



## المقدمة:

أمن الشبكات هو ممارسة تنفيذ تدابير لحماية شبكات الكمبيوتر من الوصول غير المصرح به والهجمات الإلكترونية وخروقات البيانات. يلعب دوراً حاسماً في الحفاظ على سرية وسلامة وتوافر المعلومات التي يتم تبادلها وتخزينها داخل الشبكات. في عصر يتميز باتصال رقمي واسع النطاق ، يعد أمن الشبكات ذا أهمية قصوى لأنه يحمي البيانات الحساسة ، ويحافظ على الخصوصية ، ويضمن استمرارية الأعمال ، ويمنع الهجمات الإلكترونية ، ويسهل الامتثال للوائح ، ويعزز الثقة في عالم مترابط.

بريسويت هي أداة قوية لاختبار أمان تطبيقات الويب تم تطويرها بواسطة شركة (بورت سويكر). يتم استخدامه على نطاق واسع من قبل المتخصصين في مجال الأمن ، بما في ذلك مختبرو الاختراق والمتسللون الأخلاقيون والباحثون الأمنيون ، لتحديد نقاط الضعف وتقييم أمان تطبيقات الويب. يقدم بريسويت مجموعة شاملة من الوظائف المصممة للمساعدة في جوانب مختلفة من تقييم أمان تطبيقات الويب لأغراض أمان الشبكة ، يلعب البريسويت دوراً مهماً في تقييم الوضع الأمني لتطبيقات الويب المستضافة على الشبكة.

يساعد في تحديد الثغرات الأمنية التي يمكن أن يستغلها المهاجمون والتخفيف من حدتها للحصول على وصول غير مصرح به ، أو سرقة البيانات الحساسة ، أو تعطيل وظائف التطبيق. من خلال إجراء تقييمات أمنية شاملة باستخدام بريسويت ، يمكن للمؤسسات تحديد ومعالجة نقاط الضعف بشكل استباقي في تطبيقات الويب الخاصة بهم ، وبالتالي تعزيز أمان الشبكة بشكل عام وتقليل مخاطر الهجمات الإلكترونية الناجحة.

تتضمن منهجية تقييم الشبكة باستخدام بررسويت نهجاً منظماً لتحديد ومعالجة الثغرات الأمنية داخل تطبيقات الويب والبنية التحتية الأساسية الخاصة بها.

### توضيح الخطوات التالية العملية:

1. الإعداد واختيار الهدف: حدد نطاق التقييم من خلال تحديد الشبكة المستهدفة والتطبيقات والأصول المرتبطة بها. الحصول على التفويض المناسب لإجراء الاختبار. تحديد أهداف وغايات التقييم ، مثل تحديد نقاط الضعف أو تقييم الوضع الأمني العام.
2. التكوين والإعداد: تكوين البررسويت كخادم وكيل لاعتراض وتحليل حركة المرور بين العميل (متصفح الويب) والتطبيق المستهدف. قم بإعداد خيارات الأداة ، بما في ذلك أدوات الاستماع للوكيل ، وإعدادات طبقة النقل الآمن ، والنطاق المستهدف. تأكد من تكوين الأداة بشكل صحيح لالتقاط كل حركة المرور ذات الصلة.
3. رسم الخرائط والاكتشاف: أ. عنكبوت الويب الآلي: استخدم ميزة عنكبوت الويب الآلي في البررسويت للتنقل تلقائياً عبر التطبيق ، وتحديد الصفحات والأدلة والوظائف المختلفة. يساعد هذا في بناء خريطة لهيكل التطبيق. ب. الاستكشاف اليدوي: التفاعل مع التطبيق يدوياً ، واستكشاف الميزات والأشكال والمدخلات المختلفة لاكتساب فهم أعمق لسلوكه ونقاط الضعف المحتملة.
4. الاختبار والتحليل اليدوي: أ. معالجة الطلب والاستجابة: اعتراض وتعديل الطلبات والاستجابات باستخدام وكيل البررسويت. اختبار الثغرات الأمنية مثل البرمجة النصية عبر الموقع (برمجة عابرة للمواقع) ، وحقن قواعد البيانات ، وهجمات الحقن الأخرى عن طريق حقن الحمولات ومراقبة استجابة التطبيق. ب. اختبار إدارة الجلسة: اختبار آليات مصادقة التطبيق وإدارة الجلسة لنقاط الضعف ، بما في ذلك معالجة ملفات تعريف الارتباط وتثبيت الجلسة وتصعيد الامتياز.
5. اختبار التشويش والحمولة الصافية: استخدم أدوات التشويش المضمنة أو المخصصة في البررسويت لحقن مجموعة متنوعة من الحمولات في حقول الإدخال وعناوين الروابط والمعلومات. تحليل كيفية استجابة التطبيق للمدخلات المختلفة ، وتحديد الإمكانيات.
6. المسح الآلي للثغرات الأمنية: استخدم ميزات المسح الآلي في البررسويت لتحديد نقاط الضعف الشائعة ، مثل حقن قواعد البيانات و تزوير الطلب عبر المواقع . قم بتكوين إعدادات المسح الضوئي بناءً على مجموعة تقنيات التطبيق ودرجة تعقيدها.
7. إعداد التقارير والتوثيق: قم بتحليل نتائج الاختبار اليدوي والمسح الآلي والتقييمات الأخرى التي يتم إجراؤها باستخدام البررسويت. حدد المستند نقاط الضعف وشدتها وتأثيرها المحتمل وخطوات العلاج الموصى بها.

## النتائج والتحليلات المكتشفة:

- تحليل متعمق لنقاط الضعف: ثغرة البرمجة عبر المواقع (حقن النصوص): تسمح ثغرات حقن النصوص المكتشفة للمهاجمين بحقن نصوص برمجية ضارة في التطبيق ، والتي يتم تنفيذها بعد ذلك ، قد يؤدي هذا إلى الكشف غير المصرح به للبيانات ، سرقة الجلسات أو إعادة التوجيه إلى مواقع ضارة. للتخفيف من هذا يجب ان تطبق التحقق من الصحة وتشفير الإخراج بصرامة في جميع أنحاء الطلب. يجب تعقيم المدخلات من المستخدمين لمنع حقن النصوص الضارة. بالإضافة إلى ذلك ، يمكن أن تكون رؤوس سياسة أمان المحتوى تم تنفيذها لزيادة التخفيف من مخاطر هجمات (حقن النصوص) من خلال تقييد المصادر التي يمكن تنفيذ البرامج النصية منها.
- ثغرة إدخال قواعد البيانات : الثغرة الأمنية لإدخال القيم الموجودة في تسجيل الدخول وتمثل الصفحة تهديداً كبيراً ، حيث يمكن للمهاجمين التلاعب بعملية تسجيل الدخول ويحتمل أن تحصل على وصول غير مصرح به إلى قاعدة البيانات. لمعالجة هذا الثغرة الأمنية ، يجب على المطورين استخدام استعلامات ذات معلمات أو إعدادات البيانات عند التفاعل مع قاعدة البيانات. يجب أن يكون التحقق من صحة الإدخال تم تنفيذها لضمان تعقيم البيانات التي يوفرها المستخدم قبل استخدامها في استعلامات قاعدة البيانات. يجب أن تكون اختبارات الأمان المنتظمة ومراجعات الكود تم إجراؤه لمنع حدوث ثغرات أمنية في حقن قواعد البيانات في المستقبل.
- إدارة الجلسة الغير الآمنة: نقاط الضعف في إدارة الجلسة تزيد من مخاطر هجمات تثبيت الجلسة والوصول غير المصرح به. يجب تكوين إعدادات مهلة الجلسة لضمان انتهاء صلاحية الجلسات بعد فترة معقولة من عدم النشاط. بالإضافة إلى ذلك ، يجب أن تكون الرموز المميزة للجلسة تم تجديدها عند مصادقة ناجحة ويجب أن تكون فريدة لكل منها خاصة. سيساعد تنفيذ ممارسات إدارة الجلسة الآمنة في منع حدوث ذلك المستخدمين غير المصرح لهم من استغلال نقاط الضعف المتعلقة بالجلسة.
- البيانات الحساسة المكشوفة: عرض بيانات المستخدم الحساسة غير المحمية إلى انتهاكات الخصوصية وهجمات مستهدفة. يجب إنفاذ آليات المصادقة والترخيص لضمان ذلك أن المستخدمين المصرح لهم فقط يمكنهم الوصول إلى البيانات الحساسة.

## استراتيجيات التخفيف:

- ✓ اختبار أمني منتظم: إجراء تقييمات أمنية منتظمة ، والاختراق الاختبار ومسح الثغرات الأمنية لتحديد ومعالجة الثغرات الجديدة التي قد تنشأ مع مرور الوقت.
- ✓ دورة حياة التطوير الآمن : دمج ممارسات الأمان في عملية التطوير من خلال إجراء مراجعات آمنة للكود ، باستخدام الترميز الآمن المبادئ التوجيهية ، وتثقيف المطورين حول المزالق الأمنية الشائعة.
- ✓ التدريب والتوعية الأمنية: توفير التدريب للمطورين والمستخدمين زيادة الوعي بأفضل الممارسات الأمنية ونواقل الهجوم الشائعة و كيفية التعرف على التهديدات المحتملة والاستجابة لها.
- ✓ إدارة التصحيح: احتفظ بجميع البرامج ، بما في ذلك نظام التشغيل ، على الويب الخادم ومكونات التطبيق محدثة بأحدث تصحيحات الأمان للتخفيف من الثغرات الأمنية المعروفة.
- ✓ تجزئة الشبكة: قم بتقسيم الشبكة لتقليل تأثير اختراق محتمل والحد من الحركة الجانبية للمهاجمين.
- ✓ أنظمة كشف ومنع التسلل : تنفيذ حلول كشف ومنع التسلل لمراقبة حركة مرور الشبكة واكتشاف ومنع الأنشطة الضارة
- ✓ خطة الاستجابة للحوادث: وضع خطة استجابة شاملة للحوادث يحدد كيفية الاستجابة للحوادث والانتهاكات الأمنية بشكل فعال ، تقليل الضرر ووقت التوقف عن العمل.
- ✓ التشفير: استخدم بروتوكولات وآليات تشفير قوية للبيانات غير المستقرة لمنع الوصول غير المصرح به واعتراض البيانات.

من خلال تنفيذ هذه الاستراتيجيات والحفاظ على نهج استباقي للأمن ، يمكن للمنظمات تحسين الوضع الأمني لشبكاتها بشكل كبير وتقليل خطر الهجمات الإلكترونية الناجمة.

**النتائج :** ركز المشروع على تعزيز أمن الشبكة من خلال تنفيذ تدابير هادفة للتصدي لمواطن الضعف. عبر موقع البرمجة (حقن النصوص) وثغرات حقن قواعد البيانات من خلال تطبيق التحقق من صحة الإدخال ، ترميز الإخراج ، والاستعلامات ذات المعلمات. كانت مخاطر إدارة الجلسة غير الآمنة تم تضيقه من خلال تكوين مهلة الجلسة وتجديد الرمز المميز. تم تصحيح رؤوس الأمان المفقودة باستخدام سياسة أمان المحتوى (شهادة المصادقة) و رؤوس أمن النقل الصارم . ضمان الاختبارات والتوثيق الشامل والتنفيذ الناجح لهذه التدابير ، إلى حد كبير تعزيز الموقف الأمني للشبكة.

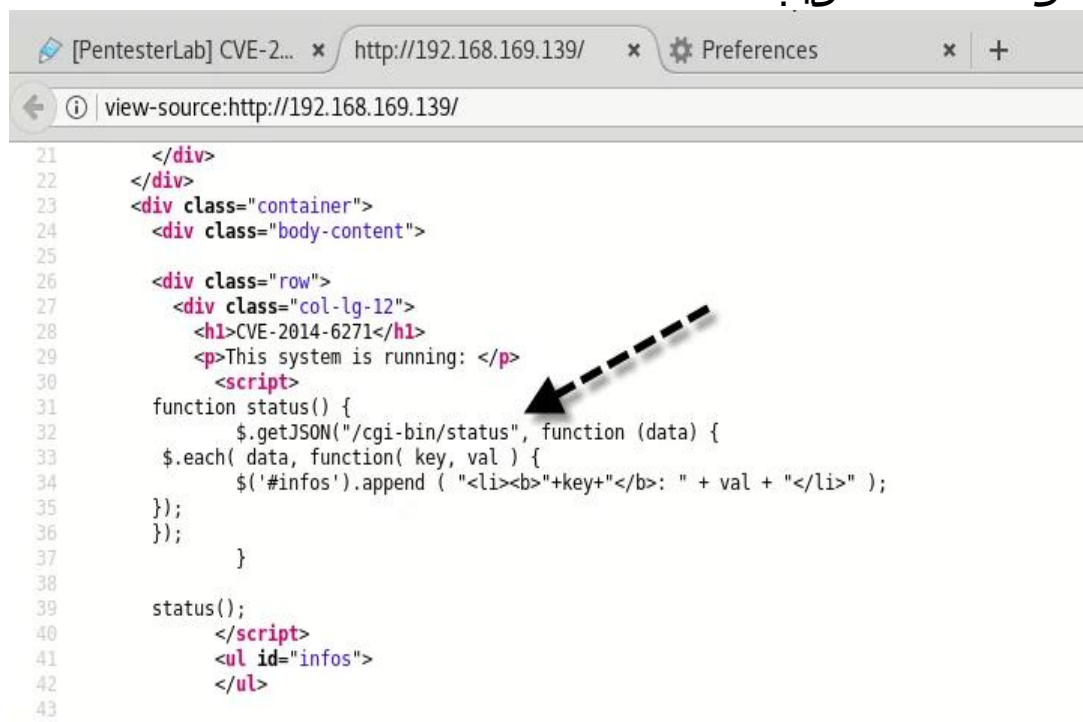
**الدروس المستفادة:** أبرز المشروع أهمية الأمن الاستباقي الممارسات طوال دورة حياة تطوير البرامج. وأكدت أن أهمية المراقبة المستمرة والتقييمات الأمنية المنتظمة والتعاون بين فرق الأمن والمطورين. كما أكد المشروع على الدور الحاسم لتدريب المستخدمين وتوعيتهم في الحفاظ على ثقافة أمنية قوية. علاوة على ذلك ، فإنه أظهر فعالية نهج منهجي لتحديد الضعف ، المعالجة والتوثيق.

**الأهمية العامة لأمن الشبكات:** في المشهد الرقمي الحديث اليوم ، أمن الشبكة له أهمية قصوى. حيث تعتمد المنظمات بشكل متزايد على الاتصالات الرقمية ، وتبادل البيانات ، والخدمات السحابية ، فإن طبيعة التهديد لديها تصبح أكثر تعقيداً وتطوراً. الهجمات الإلكترونية وخروقات البيانات و الوصول غير المصرح به يشكل مخاطر كبيرة للشركات والأفراد والحرية بنية تحتية. يلعب أمن الشبكات دوراً حيوياً في حماية المعلومات الحساسة ، الحفاظ على الخصوصية والحفاظ على استمرارية الأعمال والحفاظ على ثقة الجمهور. بواسطة معالجة الثغرات الأمنية بشكل استباقي ، وتنفيذ تدابير أمنية قوية ، و من خلال تعزيز ثقافة الوعي الأمني ، يمكن للمنظمات تخفيف المخاطر والتكيف معها مشهد الأمن السيبراني المتطور ، مما يؤدي في النهاية إلى تأمين أصولهم الرقمية و الحفاظ على ميزة تنافسية قوية.

## تنفيذ الاختراق:

هذه واحدة من احد طرق الاختراق في البربوسويت استغلال ثغرة ملفات (سي جي آي):

### اكواد صفحة الويب



```
21 </div>
22 </div>
23 <div class="container">
24 <div class="body-content">
25
26 <div class="row">
27 <div class="col-lg-12">
28 <h1>CVE-2014-6271</h1>
29 <p>This system is running: </p>
30 <script>
31 function status() {
32     $.getJSON("/cgi-bin/status", function (data) {
33         $.each( data, function( key, val ) {
34             $('#infos').append ( "<li><b>"+key+"</b>: " + val + "</li>" );
35         });
36     });
37 }
38
39 status();
40 </script>
41 <ul id="infos">
42 </ul>
43
```





## المراجع:

<https://portswigger.net/burp>

<https://www.geeksforgeeks.org/what-is-burp-suite/>

<https://www.pluralsight.com/paths/web-security-testing-with-burp-suite>

<https://www.yeahhub.com/shellshock-exploitation-burpsuite-pentesterlab-cve-2014-6271/>