بسمه تعالی

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

وب‌سایت دانشگاه علوم پزشکی شهرکرد

ارزیابی امنیتی وب‌سایت

نوع سند ..... گزارش فنی
شماره نگارش ۱
تاریخ نگارش ۱۳۹۹/۰۲/۱۸

تهران- میدان آرژانتین- ابتدای بلوار بیهقی- نبش خیابان شانزدهم- ساختمان شماره ۱ سازمان فناوری اطلاعات ایران

(۰۲۱)۴۲۶۵۰۰۰۰ ۰۲۱ ۴۲۶۵۰۰۰۰ cert.ir

فهرست مطالب

۱ معرفی سامانه

وب‌سایت تحت بررسی مربوط به دانشگاه علوم پزشکی شهرکرد است که از سال ۱۳۶۵ کار خود را با پذیرش ۲۴۰ دانشجو در سه رشته و دو مقطع تحصیلی در قالب دو دانشکده آغاز کرد. تعداد اعضای هیات علمی دانشگاه در حال حاضر ۲۲۸ نفر و شامل ۶۱ استاد، ۲۹ دانشیار، ۱۶۳ استادیار و ۲۹ مربی و ۱ نفر استادیار پژوهشی می باشد. بخش سلامت استان زیر نظر دانشگاه علوم پزشکی و خدمات بهداشتی و درمانی استان چهار محال و بختیاری مدیریت می گردد.

شکل ۱ وب‌سایت دانشگاه علوم پزشکی شهرکرد

۲ شرح آسیب‌پذیری

آنچه در این گزارش ارائه می‌گردد، تعدادی از آسیب‌پذیری‌های یافت شده در وب‌سایت دانشگاه علوم پزشکی شهرکرد به آدرس اینترنتی https://www.skums.ac.ir است. ارزیابی‌های صورت گرفته، حاکی از آن است که در این سامانه، چهار آسیب‌پذیری و مشکل امنیتی وجود دارد که در ادامه به تفصیل در مورد هر یک از این آسیب‌پذیری‌ها، مولفه‌های آسیب‌پذیر، جزئیات و راه‌حل‌های پیشنهادی توضیحاتی ارائه می‌گردد.

بررسی‌ها حاکی از آن است که وب‌سایت مذکور از DorsaPortal به عنوان سیستم مدیریت محتوای خود استفاده می‌نماید.

شکل ۲ آدرس ip و پورت‌های باز

توجه : بررسی سطحی زیر دامنه های این وب سایت نشانگر این است که زیر دامنه ها نیاز به بررسی بیشتر داشته و احتمال وجود آسیب پذیری های جدی در آن‌ها به چشم می‌خورد. لازم به ذکر است که با توجه به عدم امکان ثبت‌نام در این وب سایت، پنل کاربران نیز مورد بررسی قرار نگرفت.

۳ نقایص امنیتی موجود در برنامهٔ کاربردی

۳-۱ آسیب‌پذیری دور زدن مکانیزم کد امنیتی (کپچا)

- **درجه و نوع خطر:** بحرانی
- **مؤلفهٔ آسیب‌پذیر:** کدهای کپچای در نظر گرفته شده برای کاربران
- **توضیحات تکمیلی:**

یکی از مهم ترین ا شکالات این وب سایت در بخش فرم‌ها خود را نمایان می سازد. به این شکل که پس از پر کردن فرم‌های موجود، از کاربر خواسته می‌شود کد کپچای در نظر گرفته شده در فرم مربوطه را نیز وارد نماید. پس از پر کردن فرم مربوطه و ارسال درخواست، همانطور که در تصویر زیر نیز مشاهده می‌شود، علاوه بر کد کپچای وارد شده توسط کاربر، کد کپچای درنظر گرفته شده برای وی نیز در متن درخواست به سمت سرور ارسال می‌گردد. به عبارت دیگر علاوه بر کد وارد شده توسط کاربر، کدی که به منظور راستی‌آزمایی و مقایسه برای کاربر در نظر گرفته شده نیز در متن درخواست ارسال می‌گردد. بررسی‌های صورت گرفته حاکی از آن است که با تغییر هر دوی این مقادیر به مقدار دلخواه، قادر خواهیم بود این فرآیند را دور زده و عبارتی غیر از مقدار تعیین شده توسط سرور را جعل نماییم.

شکل ۳ درخواست ارسالی هنگام سابمیت فرم‌ها

این مسئله ناشی از آن است که سمت سرور راستی‌آزمایی و مقایسهٔ این دو مقدار صورت نمی‌گیرد. به عبارت دیگر بررسی نمی‌گردد که آیا مقدار وارد شده توسط کاربر به عنوان کپچا با مقدار در نظر گرفته شده توسط سرور یکسان است یا خیر.

- **راه‌حل:**

به عنوان راه‌حل پیشنهاد می‌گردد مقدار کپچا سمت سرور ذخیره شده و بررسی صحت عبارت وارد شده توسط کاربر با مقدار در نظر گرفته شده برای وی در سمت سرور انجام پذیرد نه در هدر ارسالی.

۳-۲ استفاده از شناسه یکتا کاربر (سشن) با ساختار ساده

- **درجه و نوع خطر:** متوسط
- **مؤلفهٔ آسیب‌پذیر:** ساز و کار احراز هویت کاربران
- **توضیحات تکمیلی:**

همانطور که در تصویر زیر نیز مشاهده می‌شود، بررسی‌ها حاکی از آن است که شناسهٔ در نظر گرفته شده برای هر کاربر، ساختار ساده‌ای داشته و استفاده از این ساختار ساده ممکن است وب‌سایت مربوطه را با مشکلات متعددی مواجه سازد.

شکل ۴ ساختار در نظر گرفته شده به عنوان سشن یکتای کاربر

- **راه‌حل:**

در نظر گرفتن ساختار مناسب به عنوان شناسهٔ یکتای کاربر

۳-۳ عدم مدیریت صحیح خطاها

- **درجه و نوع خطر:** متوسط – امکان افشای اطلاعات حساس در پیغام‌های خطا
- **مؤلفهٔ آسیب‌پذیر:** مدیریت خطاها و پیکربندی برنامه کاربردی تحت وب
- **توضیحات تکمیلی:**

بررسی‌های صورت گرفته حاکی از آن است که وارد کردن مقادیر غیر استاندارد در فرم ورود، منجر به ایجاد خطا سمت سرور و افشای مسیر و توابع برنامه می‌شود. در تصویر زیر نمونه‌ای از این خطاها مشاهده می‌گردد:

شکل ۵ خطای سرور

در این میان به نظر می‌رسد پارامتر hdnparam نیازمند توجه بیشتری است؛ همانطور که در تصویر زیر نیز مشاهده می‌گردد، دستکاری این مقدار، ممکن است منجر به عدم مدیریت صحیح کد امنیتی گردد.

شکل ۶ درخواست ارسالی

شکل ۷ عدم مدیریت صحیح کد امنیتی

- **راه‌حل:**

توجه و دقت در پروسه توسعه و آپدیت سامانه، انجام تست‌ها و ارزیابی‌های دوره‌ای در سامانه به منظور شناسایی خطاها و اشکال در پیکربندی‌های مربوطه، مدیریت خطاها و غیرفعال‌سازی قابلیت نمایش خطا در برنامه کاربردی و سرویس‌دهنده وب.

۳-۴ ذکر مسیرهای غیرضروری در فایل robots.txt

- **درجه و نوع خطر:** متوسط
- **مؤلفهٔ آسیب‌پذیر:** مسیرهای وب‌سایت
- **توضیحات تکمیلی:**

بررسی فایل robots.txt این وب‌سایت از طریق آدرس زیر:

https://www.skums.ac.ir/robots.txt

نشانگر وجود مسیرهایی است که ذکر آن‌ها در فایل robots.txt ضرورتی نداشته و تنها منجر به افشای مسیرهای این وب‌سایت می‌گردد.

```
User-agent: *
http://www.skums.ac.ir//ShowPage.aspx?page_=news&lang=1&tempname=Main&sub=0&isPopUp=false&PageID=10172&PageIDF=357
 http://www.skums.ac.ir//ShowPage.aspx?page_=news&lang=1&tempname=Main&sub=0&isPopUp=false&PageID=10183&PageIDF=357
Disallow: /attachfile
Disallow: /SDK
http://bnursefaculty.skums.ac.ir/ShowPage.aspx?page_=form&order=show&lang=1&sub=30&PageId=993&codeV=1&tempname=OparastariBroujen
http://bnursefaculty.skums.ac.ir/ShowPage.aspx?page_=form&order=show&lang=1&sub=30&PageId=991&codeV=1&tempname=OparastariBroujen
http://bnursefaculty.skums.ac.ir/ShowPage.aspx?page_=form&order=show&lang=1&sub=30&PageId=994&codeV=1&tempname=OparastariBroujen
http://bnursefaculty.skums.ac.ir/ShowPage.aspx?page_=form&order=show&lang=1&sub=30&PageId=996&codeV=1&tempname=OparastariBroujen
http://bnursefaculty.skums.ac.ir/ShowPage.aspx?page_=form&order=show&lang=1&sub=30&PageId=998&codeV=1&tempname=OparastariBroujen
http://bnursefaculty.skums.ac.ir/ShowPage.aspx?page_=form&order=show&lang=1&sub=30&PageId=989&codeV=1&tempname=OparastariBroujen
Disallow: /attachfile
Disallow: /SDK
Disallow: /attachfile
Disallow: /SDK
```

شکل ۸ محتوای فایل robots.txt

- **راه‌حل:**

از ذکر مسیرهای غیر ضروری، اضافی، حاوی اطلاعات حساس در فایل robots.txt خودداری گردد.