مرکز تحقیقات فضایی

پژوهشگاه فضایی ایران

مرکز تحقیقات فضایی

عنوان پروژه/ گروه/بخش:
عنوان اختصاری پروژه/گروه/بخش:

درج عنوان سند با فونت B Titr اندازه ۱۵

کد سند:
نوع سند:
شماره ویرایش:
طبقه‌بندی:
تاریخ:

تعداد کل صفحات: صفحه

(با احتساب برگ روی جلد)


بسم الله الرحمن الرحيم

شناسنامه سند

۱- مشخصات سند

عنوان سند			تعداد صفحات	
نوع سند		کد سند	کل سند	
ویرایش		تاریخ ویرایش	پیوست‌ها	

۲- جدول تهیه، تایید و تصویب در پژوهشکده (حوزه) مجری

	سمت*	نام و نام‌خانوادگی	امضا	تاریخ
تهیه‌کننده(گان)				
تأیید کننده(گان) با نظر مدیر پروژه	سرپرست بخش طراحی و پیاده-سازی نرم‌افزار سرپرست گروه توسعه فناوری-های مخابراتی مسئول کنترل پیکربندی			
	مدیریت پژوهش			
تصویب‌کننده	ریاست مرکز تحقیقات			

* برای مواردی که مجری، حوزه دیگری غیر از پژوهشکده است، مثل مراکز یا گروه‌های پژوهشی مستقل و ... از سمت‌های معادل بر اساس نظر رییس حوزه استفاده شود.

شناسنامه سند (ادامه)

۳- جدول توزیع نسخ (گیرندگان)

عنوان واحد	توزیع*	عنوان واحد	توزیع*
سایر گیرندگان:			

*توزیع نسخ بر اساس علامت‌های زیر انجام می‌شود:

✓: سند برای این واحدها ارسال می‌شود.

●: سند برای این واحدها ارسال نمی‌شود و صرفا اطلاع‌رسانی می‌شود.

۴- تایید مرکز اسناد

مستندسازی دانش مرکز تحقیقات فضایی
نام و نام‌خانوادگی: .....
تاریخ: .....
مهر و امضا

مدیریت پژوهش مرکز تحقیقات فضایی
نام و نام‌خانوادگی: .....
تاریخ: .....
مهر و امضا

شناسنامه سند (ادامه)

۵- جدول مشخصات و شرح وظایف دست‌اندرکاران تدوین سند*

ردیف	نام و نام‌خانوادگی	آخرین مدرک تحصیلی	رشته تحصیلی	مرتبه علمی**	محل کار	شرح وظایف	درصد مشارکت
جمع							۱۰۰

*منظور کلیه افرادی است که در انجام فعالیت‌های مرتبط با این سند نقش اصلی داشته‌اند.

**برای اعضای هیات علمی از عناوین مربوط (استاد، دانشیار، استادیار، مربی) و برای دیگر پژوهشگران از عنوان کارشناس استفاده شود.

شناسنامه سند (ادامه)

۶- جدول مشخصات ناظر(ان)

ردیف	نام و نام‌خانوادگی	آخرین مدرک	رشته	مرتبه علمی	محل کار	توضیحات

۷- جدول سوابق ویرایش و تغییرات

ویرایش	تاریخ	شرح تغییرات	علت/مرجع تغییر	واحد تهیه‌کننده مسئول
۱		نگارش سند	-	-

چکیده

امنیت یک سایت مساله مهمی است که هر سایتی باید آن را در نظر داشته باشد. امنیت یک پروسه است که در هنگام توسعه و پیاده‌سازی وب سایت باید در نظر داشت. با انجام امور مشخص می‌توان امنیت یک سایت را بهبود بخشید اما وجود امنیت یک مساله نسبی است. یعنی یک سایت می‌تواند امن‌تر باشد ولی باز هم امکان هک شدن آن وجود دارد. در این مستند ابتدا به بررسی موارد مهم و اصلی در ایجاد امنیت بر روی یک وب سایت پرداخته شده است، سپس به بررسی سامانه سنجش پرداخته شده است. در طی این بررسی‌ها چالش‌های اساسی مشخص گردیده‌اند و راه‌حل‌هایی برای حل آن‌ها پیشنهاد گردیده شده است.

واژه‌های کلیدی: بررسی امنیت سایت، سامانه سنجش.

فهرست مطالب

عنوان **صفحه**

فهرست شکل‌ها

عنوان **صفحه**

۱ مقدمه

مقدمه اولین بخش از متن اصلی گزارش است و هدف از آن معرفی کار است.

۲ امنیت سایت

امنیت سایت به مجموعه اقداماتی گفته می شود که با انجام آنها ضریب امنیت سایت به حداکثر رسیده و امکان نفوذ به آن به حداقل می رسد. توجه داشته باشید که امنیت سایت تابع موارد دیگری نیز می باشد که تمامی آنها نقش بسیار اساسی در تامین امنیت وب سایت دارند. امنیت سرور، امنیت شبکه، امنیت اینترنت، امنیت سیستم عامل، امنیت نرم افزار و بسیاری از موارد دیگر نقش کلیدی در تامین زیرساخت امنیت سایت دارند.

۲-۱ اهمیت امنیت سایت

امنیت سایت از اهمیت فوق العاده‌ای برخوردار است، به طوری که می‌توان گفت که یکی از موثرترین عوامل ادامه فعالیت، ثبات و اعتبار یک سایت موضوع مهم امنیت است. متاسفانه با بررسی وضعیت سایت‌های عادی و حتی بزرگ و حساس به این نتیجه می‌رسیم که بسیاری از مدیران و مسئولان سایت‌ها اهمیت کمی به امنیت سایت می‌دهند. هک نشدن سایت، امن بودن سایت را تضمین نمی‌کند. به عنوان مثال ممکن است بر روی یک سایت با ضعف‌های امنیتی، تلاشی برای هک و نفوذ به آن انجام نشده است ولی در صورت انجام حمله، سایت مورد بحث آسیب پذیر خواهد بود. اهمیت امنیت سایت زمانی مشخص می‌شود که سایت تحت حمله قرار دارد که محتمل به دو نتیجه خواهد بود. اگر امنیت سایت بصورت صحیح تامین شده باشد حمله ناموفق بوده و سایت آسیبی نخواهد دید، اما اگر موارد امنیتی رعایت و تامین نشده باشد ضریب آسیب پذیری سایت بسیار بالا خواهد بود و آسیبی که به سایت خواهد خورد می‌تواند بسیار جدی باشد. این نکته نیز قابل توجه است که حتی با وجود انجام و پوشش موارد امنیتی هر سایتی در هر زمان و موقعیت مستعد دریافت حملات و آسیب‌پذیری ناشی از حملات است. نوع، تعداد و روشهای هک و نفوذ بسیار گسترده هستند و مقابله در برابر تمامی آن‌ها اقدامات بسیار جدی و دائمی را طلب می‌کند. علاوه بر پوشش و رفع موارد امنیتی بحث مراقبت و رسیدگی نیز در امنیت بسیار حائز اهمیت است.

۳ موارد پایه‌ای برای ایجاد امنیت یک سایت

عوامل بسیار زیادی و متعددی در ایجاد امنیت یک سایت وجود دارد اما از پایه‌ای ترین آن‌ها می‌توان به موارد زیر اشاره کرد.

۳-۱ میزبانی سایت بر روی هاست امن

هاست سایت خود را از شرکت های معتبر و قابل اعتماد تهیه کنید. وجود بستر امن که سایت بر روی آن میزبانی می-شود از اهمیت بسیار ویژه ای برخوردار است. استفاده از سیستم‌های امنیتی شامل آنتی‌ویروس، آنتی اسپم، آنتی شل،

فایروال سخت افزاری و نرم افزاری و کانفیگ حرفه ای و اصولی سرور نقش اساسی در برخورد با حملات را ایفا می‌کند. در کل امنیت سایت وابسته به تمامی عوامل مطرح شده است که امنیت هاست نیز یکی از موارد بسیار مهم است.

۳-۲استفاده از اینترنت امن و مطمئن

غالبا ارتباط بین سایت‌ها و کاربران دو طرفه بوده و این ارتباط از طریق اینترنت انجام می‌شود. برای ثبت نام، ورود و بسیاری از موارد دیگر می‌بایست درخواستی از سمت کاربر به سایت ارسال شود تا سایت پاسخ مناسب برای آن درخواست را انجام دهد. برای مثال در هنگام ورود به یک سایت اگر در مسیر درخواست (از کامپیوتر ما تا سایت و بالعکس) شنودی انجام شود اطلاعات کاربری ما به راحتی به سرقت می‌رود. حال اگر این مورد در سطح بالاتری و برای مدیر سایت اتفاق بیافتد یک فاجعه رخ خواهد داد. برای جلوگیری از این کار می‌بایست از ارتباطی امن و حدالامکان محدود شده استفاده کرد. استفاده از اینترنت عمومی که کنترل و محدودیت امنیتی خاصی بر روی آن انجام نشده است می‌تواند بسیار خطرناک باشد. توجه به این نکته ضروری است که حتی در صورت استفاده از اینترنت شخصی نیز می‌بایست اقدامات امنیتی مناسب برای تامین اینترنت امن را انجام داد. با توجه به این که عمدتا اینترنت در کشور ما از طریق ADSL و هدایت آن‌ها از طریق مودم و روتر انجام شده و اتصال اکثر دستگاه‌ها به اینترنت از طریق Wi-Fi انجام می‌پذیرد، لذا نیاز است تا تمهیدات خاصی جهت جلوگیری از هک Wi-Fi انجام شود. می‌توان به مواردی مانند محدود کردن مودم به Mac Address دستگاه‌ها ، غیر فعال کردن WPS، فعال کردن فایروال مودم اشاره نمود.

۳-۳استفاده از سیستم عامل و نرم افزارهای معتبر و اصلی

این موضوع برای عموم کاملا قابل درک است که با استفاده از سیستم عامل و نرم افزارهای معتبر و اصلی امنیت بسیار بالاتری نسبت به حالت عکس آن خواهیم داشت. این نکته را در نظر داشته باشید که ممکن است در منابع غیر اصلی تغییراتی در هسته یا بخشی از سیستم عامل و نرم افزار مورد استفاده انجام شده باشد و بسیار محتمل است که این تغییرات به سمت سوء استفاده ، تخریب و جاسوسی و غیره باشد. مساله قابل توجه این است که متاسفانه در این حالت تشخیص و جلوگیری از این مشکل بسیار سخت خواهد بود. لذا پیشنهاد می‌شود که حتما از سیستم عامل و نرم افزارهای معتبر و اصلی استفاده کرده و به هیچ عنوان از نسخه های کرک شده و مشابه استفاده نشود. راه حل دیگر استفاده از سیستم عامل‌های لینوکسی است که برای خدمت‌دهی به عنوان سرور بهینه شده اند. به طور مثال لینوکس نسخه دبیان یکی از بهترین گزینه-ها برای این کاربرد است.

۳-۴استفاده از آنتی ویروس و فایروال قدرتمند ، بروز ، معتبر و اصل

این بخش نیز از اصول بخش قبل پیروی می‌کند اما تفاوت‌های شاخصی نیز دارد. استفاده از آنتی ویروس و فایروال قدرتمند، به روز، معتبر و اصل از اساسی ترین مواردی است که یک وب مستر باید از آن استفاده کند. حتی با در نظر گرفتن حصول تمامی شرایط دیگر و عدم قید به این موضوع می‌تواند مشکلات امنیتی بسیاری بوجود آید. محصولات امنیتی خوبی برای اینکار عرضه شده‌اند که از آن‌ها می‌توان به محصولات عرضه شده توسط شرکت‌های eset و kaspersky اشاره کرد.

۳-۵استفاده از رمز عبور قدرتمند و محافظت از آن

یکی از مواردی که همه با اتفاق نظر آن را قبول دارند و متاسفانه درصد کمی به آن اهمیت می‌دهند بحث استفاده از رمز عبور قدرتمند و محافظت از آن است. پسورد خوب و قدرتمند باید بیش از ۸ کاراکتر داشته، تلفیقی از حروف بزرگ و کوچک، اعداد و کاراکترهای خاص مانند @ , ٪ , ! و موارد مشابه باشد. مورد دیگر محافظت و تغییر آن است. اطلاعات حساس را می‌بایست بصورت مطمئنی محافظت کرد. خوشبختانه سیستم‌هایی مانند Bit Locker و مشابه آن می‌توانند از اطلاعات حساس ما مراقبت کنند. بحث دیگر تغییر دوره ای رمز عبور است که می‌بایست در بازه های زمانی مشخص تغییر داده شود.

۳-۶ تعیین سطح دسترسی مناسب اطلاعات

تعیین سطح دسترسی مناسب مخصوصا برای فایل‌هایی که محتوی اطلاعات کلیدی مانند اطلاعات دیتابیس هستند بسیار ضروری است. در این مورد باید سطحی از دسترسی را به فایل داد که تنها وب سرور و owner فایل بتوانند اطلاعات داخل فایل کانفیگ را بخوانند و غیر از آنها به هیچ نحو دیگری قابل خواندن و نوشتن نباشد. برای فایل‌ها و دایرکتوری‌های دیگر نیز باید سطح دسترسی معقول و استاندارد تعیین کرده و از اعطای دسترسی سطح بالا خودداری کنیم.

۳-۷محافظت از مسیر ورود به مدیریت سایت

پیشنهاد می‌شود از قابلیت محافظت از مسیر ورود به مدیریت سایت استفاده نمایید. این کار در تامین و کمک به امنیت سایت موثر بوده و در مواقعی محافظت اساسی به عمل می آورد. فرض کنید اگر در حالتی نام کاربری و رمز عبور سایت شما به دست هکر افتاده باشد، با اینکار می‌توانید از مشاهده مسیر مدیریت توسط هکر ممانعت به عمل آورید. همان طور که در ابتدای بحث گفته شد امنیت صد درصد نیست اما با انجام موارد امنیتی می‌توان تا حد بالایی از بروز مشکلات امنیتی جلوگیری کرد و در واقع با انجام و تامین صحیح امنیت سایت می‌توان در مواقع بحرانی روی اقدامات انجام شده حساب باز کرد. تجربه نیز اثبات کرده با کانفیگ صحیح امنیتی بسیاری از ضعف های دیگر پوشش داده می شوند. در موضوع امنیت کوچکترین موارد هم اهمیت خاص خود را دارند.

۳-۸تعیین محدودیت های دسترسی و مشاهده

با تعیین محدودیت‌های دسترسی امنیت سایت تا حد بالایی بهبود می‌یابد. در سایت‌ها این امکان وجود دارد که با اعمال محدودیت هایی مانند تعریف IP از مشاهده مسیر یا فایل خاصی توسط اشخاص غیر جلوگیری کرد. در این حالت به وب سرور دستور داده می‌شود که اگر IP کاربر غیر از مقدار یا مقادیر تعریف شده باشد آنها را با پیغام forbidden یا access denied روبرو کند. در وب سرورهای تحت لینوکس و ویندوز امکان استفاده از این قابلیت وجود دارد و به راحتی می توان از آن استفاده کرد. پیشنهاد می‌شود حتما از امکان محدودیت آی پی مخصوصا در مسیر مدیرتی سایت خود استفاده گردد.

۳-۹ محافظت سایت در برابر اسپمرها

روبات‌های اسپمر با جستجو در سایت‌ها و پیدا کردن نقاط ضعف در آنها مخصوصا فرم‌های محافظت نشده که تکمیل آنها بصورت ماشینی امکان پذیر است، اقدام به حملات انبوه اسپم می‌کنند که اگر محافظتی در اینکار انجام نشده باشد بسیار محتمل است که با ایجاد اختلال در سرور میزبان سایت، مورد برخورد شرکت میزبان سایت و دریافت استفاده بیهوده از منابع متعدد شوید. اما با یک اقدام ساده و استفاده از سیستم محافظت CAPTCHA می‌توان از بروز مشکلات امنیتی اسپمرها جلوگیری کرد. سیستم reCAPTCHA گوگل پیشنهاد بسیار خوبی در این حوزه است. بسیاری از سایت‌های بزرگ و معتبر دنیا از این سیستم استفاده می‌کنند.

۳-۱۰ راه اندازی گواهی امنیتی SSL بر روی سایت

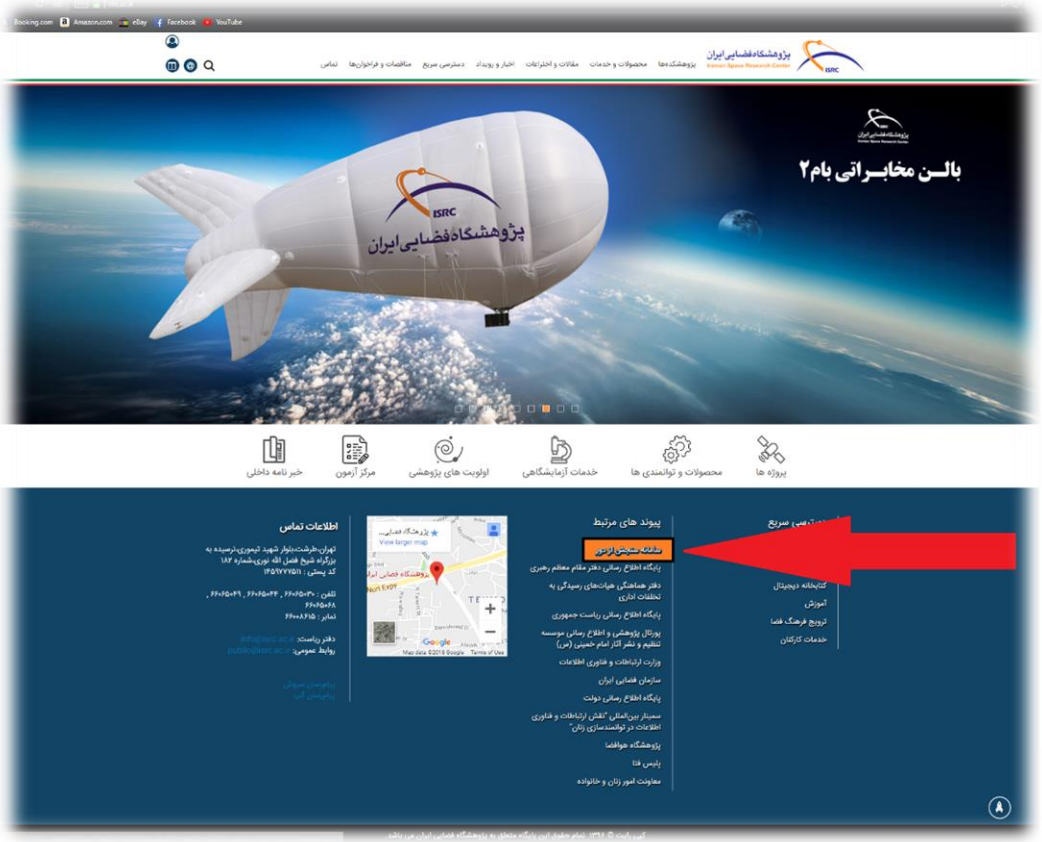
یکی از بهترین راهکارها برای حفظ امنیت اطلاعات کابران و مدیران سایت استفاده از گواهی امنیتی SSL بر روی سایت است که علاوه بر موارد امنیتی، تاثیرات بسیار خوبی در نتایج سئو و جلب اعتماد کاربران دارد. گواهی SSL بر روی سایت اطلاعات ورودی و خروجی را با الگوریتم بسیار پیچیده‌ای رمزنگاری کرده و از شنود و دزدیده شدن آنها جلوگیری می‌کند. اینکار سبب می‌شود که در بسیاری از حالات حتی در صورت استفاده کاربر یا مدیر سایت از اینترنت ناامن مشکلی ایجاد نشود. در واقع در این حالت اگر اطلاعات مورد شنود قرار گیرد نیز، قابل بهره‌برداری نخواهد بود و شنود کننده با یکسری اطلاعات رمزنگاری شده روبرو خواهد شد.

۴ تحلیل امنیتی بر سایت سنجش

۴-۱ صفحه مدیریت

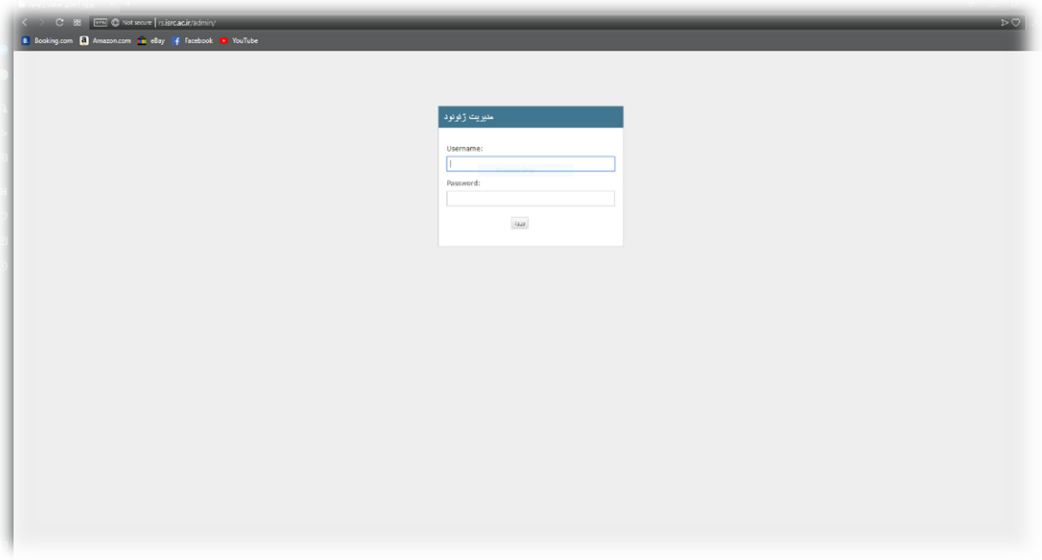
رابط مدیر یا همان صفحه مدیریت بخش مهمی برای هر پروژه وب سایت است که مدیران وب سایت با استفاده از آن، محتویات و فعالیت‌هایی مانند تعیین دسترسی کاربران، تایید درخواست‌های ثبت‌نام، تایید و ویرایش نظرات و غیره را مدیریت می‌کنند. در جانگو از طریق صفحه ادمین می‌توان به بالاترین سطح دسترسی دست یافت، از طریق آن می‌توان به ارتباط مستقیم با پایگاه داده و رکورد های ذخیره شده دسترسی داشت و اطلاعات ذخیره شده را درج یا حذف و یا تغییر داد. به طور کلی از نظر امنیتی فقط مدیر اصلی سایت باید به این صفحه دسترسی داشته باشد و سایر کاربران با دیگر دسترسی‌ها نباید به این صفحه دسترسی داشته باشند.

در بررسی های صورت گرفته از سایتی که بر روی وب پژوهشگاه در حال حاضر در دسترس است. تیم ما قادر بود تا بدون داشتن نام کاربری و پسورد وارد سایت شود. پس از ورود این تیم قادر است، تمام اطلاعات موجود روی سایت را حذف یا تغییر دهد، کاربر جدید تعریف کند و تمام دسترسی‌ها را تغییر دهد. تصاویر ورود غیر مجاز شامل تصویر۱، تصویر۲، تصویر۳ و تصویر۴ در ادامه آورده شده‌اند.

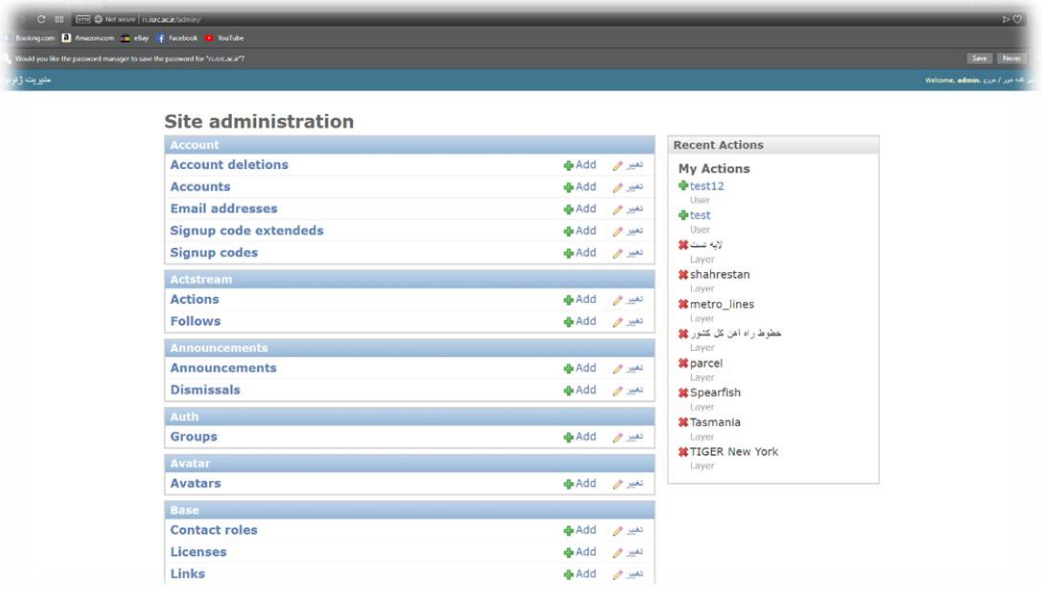


تصویر۱ – لینک سامانه سنجش از دور در سایت پژوهشگاه فضایی

تصویر۲- صفحه ورود به سامانه سنجش از دور



تصویر۳- صفحه ورود به صفحه مدیریت



تصویر۴- ورود غیر مجاز به صفحه مدیریت سامانه

۵ بررسی وب سرور سامانه

۵-۱ تعریف وب سرور

وب سرور وظیفه ارائه صفحات کاربران را به آن‌ها دارد، به گونه ای که هر گونه صفحه HTML همراه با هر نوع مطالب مانند تصاویر ، متن یا CSS و همینطور جاوا اسکریپت ها را به ما بر می‌گرداند. در واقعیت می‌توان گفت وب سرور برنامه

کامپیوتری می‌باشد، که در خواست های HTTP را قبول می‌کند و طبق شیوه عملکردی مشخص پاسخ‌ها را با یک سری اطلاعات به کاربر ارائه کند که این پاسخ ها همان صفحاتHTML است.

۲-۵ نحوه عملکرد وب سرور

ساختار مرورگر ها به گونه ای است که با استفاده از DNS های دامنه که آن را به عنوان یک آدرس IP منحصر به فرد برای هر سایت می‌شناسد، می‌تواند از این طریق به سرورهای خاصی دسترسی داشته باشد. مرورگر پس از ایجاد ارتباط با سرویس دهنده‌های وب از طریق آدرسIP به درخواست صفحه مربوط به وب پاسخ می‌دهد. اساس صفحات وب HTML است که این صفحات پیش فرض به طور رایج برای بسیاری از وب سایت‌ها فرمت INDEX.HTML را دارد و به همین جهت است که هر آدرسی را که در مرور گر وارد می‌کنیم به طور پیش فرض فایل HTML را برای شما به عنوان پاسخ بر می-گرداند و پس از این مرحله کد های HTML بررسی می‌شود تا صفحه نمایش داده شود.

۳-۵ وب سرور Nginx

یک سرور متن باز برای پروتکل های HTTP, HTTPS, SMTP, POP۳ و IMAP است. پروژه Nginx از همان ابتدای شکل گیری بر روی کارایی بالا، و استفاده کمتر و بهینه شده از حافظه اصلی شکل گرفته است. Nginx بر روی سیستم عامل های مختلفی از جمله Linux, OS X, Solaris, AIX, HP-UX و انواع BSD قابلیت اجرا دارد. اساس توسعه Nginx را می‌توان برای خدمت رسانی به محتوای صفحات پویای HTTP بر روی شبکه از طریق FastCGI, SCGI برای اسکریپت‌ها و سرویس دهنده های نرم افزار WSGI یا ماژول‌های Phusion و همچنین استفاده به عنوان توزیع کننده بار استفاده کرد.

توسعه Nginx توسط Igor Sysoev در سال ۲۰۰۲ اغاز گردید. در جولای سال ۲۰۱۱ شرکت به نام Nginx, Inc در سان فرانسیسکو، کالیفرنیا تغییر شکل داد. این شرکت در واقع یک کمپانی است که نرم افزار های وب سرور را تولید و ارائه می‌کند. بر اساس بررسی‌های Netcraft در اگوست سال ۲۰۱۴، nginx به عنوان دومین وب سرور پرطرفدار در سایت‌های فعال شناخته شد. از برخی از ویژگی‌ها و قابلیت‌های Nginx می‌توان به موارد زیر اشاره کرد :

۱. قابلیت پشتیبانی و مدیریت بیش از ۱۰،۰۰۰ اتصال همزمان با مصرف رم بسیار پایین.
۲. قابلیت توزیع بار.
۳. قابلیت Fault tolerance.
۴. پشتیبانی از OCSP با OpenSSL.
۵. پشتیبانی از FastCGI, SCGI, uWSGI به همراه caching.
۶. سازگار با IP ورژن ۶.
۷. پشتبانی از پروتکل SPDY.
۸. فشرده سازی و اکسترکت gzip.
۹. باز نویسی URL یا URL rewriting.
۱۰. قابلیت Bandwidth throttling.
۱۱. پردازش داده های XSLT.
۱۲. پشتیبانی از TLS/SSL.
۱۳. پشتیبانی از STARTTL ها.

۱۴. احراز هویت با استفاده از سرور HTTP خارجی.

۴-۵ وب سرور مورد استفاده بر روی سامانه

فریم‌ورک جانگو دارای یک وب سرور بسیار ساده و مناسب فاز توسعه نرم‌افزار است، که برنامه نویسان از طریق آن می‌توانند خروجی‌های کار خود را در هنگام کد نویسی تحلیل و بررسی کرده تا برنامه را توسعه و اشکال زدایی کنند. این سرور اصلا برای دنیای واقعی طراحی نشده است و هیچ‌گونه قابلیت‌های اصلی یک سرور را ندارد. ویژگی این سرور سادگی، سبک بودن و عدم نیاز به تنظیمات برای راه اندازی است. مساله واضح این است که پس از اتمام فاز توسعه نرم افزار و قرارگیری در فاز تحویل نرم افزار این سرور باید با یک وب سرور واقعی جایگزین گردد. در طی بررسی‌های صورت گرفته مشخص گردید که در سامانه سنجش از دور وب سروری که در حال ارائه خدمات است، هنوز همان وب سرور توسعه جانگو است و کاملا بدیهی است که، این وب سرور باید با یک سرور مناسب جایگزین گردد. یکی از جایگزین‌های خوب می‌تواند Nginx باشد که در قسمت ۳-۵ تشریح شده است.

۶ نتیجه‌گیری

امنیت یک سایت مساله مهمی است که قطعا ارزش هزینه صرف زمان و هزینه را دارد. امنیت سایت به مجموعه اقداماتی گفته می شود که با انجام آنها ضریب امنیت سایت به حداکثر رسیده و امکان نفوذ به آن به حداقل می رسد. توجه داشته باشید که امنیت سایت تابع موارد دیگری نیز می باشد که تمامی آنها نقش بسیار اساسی در تامین امنیت وب سایت دارند. امنیت سرور، امنیت شبکه، امنیت اینترنت، امنیت سیستم عامل، امنیت نرم افزار و بسیاری از موارد دیگر نقش کلیدی در تامین زیرساخت امنیت سایت دارند. ایجاد امنیت یک پروسه است که در هنگام توسعه و پیاده‌سازی وب سایت نیز باید در نظر داشت. در این مستند ابتدا به بررسی موارد مهم و اصلی در ایجاد امنیت بر روی یک وب سایت پرداخته شده است. موارد مورد بررسی در بخش ۳ گزارش ارائه گردیده است. در نهایت به بررسی سامانه سنجش پرداخته شده است. در طی این بررسی‌ها چالش‌های اساسی مشخص گردیده‌اند و راه‌حل‌هایی برای حل آن‌ها پیشنهاد گردیده شده است. پیشنهادات در بخش ۵ گزارش ارائه گردیده است. به طور کلی پیشنهاد می‌شود که موارد مطروحه هر چه زودتر بر روی سایت مورد نظر اعمال شود تا مساله امنیتی سایت به سطح بالاتری ارتقاع یابد.