در Plogger 1.0 (RC1)

۱۸۵..... ۱۱۳. آسیب پذیری CSRF در Plogger 1.0 (RC1)

۱۸۷..... ۱۱۴. بارگذاری فایل دلخواه در Plogger 1.0-RC1

۱۸۸..... LINPHA

۱۸۸..... ۱۱۵. آسیب پذیری تزریق اسکریپت در LinPHA 1.3.4

۱۹۰..... ۱۱۶. آسیب پذیری CSRF در LinPHA 1.3.4

۱۹۱..... PIWIGO

۱۹۱..... ۱۱۷. آسیب پذیری CSRF در نرم افزار Piwigo نسخه ۲.۶.۱

۱۹۲..... ۱۱۸. آسیب پذیری XSS در نرم افزار Piwigo نسخه 2.7.2

|     |                                                          |
|-----|----------------------------------------------------------|
| ۱۹۴ | آسیب‌پذیری تزریق SQL در نرم‌افزار Piwigo نسخه 2.7.2      |
| ۱۹۵ | آسیب‌پذیری تزریق SQL در Piwigo نسخه ۲.۶.۰ و قبل از آن    |
| ۱۹۷ | .....SPHIDER                                             |
| ۱۹۷ | آسیب‌پذیری تزریق SQL در Sphider 1.3.6                    |
| ۱۹۸ | آسیب‌پذیری تزریق PIHP در Sphider 1.3.6                   |
| ۱۹۹ | آسیب‌پذیری XSS در Sphider 1.3.6                          |
| ۲۰۰ | آسیب‌پذیری تزریق SQL در Sphider-1.3.6                    |
| ۲۰۱ | آسیب‌پذیری دور زدن احراز هویت در Sphider-1.3.6           |
| ۲۰۲ | آسیب‌پذیری اجرای کد از راه دور در Sphider-1.3.6 plus/pro |
| ۲۰۳ | آسیب‌پذیری پیمایش دایرکتوری در Ajax File Manager         |
| ۲۰۴ | نمایش فایل مای سرور توسط HttpCombiner ASP.NET            |
| ۲۰۵ | آسیب‌پذیری XSS در نرم‌افزار PhpOnlineChat نسخه ۳.۰       |
| ۲۰۶ | .....CHART                                               |
| ۲۰۶ | آسیب‌پذیری پیمایش فایل در pChart 2.1.3                   |
| ۲۰۷ | آسیب‌پذیری XSS در pChart 2.1.3                           |
| ۲۰۹ | .....فصل پنجم: سامانه‌های طراحی خاص                      |
| ۲۱۰ | .....MYBB                                                |
| ۲۱۰ | آسیب‌پذیری XSS در MyBB نسخه ۱.۶.۱                        |
| ۲۱۱ | آسیب‌پذیری تزریق SQL در MyBB نسخه ۳.۱۰.۸                 |
| ۲۱۳ | .....OMEKA                                               |
| ۲۱۳ | آسیب‌پذیری CSRF در Omeka 2.2                             |
| ۲۱۵ | آسیب‌پذیری XSS در Omeka 2.2                              |
| ۲۱۷ | .....OXWALL                                              |
| ۲۱۷ | آسیب‌پذیری XSS در Oxwall 1.7.0                           |
| ۲۱۹ | آسیب‌پذیری CSRF در Oxwall 1.7.0                          |
| ۲۲۱ | آسیب‌پذیری تزریق SQL در OpenEMR نسخه ۴.۸.۲               |
| ۲۲۷ | آسیب‌پذیری اجرای کد از راه دور در HybridAuth 2.2.2       |
| ۲۲۸ | آسیب‌پذیری XSS در eFront 3.6.14.4 Vulnerability          |
| ۲۲۹ | .....OPENDOCMAN                                          |
| ۲۲۹ | آسیب‌پذیری تزریق SQL در OpenDocMan 1.2.7                 |
| ۲۳۰ | آسیب‌پذیری CSRF در OpenDocMan 1.2.7                      |
| ۲۳۱ | .....فصل ششم: سامانه‌های مربوط به مدیریت وبگاه           |
| ۲۳۲ | .....GNUPANEL                                            |
| ۲۳۲ | آسیب‌پذیری XSS در GNUPanel 0.3.5_R4                      |
| ۲۳۴ | آسیب‌پذیری CSRF در GNUPanel 0.3.5_R4                     |
| ۲۳۶ | آسیب‌پذیری CSRF در XCloner Standalone 3.5                |
| ۲۳۷ | آسیب‌پذیری CSRF در XAMPP 3.2.1 & phpMyAdmin 4.1.6        |



|     |                                                                                                               |
|-----|---------------------------------------------------------------------------------------------------------------|
| ۲۳۹ | ۱۴۷. آسیب‌پذیری XSS در نرم‌افزار Easy File Sharing Webserver نسخه 6.8 و کمتر                                  |
| ۲۴۰ | ۱۴۸. آسیب‌پذیری تزریق SQL در نرم‌افزار phpMyRecipes نسخه ۱.۲.۲                                                |
| ۲۴۱ | ۱۴۹. آسیب‌پذیری اجرای کد از راه دور در SQL Buddy نسخه ۱.۳.۳                                                   |
| ۲۴۲ | ۱۵۰. آسیب‌پذیری وارد کردن فایل محلی در DnPHP 1.0                                                              |
| ۲۴۳ | <b>فصل هفتم: راهکارهای پیشگیری</b>                                                                            |
| ۲۴۵ | ۱. راهکار پیشگیری از تزریق SQL                                                                                |
| ۲۴۹ | ۲. راهکار پیشگیری از CSRF برای پیشگیری از این آسیب‌پذیری و حمله CSRF می‌بایست موارد زیر را همزمان بکار بستید: |
| ۲۵۰ | ۲. راهکار پیشگیری از XSS                                                                                      |
| ۲۵۰ | ۴. راهکار پیشگیری از بارگذاری فایل غیرمجاز                                                                    |
| ۲۵۱ | ۵. راهکار پیشگیری از URL redirection                                                                          |
| ۲۵۱ | ۶. راهکار پیشگیری از نمایش پیام خطا                                                                           |
| ۲۵۱ | ۷. راهکار پیشگیری از دسترسی غیر مجاز به صفحه هویت سنجی                                                        |
| ۲۵۱ | ۸. راهکار پیشگیری از نمایش پیام خطا                                                                           |
| ۲۵۱ | ۹. راهکار پیشگیری از احتمال اجرای نام کاربری یا کلمه عبور                                                     |
| ۲۵۲ | ۱۰. راهکار پیشگیری از نگهداری نام کاربری و کلمات عبور                                                         |
| ۲۵۲ | ۱۱. راهکار پیشگیری از گرفتن فمست برکنور                                                                       |
| ۲۵۲ | ۱۲. راهکار پیشگیری از اجرای دستور از راه دور                                                                  |
| ۲۵۲ | ۱۳. راهکار پیشگیری از وارد کردن فایل از راه دور                                                               |
| ۲۵۵ | <b>واژه‌نامه</b>                                                                                              |
| ۲۵۷ | <b>منابع</b>                                                                                                  |