راهنمای جامـع کاربـران

سامانه امن نگار ویـــــرا

نسخه : ۱/۰

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 امن‌نگار ویرا که در مرکز آپا 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

AJAX, php, jQuery, B, HTML, CSS, JS, jsPDF

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

- **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 درخصوص 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 ثبت‌نام در سامانه

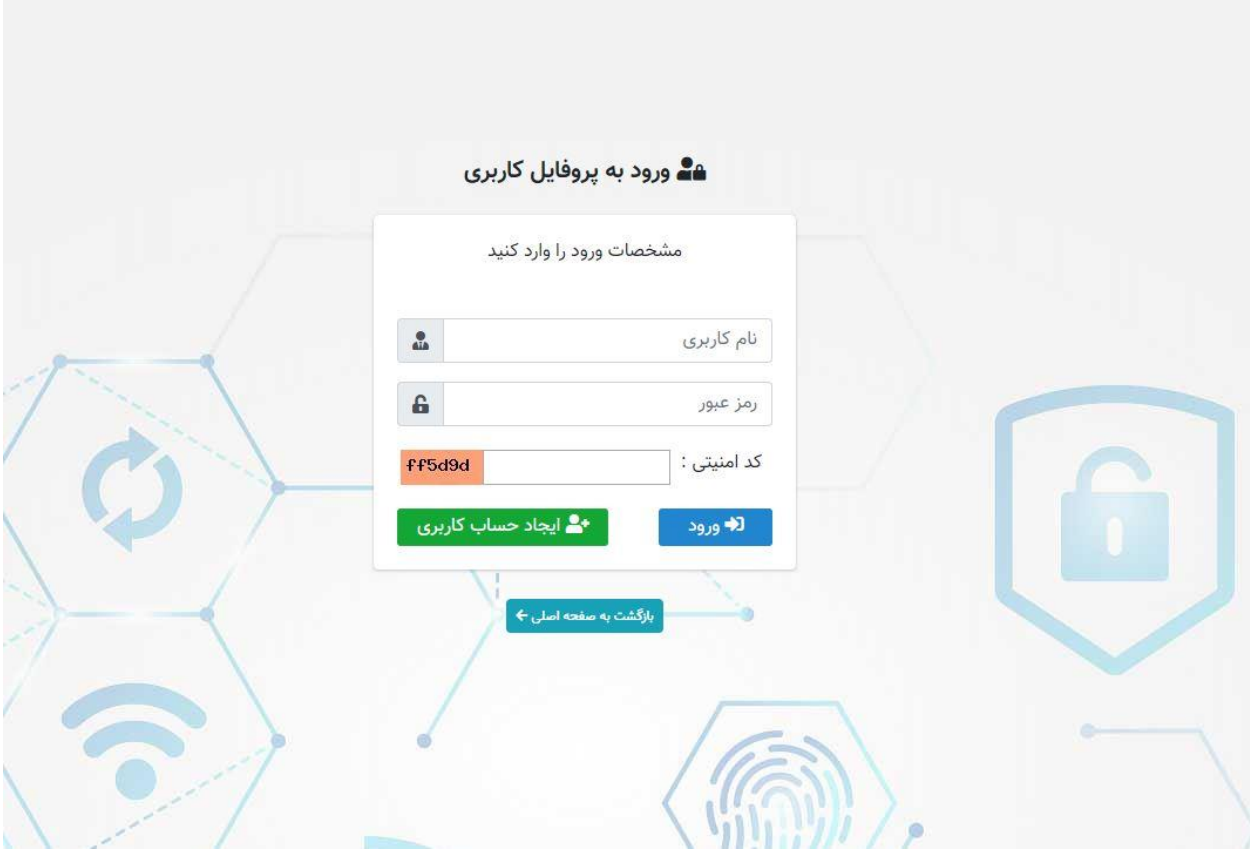
۶- گزینه "وبسایت – پورتال" – هدایت کاربر به صفحه نگارش گزارش تست نفوذ و آسیب‌پذیری وب

۷- گزینه " اپلیکیشن موبایل" – در نسخه‌های بعدی تکمیل خواهد شد..

۸- گزینه " نرم افزار ویندوز" – در نسخه‌های بعدی تکمیل خواهد شد..

- **صفحه ورود کاربران**

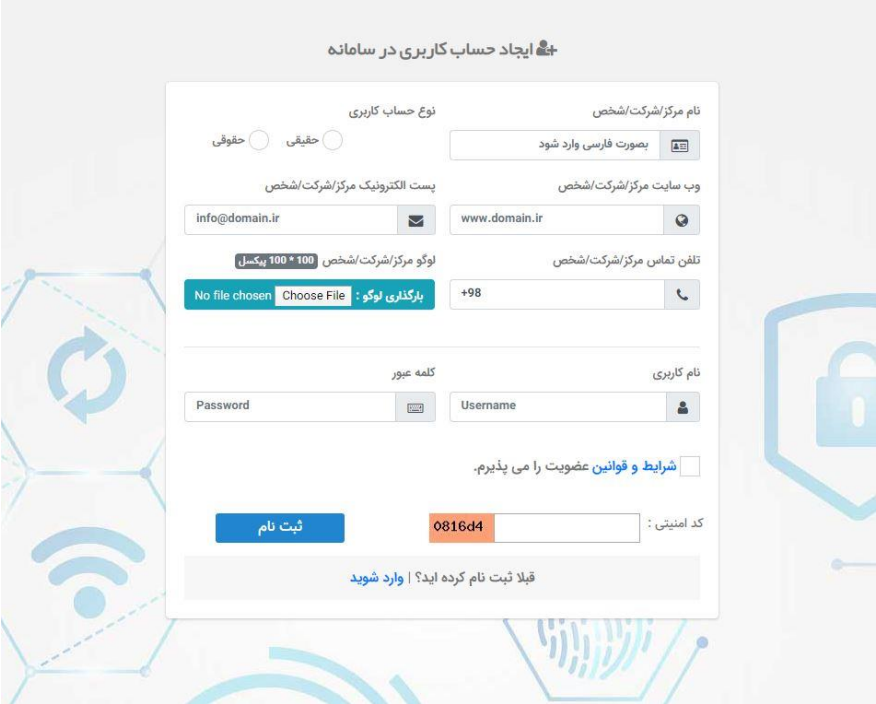
کاربر با کلیک بر روی این گزینه به صفحه ورود کاربران هدایت خواهد شد.



در این صفحه کاربر چنانچه قبلاً در سامانه ثبت‌نام کرده باشد با استفاده از نام کاربری و رمزعبور خود می‌تواند 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**



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

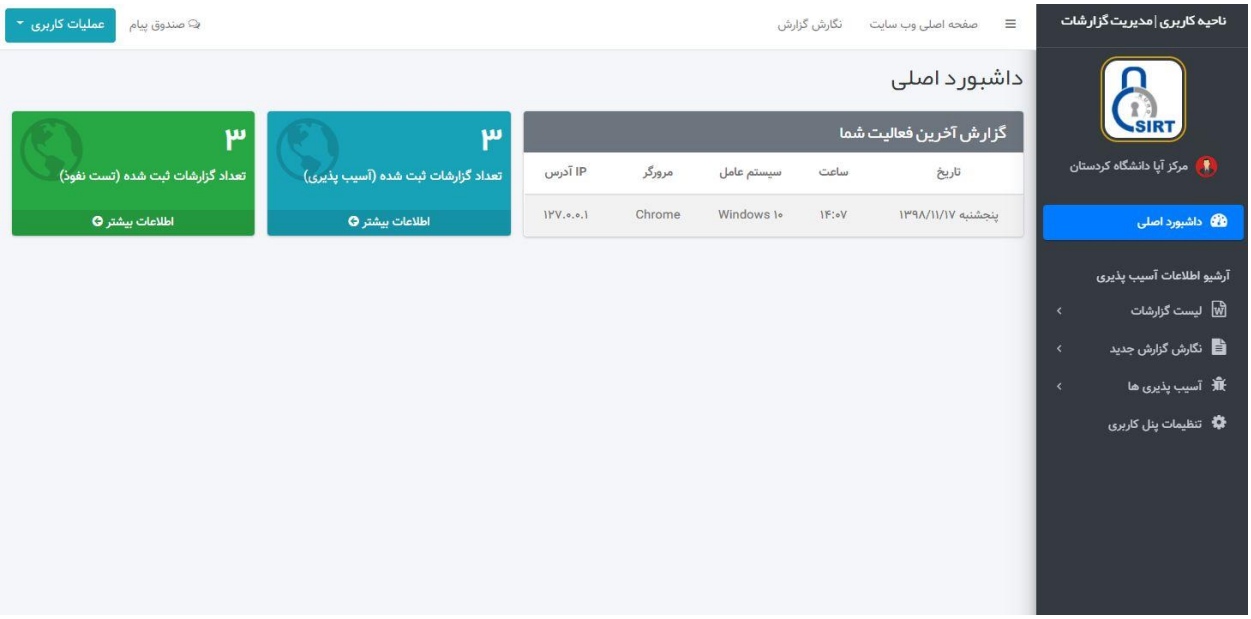
۶. لوگو مرکز/شرکت/شخص

۷. نام کاربری

۸. کلمه عبور

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

- **صفحه اصلی** پروفایل کاربران



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 پیش‌فرض 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. آسیب‌پذیری وب‌سایت : هدایت کاربر به صفحه "لیست گزارشات آسیب‌پذیری 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 آسیب‌پذیری وب‌سایت : هدایت کاربر به صفحه "ایجاد گزارش آسیب‌پذیری وب‌سایت"

۵,۲. گزارش تست نفوذ وب‌سایت : هدایت کاربر به صفحه "ایجاد گزارش تست نفوذ وب‌سایت"

۶. منو "آسیب‌پذیری‌ها" – شامل دو زیرمنو:

۶,۱. لیست آسیب‌پذیری های من : هدایت کاربر به صفحه " لیست آسیب‌پذیری‌ها"

۶,۲. افزودن آسیب‌پذیری : هدایت کاربر به صفحه " افزودن آسیب‌پذیری 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 آسیب‌پذیری وب‌سایت" – نمایش تعداد گزارشات آسیب‌پذیری وب‌سایت ثبت شده توسط کاربر

۳. پنل "گزارشات تست نفوذ وب‌سایت" – نمایش تعداد گزارشات تست نفوذ وب‌سایت ثبت شده توسط کاربر

- **صفحه** پروفایل

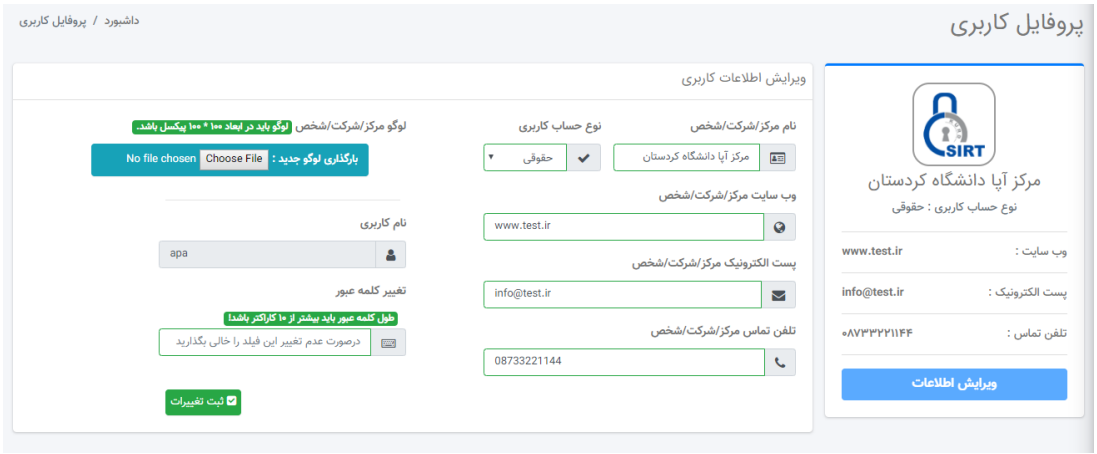
این صفحه شامل ۲ بخش است:

- پنل سمت راست : نمایش اطلاعات حساب کاربری

- پنل سمت چپ : تصویر پس‌زمینه پروفایل کاربر که بصورت پیشفرض توسط سامانه ست می‌شود، کاربر می‌تواند از قسمت تنظیمات پنل 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.**

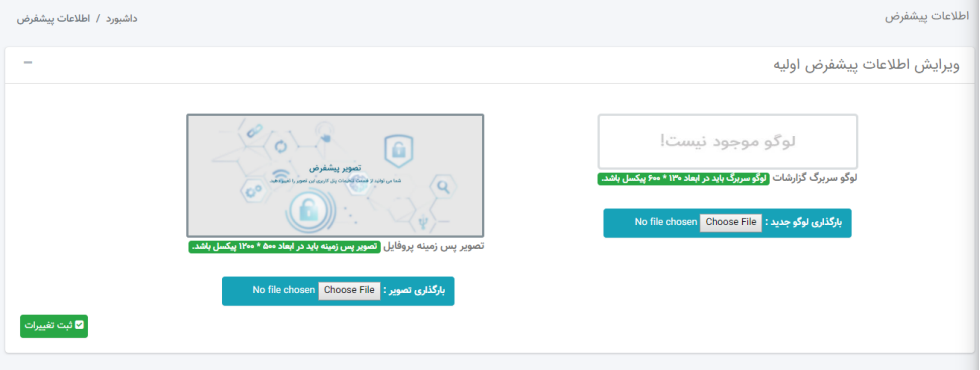
- **صفحه** ویرایش اطلاعات کاربری



در این صفحه کاربر می‌تواند 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 می‌تواند یک لوگو ثابت برای سربرگ گزارشات خود بارگذاری نماید.

همچنین از این بخش می‌تواند تصویر پس‌زمینه پیش‌فرض پروفایل خود را تغییر دهد.

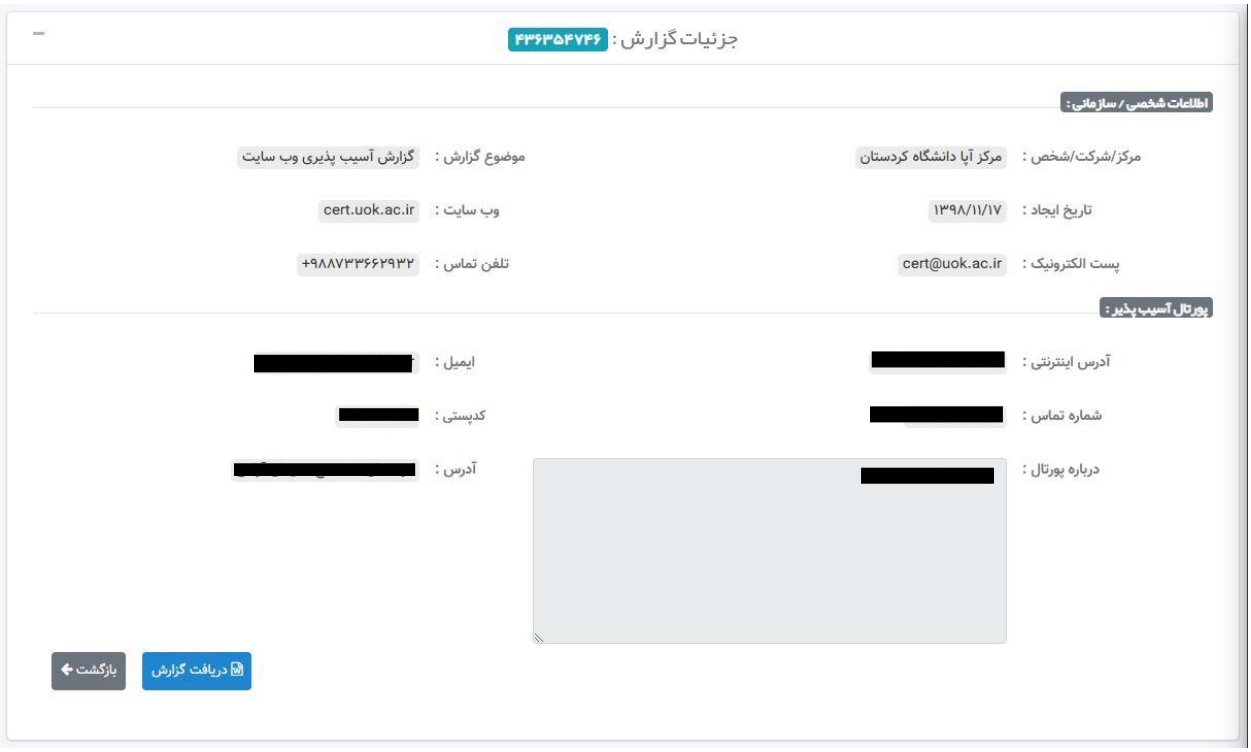
- **صفحه لیست گزارشات**

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

با انتخاب گزینه حذف کاربر می‌تواند گزارش را حذف نماید.

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

- **صفحه جزئیات گزارش**



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

در این صفحه همچنین کاربر می‌تواند با کلیک برروی گزینه دریافت گزارش **فایل گزارش خود را مجدداً دریافت نماید.**

نگارش گزارش آسیب‌پذیری:

- **صفحه انتخاب قالب گزارش**

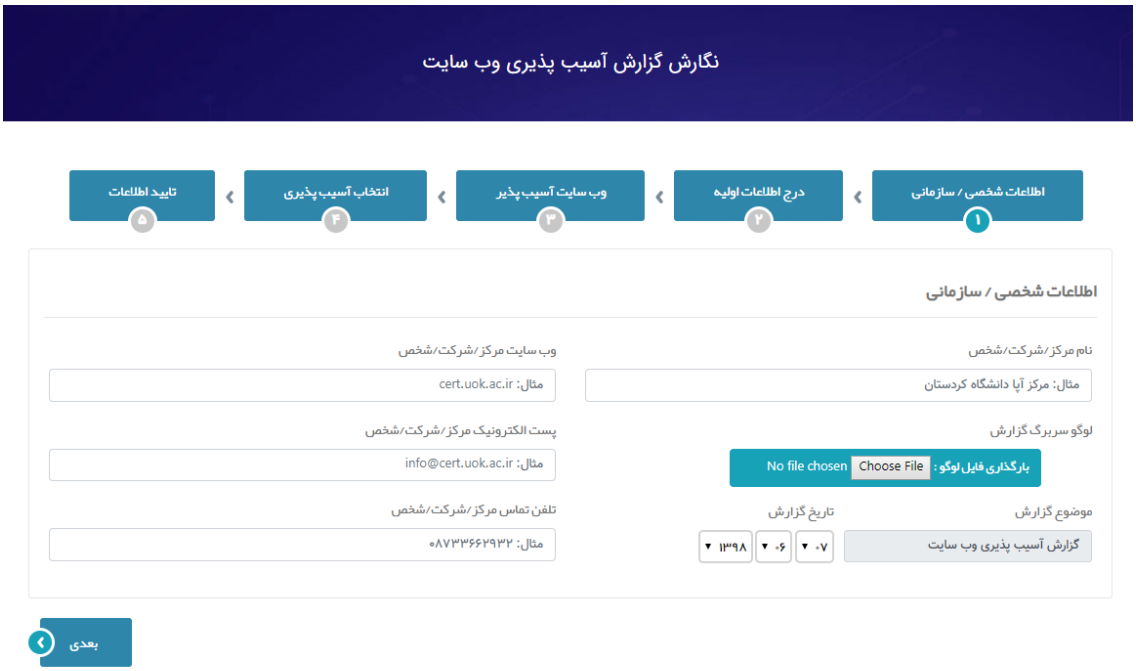
در این صفحه کاربر بر اساس نوع گزارش قالب موردنیاز خود را انتخاب می‌نماید:

- قالب گزارش آسیب‌پذیری

- قالب گزارش تست نفوذ

نگارش گزارش بصورت کاربر مهمان:

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



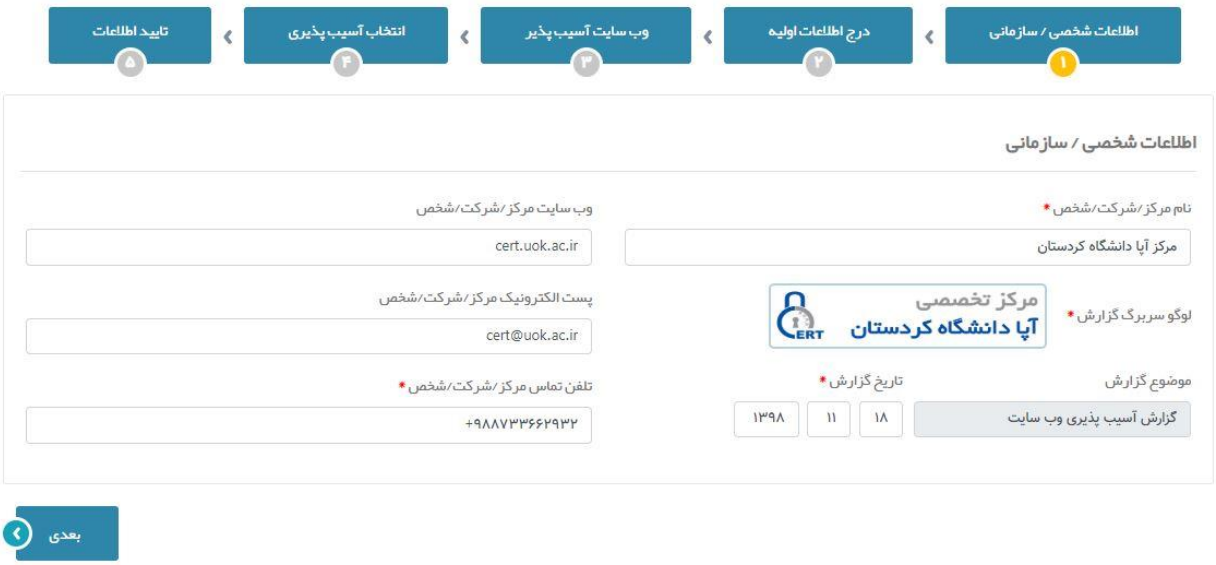
❋ درصورت عدم ورود به سامانه کاربر میبایست هربار این اطلاعات را مجدداً وارد نماید اما درصورت ایجاد حساب کاربری، این اطلاعات بصورت خودکار با استفاده از اطلاعات کاربری موجود تکمیل خواهد شد.

❋ همچنین لازم به ذکر است کاربرانی که بصورت مهمان اقدام به نگارش گزارش می‌کنند در آینده نمی‌توانند به اطلاعات و جزئیات گزارش از طریق این سامانه دسترسی داشته باشند.

صفحه نگارش گزارش آسیب‌پذیری

نگارش گزارش آسیب‌پذیری – مرحله اول : اطلاعات شخصی/سازمانی

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



در این مرحله اطلاعات مرکز، شرکت یا شخص تهیه‌کننده گزارش توسط کاربر وارد خواهد شد که شامل موارد زیر می‌باشد:

۱. نام مرکز/شرکت/شخص *

۲. لوگو سربرگ گزارش*

۳. تاریخ گزارش*

۴. وب‌سایت 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 آسیب‌پذیری – مرحله دوم : درج اطلاعات اولیه

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 آسیب‌پذیری - مرحله سوم : اطلاعات وب‌سایت آسیب‌پذیر

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

۱. آدرس اینترنتی وب‌سایت *

۲. پست الکترونیک وب‌سایت

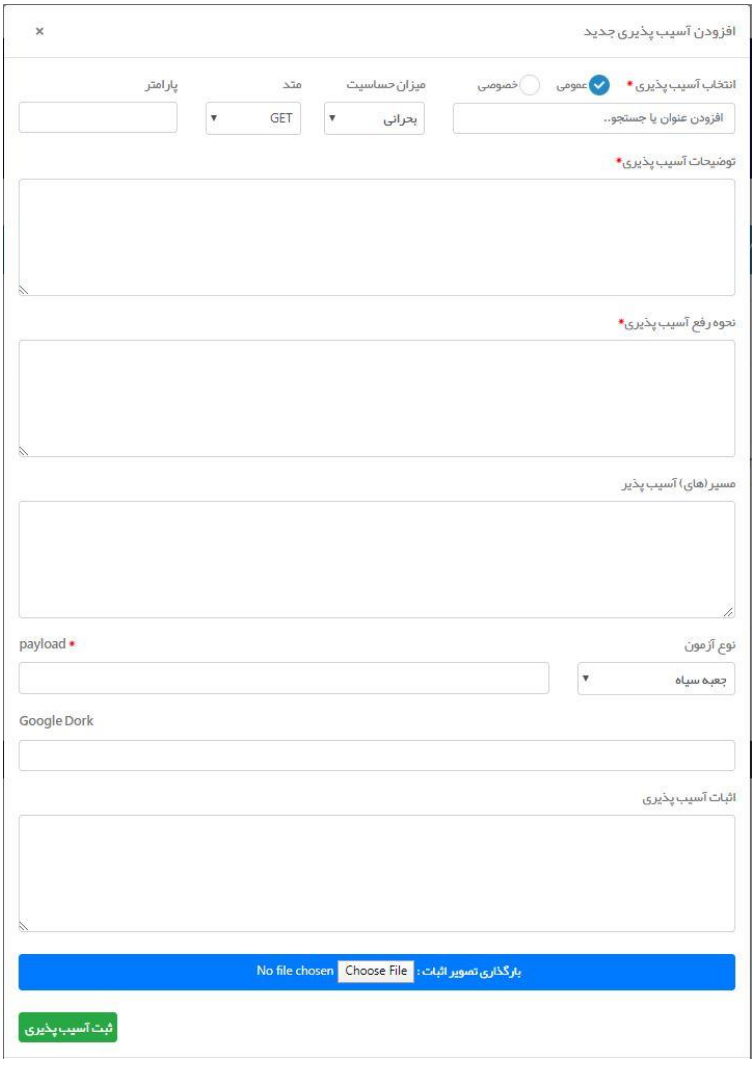
۳. شماره تماس مدیر وب‌سایت

۴. آدرس پستی مدیر وب‌سایت

۵. کدپستی مدیر وب‌سایت

نگارش گزارش آسیب‌پذیری – مرحله چهارم : انتخاب آسیب‌پذیری

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



صفحه انتخاب آسیب‌پذیری:

۱. انتخاب آسیب‌پذیری *

عمومی : انتخاب آسیب‌پذیری از لیست اصلی

خصوصی : انتخاب آسیب‌پذیری از لیست شخصی

۲. میزان حساسیت آسیب‌پذیری

۳. متد ۴. پارامتر

۵. توضیحات آسیب‌پذیری *

۶. توضیحات نحوه رفع آسیب‌پذیری *

۷. مسیرهای آسیب‌پذیر

۸. نوع آزمون

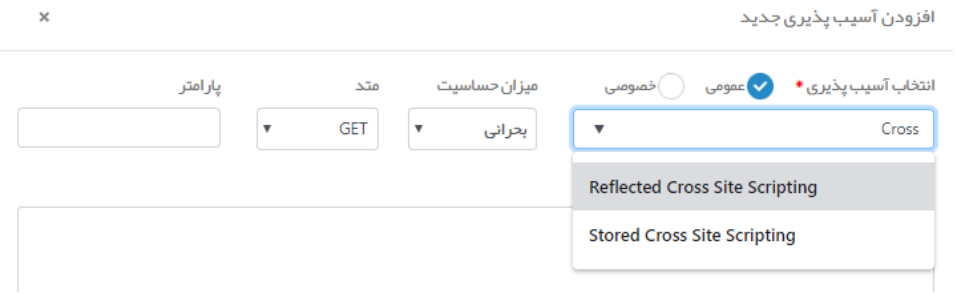
۹. payload * ۱۰. Google Dork

۱۱. اثبات آسیب‌پذیری

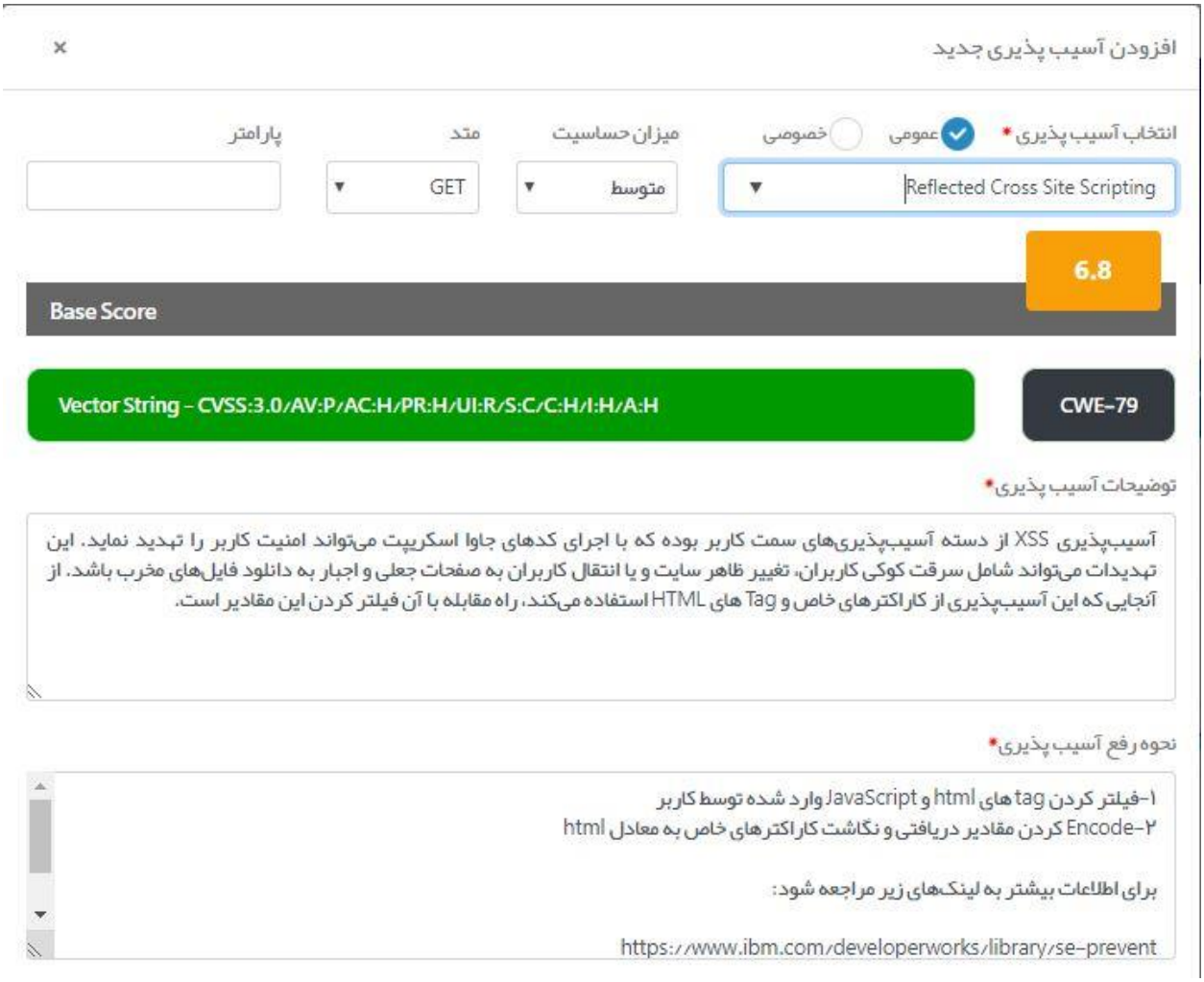
۱۲. تصویر اثبات آسیب‌پذیری

جستجو در بانک اطلاعاتی آسیب‌پذیری‌ها:

کاربر می‌تواند نام آسیب‌پذیری موردنظر خود را در کادر جستجو وارد نماید تا اطلاعات مربوط به آن آسیب‌پذیری بصورت خودکار تکمیل شود:



مثال:



بعد از انتخاب و ثبت آسیب‌پذیری‌های موردنظر، لیست موارد ثبت شده در جدولی مطابق شکل زیر به شما نشان داده خواهد شد که شامل ۳ گزینه مشاهده، ویرایش و حذف می‌باشد.

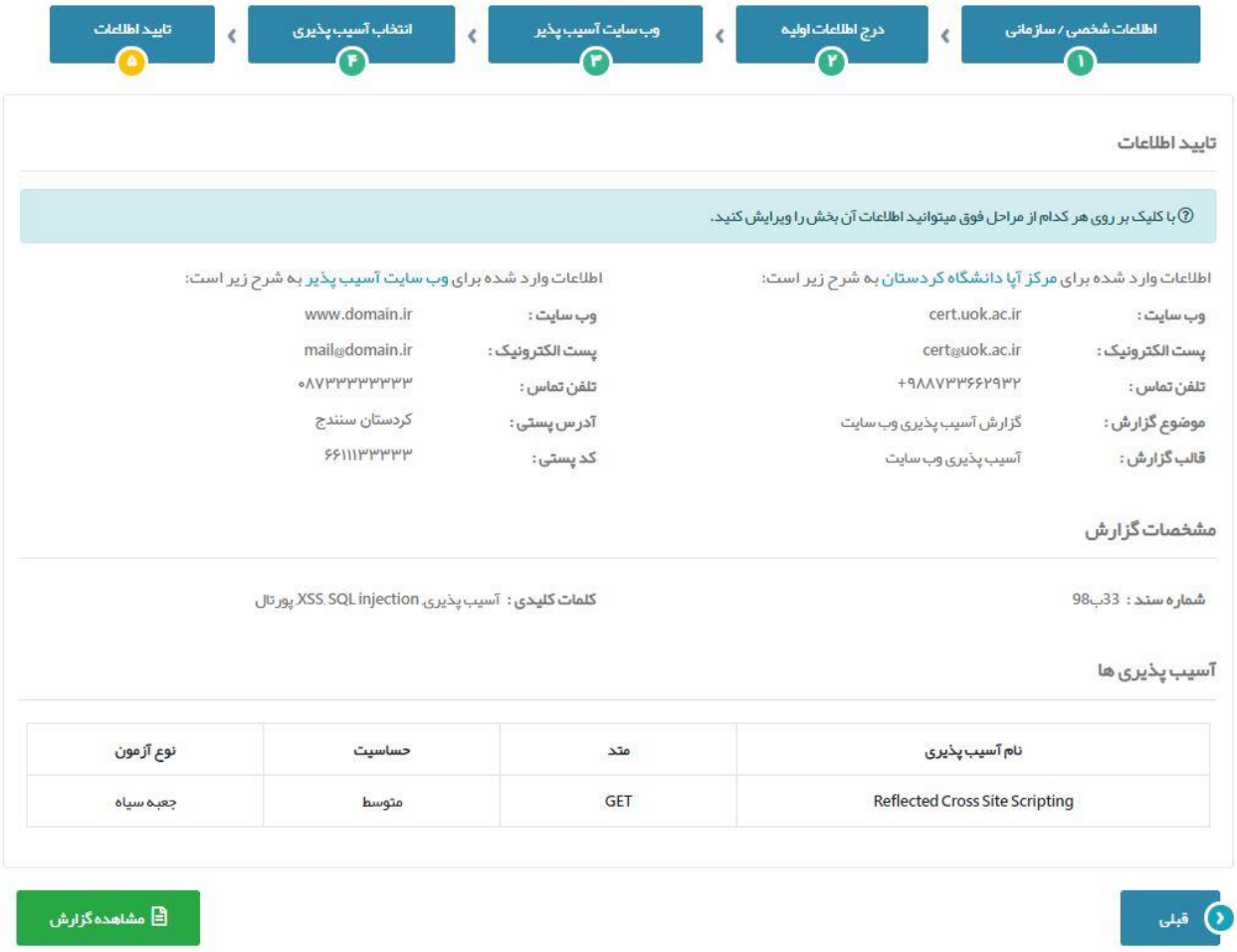
با کلیک برروی آیکن اطلاعات مربوط به آسیب‌پذیری مربوطه در صفحه جدید به شما نشان داده می‌شود.

درصورت نیاز به ویرایش اطلاعات آسیب‌پذیری با کلیک برروی آیکن یک صفحه جدید جهت ویرایش اطلاعات آسیب‌پذیری به شما نشان داده خواهد شد که در آنجا می‌توانید اطلاعات مربوط به آسیب‌پذیری را تغییر دهید.

درصورت نیاز به حذف یک آسیب‌پذیری از گزارش خود با کلیک برروی آیکن پیغام هشدار زیر به شما نشان داده خواهد شد:

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

نگارش گزارش آسیب‌پذیری – مرحله پنجم : کنترل و تایید اطلاعات



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

درنهایت با مشاهده این مرحله اطلاعات وارد شده را مجدداً بررسی کرده و درصورت 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 آسیب‌پذیری - مشاهده و دریافت گزارش

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

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

مرکز تخصصی
آپا دانشگاه کردستان

گزارش آسیب پذیری وب سایت

مرکز آپا دانشگاه کردستان

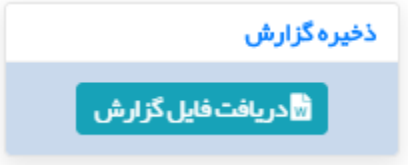
گزارش آسیب پذیری پورتال (نام پورتال)

www.domain.ir

تاریخ گزارش : ۱۳۹۸/۱۱/۱۸
شماره سند : ۹۸/ب/۳۳

cert.uok.ac.ir
cert@uok.ac.ir
+۹۸۸۷۳۳۶۶۲۹۳۲

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



برای اینکار کافیست برروی دکمه دریافت فایل گزارش **کلیک نمایید تا کمتر از چندثانیه فایل گزارش برروی رایانه شما بارگیری گردد.**

صفحه نگارش گزارش تست نفوذ

نگارش گزارش تست نفوذ – مرحله اول : اطلاعات شخصی/سازمانی

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

در این مرحله اطلاعات مرکز، شرکت یا شخص تهیه‌کننده گزارش توسط کاربر وارد خواهد شد که شامل موارد زیر می‌باشد:

۱. نام مرکز/شرکت/شخص *

۲. لوگو سربرگ گزارش*

۳. تاریخ گزارش*

۴. وب‌سایت 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 تست نفوذ – مرحله دوم : مفاد قرارداد

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

۱. متن مقدمه گزارش

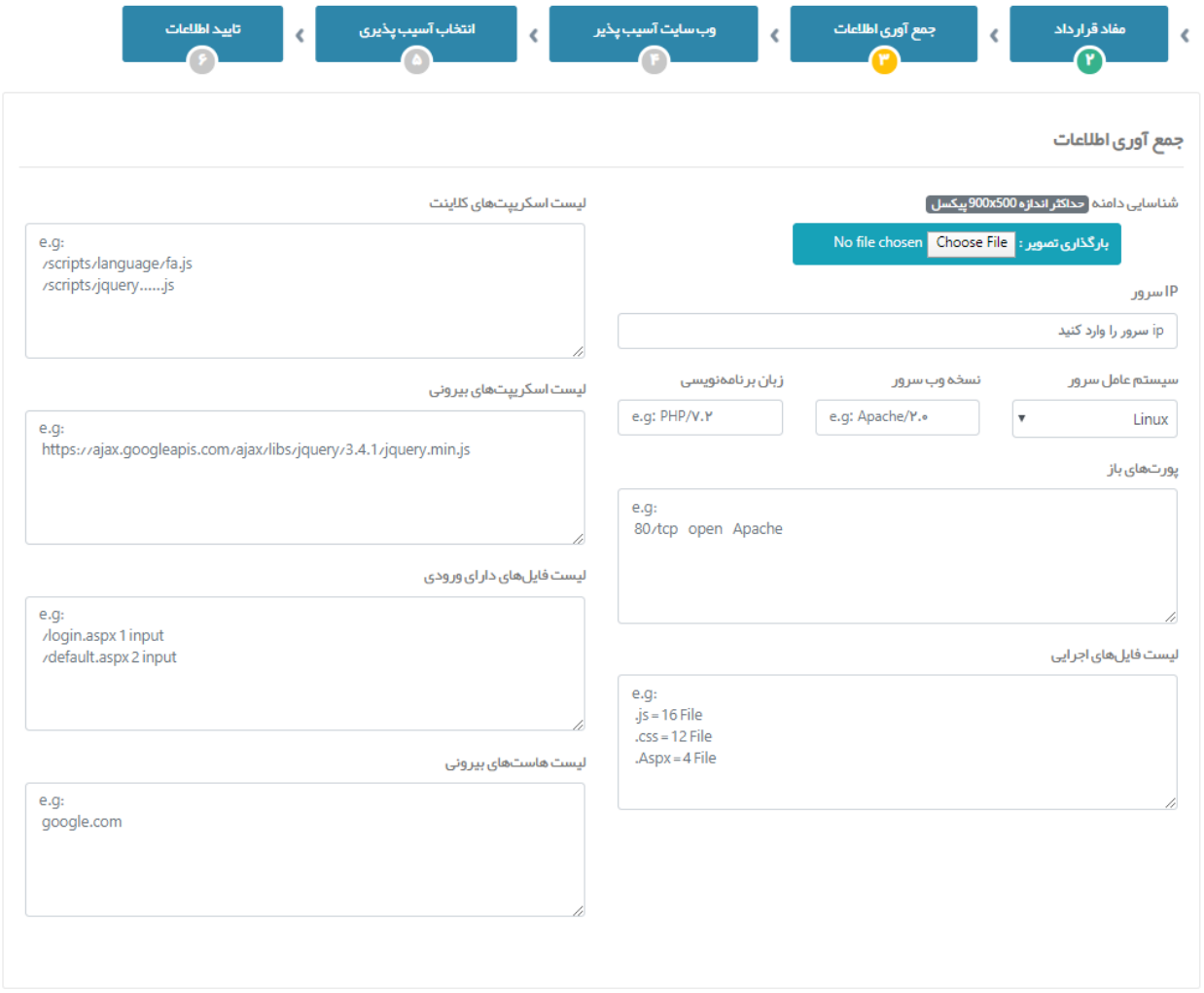
۲. دسترس ها و نوع آزمون نفوذپذیری

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



در این مرحله اطلاعات جمع آوری شده مربوط به وب‌سایت آسیب‌پذیر توسط کاربر وارد خواهد شد که شامل موارد زیر می‌باشد:

۱. تصویر شناسایی دامنه (اطلاعات whois)

۲. ip سرور (سرور وب‌سایت) **۳. سیستم‌عامل سرور**

۴. نسخه وب‌سرور **۵. زبان برنامه‌نویسی** **۶. پورت‌های باز**

۷. لیست فایل‌های اجرایی **۸. لیست اسکریپت‌های کلاینت** **۹. لیست اسکریپت‌های بیرونی**

۱۰. لیست فایل‌های دارای ورودی **۱۱. لیست هاست‌های بیرونی**

که میبایست طبق راهنمای فیلدها تکمیل گردد.

نگارش گزارش تست نفوذ – مرحله چهارم : اطلاعات وب‌سایت آسیب‌پذیر

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

۱. عنوان پورتال آسیب‌پذیر *

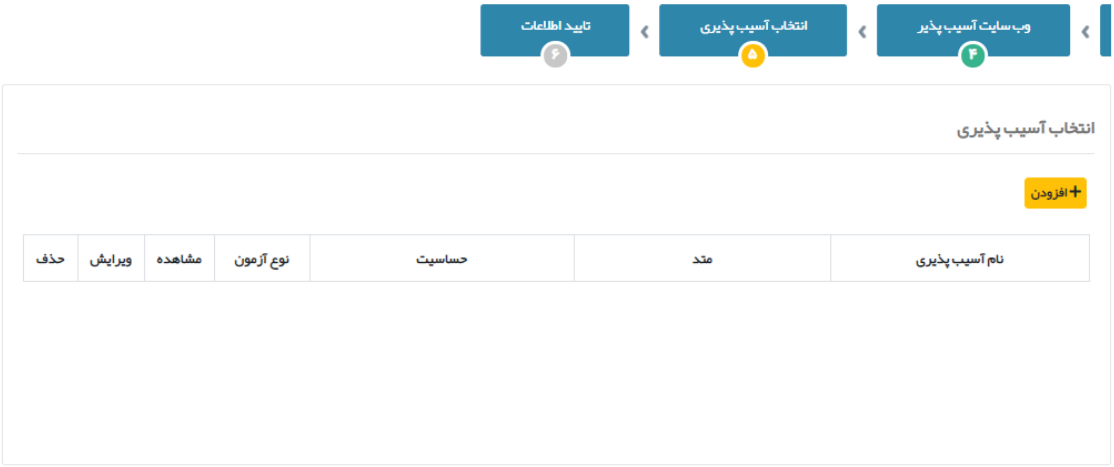
۲. آدرس اینترنتی وب‌سایت *

۳. پست الکترونیک وب‌سایت

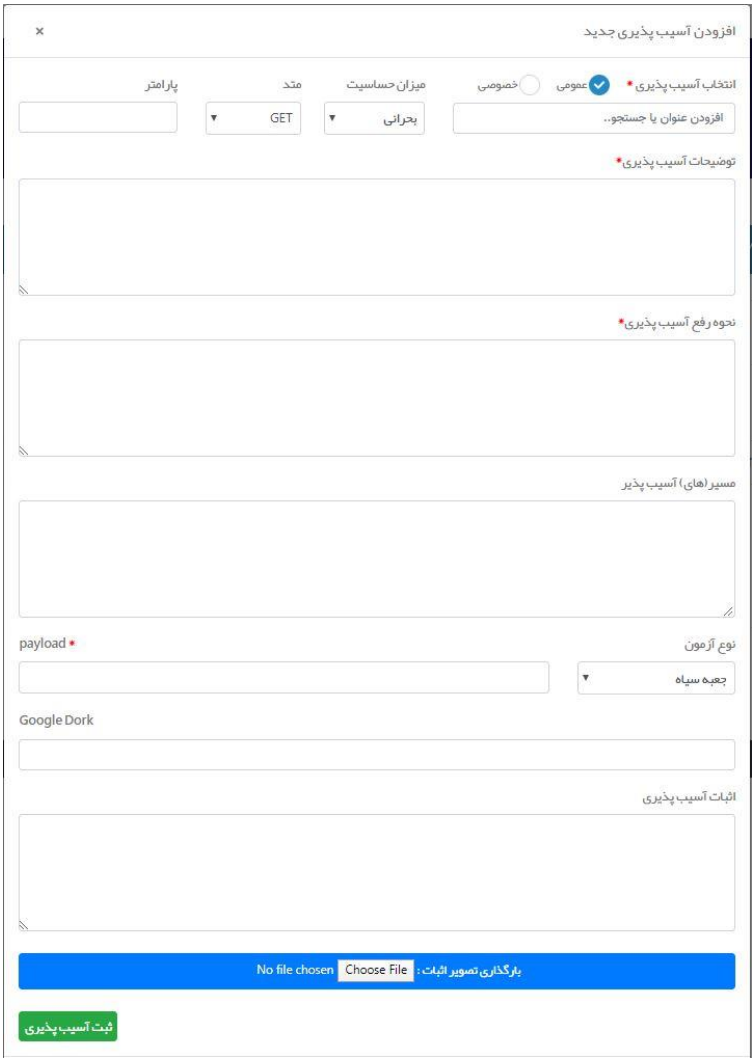
۴. شماره تماس مدیر وب‌سایت

۵. آدرس پستی مدیر وب‌سایت

۶. کدپستی مدیر وب‌سایت



در این مرحله اطلاعات مربوط به آسیب‌پذیری‌ها توسط کاربر وارد خواهد شد. کاربر با انتخاب گزینه +افزودن صفحه انتخاب آسیب‌پذیری به وی نشان داده خواهد شد.



صفحه انتخاب آسیب‌پذیری:

۱. انتخاب آسیب‌پذیری *

عمومی : انتخاب آسیب‌پذیری از لیست اصلی

خصوصی : انتخاب آسیب‌پذیری از لیست شخصی

۲. میزان حساسیت آسیب‌پذیری

۳. متد ۴. پارامتر

۵. توضیحات آسیب‌پذیری *

۶. توضیحات نحوه رفع آسیب‌پذیری *

۷. مسیرهای آسیب‌پذیر

۸. نوع آزمون

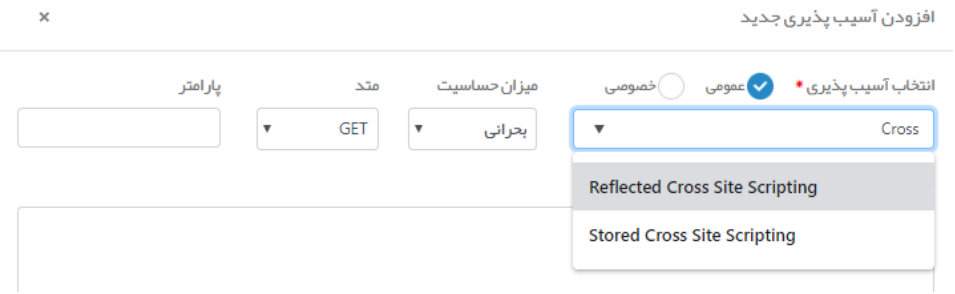
۹. payload * ۱۰. Google Dork

۱۱. اثبات آسیب‌پذیری

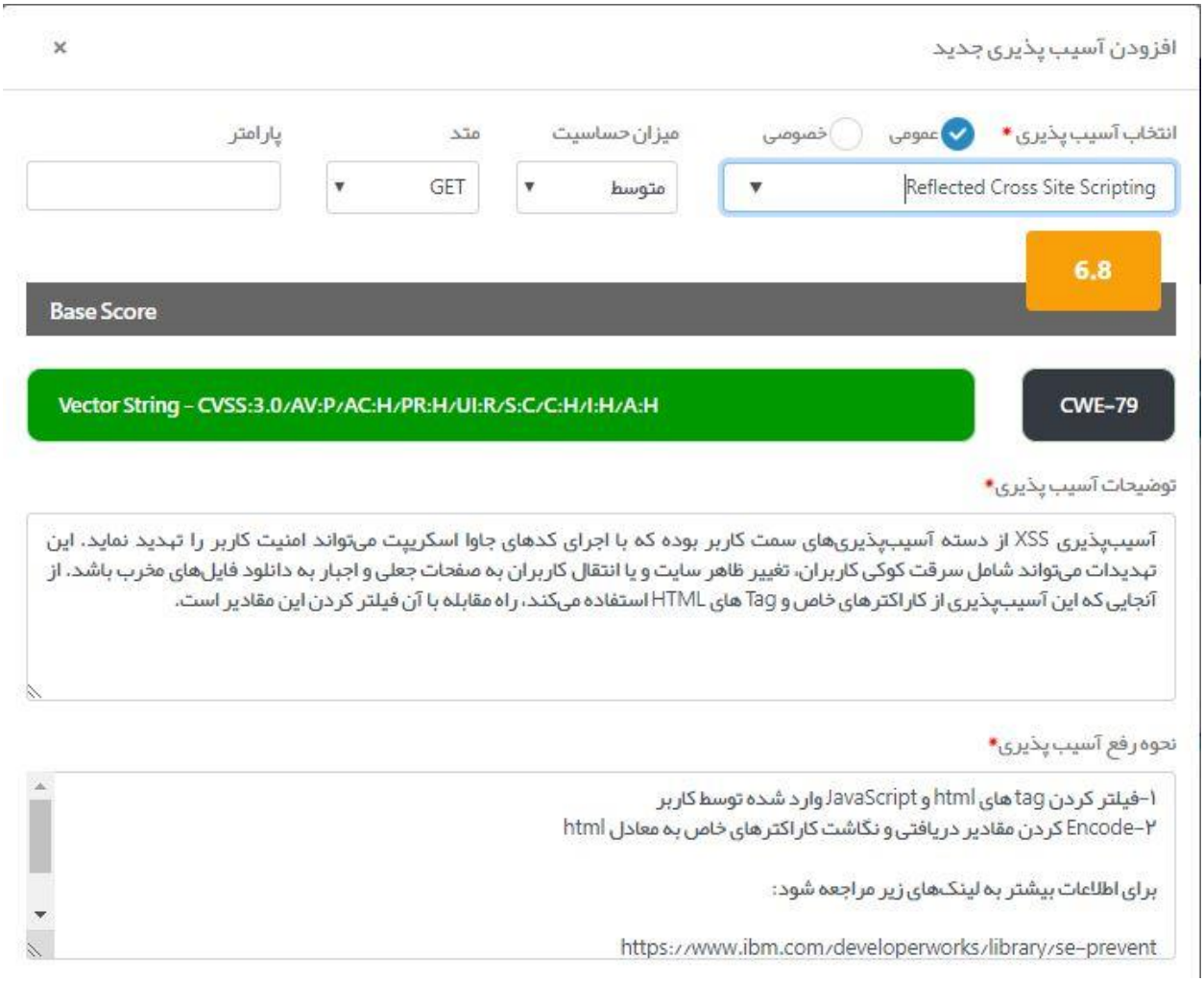
۱۲. تصویر اثبات آسیب‌پذیری

جستجو در بانک اطلاعاتی آسیب‌پذیری ها:

شما می‌توانید نام آسیب‌پذیری موردنظر خود را در کادر جستجو وارد نمایید تا اطلاعات مربوط به آن آسیب‌پذیری بصورت خودکار تکمیل شود:



مثال:



بعد از انتخاب و ثبت آسیب‌پذیری‌های موردنظر، لیست موارد ثبت شده در جدولی مطابق شکل زیر به شما نشان داده خواهد شد که شامل ۳ گزینه مشاهده، ویرایش و حذف می‌باشد.

با کلیک برروی آیکن اطلاعات مربوط به آسیب‌پذیری مربوطه در صفحه جدید به شما نشان داده می‌شود.

درصورت نیاز به ویرایش اطلاعات آسیب‌پذیری با کلیک برروی آیکن یک صفحه جدید جهت ویرایش اطلاعات آسیب‌پذیری به شما نشان داده خواهد شد که در آنجا می‌توانید اطلاعات مربوط به آسیب‌پذیری را تغییر دهید.

درصورت نیاز به حذف یک آسیب‌پذیری از گزارش خود با کلیک برروی آیکن پیغام هشدار زیر به شما نشان داده خواهد شد:

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

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

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

درنهایت با مشاهده این مرحله اطلاعات وارد شده را مجدداً بررسی کرده و درصورت تایید جهت ثبت و مشاهده گزارش گزینه مشاهده گزارش **را کلیک نمایید.**

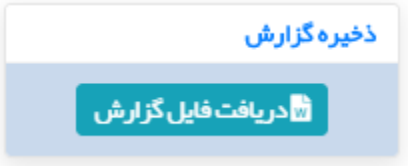
نکته: پس از ثبت گزارش نیز کماکان می‌توانید با بازگشت به زبانه فعلی اطلاعات را مجدداً ویرایش و ثبت نمایید.

نگارش گزارش تست نفوذ - مشاهده و دریافت گزارش

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

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

درنهایت با استفاده از کادر موجود در گوشه پایین سمت چپ صفحه، گزارش خودرا بصورت فایل WORD دریافت نمایید.



برای اینکار کافیست برروی دکمه دریافت فایل گزارش **کلیک نماید تا کمتر از چندثانیه فایل گزارش بر روی رایانه شما بارگیری گردد.**