

۷۵ آسیب‌پذیری رایج

وبگاه‌ها

مؤلف: یاسر نبهانی

عنوان و نام پدیدآور : ۷۵ آسیب‌پذیری رایج و بگاه‌ها/ مولف یاسر نبهانی
 مشخصات نشر : تهران: انتشارات ناقوس، ۱۳۹۴.
 مشخصات ظاهری : ۱۱۴ ص. مصور، جدول.
 شابک : ۹۷۸-۹۶۴-۳۷۷-۸۲۳-۱ بها : ۱۰۰,۰۰۰ ریال

وضعیت فهرست‌نویسی : فیبا
 عنوان گسترده : هفتادوپنج آسیب‌پذیری رایج و بگاه‌ها
 موضوع : وبگاه‌ها-تدابیر ایمنی
 موضوع : وبگاه‌ها-ایران
 رده بندی کنگ : TK5۱۰۵/۵۹/ن۲۵۷ ۱۳۹۴
 رده بندی دیویی : ۰۰۵/۸
 شماره کتابشناسی ملی : ۳۰۹۸۰۸۳



**NAGHOOS
PUBLICATION**

برای خرید Online به آدرس زیر مراجعه کنید:

www.naghoospress.ir

انتشارات ناقوس

چاپ اول

S.M.S : ۳۰۰۰۴۵۲۳۲۳

این اثر به صورت
 تکثیر شده یا به صورت
 حرفه‌ای یا چاپ مجدد است، پلی‌کپی،
 فتوکپی و انون دیگر چاپ ممنوع است و
 پیگرد قانونی دارد.

نام کتاب : ۷۵ آسیب‌پذیری رایج و بگاه‌ها
 ناشر : انتشارات ناقوس
 مولف : یاسر نبهانی
 چاپ اول : ۱۳۹۴
 تیراژ : ۵۰۰ جلد
 چاپ و صحافی : نارنجستان
 سرپرست صفحه‌آرا : صدف پورعبدی
 قیمت : ۱۰۰,۰۰۰ ریال
 شابک : ۹۷۸-۹۶۴-۳۷۷-۸۲۳-۱
 ISBN : 978-964-377-823-1

مرکز پخش: انتشارات ناقوس

۱- خیابان انقلاب-خیابان ۱۲ فروردین- بین وحیدنظری و روانمهر- بن‌بست حقیقت- پلاک ۴

تلفن و فاکس: ۶۶۴۷۸۹۵۸-۶۶۴۷۸۹۵۷

۲- کتابفروشی الیاس: خیابان انقلاب، نبش ۱۲ فروردین تلفن: ۶۶۴۰۵۰۸۴

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

پیشگفتار

با ظهور وب و رایج شدن استفاده از وبگاه‌های ایجاد شده در آن، آسیب‌پذیری‌های زیادی نیز بروز نموده و هر ساله تولید کنندگان و استفاده کنندگان در این حوزه را تهدید می‌کند.

با بررسی امنیتی تعداد زیادی وبگاه توسط مولف، مشخص شد تعداد زیادی از آسیب‌پذیری‌های آنها مشترک می‌باشد. بنابراین می‌توان با بکار بستن راهکارهای پیشگیری مشترک مرتبط، از نوع بسیاری از رخدادهای ناگوار مانند افشا، سرقت و دستکاری اطلاعات، پیشگیری نمود.

این آسیب‌پذیری‌های رایج به همراه راهکارهای پیشگیری از آنها، در این کتاب آماده شده است تا هم قابل استفاده ی محققان این حوزه باشد و هم با قرار گرفتن آن در اختیار فعالان حوزه ارزیابی، طراحی و نگهداری وبگاه‌ها، قدمی در ارتقا سطح دانش این حوزه صورت پذیرد. در اینجا از تمامی عزیزان که از جانب را در تالیف این کتاب یاری نموده‌اند، تشکر و قدردانی می‌کنم.

امیدوارم با تالیف این کتاب توانسته باشم گامی هر چند کوچک در جهت ارتقاء امنیت فضای تبادل اطلاعات کشور برداشته باشم.

در پایان از تمامی خوانندگان گرامی درخواست دارم نظرات سازنده خود را به آدرس رایانامه nabhani@payammail.ir ارسال نمایند.

فهرست مطالب

۱۱	۱. دستکاری محاوره پروتکل HTTP - HTTP VERB TAMPERING
۱۲	۲. امکان دانلود فایل‌های موقت - TEMPORARY/BACKUP FILE DOWNLOAD
۱۳	۳. تعلیق کار PHP هنگام تبدیل رشته به ممیز شناور - PHP HANGS ON PARSING PARTICULAR STRINGS AS FLOATING POINT NUMBER
۱۵	۴. ایجاد XSS در حالت PHP MULTIPART/FORM-DATA DENIAL OF SERVICE-MULTIPART/FORM-DATA
۱۷	۵. آپاچی نسخه ۲ ویرایش قبل از ۲.۲.۱۰ - APACHE 2.X VERSION OLDER THAN 2.2.10
۱۸	۶. حدس کلمه عبور صفحه ورود - LOGIN PAGE PASSWORD-GUESSING
۱۸	۷. دایرکتوری‌های حساس احتمالی - POSSIBLE SENSITIVE DIRECTORIES
۲۰	۸. فایل‌های حساس احتمالی - POSSIBLE SENSITIVE FILES
۲۱	۹. وجود صفحه ورود آسیب‌پذیر - VULNERABLE LOGIN PAGE
۲۳	۱۰. فعال بودن قابلیت تکمیل خودکار برای ورودی کلمه عبور - PASSWORD TYPE INPUT WITH AUTOCOMPLETE ENABLED
۲۳	۱۱. احتمال افشای مسیر سرور - POSSIBLE SERVER PATH DISCLOSURE
۲۵	۱۲. احتمال افشای نام کاربری یا کلمه عبور - POSSIBLE USERNAME OR PASSWORD DISCLOSURE
۲۶	۱۳. عدم رمزنگاری فیلدهای LOGIN - UNENCRYPTED LOGIN REQUEST
۲۷	۱۴. نگهداری اطلاعات حساس نشست در یک کوکی دائمی - TV PERMANENT COOKIE CONTAINS SENSITIVE SESSION INFORMATION
۲۸	۱۵. نمایش ساختار وبگاه توسط فایل ROBOTS.TXT - ROBOTS.TXT FILE WEB SITE STRUCTURE EXPOSURE
۳۰	۱۶. دایرکتوری‌های مخفی قابل کشف - HIDDEN DIRECTORY DETECTED
۳۱	۱۷. امکان بارگذاری فایل بر روی وبگاه - POTENTIAL FILE UPLOAD
۳۳	۱۸. تزریق SQL - SQL INJECTION
۳۹	۱۹. نمایش پیام خطای برنامه کاربردی - APPLICATION ERROR MESSAGE
۴۰	۲۰. وجود آدرس پست الکترونیک - EMAIL ADDRESS PATTERN FOUND
۴۱	۲۱. افشای کد منبع - SOURCE CODE DISCLOSURE
۴۲	۲۲. در حال اجرا بودن TERMINAL SERVICES ویندوز - WINDOWS TERMINAL SERVICES SERVER RUNNING
۴۳	۲۳. آسیب‌پذیری پیش‌بینی پنهان کاری ASP.NET - ASP.NET PADDING ORACLE VULNERABILITY
۴۵	۲۴. صفحه خطای افشاکننده نسخه کارگزار وب - ERROR PAGE WEB SERVER VERSION DISCLOSURE
۴۵	۲۵. نمایش پیام خطای ASP.NET - ASP.NET ERROR MESSAGE
۴۷	۲۶. امکان اجرای اسکریپت نقلی در سایت - CROSS SITE SCRIPTING(XSS)
۵۰	۲۷. کوکی نشست فاقد تنظیم SECURE FLAG SET-SECURE FLAG - SESSION COOKIE WITHOUT SECURE FLAG
۵۱	۲۸. استفاده از تابع جاوااسکریپت EVAL() - JAVASCRIPT EVAL() USAGE
۵۲	۲۹. افشای اطلاعات حساس توسط توضیحات HTML - SUSPICIOUS COMMENT
۵۳	۳۰. فعال بودن قابلیت اشکال‌زدایی ASP.NET - ASP.NET DEBUGGING ENABLED

۳۱. قابل خواندن بودن فایل .HTACCESS - HTACCESS FILE READABLE
۳۲. گرفتن فهرست دایرکتوری‌ها - DIRECTORY LISTING
۳۳. فعال بودن متد ردیابی و پیگیری HTTP - TRACE AND TRACK HTTP METHODS ENABLED
۳۴. تنظیم نادرست مجوزهای فایل های کنترل دسترسی کارگزار وب - WEB SERVER ACCESS CONTROL FILES IMPROPER PERMISSIONS SETTING
۳۵. فعال بودن ویژگی MULTIVIEWS آپاچی - APACHE MULTIVIEWS ENABLED
۳۶. گرفتن فهرست دایرکتوری های FRONTPAGE مایکروسافت - MICROSOFT FRONTPAGE DIRECTORY LISTING
۳۷. نشت اطلاعات حیاتی صفحات کارگزار MICROSOFT FRONTPAGE - MICROSOFT FRONTPAGE SERVER EXTENSIONS VITAL INFORMATION LEAKAGE
۳۸. نشت اطلاعات MICROSOFT FRONTPAGE ' _VTI_CNF' INFORMATION LEAKAGE - MICROSOFT FRONTPAGE ' _VTI_CNF'
۳۹. دسترسی مستقیم به صفحات مدیریت - DIRECT ACCESS TO ADMINISTRATION PAGES
۴۰. فعال بودن متد های HTTP نا امن - INSECURE HTTP METHODS ENABLED
۴۱. مقدار __VIEWSTATE پارامتر رمزنگاری نشده - UNENCRYPTED __VIEWSTATE PARAMETER
۴۲. کلمه عبور اشتراکی NETBIOS/SMB SHARE PASSWORD IS THE DEFAULT, NULL, OR MISSING - NETBIOS/SMB SHARE PASSWORD IS THE DEFAULT, NULL, OR MISSING
۴۳. کوکی نشست فاقد تنظیم HTTPONLY FLAG SET - HTTPONLY FLAG
۴۴. تعیین مسیر مجدد URL - URL REDIRECTION
۴۵. عدم تعریف نوع محتوا - CONTENT TYPE IS NOT SPECIFIED
۴۶. رمز ضعیف SSL - SSL WEAK CIPHERS
۴۷. انتقال (داده های) ناحیه DNS - DNS ZONE TRANSFER
۴۸. پروتکل منسوخ شده SSL 2.0 - SSL 2.0 OBSOLETE PROTOCOL
۴۹. صفحه ورود ارتباط وبی MICROSOFT REMOTE DESKTOP - MICROSOFT REMOTE DESKTOP LOGIN PAGE
۵۰. در حال اجرا بودن سرویس TELNET - TELNET SERVICE RUNNING
۵۱. تزریق CRLF - CRLF INJECTION/HTTP RESPONSE SPLITTING
۵۲. افشای نسخه سامانه مدیریت محتوای استفاده شده - CMS VERSION DISCLOSURE
۵۳. کلیک رایبی: سرآیند فاقد X-FRAME-OPTIONS - CLICKJACKING: X-FRAME-OPTIONS HEADER MISSING
۵۴. DOS با آهسته کردن پروتکل HTTP - SLOW HTTP DOS ATTACK
۵۵. زمان پاسخ دهی کند - SLOW RESPONSE TIME
۵۶. پیمایش مسیر - PATH TRAVERSAL
۵۷. وجود بلیط ورود نشست در URL - SESSION TOKEN IN URL
۵۸. فعال بودن متد OPTIONS - OPTIONS METHOD IS ENABLED
۵۹. از کار افتادن سرویس HTTPD آپاچی از راه دور - APACHE HTTPD REMOTE DENIAL OF SERVICE
۶۰. ارائه فیلد کلمه عبور با استفاده از متد GET - PASSWORD FIELD SUBMITTED USING GET METHOD
۶۱. باقی ماندن نشست هنگام خروج از سیستم - REMAIN SESSION ON LOGOUT
۶۲. امکان افشای آدرس IP داخلی - POSSIBLE INTERNAL IP ADDRESS DISCLOSURE
۶۳. امکان اجرای اسکریپت تقلبی در سایت با استفاده از JQUERY - JQUERY CROSS SITE SCRIPTING
۶۴. افشای کوکی HTTPONLY کارگزار وب آپاچی - APACHE HTTPONLY COOKIE DISCLOSURE
۶۵. فرم HTML حفاظت نشده در برابر CSRF - HTML FORM WITHOUT CSRF PROTECTION
۶۶. استفاده از نام اختصاری برای دایرکتورها در IIS - MICROSOFT IIS TILDE DIRECTORY ENUMERATION
۶۷. آلودگی پارامتر HTTP - HTTP PARAMETER POLLUTION

۶۸. حمله با استفاده از فیلد HOST در هدر درخواست - HOST HEADER ATTACK
۶۹. نمایش صفحه پیش فرض پتل مدیریتی میزبان وبگاه هنگام وارد نمودن آی پی آن
۷۰. یافتن فیلد ورودی فرم مخفی با نام PRICE - PRICE - HIDDEN FORM INPUT NAMED PRICE WAS FOUND
۷۱. آسیب پذیری XSS فایل SPELLCHECKER.PHP ویرایشگر FCKEDITOR - FCKEDITOR SPELLCHECKER.PHP CROSS SITE SCRIPTING VULNERABILITY
۷۲. استفاده از WEBALIZER SCRIPT - WEBALIZER SCRIPT
۷۳. نمایش آمارهای برنامه WEBALIZER - WEBALIZER STATISTICS
۷۴. فعال بودن ALLOW_URL_FOPEN در PHP - PHP ALLOW_URL_FOPEN ENABLED
۷۵. آسیب پذیری دور زدن احراز هویت MYSQL - MYSQL AUTHENTICATION BYPASS VULNERABILITY
- ضمائم
- منابع