



دانشگاه آزاد اسلامی

واحد شیروان

**گروه کامپیوتر**

عنوان :

**تست امنیت security testing))**

استاد :

جناب آقای دکتر اکبرپور

تهیه کننده :

میثم نجفی

دی ماه ۱۳۹۸

تست امنیت (Security testing)

منظور از تست امنیت، تست‌هایی هستند كه برای بررسی ورود به سیستم از راه‌های غیر معتبر، تغییر غیرمجاز سطوح دسترسی، افشای اطلاعات سیستم، تخریب سیستم یا كندسازی بیش از حدآن و سایر تهدیداتی كه امنیت سیستم را به مخاطره می‌اندازد صورت می‌گیرد.

اهم خدماتی كه در زمینه **تست امنیت** و تست نفوذ ارائه می‌گردد عبارتند از:

1. تحلیل ریسك‌های امنیت
2. برنامه‌ریزی تست امنیت و تست نفوذ
3. طراحی و اجرای تست امنیت :

* تكنیك‌های جمع آوری اطلاعات یك برنامه كاربردی( عمدتا وب سایت­ها)
* تست مدیریت پیكربندی (Configuration Management)
* تست منطق كاری (Business Logic)
* تست مدیریت نشست (Session Management)
* تست احراز هویت (Authentication)
* تست كنترل دسترسی (Authorization)
* تست‌های مربوط به اعتبارسنجی داده های وروردی Injections)،(Buffer overflow

1. تشریح عملی ابزارهای **تست امنیت** شامل ابزارهای:

Security Scanner، Web Application Scanner ، Exploit Framework

نقاط مهمی که توسط تست امنیت پوشش داده می­شوند عبارتند از :

* احراز هویت
* مجوز
* دسترسی ها
* اطلاعات محرمانه
* عدم تسویه حساب

هدف اصلی از تست امنیت را می­توان در موارد زیر خلاصه کرد :

* کمک برای بهبود امنیت و عمر محصول
* شناسایی و رفع مشکلات امنیتی مختلف در طول توسعه اپلیکیشن
* ارزیابی ثبات اپلیکیشن

# مدیریت تست

این راهكار مطابق استانداردهای IEEE و متدولوژی STEP می­باشد.

متدولوژی STEP كه حروف اختصاری Systematic Test & Evaluation Process است، یك متدولوژی برای تست سیستماتیك و مبتنی بر استانداردهای IEEE می­باشد.

فازهای مختلف فرآیند تست عبارتند از:

1. **تحلیل ریسک (Risk Analysis):**

ریسك به دو دسته ریسك محصول و ریسك برنامه ریزی تقسیم می­گردد. منظور از ریسك محصول، ریسك­هایی هستند كه قابلیت­های محصول را به مخاطره می­اندازند. این مخاطره می­تواند به دلیل پیچیدگی تولید آن قابلیت یا اهمیت ویژه آن برای كاربر نهایی باشد. منظور از ریسك برنامه ریزی تست، ریسك­هایی هستند كه بروز آنها باعث به تاخیر افتادن برنامه­ریزی می­گردد.

1. **برنامه­ریزی تست (Test Planning):**

در این فاز تصمیم­گیری­های كلیدی روی فرآیند تست محصول صورت می­گیرد كه اهم آنها عبارتند از:

* تعیین قابلیت­هایی كه باید تحت تست قرار گیرد (از روی مستند ریسك­های محصول)
* تعیین استراتژی تست شامل متدولوژی تست، تعیین تكنیك­های بازنگری كه مكمل تست می باشد، تعیین قابلیت­هایی از سیستم كه لازم است اجرای تست آنها خودكارسازی شود، مدیریت تغییرات و پیكربندی سیستم در زمینه تست، تعیین متریك­های لازم برای سنجش كیفیت محصول، اثربخشی تست و موارد دیگر.
* تعیین سازمان تست(نقش­ها و شرح وظایف تست)
* زمانبندی تست

1. **تحلیل و طراحی تست (Test Analysis & Design)**:

در این فاز روال­های تست و موارد تست مطابق تكنیك­های طراحی تست تعیین می­گردد. منظور از روال تست رویه­ای است كه برای اجرای تست باید دنبال گردد. منظور از موارد تست یك قابلیت، تعیین حالت­های مختلف جهت تست آن قابلیت می باشد كه با استفاده از تكنیك­های طراحی تست سعی در انتخاب كمترین حالت­هایی داریم كه بیشترین پوشش تست را داشته باشند. در هر مورد تست، ورودی­های مختلف معرف هر حالت و نتیجه مورد انتظار تعیین می گردد.

1. **پیاده سازی تست (Test Implementation)­:**

در این فاز محیط مورد نیاز برای اجرای تست راه اندازی می­گردد. به عبارت دیگر موارد زیر تعیین و راه­اندازی می­گردد :

* داده های مورد نیاز برای اجرای تست
* سخت افزار و تجهیزات شبكه مورد نیاز
* نرم افزار مورد تست
* سایر منابع مورد نیاز برای تست

1. **اجرای تست (Test Execution):**

در این فاز موارد تست طبق روال­های مربوطه مورد اجرا قرار می­گیرند. مستندات خروجی این فاز عبارتند از: گزارش خطاهای سیستم و گزارش چكیده تست كه نتیجه اجرای فرآیند تست روی یك محصول را نشان می­دهد.



ارزیابی امنیت و تست نفوذ (Penetration Test)

آزمون نفوذ عبارت است از کشف راه­‌ها و بررسی روش­‌های دسترسی غیر مجاز به منابع حساس و اطلاعات محرمانه­‌ی سازمان­ ها، در کوتاه‌ترین زمان ممکن. هدف از انجام آزمون­‌های نفوذ، پی بردن به نقاط ضعف موجود در سامانه‌ها و ارائه‌ی راهکارهای مناسب برای برطرف نمودن آن‌ها است.

در فرآیند آزمون نفوذ، تیم آزمون‌گر علاوه بر داشتن نگاه مستقل به هر آسیب‌پذیری، به  ترکیب آن‌ها برای شبیه‌سازی یک سناریوی واقعی نیز توجه دارد. این امر باعث به وجود آمدن شناخت دقیق‌تر از خسارات احتمالی می­‌شود، که ممکن است در اثر بروز رخدادهای رایانه­‌ای به سیستم‌های اطلاعاتی و شبکه‌ی سازمان تحمیل گردد.

 از لحاظ جایگاه تیم آزمون‌گر، آزمون­‌های نفوذ را می­‌توان به دو دسته‌ی زیر تقسیم نمود :

* آزمون نفوذ خارجی
* آزمون نفوذ داخلی

باتوجه به دسترسی‌های فراهم شده برای تیم آزمون نفوذ، انجام هر یک از روش‌های فوق می‌تواند به اشکال زیر صورت پذیرد :

* آزمون جعبه سیاه
* آزمون جعبه خاکستری
* آزمون جعبه سفید

خدمات آزمون نفوذ امن پرداز با مشخصات ذیل ارائه می‌شود :

* آزمون نفوذپذیری برنامه‌های کاربردی تحت وب
* آزمون نفوذپذیری شبکه
* آزمون نفوذپذیری برنامه‌های رومیزی

امروزه با فراگیر شدن استفاده از خدمات اینترنتی (بانک‌داری، خرید، فروش و ...) نیاز به حفاظت از اطلاعات حساس و محرمانه‌ی کاربران این خدمات اهمیت ویژه‌ای یافته است. کوچک‌ترین آسیب‌پذیری در سیستم‌های پرداخت آنلاین می‌تواند خسارت‌های سنگین و گاه جبران‌ناپذیر مالی و اعتباری را متحمل سازمان‌های ارائه دهنده‌ی این خدمات نماید. همان طور که در استانداردهای امنیتی نظیر ISMS بیان می‌شود، تست‌های دوره‌ای آزمون نفوذپذیری برنامه‌های کاربردی تحت وب، راه حلی مناسب برای رفع این مشکل است. واحد امنیت شرکت امن پرداز با توجه به توانایی و مهارت نیروهای خود، این نوع از آزمون نفوذ را برای ارتقاء امنیت مشتریان خود در برنامه‌های کاربردی تحت وب مبتنی بر تکنولوژی‌های ذیل ارائه می‌نماید:

 زبان‌های برنامه‌نویسی :

* Java
* ASP.Net
* PHP
* ASP

بانک‌های اطلاعاتی :

* MSSQL
* MySQL
* Oracle

امنیت شبکه­‌های داخلی از دو منظر حائز اهمیت است :

* احتمال وجود تهدیدات داخلی نظیر کارمندان ناراضی و یا مهاجمینی که به هر طریق دسترسی فیزیکی به شبکه سازمان راه پیدا کرده­‌اند.
* احتمال وجود تهدیدات خارجی توسط نفوذگران خارج از سازمان که به هر روشی توانسته باشند به شبکه­‌های داخلی نفوذ نمایند.

یکی دیگر از سرویس­‌های ارایه شده توسط شرکت امن پرداز، انجام آزمون نفوذپذيري شبکه‌های LAN و Wireless می‌باشد.

استفاده از برنامه­‌های رومیزی در بانک‌‌ها، دستگاه‌های  ATM و شبکه­‌های داخلی سازمان­‌ها امری متداول است. اما آیا به راستی این برنامه­‌ها به درستی طراحی شده­‌اند؟ آیا از هر نوع آسیبی در امان هستند؟

بررسی این برنامه­‌ها برای اطمینان از عدم وجود آسیب‌پذیری­‌هایی همچون :

* + - * Buffer Overflow
      * Memory Corruption
      * Denial Of Service
      * And …

مورد نیاز است، به صورتی که حتی شرکت­‌های بزرگ دنیا نظیر مایکروسافت،  Adobe و ... نیز اینگونه تست­‌های امنیتی را برای برنامه­‌های خود پیاده­‌سازی می­‌نمایند.

از نمونه فعالیت‌های شرکت امن پرداز در این حوزه می‌توان به کشف چندین آسیب‌پذیری بر روی مرورگر معروف Mozilla Firefox و برنامه‌های Microsoft Office Groove  و Adobe LiveCycle   ES اشاره نمود.

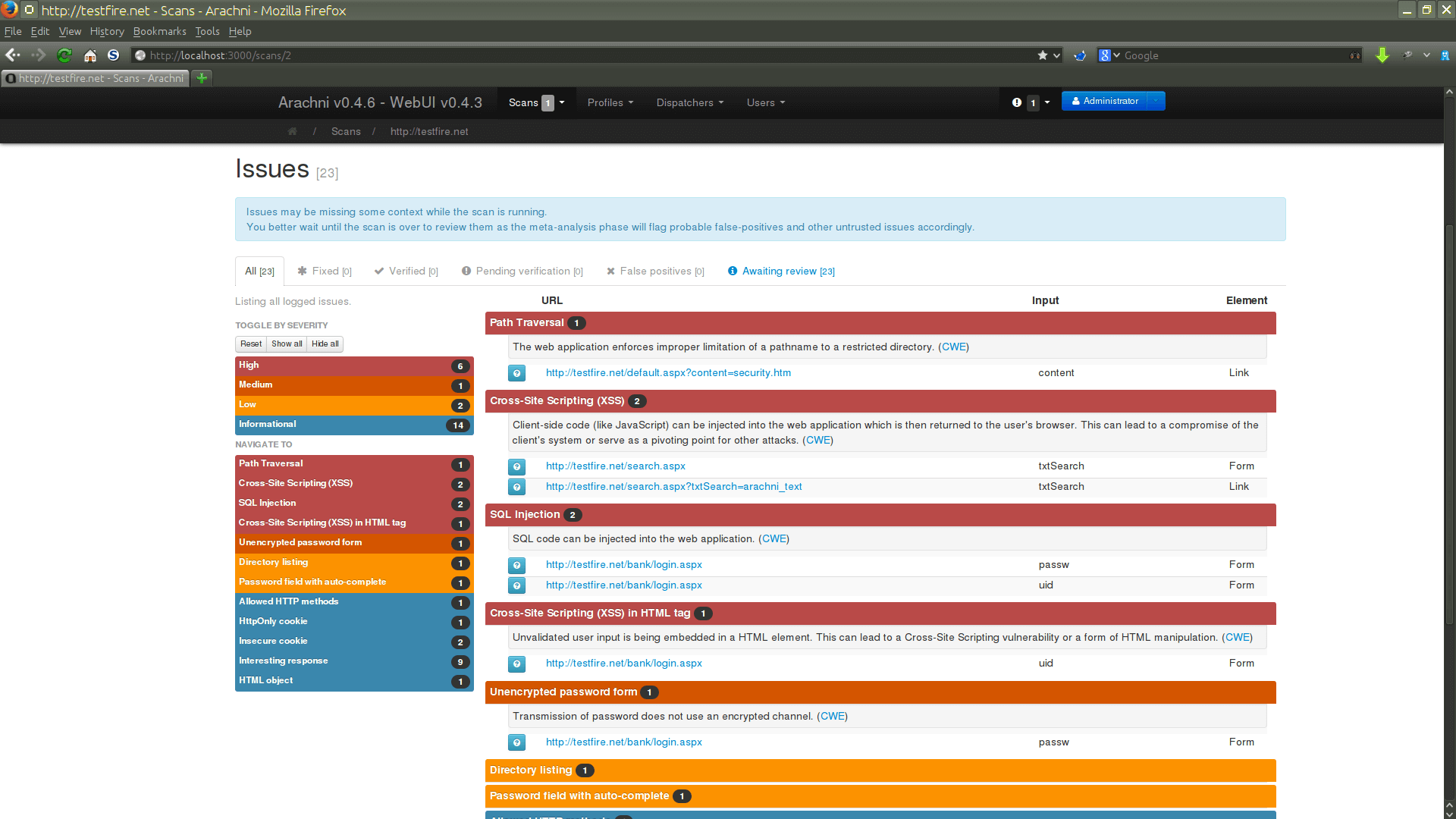
# ۱۰ ابزار برتر تست امنیت رایگان و متن باز

## **ابزار Arachni**

با استفاده از این ابزار قادر هستید که تعدادی از آسیب­پذیری­ها از جمله ورود نامعتبر، درج فایل­های محلی از راه دور، SQL injection و XSS injection را شناسایی کند.

**مزایا :**

استفاده راحت سریع، ماژولار است و عملکرد بالایی دارد، از پلتفرم­های مختلف پشتیبانی می­کند.



## **ابزار Grabber**

ابزار Grabber یک ابزار است که می­توانید به صورت پرتابل از آن استفاده کنید، این ابزار برای تست امنیت در انجمن­ها و وب سایت­های شخصی طراحی شده است و دارای رابط گرافیکی نیست. این ابزار قدرتمند به زبان برنامه­نویسی پایتون نوشته شده است و می­تواند آسیب­پذیری­هایی از جمله تایید فایل­های پشتیبان، File inclusion، تایید هویت AJAX و SQL injection را شناسایی کند.

**مزایا:**

تولید فایل­های تجزیه و تحلیل آماری، ساده و پرتابل، پشتیبانی از تجزیه و تحلیل [جاوا اسکریپت](https://7learn.com/course/js)

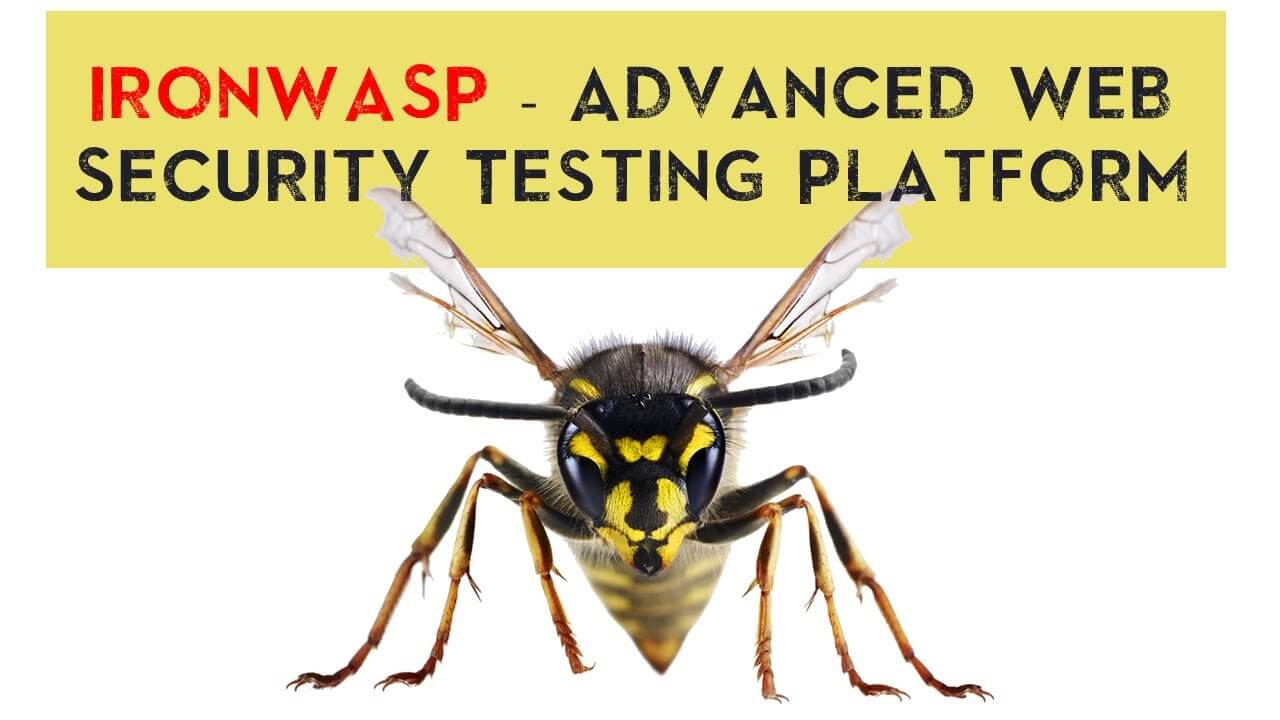
## **ابزار iron wasp**

یک ابزار متن باز و قدرتمند است که برای تست امنیت مورد استفاده قرار می­گیرد، این ابزار می­تواند تقریبا 25 نوع از آسیب­پذیری­های وب را شناسایی کند که از جمله آنها می­توان به موارد ذیل اشاره نمود :

Broken authentication ، Cross-site scripting ، CSRF، Hidden parameters،Privilege escalation

**مزایا :**

استفاده از ماژول­های قدرتمند، دارای رابط گرافیکی، ارائه گزارشات بر اساس html.



## **ابزار Nogotofail**

یک ابزار تست امنیت می­باشد که توسط شرکت گوگل طراحی شده است، این ابزار یک ابزار بسیار کم حجم است که قادر است آسیب­پذیری­های TLS و SSL را شناسایی کند. از جمله سایر آسیب­پذیری­هایی که این ابزار قادر به شناسایی آنها می­باشد می­توان به مواردی از قبیل :

MiTM attacks، SSL certificate verification issues، SSL injection، TLS injection.

**مزایا :**

استفاده راحت، کم حجم، پشتیبانی از vpn

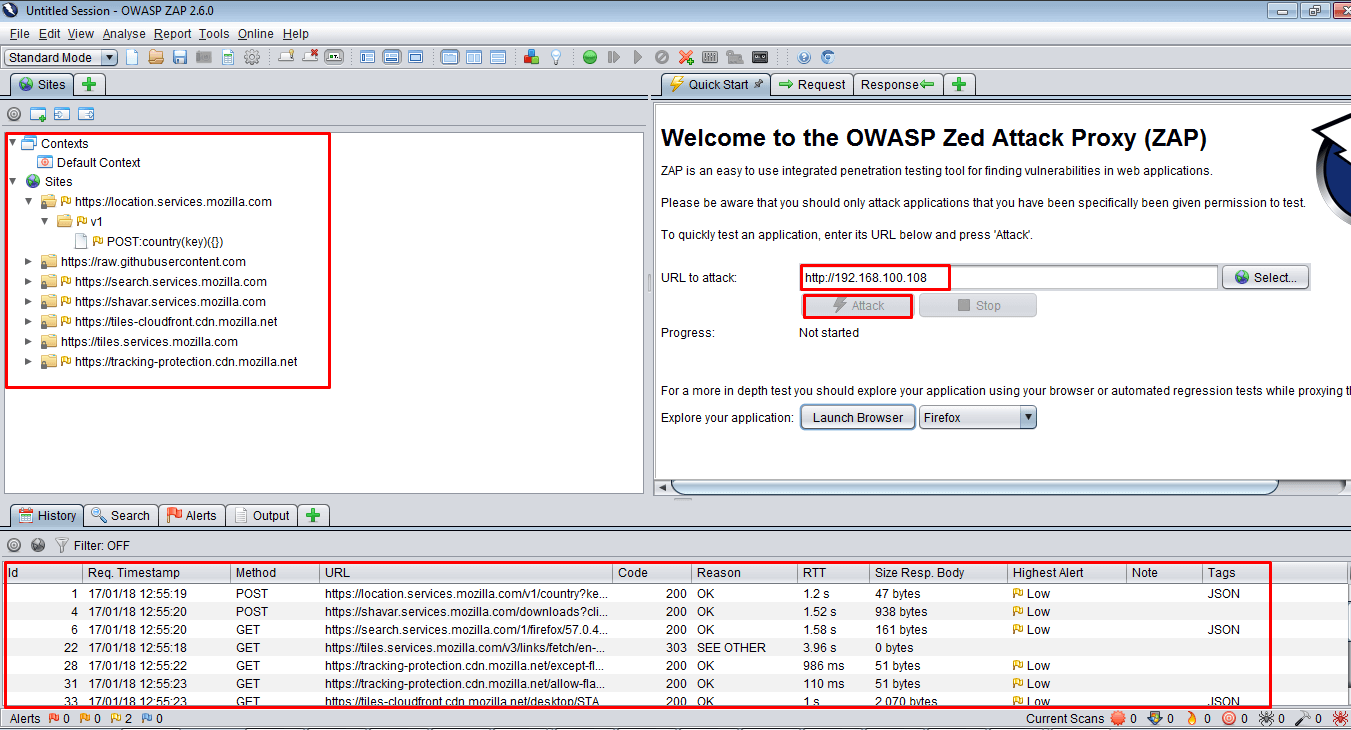
## 

## **ابزار SonarQube**

یکی دیگر از ابزارهای تست امنیت که یک ابزار متن باز است، این ابزار علاوه بر آشکارسازی آسیب­پذیری­ها برای اندازه­گیری کیفیت کد شما نیز مورد استفاده قرار می­گیرد. با این که این ابزار توسط زبان جاوا نوشته شده است ولی قادر است بیش از 20 زبان برنامه نویسی را مورد بررسی قرار دهد. از جمله آسیب­پذیری­هایی که این ابزار قادر به تشخیص آن­ها می­باشد می­توان به مواردی از قبیل Cross-site scripting، حملات DOS، SQL injection، Memory corruption اشاره کرد.

**مزایا :**

مسائل دشوار را شناسایی می کند، ادغام DevOps، استفاده کوتاه مدت و طولانی مدت، فراهم کردن تاریخچه یک پروژه و ..



## **ابزار : SQLMap**

با استفاده از این ابزار می­توانید به صورت خودکار آسیب­پذیری­های وب را تشخیص دهید، در این ابزار فرآیند تشخیص آسیب­پذیری­ها از طریق SQL صورت می­گیرد. این ابزار دارای یک موتور تست امنیت بسیار قدرتمند می­باشد که قادر است 6 نوع SQL Injection را شناسایی کند :

* + Boolean-based blind
  + Error-based
  + Out-of-band
  + Stacked queries
  + Time-based blind
  + UNIO query

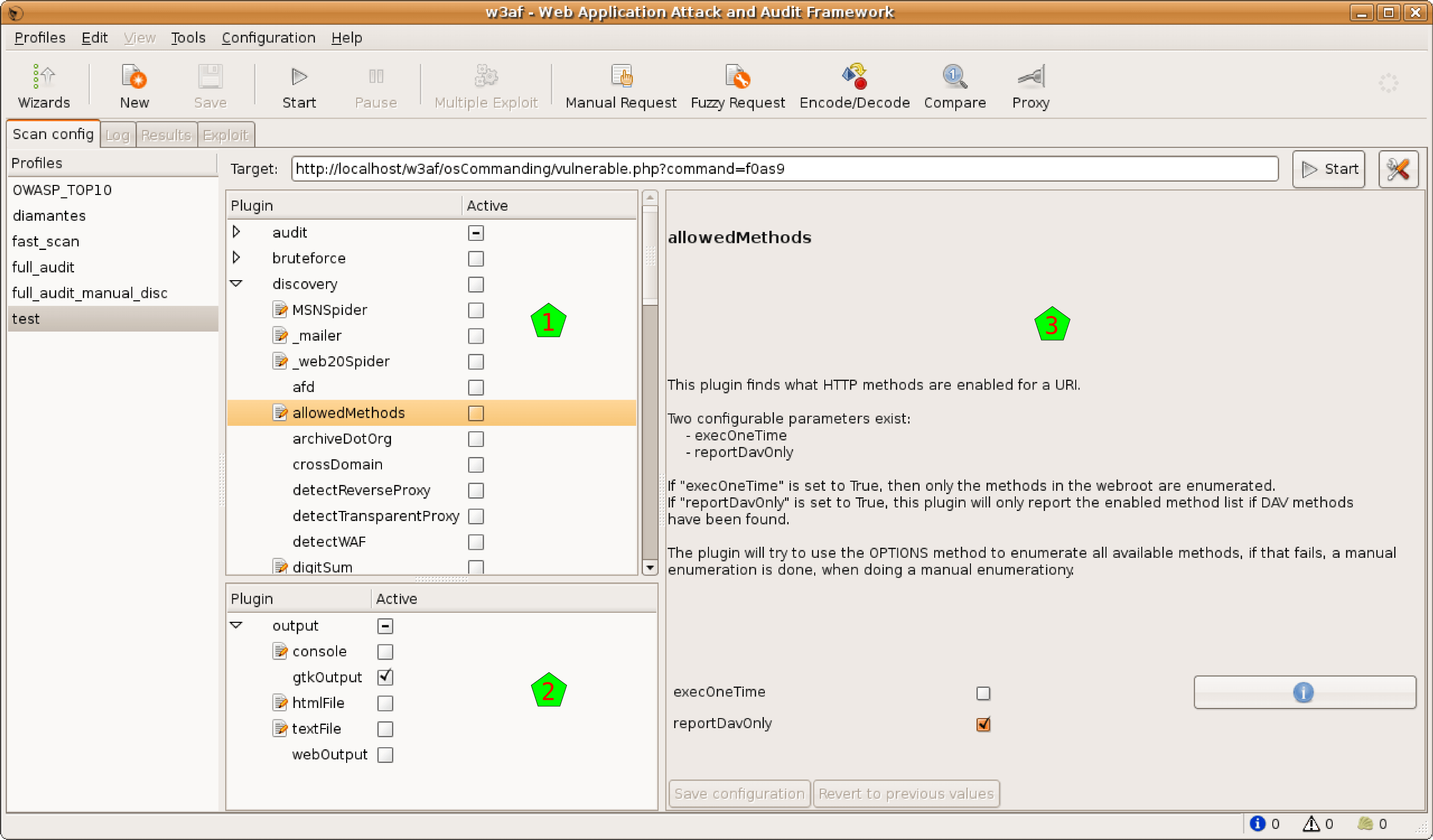
**مزایا :**

به صورت خودکار تست امنیت را انجام می­دهد، برای تست امنیت وب سایت نیز مورد استفاده قرار می­گیرد، دارای یک موتور تشخیص قوی است و ...

## **ابزار : W3af**

یکی از ابزارهای مشهور تست امنیت اپلیکیشن های تحت وب می­باشد که توسط زبان برنامه­نویسی پایتون طراحی و ساخته شده است، این ابزار به تست کننده­ها اجازه می­دهد که بیش از 200 نوع از آسیب­پذیری­ها را شناسایی کند که از جمله آنها می­توان به موارد ذیل اشاره نمود :

Blind SQL injection، Buffer overflow، Cross overflow ، CSRF



## **ابزار Wapiti:**

این ابزار یکی از بهترین ابزارهای تست امنیت در وب می­باشد که به صورت رایگان و متن باز در اختیار توسعه دهندگان قرار می­گیرد، از این ابزار برای بررسی آسیب­پذیری­های امنیتی در بسیاری از شرکت­های مهم استفاده می­شود، توجه داشته باشید که تست امنیت جعبه سیاه هواپیما نیز توسط همین ابزار صورت می گیرد.

## **ابزار Wfuzz:**

این ابزار تست امنیت وب توسط زبان برنامه­نویسی پایتون نوشته شده است و به شدت مورد علاقه توسعه دهندگان وب سایت­ها قرار دارد. این ابزار تست امنیت دارای رابط گرافیکی نمی­باشد و تنها از طریق خط فرمان می­توان از آن استفاده کرد.

## 

## **ابزار ZAP یا Zed Attack Proxy:**

یک ابزار تست امنیت است که از پلتفرم­های مختلف پشتیبانی می­کند و از آن می­توان برای انجام تست­های امنیت مربوط به اپلیکیشن­های وب استفاده کرد. این ابزار دارای یک رابط گرافیکی می­باشد که کمک بسیار زیادی به تست امنیت برای توسعه­دهندگان می­کند.

**منابع :**

* 1. <https://www.mohandespishegan.com/security-testing/>
  2. <https://www.mohandespishegan.com/test-managment/>
  3. <https://www.amnpardaz.com/contents.php/fa/>
  4. <https://7learn.com/tutorials/open-source-security-testing-tools>/