الفصل الثامن
أساليب معالجة المدخلات فى تطبيقات الويب

المؤلف
د.م/ أحمد هاشم الفقي
استشارى أمن المعلومات و التحول الرقمي
Ahmed.Hashem.ElFiky@outlook.com

أساليب معالجة المدخلات فى تطبيقات الويب

- هذه الفصل تُناقش المنهجيات المختلفة التي يتبعها المبرمجين لحماية تطبيقات الويب من الـ User Input "مدخلات المستخدمين".
- أساليب معالجة المُدخلات في تطبيقات الويب بالإمكان تقسيمها كالتالي:
- 1- حجب المُدخلات المُعرّفة مُسبقًا بأنها ضارّة، أو ما يُعرف بـ Reject Known Bad
- في هذا النوع يُعرّف المبرمج قائمة بالمدخلات الشائعة الاستخدام في عملية الاختراق.
- هذا النوع يعتبر سيئ جدًا في الحماية لأن عملية تجاوزه ستكون بكل بساطة إدخال مُدخل خارج نطاق هذه القائمة.
- التطبيقات التي تتبع هذه المنهجية قد تكون معرّضة أيضًا لهجوم NULL Byte Attack
- NULL Byte Attack هو نوع من أنواع تجاوز أسلوب الحماية هذا ، والذي يرمز له أحيانًا بالاسم Null Byte، في هذا النوع من الهجوم يقوم المخترق بإدراج Black-Listed filters قبل المُدخل المحجوب ، مما يؤدي إلى تعطيل عمل الـ filter، وبالتالي سيتجاوز المخترق هذا النوع من الحمايات.

أساليب معالجة المدخلات فى تطبيقات الويب
(تكمله...)

- 2- السماح فقط بالمُدخلات المُعرّفة مُسبقًا بأنها سليمة، أو ما يُعرف بـ Accept Known Good
- في هذا النوع يُعرّف المُبرمج قائمة بالمُدخلات التي يتم قبولها، وما دونها لن يتم معالجته.
- القائمة التي يعرفها المبرمج قد تكون:
- Set of Literal Strings يعرف المبرمج هنا قائمة تسمح باستخدام الحروف فقط.
- Patterns يعرف المبرمج هنا قائمة تتبع "شكل" معين.
- Set of Criteria يعرف المبرمج هنا عدة معايير يجب أن تنطبق على المُدخل حتى تتم معالجته.
- هذا النوع من الحماية يعتبر جيد وأفضل من السابق، لكن لا يجب الاعتماد عليه فقط في عملية الحماية، لابد أن يؤخذ بعين الاعتبار أساليب الحماية الأخرى أيضًا.

أساليب معالجة المدخلات فى تطبيقات الويب (تكمله...)

- 3- تصحيح المُدخل، أو ما يعرف بـ Data Sanitization
- في هذا النوع المُبرمج لا يقوم بحجب المُدخل الضّار، ولكن يقوم بعملية "تصحيح" هذا المدخل، على سبيل المثال عن طريق حذف أحد الأحرف التي قد تؤدي الى إحداث الضرر بتطبيق الويب.
- هذا المنهج قد يعتبر جيد جدًا في الحماية.
- على الرغم من كون هذا المنهج جيد إلى حدٍ ما، لكنه يملك بعض القصور في بعض الحالات مثل: عندما يريد المبرمج تصحيح العديد من "أنواع البيانات الضارّة" الخاصة بمُدخل واحد، في هذه الحالة الأفضل استخدام منهج Boundary Validation

أساليب معالجة المدخلات فى تطبيقات الويب
(تكمله...)

- 4- معالجة البيانات السليمة، أو ما يُعرف بـ Safe Data Handling
- الثغرات المتعلقة بتطبيقات الويب يتم تجنبها ليس فقط من خلال "التحقق من مدخلات المستخدم" ولكن أيضًا عن طريق التأكد بأن هذه المدخلات يتم "معالجتها" بصورة آمنه، هذا المنهج يركز على "معالجة" البيانات الآمنة فقط، والبيانات الآمنة هي فقط ما يقوم المبرمج بتعريفها وليست المُدخلة من قبل المستخدم.
- أحد الأمثلة على هذا المنهج: عندما يقوم المبرمج بتعريف الـ SQL Queries التي يتم إرسالها لأحد الدوال methods/functions لتعالجها، بدلًا من ارسال المدخل الخاص بالمستخدم كـ parameter لهذه الدوال.

أساليب معالجة المدخلات فى تطبيقات الويب (تكمله...)

- 5- التحقق من دلالة البيانات المُدخلة أو ما يُعرف بـ Semantic Checks
- هذا المنهج يُعالج الثغرات التي تحدث ليس بسبب كون المُدخل ضار، ولكن بسبب أن المُدخل سليم ولكنّه أدّى إلى الوصول لبيانات متعلقة بمستخدم آخر.
- مثلًا: قد يقوم المخترق بإدخال مُدخل متعلق بمستخدم ما "مثلًا رقم الحساب البنكي الخاص بالمستخدم هذا" وبعد ادخال هذا المُدخل يستطيع المخترق الوصول إلى بيانات هذا المستخدم أو صلاحياته ؛ قد تحدث مثل هذه الحالة بسبب كون المخترق قام بإدخال مُدخل مرتبط في الأساس بهذا المستخدم، الثغرة هنا ليست في أن المدخل غير سليم، ولكن تطبيق الويب لم يقم بالتأكد من أن المُدخل مرتبط بشكل صحيح مع الذي قام بعملية الإدخال، لذلك هذا المنهج يقوم بالتأكد من أن "دلالات البيانات المُدخلة" صحيحة وسليمة (أي كُل مُدخل يتم معالجته هو بالفعل متعلق بالمستخدم الذي قام بإدخاله وليس لمستخدم آخر).

تم بحمد الله انتهاء الفصل الثامن