

راهنمای جامع کاربران

سامانه امن نگار ویرا

نسخه : ۱/۰

ورود/ثبت نام

صفحه اصلی نگارش گزارش راهنمای سامانه تماس با ما

مرکز آریا دانشگاه کردستان
سامانه امن نگار ویرا

سامانه نگارش آنلاین گزارش آسیب پذیری امنیتی
امن نگار ویرا

نرم افزار ویندوز اپلیکیشن موبایل وبسایت - پورتال

SIRT
مرکز پاسخگویی حوادث امنیتی

مرکز مدیریت تهدیدات و هماهنگی عملیات در سطح ملی رایانه‌ای

سازمان فناوری اطلاعات ایران



سامانه امن نگار



VIRA
Vulnerability Reporting System

مرکز آرا دانشگاه کردستان
گزارش آسیب پذیری

صفحه اصلی | گزارش امن‌رسی | تماس با ما | ورود/ثبت نام

سامانه نگارش آنلاین گزارش آسیب پذیری امنیتی
امن نگار ویبرا

وبسایت - پورتال | اپلیکیشن موبایل | نرم افزار ویندوز





cert.uok.ac.ir



apa@uok.ac.ir

سامانه امن نگار ویبرا

VIRA Vulnerability Reporting System

ویژگی‌های سامانه

- ۱ تسریع و سهولت در آماده‌سازی گزارش ارزیابی‌های امنیتی
- ۲ استانداردسازی قالب مربوط به گزارش‌نویسی
- ۳ مدیریت مستندات و گزارش‌ها
- ۴ پایگاه‌داده به‌روز و جامع آسیب‌پذیری‌های وب
- ۵ امکان ثبت‌نام کاربر و کار در محیط کاربری
- ۶ ذخیره و دانلود گزارش به صورت PDF



معرفی سامانه

تهیه و تدوین گزارش ارزیابی امنیتی از بخش‌های مهم فرآیند در ارزیابی یک سامانه حوزه فناوری اطلاعات است. این گزارش باید حاوی اطلاعات مهمی از قبیل قسمت‌های نشانه‌گذاری شده سامانه، انواع آسیب پذیری‌ها و همچنین نحوه رفع آنها باشد. به همین دلیل تهیه یک گزارش ارزیابی برای کارشناسان این حوزه کاری زمان‌بر است و عموماً از استاندارد مشخصی در این زمینه تبعیت نمی‌شود.

سامانه امن نگار ویبرا که در مرکز آرا دانشگاه کردستان طراحی و پیاده سازی شده است ابزاری توانمند برای آماده‌سازی گزارش‌های ارزیابی امنیتی سامانه‌ها می‌باشد که ضمن فراهم‌سازی یک قالب استاندارد و جامع در گزارش‌گیری، فرآیند ارزیابی را تسریع و تسهیل می‌کند.

زبان‌ها، ابزارها و تکنولوژی‌های استفاده شده











صفحه اصلی سامانه



با وارد کردن آدرس دسترسی به سامانه توسط کاربر، صفحه اصلی به وی نشان داده خواهد شد.

- ۱- منو "صفحه اصلی" - هدایت کاربر به صفحه اصلی وبسایت در تمامی صفحات
- ۲- منو "نگارش گزارش" - هدایت کاربر به صفحه نگارش گزارش
- ۳- منو "راهنمای سامانه" - ارائه یک فایل برای راهنمای کاربران در خصوص استفاده از سامانه
- ۴- منو "تماس با ما" - راههای ارتباطی جهت ارتباط با مرکز آپا دانشگاه کردستان
- ۵- دکمه "ورود/ثبت نام" - هدایت کاربر به فرم ورود، پنل کاربری و ثبت نام در سامانه
- ۶- گزینه "وبسایت - پورتال" - هدایت کاربر به صفحه نگارش گزارش تست نفوذ و آسیب پذیری وب
- ۷- گزینه "اپلیکیشن موبایل" - در نسخه های بعدی تکمیل خواهد شد..
- ۸- گزینه "نرم افزار ویندوز" - در نسخه های بعدی تکمیل خواهد شد..

● صفحه ورود کاربران

کاربر با کلیک بر روی این گزینه به صفحه ورود کاربران هدایت خواهد شد.

ورود به پروفایل کاربری

مشخصات ورود را وارد کنید

نام کاربری

رمز عبور

کد امنیتی: ff5d9d

ایجاد حساب کاربری

ورود

بازگشت به صفحه اصلی

در این صفحه کاربر چنانچه قبلاً در سامانه ثبت نام کرده باشد با استفاده از نام کاربری و رمز عبور خود می تواند به سامانه وارد شود.

– چنانچه کاربر در سامانه حساب کاربری نداشته باشد با انتخاب گزینه **ایجاد حساب کاربری** به صفحه ثبت نام هدایت خواهد شد.

● صفحه ثبت نام کاربران

The screenshot shows a registration form with the following fields and options:

- نام مرکز/شرکت/شخص:** Text input field.
- نوع حساب کاربری:** Radio buttons for "حقوقی" (Legal) and "حقیقی" (Physical).
- بصورت فارسی وارد شود:** Checkmark icon.
- پست الکترونیک مرکز/شرکت/شخص:** Text input field with "info@domain.ir" as an example.
- وبسایت مرکز/شرکت/شخص:** Text input field with "www.domain.ir" as an example.
- لوگو مرکز/شرکت/شخص (100 * 100 پیکسل):** File upload button labeled "پارگذاری لوگو" and "Choose File".
- تلفن تماس مرکز/شرکت/شخص:** Text input field with "+98" as a prefix.
- نام کاربری:** Text input field labeled "Username".
- کلمه عبور:** Text input field labeled "Password".
- کد امنیتی:** Text input field with "0816d4" as an example.
- شرایط و قوانین عضویت را می پذیرم:** Checkmark box.
- ثبت نام:** Blue button.
- قبلا ثبت نام کرده اید؟ | وارد شوید:** Link.

در این صفحه جهت ایجاد حساب کاربری از کاربر اطلاعات ذیل دریافت خواهد شد:

۱. نام مرکز/شرکت/شخص

۲. نوع حساب کاربری (حقیقی-حقوقی)

۳. وبسایت مرکز/شرکت/شخص

۴. پست الکترونیک مرکز/شرکت/شخص

۵. تلفن تماس مرکز/شرکت/شخص

۶. لوگو مرکز/شرکت/شخص

۷. نام کاربری

۸. کلمه عبور

در انتها کاربر با مشاهده و موافقت با "شرایط و قوانین عضویت" بر روی دکمه **ثبت نام** کلیک کرده و اطلاعات و حساب کاربری وی ایجاد میگردد.

صفحه اصلی پروفایل کاربر

The screenshot shows a user profile page with the following elements:

- Header:** "ناحیه کاربری | مدیریت گزارشات" (User Area | Report Management), "صفحه اصلی وب سایت" (Website Home Page), "نگارش گزارش" (Report Writing), "عملیات کاربری" (User Operations), and "م صندوق پیام" (Message Box).
- Main Content:**
 - داشبورد اصلی** (Main Dashboard)
 - گزارش آخرین فعالیت شما** (Your Latest Activity Report) table:

تاریخ	ساعت	سیستم عامل	مرورگر	IP آدرس
پنجشنبه ۱۳۹۸/۱۱/۱۷	۱۴:۰۷	Windows ۱۰	Chrome	۱۲۷.۰.۰.۱
 - Two summary cards:
 - تعداد گزارشات ثبت شده (تست نفوذ) - ۳ (Number of reports registered (penetration test) - 3)
 - تعداد گزارشات ثبت شده (آسیب پذیری) - ۳ (Number of reports registered (vulnerability) - 3)
- Sidebar:**
 - Logo: SIRT (Security Incident Response Team)
 - مرکز آقا دانشگاه کردستان (Agfa University Center of Kurdistan)
 - داشبورد اصلی (Main Dashboard)
 - آرشیو اطلاعات آسیب پذیری (Vulnerability Information Archive)
 - لیست گزارشات (Report List)
 - نگارش گزارش جدید (Write New Report)
 - آسیب پذیری ها (Vulnerabilities)
 - تنظیمات پنل کاربری (User Panel Settings)

گزینه‌های نوار بالا:

۱. منو "صفحه اصلی وبسایت" - هدایت کاربر به صفحه اصلی سامانه

۲. منو "نگارش گزارش" - هدایت کاربر به صفحه نگارش گزارشات

۳. منو **عملیات کاربری** شامل سه زیرمنو می‌باشد:

مشاهده پروفایل - برای مشاهده پروفایل کاربری خود و ویرایش اطلاعات از این گزینه استفاده نمایید.

تنظیمات کاربری - برای بارگذاری لوگو سربرگ گزارشات و تغییر تصویر پیش فرض پروفایل خود از این گزینه استفاده نمایید.

خروج از سامانه - برای اتمام نشست و خروج از حساب کاربری خود از این گزینه استفاده نمایید.

گزینه‌های نوار کناری (سمت راست):

۱. کادر "لوگو" - نمایش لوگو مرکز/شرکت/شخص
۲. نام مرکز/شرکت/شخص
۳. منو "داشبورد اصلی" - هدایت کاربر به صفحه اصلی پروفایل در تمامی صفحات
۴. منو "لیست گزارشات" - شامل دو زیرمنو:
 - ۴.۱. آسیب پذیری وبسایت : هدایت کاربر به صفحه "لیست گزارشات آسیب پذیری وبسایت"
 - ۴.۲. تست نفوذ وبسایت : هدایت کاربر به صفحه "لیست گزارشات تست نفوذ وبسایت"
۵. منو "نگارش گزارش جدید" - شامل دو زیرمنو:
 - ۵.۱. گزارش آسیب پذیری وبسایت : هدایت کاربر به صفحه "ایجاد گزارش آسیب پذیری وبسایت"
 - ۵.۲. گزارش تست نفوذ وبسایت : هدایت کاربر به صفحه "ایجاد گزارش تست نفوذ وبسایت"
۶. منو "آسیب پذیری‌ها" - شامل دو زیرمنو:
 - ۶.۱. لیست آسیب پذیری های من : هدایت کاربر به صفحه "لیست آسیب پذیری‌ها"
 - ۶.۲. افزودن آسیب پذیری : هدایت کاربر به صفحه "افزودن آسیب پذیری جدید"
۷. منو "تنظیمات پنل کاربری" - هدایت کاربر به صفحه تنظیمات پنل کاربری

پنل‌های صفحه اصلی داشبورد:

۱. پنل "گزارش آخرین فعالیت شما" - نمایش جزئیات فنی آخرین فعالیت شما در نشست قبلی
۲. پنل "گزارشات آسیب پذیری وبسایت" - نمایش تعداد گزارشات آسیب پذیری وبسایت ثبت شده توسط کاربر
۳. پنل "گزارشات تست نفوذ وبسایت" - نمایش تعداد گزارشات تست نفوذ وبسایت ثبت شده توسط کاربر

صفحه پروفایل

داشبورد / پروفایل کاربری

پروفایل کاربری



مرکز آپا دانشگاه کردستان
نوع حساب کاربری : حقوقی

وب سایت : www.test.ir
پست الکترونیک : info@test.ir
تلفن تماس : ۰۸۷۳۳۳۲۱۱۴۴

[ویرایش اطلاعات](#)

تصویر پیشفرض

شما می توانید از قسمت تنظیمات پیل کاربری این تصویر را تغییر دهید.

این صفحه شامل ۲ بخش است:

- پنل سمت راست : نمایش اطلاعات حساب کاربری
- پنل سمت چپ : تصویر پس زمینه پروفایل کاربر که بصورت پیشفرض توسط سامانه ست می شود، کاربر می تواند از قسمت تنظیمات پیل کاربری این تصویر را به دلخواه تغییر دهد.

در این صفحه کاربر با انتخاب گزینه **ویرایش اطلاعات** به صفحه ویرایش اطلاعات کاربری هدایت خواهد شد.

صفحه ویرایش اطلاعات کاربری

داشبورد / پروفایل کاربری

پروفایل کاربری

ویرایش اطلاعات کاربری

نام مرکز/شرکت/شخص: مرکز آپا دانشگاه کردستان

نوع حساب کاربری: حقوقی

وب سایت مرکز/شرکت/شخص: www.test.ir

پست الکترونیک مرکز/شرکت/شخص: info@test.ir


تلفن تماس مرکز/شرکت/شخص: 08733221144

لوگو مرکز/شرکت/شخص: [لوگو باید دربعاد 100 * 100 پیکسل باشد.](#)
No file chosen [Choose File](#) بارگذاری لوگو جدید:

نام کاربری: apa

تغییر کلمه عبور: [طول کلمه عبور باید بیشتر از 14 کاراکتر باشد.](#)
در صورت عدم تغییر این فیلد را خالی بگذارید

[ثبت تغییرات](#)



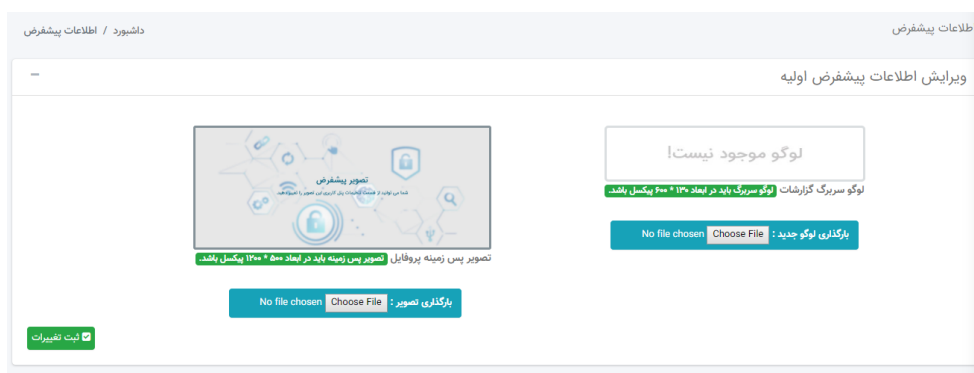
مرکز آپا دانشگاه کردستان
نوع حساب کاربری : حقوقی

وب سایت : www.test.ir
پست الکترونیک : info@test.ir
تلفن تماس : ۰۸۷۳۳۳۲۱۱۴۴

[ویرایش اطلاعات](#)

در این صفحه کاربر می تواند مشخصات تماس و اطلاعات کاربری خود را ویرایش نماید. همچنین قادر است لوگو و کلمه عبور خود را نیز تغییر دهد.

● صفحه تنظیمات پنل کاربری



در این صفحه کاربر می تواند یک لوگو ثابت برای سربرگ گزارشات خود بارگذاری نماید. همچنین از این بخش می تواند تصویر پس زمینه پیش فرض پروفایل خود را تغییر دهد.

● صفحه لیست گزارشات

شناسه	شماره سند	مرکز/شرکت/شخص	عنوان	آدرس اینترنتی	تاریخ گزارش	عملیات
۴۳۴۳۵۴۷۴۶	۳۲۴۳۲۴۲۳	مرکز آبا دانشگاه کردستان			۱۳۹۸/۱/۱۷	مشاهده حذف
۲۰۶۲۱۱۶۲۸۲	۰۰۰۰۰۰۱۱۱۱۱	مرکز آبا دانشگاه کردستان			۱۳۹۸/۱/۱۷	مشاهده حذف
۱۷۲۵۸۱۶۵۵۶	وارد نشده	مرکز آبا دانشگاه کردستان			۱۳۹۸/۱/۱۷	مشاهده حذف

در این صفحه کاربر می تواند گزارشات ثبت شده خود را مشاهده نماید.

با انتخاب گزینه **حذف** کاربر می تواند گزارش را حذف نماید.

جهت مشاهده اطلاعات کامل گزارش کاربر با انتخاب گزینه **مشاهده** به صفحه جزئیات گزارش هدایت خواهد شد.

صفحه جزئیات گزارش

جزئیات گزارش: ۴۳۶۳۵۴۷۳۶

اطلاعات شخصی / سازمانی:

موضوع گزارش: گزارش آسیب پذیری وب سایت	مرکز/شرکت/شخص: مرکز آبا دانشگاه کردستان
وب سایت: cert.uok.ac.ir	تاریخ ایجاد: ۱۳۹۸/۱۱/۱۷
تلفن تماس: +۹۸۸۷۳۳۶۶۷۹۳۲	پست الکترونیک: cert@uok.ac.ir

پورتال آسیب پذیر:

ایمیل: [مخفی]	آدرس اینترنتی: [مخفی]
کدپستی: [مخفی]	شماره تماس: [مخفی]
آدرس: [مخفی]	درباره پورتال: [مخفی]

[بازگشت] [دریافت گزارش]

در این صفحه جزئیات هر گزارش شامل اطلاعات شخصی/سازمانی و اطلاعات مربوط به پورتال آسیب پذیر به کاربر نشان داده خواهد شد.

در این صفحه همچنین کاربر می تواند با کلیک بر روی گزینه [دریافت گزارش](#) فایل گزارش خود را مجدداً دریافت نماید.

نگارش گزارش آسیب پذیری:

● صفحه انتخاب قالب گزارش



در این صفحه کاربر بر اساس نوع گزارش قالب مورد نیاز خود را انتخاب می نماید:

- قالب گزارش آسیب پذیری

- قالب گزارش تست نفوذ

نگارش گزارش بصورت کاربر مهمان:

در این سامانه امکان نگارش گزارش بصورت مهمان نیز وجود دارد، کاربران می توانند بدون ایجاد حساب کاربری در سامانه نسبت به ایجاد گزارش اقدام نمایند.

نگارش گزارش آسیب پذیری وب سایت

اطلاعات شخصی / سازمانی 1درج اطلاعات اولیه 2وب سایت آسیب پذیر 3انتخاب آسیب پذیری 4تایید اطلاعات 5

اطلاعات شخصی / سازمانی

نام مرکز / شرکت / شخص	مثال: مرکز آيا دانشگاه كردستان
وب سایت مرکز / شرکت / شخص	مثال: cert.uok.ac.ir
پست الکترونیک مرکز / شرکت / شخص	مثال: info@cert.uok.ac.ir
تلفن تماس مرکز / شرکت / شخص	مثال: ۰۸۷۳۳۶۶۴۹۳۲
لوگو سربرگ گزارش	بارگذاری فایل لوگو: <input type="button" value="Choose File"/> No file chosen
موضوع گزارش	تاریخ گزارش
گزارش آسیب پذیری وب سایت	۱۳۹۸ ۰۶ ۰۷

* در صورت عدم ورود به سامانه کاربر میبایست هر بار این اطلاعات را مجدداً وارد نماید اما در صورت ایجاد حساب کاربری، این اطلاعات بصورت خودکار با استفاده از اطلاعات کاربری موجود تکمیل خواهد شد.

* همچنین لازم به ذکر است کاربرانی که بصورت مهمان اقدام به نگارش گزارش می کنند در آینده نمی توانند به اطلاعات و جزئیات گزارش از طریق این سامانه دسترسی داشته باشند.

● صفحه نگارش گزارش آسیب پذیری

نگارش گزارش آسیب پذیری - مرحله اول : اطلاعات شخصی / سازمانی

کاربر پس از ورود به حساب کاربری خود و انتخاب گزینه نگارش گزارش آسیب پذیری صفحه زیر به وی نشان داده خواهد شد:

اطلاعات شخصی / سازمانی < درج اطلاعات اولیه < وب سایت آسیب پذیر < انتخاب آسیب پذیری < تایید اطلاعات

اطلاعات شخصی / سازمانی

نام مرکز/شرکت/شخص *	وب سایت مرکز/شرکت/شخص
<input type="text" value="مرکز آيا دانشگاه كردستان"/>	<input type="text" value="cert.uok.ac.ir"/>
لوگو سربرگ گزارش *	پست الکترونیک مرکز/شرکت/شخص
	<input type="text" value="cert@uok.ac.ir"/>
موضوع گزارش	تلفن تماس مرکز/شرکت/شخص *
گزارش آسیب پذیری وب سایت	<input type="text" value="+9888733662932"/>
تاریخ گزارش *	
<input type="text" value="۱۳۹۸"/> <input type="text" value="۱۱"/> <input type="text" value="۱۸"/>	

[بهدی](#)

در این مرحله اطلاعات مرکز، شرکت یا شخص تهیه کننده گزارش توسط کاربر وارد خواهد شد که شامل موارد زیر می باشد:

۱. نام مرکز/شرکت/شخص *
۲. لوگو سربرگ گزارش *
۳. تاریخ گزارش *
۴. وب سایت مرکز/شرکت/شخص
۵. پست الکترونیک مرکز/شرکت/شخص
۶. تلفن تماس مرکز/شرکت/شخص *

* چنانچه کاربر در سامانه وارد شده باشد این اطلاعات بصورت خودکار از پایگاه داده تکمیل خواهد شد.

نگارش گزارش آسیب پذیری - مرحله دوم : درج اطلاعات اولیه

اطلاعات شخصی / سازمانی 1 < درج اطلاعات اولیه 2 < وب سایت آسیب پذیر 3 < انتخاب آسیب پذیری 4 < تایید اطلاعات 5

درج اطلاعات اولیه

عنوان پورتال آسیب پذیر *

متن مقدمه

آسیب‌پذیری‌های بحرانی که در پورتال‌ها و شبکه‌هایی که در سطح ملی وجود دارد، می‌تواند برای کشور بسیار تهدیدآمیز باشد، در نتیجه شناسایی آن‌ها یکی از مأموریت‌های مهم مراکز آ‌پا محسوب می‌شود. در این راستا مراکز آ‌پا در کشور اقدام به شناسایی این نوع آسیب‌پذیری‌ها می‌نمایند. در این گزارش که توسط .. نام مرکز .. تهیه شده، آسیب‌پذیری‌های .. نام وبسایت آسیب پذیر .. با آدرس .. دامنه وبسایت .. بررسی می‌شوند.

عنوان پورتال آسیب پذیر

توضیحات وب سایت آسیب پذیر را اینجا وارد نمایید.

کلمات کلیدی

شماره سند

در این مرحله اطلاعات مربوط به گزارش توسط کاربر وارد خواهد شد که شامل موارد زیر می‌باشد:

۱. متن مقدمه گزارش
۲. کلمات کلیدی مرتبط با گزارش
۳. درج یک شماره سند برای گزارش
۴. عنوان پورتال آسیب‌پذیر*
۵. متن درباره پورتال آسیب‌پذیر

نگارش گزارش آسیب پذیری - مرحله سوم : اطلاعات وبسایت آسیب پذیر

اطلاعات شخصی / سازمانی ۱ < درج اطلاعات اولیه ۲ < وبسایت آسیب پذیر ۳ < انتخاب آسیب پذیری ۴ < تایید اطلاعات ۵

وبسایت آسیب پذیر

آدرس اینترنتی وبسایت *
مثال: www.domain.ir

پست الکترونیک وبسایت
مثال: info@domain.ir

شماره تماس
مثال: ۰۸۷۱۲۳۴۵۶۷۸

آدرس پستی
آدرس پستی محل شرکت یا سازمان مربوط به وبسایت آسیب پذیر

کد پستی
مثال: ۶۶۱۱۱۲۲۳۳۴

در این مرحله اطلاعات مربوط به وبسایت آسیب پذیر توسط کاربر وارد خواهد شد که شامل موارد زیر می باشد:

۱. آدرس اینترنتی وبسایت *
۲. پست الکترونیک وبسایت
۳. شماره تماس مدیر وبسایت
۴. آدرس پستی مدیر وبسایت
۵. کد پستی مدیر وبسایت

نگارش گزارش آسیب پذیری - مرحله چهارم : انتخاب آسیب پذیری

در این مرحله اطلاعات مربوط به آسیب پذیری‌ها توسط کاربر وارد خواهد شد. کاربر با انتخاب گزینه **+ افزودن** صفحه انتخاب آسیب پذیری به وی نشان داده خواهد شد.

صفحه انتخاب آسیب پذیری:

۱. انتخاب آسیب پذیری *

- عمومی : انتخاب آسیب پذیری از لیست اصلی
- خصوصی : انتخاب آسیب پذیری از لیست شخصی

۲. میزان حساسیت آسیب پذیری

۳. متد ۴. پارامتر

۵. توضیحات آسیب پذیری *

۶. توضیحات نحوه رفع آسیب پذیری *

۷. مسیرهای آسیب پذیر

۸. نوع آزمون

۹. payload * ۱۰. Google Dork

۱۱. اثبات آسیب پذیری

۱۲. تصویر اثبات آسیب پذیری

جستجو در بانک اطلاعاتی آسیب پذیری‌ها:

کاربر می‌تواند نام آسیب پذیری مورد نظر خود را در کادر جستجو وارد نماید تا اطلاعات مربوط به آن آسیب پذیری بصورت خودکار تکمیل شود:

افزودن آسیب پذیری جدید

انتخاب آسیب پذیری * عمومی خصوصی

پارامتر:

متد: GET

میزان حساسیت: بحرانی

Cross

Reflected Cross Site Scripting

Stored Cross Site Scripting

مثال:

افزودن آسیب پذیری جدید

انتخاب آسیب پذیری * عمومی خصوصی

پارامتر:

متد: GET

میزان حساسیت: متوسط

Reflected Cross Site Scripting

6.8

Base Score

Vector String – CVSS:3.0/AV:P/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H

CWE-79

توضیحات آسیب پذیری *

آسیب‌پذیری XSS از دسته آسیب‌پذیری‌های سمت کاربر بوده که با اجرای کدهای جاوا اسکریپت می‌تواند امنیت کاربر را تهدید نماید. این تهدیدات می‌تواند شامل سرقت کوکی کاربر، تغییر ظاهر سایت و یا انتقال کاربر به صفحات جعلی و اجبار به دانلود فایل‌های مخرب باشد. از آنجایی که این آسیب‌پذیری از کاراکترهای خاص و Tag های HTML استفاده می‌کند، راه مقابله با آن فیلتر کردن این مقادیر است.

نحوه رفع آسیب پذیری *

۱- فیلتر کردن tag های html و JavaScript وارد شده توسط کاربر
۲- Encode کردن مقادیر دریافتی و نگاشت کاراکترهای خاص به معادل html

برای اطلاعات بیشتر به لینک‌های زیر مراجعه شود:

<https://www.ibm.com/developerworks/library/se-prevent>

بعد از انتخاب و ثبت آسیب پذیری های مورد نظر، لیست موارد ثبت شده در جدولی مطابق شکل زیر به شما نشان داده خواهد شد که شامل ۳ گزینه مشاهده، ویرایش و حذف می باشد.

نام آسیب پذیری	متد	حساسیت	نوع آزمون	مشاهده	ویرایش	حذف
Reflected Cross Site Scripting	GET	متوسط	جعبه سیاه			

با کلیک بر روی آیکن اطلاعات مربوط به آسیب پذیری مربوطه در صفحه جدید به شما نشان داده می شود. در صورت نیاز به ویرایش اطلاعات آسیب پذیری با کلیک بر روی آیکن یک صفحه جدید جهت ویرایش اطلاعات آسیب پذیری به شما نشان داده خواهد شد که در آنجا می توانید اطلاعات مربوط به آسیب پذیری را تغییر دهید. در صورت نیاز به حذف یک آسیب پذیری از گزارش خود با کلیک بر روی آیکن پیغام هشدار زیر به شما نشان داده خواهد شد:



در صورت انتخاب گزینه تایید، آسیب پذیری انتخاب شده از گزارش شما حذف خواهد شد.

نگارش گزارش آسیب پذیری - مرحله پنجم : کنترل و تایید اطلاعات

اطلاعات شخصی / سازمانی (1) < درج اطلاعات اولیه (2) < وبسایت آسیب پذیر (3) < انتخاب آسیب پذیری (4) < تایید اطلاعات (5)

تایید اطلاعات

(?) با کلیک بر روی هر کدام از مراحل فوق میتوانید اطلاعات آن بخش را ویرایش کنید.

<p>اطلاعات وارد شده برای وبسایت آسیب پذیر به شرح زیر است:</p> <table style="width: 100%;"><tr><td>وبسایت :</td><td>www.domain.ir</td></tr><tr><td>پست الکترونیک :</td><td>mail@domain.ir</td></tr><tr><td>تلفن تماس :</td><td>۰۸۷۳۳۳۳۳۳۳۳</td></tr><tr><td>آدرس پستی :</td><td>کردستان سنندج</td></tr><tr><td>کد پستی :</td><td>۶۶۱۱۱۳۳۳۳۳</td></tr></table>	وبسایت :	www.domain.ir	پست الکترونیک :	mail@domain.ir	تلفن تماس :	۰۸۷۳۳۳۳۳۳۳۳	آدرس پستی :	کردستان سنندج	کد پستی :	۶۶۱۱۱۳۳۳۳۳	<p>اطلاعات وارد شده برای مرکز آقا دانشگاه کردستان به شرح زیر است:</p> <table style="width: 100%;"><tr><td>وبسایت :</td><td>cert.uok.ac.ir</td></tr><tr><td>پست الکترونیک :</td><td>cert@uok.ac.ir</td></tr><tr><td>تلفن تماس :</td><td>+۹۸۸۷۳۳۶۶۲۹۳۲</td></tr><tr><td>موضوع گزارش :</td><td>گزارش آسیب پذیری وبسایت</td></tr><tr><td>قالب گزارش :</td><td>آسیب پذیری وبسایت</td></tr></table>	وبسایت :	cert.uok.ac.ir	پست الکترونیک :	cert@uok.ac.ir	تلفن تماس :	+۹۸۸۷۳۳۶۶۲۹۳۲	موضوع گزارش :	گزارش آسیب پذیری وبسایت	قالب گزارش :	آسیب پذیری وبسایت
وبسایت :	www.domain.ir																				
پست الکترونیک :	mail@domain.ir																				
تلفن تماس :	۰۸۷۳۳۳۳۳۳۳۳																				
آدرس پستی :	کردستان سنندج																				
کد پستی :	۶۶۱۱۱۳۳۳۳۳																				
وبسایت :	cert.uok.ac.ir																				
پست الکترونیک :	cert@uok.ac.ir																				
تلفن تماس :	+۹۸۸۷۳۳۶۶۲۹۳۲																				
موضوع گزارش :	گزارش آسیب پذیری وبسایت																				
قالب گزارش :	آسیب پذیری وبسایت																				

مشخصات گزارش

کلمات کلیدی: آسیب پذیری XSS.SQL injection پورتال	شماره سند: 98ب33
--	------------------

آسیب پذیری ها

نام آسیب پذیری	متد	حساسیت	نوع آزمون
Reflected Cross Site Scripting	GET	متوسط	جعبه سیاه

مشاهده گزارشقبلی

در گام آخر اطلاعات وارد شده به شما نشان داده خواهد شد که در صورت وجود مشکل می‌توانید با کلیک بر روی هر کدام از زبانه‌های بالا به مرحله فوق بازگردید و اطلاعات آن بخش را ویرایش نمایید.

در نهایت با مشاهده این مرحله اطلاعات وارد شده را مجدداً بررسی کرده و در صورت تایید جهت ثبت و مشاهده گزارش گزینه مشاهده گزارش را کلیک نمایید.

نکته: پس از ثبت گزارش نیز کماکان می‌توانید با بازگشت به زبانه فعلی اطلاعات را مجدداً ویرایش و ثبت نمایید.

نگارش گزارش آسیب پذیری - مشاهده و دریافت گزارش

در زبانه جدید گزارش نهایی به شما نشان داده خواهد شد که می توانید مجدداً اطلاعات آن را بررسی کنید:

(در این مرحله نیز در صورت نیاز به ویرایش می توانید به زبانه قبلی بازگردید و اطلاعات را ویرایش نمایید.)



مرکز تخصصی آپا دانشگاه کردستان

گزارش آسیب پذیری وب سایت

مرکز آپا دانشگاه کردستان

گزارش آسیب پذیری پورتال (نام پورتال)


www.domain.ir

تاریخ گزارش : ۱۳۹۸/۱۱/۱۸

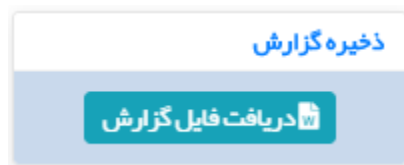
شماره سند : ۹۸/ب/۳۳


 cert.uok.ac.ir

 cert@uok.ac.ir

 +۹۸۸۷۳۳۶۶۲۹۳۲

در نهایت با استفاده از کادر موجود در گوشه پایین سمت چپ صفحه، گزارش خود را بصورت فایل WORD دریافت نماید.



برای اینکار کافیست بر روی دکمه  کلیک نمایید تا کمتر از چندثانیه فایل گزارش بر روی رایانه شما بارگیری گردد.

نگارش گزارش تست نفوذ - مرحله دوم : مفاد قرارداد



مفاد قرارداد

متن مقدمه

دسترس‌ها و نوع آزمون نفوذپذیری

سند حاضر شامل گزارش اولیه آزمون نفوذپذیری نرم‌افزار .. نام نرم افزار .. به نشانی اینترنتی .. آدرس اینترنتی .. است. آزمون نفوذپذیری مذکور با هدف کشف آسیب‌پذیری‌ها و مشکلات امنیتی موجود در این برنامه کاربردی تحت وب انجام پذیرفته است. موارد زیر در ادامه این گزارش به تفصیل شرح داده شده‌اند:

۱. جزئیات آزمون نفوذپذیری
۲. جمع آوری اطلاعات

شماره سند

یک شماره سند برای این گزارش وارد نمایید.

تاریخ و محل انجام آزمون نفوذپذیری

آزمون نفوذپذیری نرم‌افزار .. نام نرم افزار .. در تاریخ .. تاریخ .. با استفاده از روش جعبه سیاه انجام گرفته است. در طول آزمون، گروه آزمون نفوذپذیری کاملاً مشابه با سایر کاربران عادی به شبکه متصل بوده و به سرویس‌دهنده میزبان برنامه کاربردی دسترسی داشته است.

حوزه آزمون نفوذپذیری

آزمون نفوذپذیری انجام گرفته موارد زیر را شامل می‌شود:

۱. امنیت برنامه کاربردی در برابر حملات شناخته شده در بستر وب
۲. آسیب‌پذیری‌ها و نقایص امنیتی بستر و چارچوب برنامه کاربردی
۳. مشکلات امنیتی موجود در ساز و کارهای به کار گرفته شده در برنامه کاربردی
۴. نقایص و ضعف‌های امنیتی برنامه کاربردی ناشی از مشکلات موجود در منطق کاری آن
۵. آسیب‌پذیری‌ها و مشکلات امنیتی ناشی از بیکریندی نادرست سرویس‌دهنده وب برای میزبانی برنامه کاربردی مورد نظر

موارد زیر حتی در صورتی که در مورد آن‌ها مطالبی در گزارش درج شده باشد، خارج از حوزه آزمون نفوذپذیری محسوب شده و مرکز در قبال بررسی کامل آن‌ها مسئولیتی ندارد:

 ۱. آسیب‌پذیری‌های نرم‌افزار کارگزار وب

در این مرحله اطلاعات مربوط به مفاد قرارداد توسط کاربر وارد خواهد شد که شامل موارد زیر می‌باشد:

۱. متن مقدمه گزارش

۲. دسترس‌ها و نوع آزمون نفوذپذیری

۳. درج یک شماره سند برای گزارش

۴. تاریخ و محل انجام آزمون نفوذپذیری

۵. حوزه آزمون نفوذپذیری

نگارش گزارش تست نفوذ - مرحله سوم : جمع آوری اطلاعات

مفاد قرارداد ۲ < جمع آوری اطلاعات ۳ < وب سایت آسیب پذیر ۴ < انتخاب آسیب پذیری ۵ < تایید اطلاعات ۶ <

جمع آوری اطلاعات

شناسایی دامنه: حداکثر اندازه 900x500 پیکسل

پارگذاری تصویر:

IP سرور:

سیستم عامل سرور:

نسخه وب سرور:

زبان برنامه نویسی:

پورت های باز:

لیست اسکرپت های کلاینت:

لیست اسکرپت های بیرونی:

لیست فایل های دارای ورودی:

لیست فایل های اجرایی:

لیست هاست های بیرونی:

در این مرحله اطلاعات جمع آوری شده مربوط به وبسایت آسیب پذیر توسط کاربر وارد خواهد شد که شامل موارد زیر می باشد:

۱. تصویر شناسایی دامنه (اطلاعات whois)
 ۲. ip سرور (سرور وبسایت) ۳. سیستم عامل سرور
 ۴. نسخه وب سرور ۵. زبان برنامه نویسی
 ۶. پورت های باز
 ۷. لیست فایل های اجرایی
 ۸. لیست اسکرپت های کلاینت ۹. لیست اسکرپت های بیرونی
 ۱۰. لیست فایل های دارای ورودی ۱۱. لیست هاست های بیرونی
- که میبایست طبق راهنمای فیلدها تکمیل گردد.

نگارش گزارش تست نفوذ - مرحله چهارم : اطلاعات وبسایت آسیب پذیر

تایید اطلاعات < انتخاب آسیب پذیری < وبسایت آسیب پذیر < جمع آوری اطلاعات

۴ ۵ ۶ ۳

وبسایت آسیب پذیر

شماره تماس	عنوان پورتال آسیب پذیر *
مثال: ۰۸۷۱۲۳۴۵۶۷۸	عنوان پورتال آسیب پذیر را وارد نمایید.
آدرس پستی	آدرس اینترنتی وبسایت *
آدرس پستی محل شرکت یا سازمان مربوط به وبسایت آسیب پذیر	www.domain.ir
کدپستی	پست الکترونیک وبسایت
مثال: ۶۶۱۱۱۲۲۳۳۴	مثال: info@domain.ir

در این مرحله اطلاعات مربوط به وبسایت آسیب پذیر توسط کاربر وارد خواهد شد که شامل موارد زیر می باشد:

۱. عنوان پورتال آسیب پذیر *
۲. آدرس اینترنتی وبسایت *
۳. پست الکترونیک وبسایت
۴. شماره تماس مدیر وبسایت
۵. آدرس پستی مدیر وبسایت
۶. کدپستی مدیر وبسایت

جستجو در بانک اطلاعاتی آسیب پذیری ها:

شما می توانید نام آسیب پذیری مورد نظر خود را در کادر جستجو وارد نمایید تا اطلاعات مربوط به آن آسیب پذیری بصورت خودکار تکمیل شود:

افزودن آسیب پذیری جدید

انتخاب آسیب پذیری * عمومی خصوصی

میزان حساسیت: بحرانی

متد: GET

پارامتر:

Cross

Reflected Cross Site Scripting

Stored Cross Site Scripting

مثال:

افزودن آسیب پذیری جدید

انتخاب آسیب پذیری * عمومی خصوصی

میزان حساسیت: متوسط

متد: GET

پارامتر:

Reflected Cross Site Scripting

6.8

Base Score

Vector String – CVSS:3.0/AV:P/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H

CWE-79

توضیحات آسیب پذیری *

آسیب پذیری XSS از دسته آسیب پذیری های سمت کاربر بوده که با اجرای کدهای جاوا اسکریپت می تواند امنیت کاربر را تهدید نماید. این تهدیدات می تواند شامل سرقت کوکی کاربر، تغییر ظاهر سایت و یا انتقال کاربر به صفحات جعلی و اجبار به دانلود فایل های مخرب باشد. از آنجایی که این آسیب پذیری از کاراکترهای خاص و Tag های HTML استفاده می کند، راه مقابله با آن فیلتر کردن این مقادیر است.

نحوه رفع آسیب پذیری *

۱- فیلتر کردن tag های html و JavaScript وارد شده توسط کاربر
۲- Encode کردن مقادیر دریافتی و نگاشت کاراکترهای خاص به معادل html

برای اطلاعات بیشتر به لینک های زیر مراجعه شود:

<https://www.ibm.com/developerworks/library/se-prevent>

بعد از انتخاب و ثبت آسیب پذیری های مورد نظر، لیست موارد ثبت شده در جدولی مطابق شکل زیر به شما نشان داده خواهد شد که شامل ۳ گزینه مشاهده، ویرایش و حذف می باشد.

وبسایت آسیب پذیر < انتخاب آسیب پذیری < تایید اطلاعات

انتخاب آسیب پذیری

افزودن +

نام آسیب پذیری	متد	حساسیت	نوع آزمون	مشاهده	ویرایش	حذف
Reflected Cross Site Scripting	GET	متوسط	جعبه سیاه			

با کلیک بر روی آیکن اطلاعات مربوط به آسیب پذیری مربوطه در صفحه جدید به شما نشان داده می شود.

در صورت نیاز به ویرایش اطلاعات آسیب پذیری با کلیک بر روی آیکن یک صفحه جدید جهت ویرایش اطلاعات آسیب پذیری به شما نشان داده خواهد شد که در آنجا می توانید اطلاعات مربوط به آسیب پذیری را تغییر دهید.

در صورت نیاز به حذف یک آسیب پذیری از گزارش خود با کلیک بر روی آیکن پیغام هشدار زیر به شما نشان داده خواهد شد:



در صورت انتخاب گزینه تایید، آسیب پذیری انتخاب شده از گزارش شما حذف خواهد شد.

نگارش گزارش تست نفوذ - مرحله ششم: کنترل و تایید اطلاعات

تایید اطلاعات < انتخاب آسیب پذیری < وب سایت آسیب پذیر < |

۶ ۵ ۴

تایید اطلاعات

② با کلیک بر روی هر کدام از مراحل فوق می‌توانید اطلاعات آن بخش را ویرایش کنید.

اطلاعات وارد شده برای وب سایت آسیب پذیر به شرح زیر است:

وب سایت:	www.domain.ir
پست الکترونیک:	mail@domain.ir
تلفن تماس:	۰۸۷۳۳۳۳۳۳۳۳
آدرس پستی:	کردستان سنندج
کد پستی:	۶۶۱۱۱۳۳۳۳۳

اطلاعات وارد شده برای مرکز آپا دانشگاه کردستان به شرح زیر است:

وب سایت:	cert.uok.ac.ir
پست الکترونیک:	cert@uok.ac.ir
تلفن تماس:	+۹۸۸۷۳۳۳۳۳۳۳۳
موضوع گزارش:	گزارش تست نفوذ وب سایت
قالب گزارش:	آسیب پذیری وب سایت

آسیب پذیری ها

نوع آزمون	حساسیت	متد	نام آسیب پذیری
جعبه سیاه	متوسط	GET	Reflected Cross Site Scripting

مشاهده گزارش قبلی

در گام آخر اطلاعات وارد شده به شما نشان داده خواهد شد که در صورت وجود مشکل می‌توانید با کلیک بر روی هر کدام از زبانه‌های بالا به مرحله فوق بازگردید و اطلاعات آن بخش را ویرایش نمایید.

در نهایت با مشاهده این مرحله اطلاعات وارد شده را مجدداً بررسی کرده و در صورت تایید جهت ثبت و مشاهده گزارش گزینه

را کلیک نمایید.

مشاهده گزارش

نکته: پس از ثبت گزارش نیز کماکان می‌توانید با بازگشت به زبانه فعلی اطلاعات را مجدداً ویرایش و ثبت نمایید.

نگارش گزارش تست نفوذ - مشاهده و دریافت گزارش

در زبانه جدید گزارش نهایی به شما نشان داده خواهد شد که می توانید مجدداً اطلاعات آن را بررسی کنید:
(در این مرحله نیز در صورت نیاز به ویرایش می توانید به زبانه قبلی بازگردید و اطلاعات را ویرایش نمایید.)



مرکز تخصصی آپا دانشگاه کردستان

گزارش تست نفوذ وب سایت

مرکز آپا دانشگاه کردستان


گزارش آسیب پذیری پورتال (نام پورتال)


www.domain.ir

تاریخ گزارش : ۱۳۹۸/۱۱/۱۸

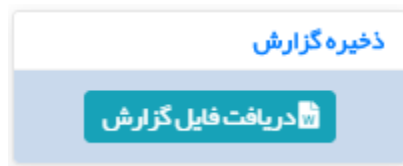
شماره سند : ۷۶۷۶۷۶


 cert.uok.ac.ir

 cert@uok.ac.ir

 +۹۸۸۷۳۳۶۶۲۹۳۲

در نهایت با استفاده از کادر موجود در گوشه پایین سمت چپ صفحه، گزارش خود را بصورت فایل WORD دریافت نمایید.



برای اینکار کافیست بر روی دکمه  کلیک نمایید تا کمتر از چند ثانیه فایل گزارش بر روی رایانه شما بارگیری گردد.