گزارش اولیه دسترسی و اطلاعات جمع‌آوری شده

wise.edu.jo

آبان ماه 1403

نسخه 1.0

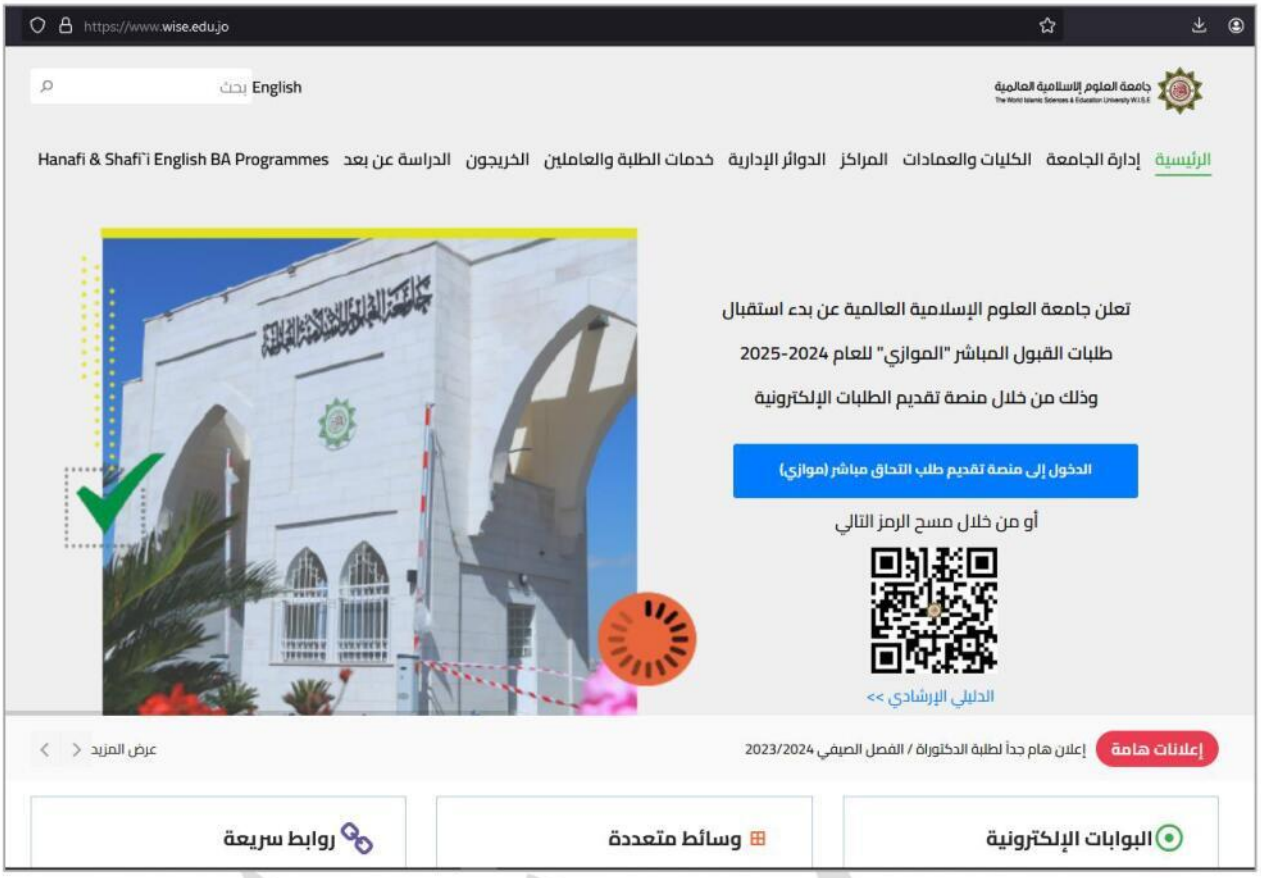
فهرست

مقدمه

گزارش زیر حاوی اطلاعات جمع‌آوری شده به همراه سناریوی حمله در ارتباط با تارگت wise.edu.jo می‌باشد. در روند کار بر روی این تارگت، یکی از زیردامنه‌هایی که از آن بدست آمد عبارت است از hr.wise.edu.jo . در این گزارش موضوع گرفتن دسترسی و اجرای کد از راه دور بر روی این زیردامنه بررسی شده است. در پایان نیز جهت تثبیت دسترسی خود به سرور، یک صفحه با قابلیت بارگذاری هر نوع فایل بر روی سرور، بر روی زیردامنه evaluation.wise.edu.jo ایجاد شد.

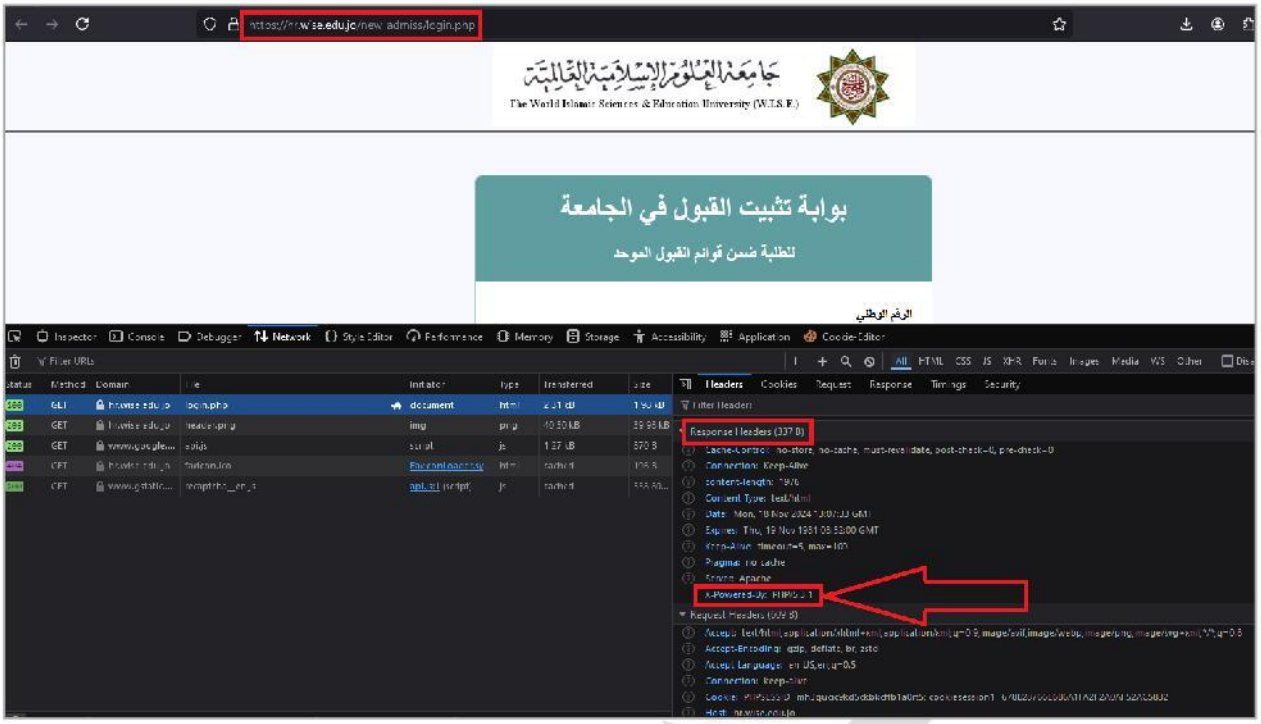
شناخت ماهیت هدف

دامنه wise.edu.jo مربوط به دانشگاه بین‌المللی علوم اسلامی (The World Islamic Sciences and Education University) در اردن می‌باشد. طبق آنچه در وب سایت این دانشگاه عنوان شده است، تعداد 11164 دانشجو، 19217 فارغ التحصیل و 13 دانشکده در این دانشگاه وجود دارد. در بخش علوم و فنون، از علوم مهندسی تا مباحث فقه، نام برده شده و در بخش علوم فقه، بر روی فقه شافعی، فقه حنفی و فقه مالکی متمرکز هستند.



شکل 1 : نمایی از صفحه اصلی وب سایت

طی بررسی‌های انجام شده یکی از زیردامنه‌های بدست آمده از این دامنه عبارت است از hr.wise.edu.jo . این زیردامنه مربوط به بخش پورتال پذیرش دانشگاه می‌باشد و دارای یک صفحه لاگین است. در طراحی وب سایتی که بر روی این زیردامنه قرار دارد از زبان برنامه نویسی Php نسخه 5.3.1 استفاده شده است.



شکل 2 : استفاده از Php نسخه 5.3.1 در وب سایت

این نسخه از زبان برنامه نویسی Php دارای آسیب‌پذیری RCE بوده و امکان اجرای کد از راه دور بر روی سسیتم عامل را به مهاجم می‌دهد. در این مرحله با استفاده از CVE-2012-1823 اقدام به تست و اسکپلویت آسیب‌پذیری گردید. همانطور که در تصویر زیر مشاهده می‌شود، امکان اجرای کد از راه دور وجود دارد.

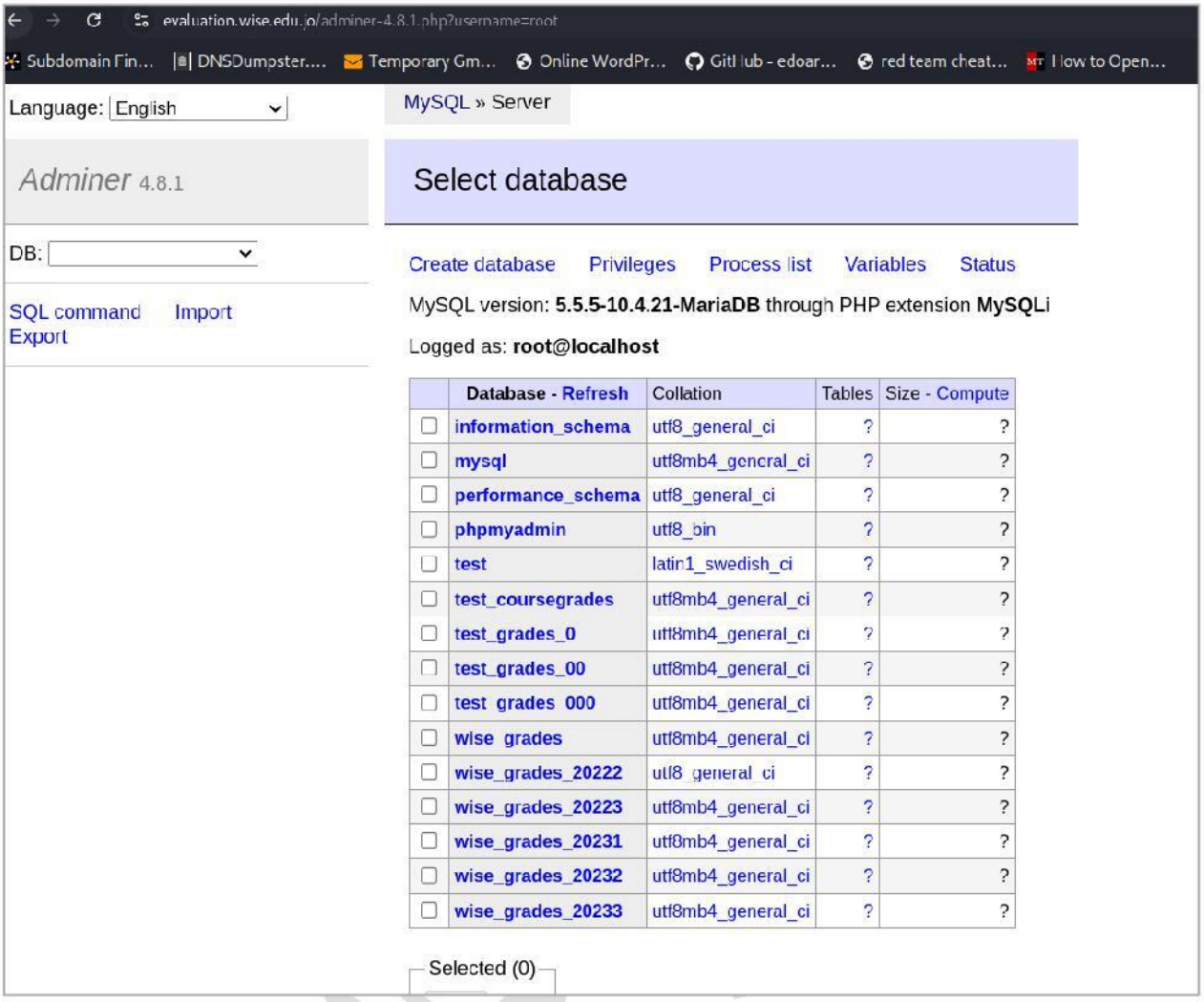
```
┌──(user13㉿kali)-[~/Desktop/Tools/moodle/cve]
└─$ ./php_cgi.sh https://hr.wise.edu.jo/ "whoami"

win-a825sbma0e2\administrator
```

شکل 3 : اجرای دستور whoami و دریافت پاسخ از سرور

در مرحله بعد با استفاده از این آسیب‌پذیری، اقدام به شناخته اولیه سیستم عامل و وضعیت تارگت از نظر تنظیمات شبکه، وضعیت سخت‌افزاری، فرآیندهای در حال اجرا، نوع و سطح دسترسی و غیره گردید. این اطلاعات در قالب یک فایل Text در مستندات قرار داده شده است.

در فاز جمع‌آوری اطلاعات از سیستم تارگت، نام کاربری و رمزعبور مربوط به دیتابیس کشف شد. با نصب ابزار Adminer و تست نام کاربری و رمزعبور مذکور، اتصال به دیتابیس برقرار شده و امکان دسترسی به حدوداً 4 GB داده فراهم شد.



شکل 4 : دسترسی به اطلاعات دیتابیس با ابزار Adminer

تثبیت دسترسی

یکی دیگر از زیردامنه‌های دامنه اصلی wise.edu.jo عبارت است از evaluation.wise.edu.jo . در این مسیر یک صفحه با قابلیت بارگذاری فایل قرار داده شده است که از طریق آدرس زیر در دسترس می‌باشد :

https://evaluation.wise.edu.jo/src.php

با استفاده از این صفحه می‌توان فایل‌های دلخواه خود را بر روی سرور قرار داد. جهت تثبیت دسترسی بر روی تارگت wise.edu.jo از این رویکرد استفاده شده است.

نتیجه‌گیری

وب سایت hr.wise.edu.jo یکی از زیردامنه‌های دامنه اصلی wise.edu.jo می‌باشد که مربوط به پورتال پذیرش دانشجویان دانشگاه بین‌المللی علوم اسلامی در اردن می‌باشد. این وب سایت از آن جهت حائز اهمیت است که حاوی اطلاعاتی همچون لیست دانشجویان داخلی و خارجی که در این دانشگاه در حال تحصیل هستند، می‌باشد. در حال حاضر به واسطه آسیب‌پذیری وجود در نسخه Php مورد استفاده در hr.wise.edu.jo ، دارای دسترسی برای اجرای کد از راه دور (RCE) هستیم. در قدم بعدی اقدام به تثبیت دسترسی بر روی آدرس https://evaluation.wise.edu.jo شد و در حال حاضر امکان بارگذاری هر نوع فایلی بر روی سرور وجود دارد. همچنین با بدست آوردن نام کاربری و رمزعبور مربوط به دیتابیس، دسترسی به 4 GB داده، اعم از نام کاربری، رمزعبور و اطلاعات کاربران فراهم شده است.

در مجموع از این شرایط می‌توان برای تخلیه اطلاعات سرور، جعل و دستکاری اطلاعات دیتابیس، تخریب و از بین بردن اطلاعات و یا نگه‌داری و رصد تارگت در طول زمان استفاده نمود.