

به نام (او)



IranPrisons Hacking Eposed

سازمان زندانها چگونه هک شد!

نویسنده: **HU_Cracker_Kurd**

Kurd.Wacker@Gmail.com

تاریخ:

HU_Cracker_Kurd

HU Security Team

توجه!

تمامی مطالبی که در این متد نوشته شده فقط جنبه آموزش و نویسنده آن و همچنین مدیریت سایت امنیت وب هیچگونه مسئولیتی در برابر هر گونه آسیب رسانی را بر عهده نمی گیرد .

مقدمه:

بلاخره بعد از این مدت طولانی تصمیم گرفتم که دلیل اینکه چرا و چگونه ۱۱ سایت سازمان زندانهای کشور را هک کردم را برای بعضی از دوستانم و یکسری کسان دیگه روشن و واضح تر کنم چون ما کراکرها بیجهت سایت هک نمی کنیم .

۱- هدف من از هک کردن سایت آنها اطلاع دادن وضعیت سربازان زندانها بخصوص زندان (سنندج) بوده که بشرح زیر است .

حدود ۲ سال پیش که تازه نامم به اعزام خدمت در آمد اتفاقی در قسمت سازمان زندانها در آمد در آن دو ماه آموزشی که ما دیدم حسابی از نظر روحیه و از نظر جسمی آنها به ما فشار آورده بودند یعنی در پادگان (شهید کچوئی) این مشکلاتی که برای من در آنجا به وجود آمد بماند.

بدلیل اینکه امکان سو استفاده از ابزارهایی و ایکسپلویت هایی که معرفی می کنم از معرفی تعداد زیادی از آنها پرهیز می کنم. در کل روش هک شدن آنها را توضیح می دهم.

خلاصه بعد از آموزش به سنندج برگشتیم در آنجا هم وضعیت غذای من خیلی بد بود از همه نظر ما مشکل داشتیم همیشه با خود فکر می کردم که چگونه می توان به آنها ضربه ای بزرگ وارد کنم و جبران نشود هیچ کاری از دست یک سرباز ساده اونجا بر نمی آمد بجز هک کردن سایت آنها با خودم گفتم حتماً سرور از سرورهای گردن کلفت است و گفتم آزمایش آن که ضرر نداره با پرس جو فهمیدم آن سازمان فعلاً سایتی ندارد بعد از ۸ ماه انتظار بلاخره وقتش رسید

آنها تازه سایتهای زیر را افتتاح کرده بودند.

همدان
مازندران
ایلام
سنندج
لرستان
سمنان
چهارمحال بختیاری
کهگیلویه و بویراحمد
یزد
فارس
هرمزگان

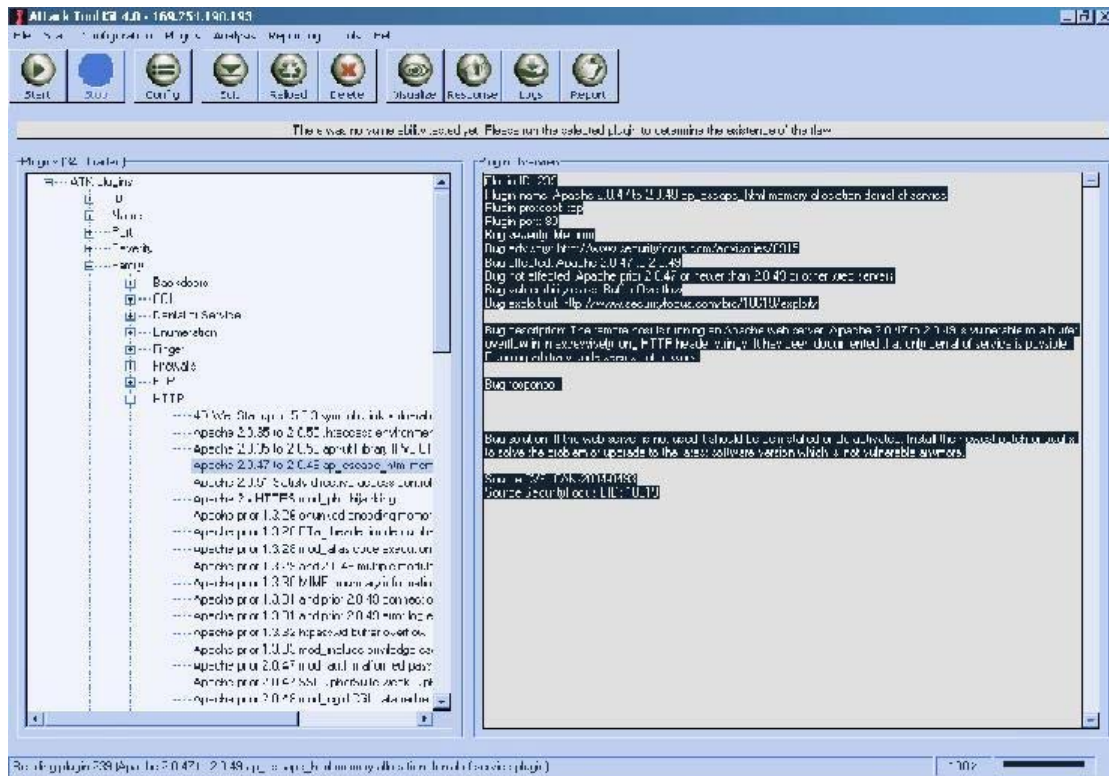
در این مقاله شما روش هک شدن سازمان زندانها را می خوانید !



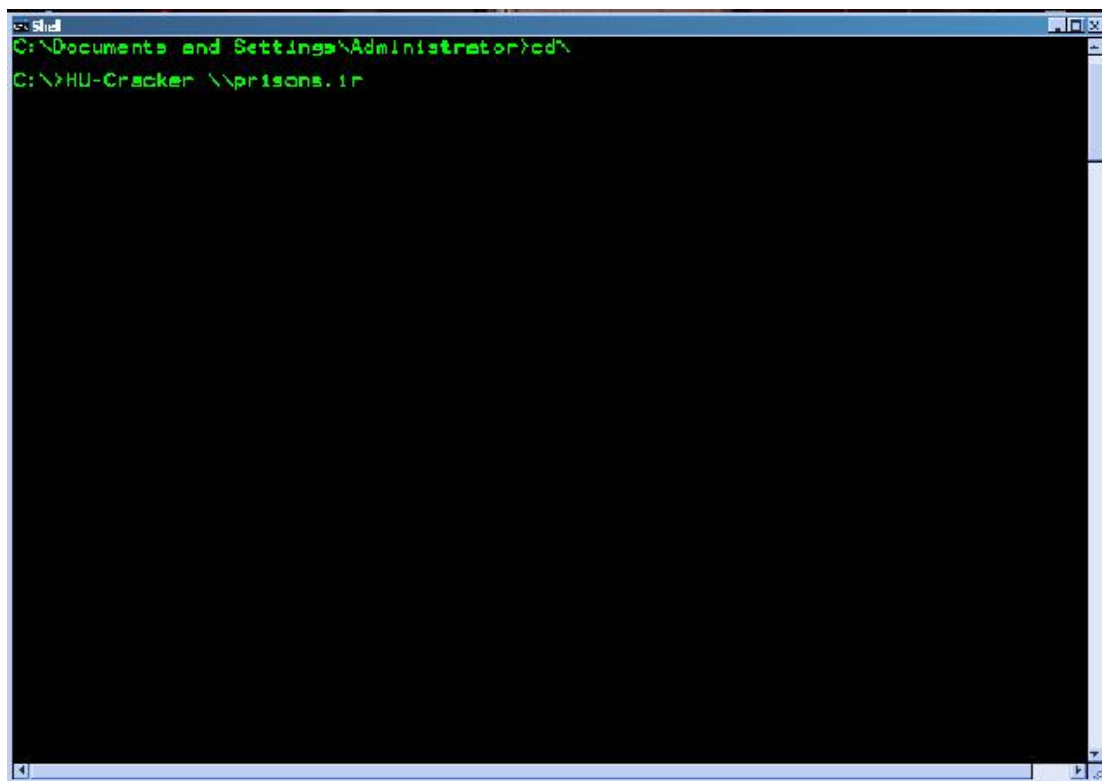
اولین هدفم عوض کردن صفحه و جایگزین کردن آن با صفحه دلخواه خودم بود سایت زندانهای کردستان برای خودم یک ماه وقت تعیین کردم که بتوانم تمام اطلاعاتی که برای نفوذ به سرور اصلی بود بدست آورم.

بعد از یک هفته گل گل کردن با سرور آنها فهمیدم که سرور خیلی ایمن تر و قوی تر از این حرفهاست اما اون روزهایی که ما را شکنجه می دادند یادم نمی رفت و بازهم دلگرم تر میشدم جدیدترین ایکسپلویتها را برای رو سرور اجرا می کردم اما سرور از هر نظر پچ شده و ایمن بود.

یکی از ابزارهایی که برای چک کردن قسمتهایی که بچ نشده بودن ابزار یکی از ابزارهایی که بود که Attack Tool Kit 4.0 بود که ویژگیهای خاص خودش را نسبت به دیگر ابزارها داشت .



تمام روش هایی که بدرد بخور بودند را آزمایش کردم و هنوز چند روش داشتم که خیلی از دوستان هکر بر کراکر بودن من تاکید می کردند چون ابزارهایی را که خودم برای کراک نوشته بودن را در اختیار آنان هم قرار داده بودم که یکی از پرستفاده ترین آنها که بصورت خصوصی از آن استفاده میکنیم HU Speed Cpanel Cracker بود که واقعاً سرعت آن برای کراک کردن پسورد Cpanel بی نظیر بود تنها چیزی که به فکر می رسید این بود که این روش را هم آزمایش کنم.



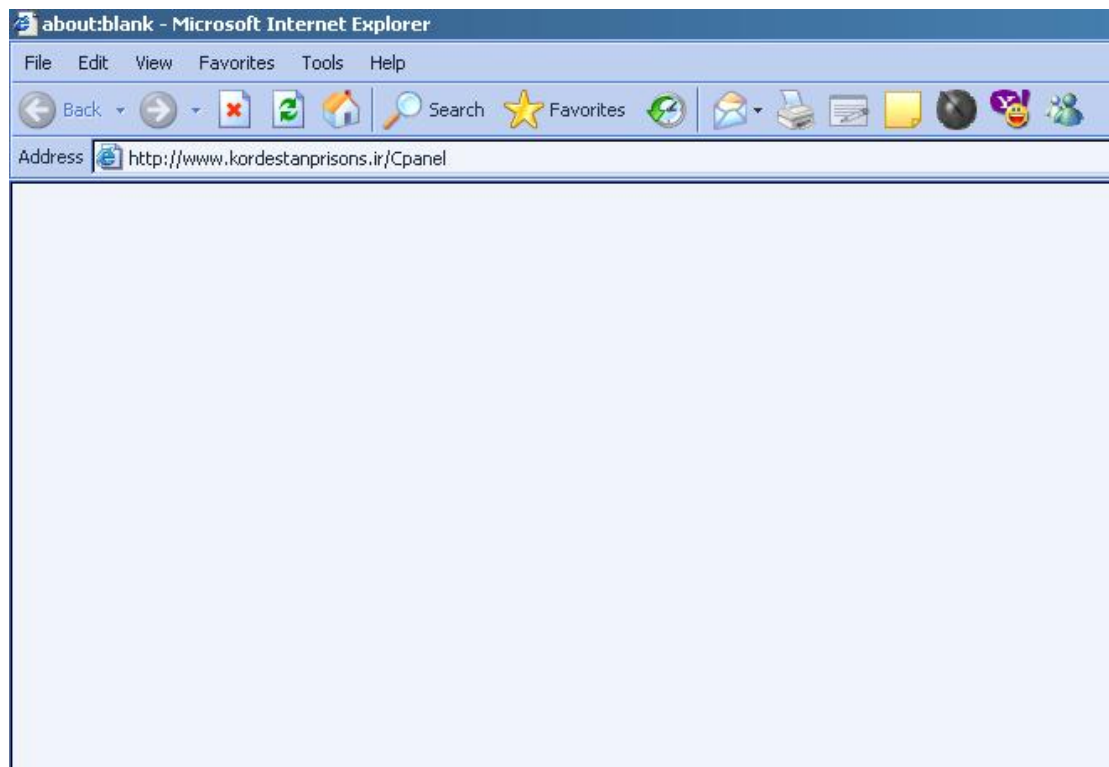
```
C:\Documents and Settings\Administrator>cd\  
C:\>HU-Cracker \prisons.in
```

یکی از مزایای این نرم افزار تحت داس بودن آن بود که همین انعطاف و پرسرعت و دقیق بودن آن را تضمین می کرد .

که خودم را از اعداد شروع کردم ۰ - ۹۹۹۹۹۹۹۹ چون یوزر کنترل پانل آنها ۸ کاراکتر بود و دامین و هاست تازه ساخته شده بود پسورد آن هم ۸ کاراکتر بود یعنی اکثراً بصورت پیش فرض اینطور است حدود ۳ روز این گل گل ها با سرور ادامه داشت بعد از روز چهارم که از خواب بلند شدم حدود ساعت ۶:۳۲ دقیقه صبح بود یک لحظه نگاهی به کراکرم انداختم بیغام تمام شدن پسورد ها و جالبتر از آن پیدا کردن پسورد کنترل پانل بود آنقدر خوشحال شدم که انگار به تمام آرزوهایم رسیده ام وای خدای من تمام شد .

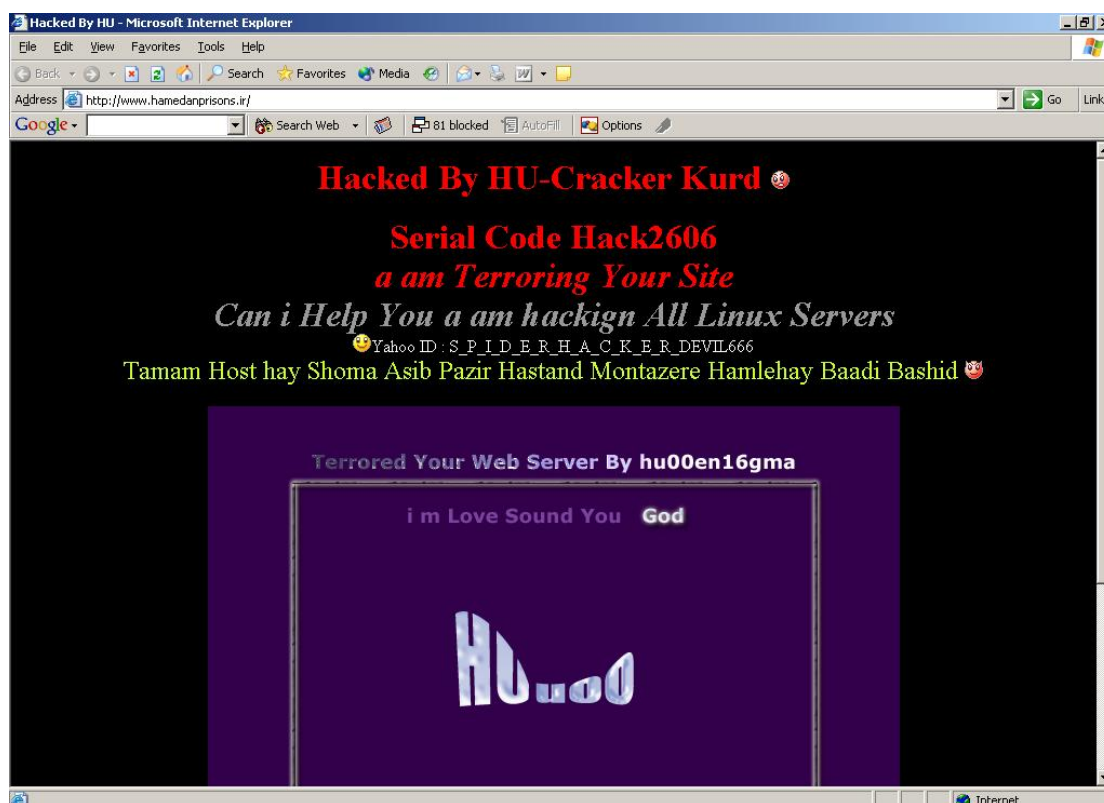
End Crack . !

Password: kord1234



یک ضرب المثل برای هکرهاى حرفه ای وجود دارد که می گوید : هک کردن کار ساده و راحتی است اما پاک کردن رد پای خود حرفه ای بودن تو را ثابت می کند.

من هم طبق معمول برای ورود به کنترل پانل با استفاده از پروکسی وارد سرور شدم و این صفحه را جایگزین آنها کردم که ناگفته نماند برای صفحه زندان کردستان یک صفحه دیگر آماده کرده و آن را تغییر دادم.



برای بدست آوردن پسورد بقیه کار سختی انجام ندادم و آنها از یک فرمول بندی که شبیه به هم بود استفاده کرده بودند و من آنها را راحت کراک کردم و چون حرفه اصلی من در فرمول بندی و کراک کردن پسورد است.

برایم اصلاً لذت نداشت که رکورد زنی کنم و آن را در سایت Zone-H.org ثبت کنم چون هدفم مهم بود و من به آن رسیدم .

جا دارد از دوستان خودم Rivir که به صورت سیاسی و بر علیه کشور های ستم گو فعالیت می کند تشکر کنم.



ناگفته نماند که ۱۱ سایتی را که هک کردم فقط صفحه Index.asp آن را تغییر دادم و بقیه داده ها هیچ کاری نداشتیم و وقت هدم عوض کردن صفحه اول آن بود.

<http://www.hamedanprisons.ir/>
<http://www.mazandaranprisons.ir/>
<http://www.kordestanprisons.ir/>
<http://www.ilamprisons.ir/>
<http://www.lorestanprisons.ir/>
<http://www.semnanprisons.ir/>
<http://www.charmahalprisons.ir/>
<http://www.kohgiluyehprisons.ir/>
<http://www.yazdprisons.ir/>
<http://www.farsprisons.ir/>
http://www.hormozganprisons.ir

تذکر به مدیران سرورها:

هکرها خوراک می خواهند تغذیه می خواهند تا رشت کنند و قوی شوند
حالا خوراک این هکرها چیست ؟ خوراک هکر ها سرور های ضعیف و با
پیکربندی های ضعیف است وقتی سرور ضعیفی وجود نداشته باشد هکرها
هم در زمینه مثبت و به صورت کلاه سفید رشد می کنند.

برای تمام دوستان که در زمینه امنیت کامپیوتر فعالیت دارند بخصوص
مدیریت سایت امنیت وب آروزی موفقیت میکنم و همچنین برای هکرها
سندجی شماره کـــم سنه

Yahoo ID : S_P_I_D_E_R_H_A_C_K_E_R_DEVIL666
Yahoo ID : HU00EN16MA

<http://hu00en16ma.blogspot.com>

