99/1/25

«بسمه تعالی»

سوالات و ابهامات اقراد فنی در زمینه نفوذ

1. روش bypass در صورت غیر قابل اجرا بودن wget در باگ RCE (مثال: از طریق urlencode, base64)

پاسخ: پاسخ به این سوال کاملا بستگی به خلاقیت فرد و تسلط او بر خط فرمان دارد.

پیشنهاد برای تبدیل آسیب پذیری به shell در صورت غیرفعال بودن wget ساخت فایل و انتقال محتویات کدهای کوتاه و کاربردی مثل «آپلودر فایل» به آن است.

دستور پیشنهادی جهت تست:

```
Echo '<?php phpinfo(); ?>' > /home/user/public_html/info.php
```

امکان base64 در RCE وجود ندارد، ولی در صورتی که آسیب پذیری PHP code Inject وجود داشته باشد به منظور تبدیل این آسیب پذیری به RCE می توان از تابع php base64 decode استفاده نمود.

2. اگر در یک سرور که باگ RCE در آن موجود باشد و user آن سطح دسترسی write نداشته باشد روش بایپس آن چگونه است

پاسخ: باید دید هدف از نفوذ به هدف چیست، هدف اصلی قطعا دریافت shell نیست

هدف آیا برداشت اطلاعات است؟ آیا درج خبر است؟

باتوجه به هدف باید اقدامات مقتضی را انجام داد.

برای مثال برای برداشت اطلاعات و یا درج خبر میتوان اطلاعات اتصال به پایگاه داده را استخراج نمود.

درضمن ضروری نیست که پوشه ای برای write نداشته باشد، باید دقیق در جستجو نمود.

محمدی: روش پیدا کردن این نوع پوشه ها چیست

مهندس کریمی : پوشه های مربوط به تصاویر و فایلها و ضمایم

3. روش های بایپس php inject (base64 و....)

پاسخ: عنوان سوال غلط است. بایپس به معنی دور زدن است و یک آسیب پذیری را دور نمیزنند بلکه از آن جهت تعمیق دسترسی استفاده میکنند.

در آسیب پذیریهای Code Injection بهترین اقدام، تبدیل آسیب پذیری به RCE میباشد که با استفاده از توابع سیستمی همچون SYSTEM, EXEC,... صورت میپذیرد.

در صورتی که سرور به محتوای ارسالی حساس بود، میتوان از انکودینگ BASE64 جهت بایپس استفاده نمود.

4. روش های symlink سرور از طریق ابزار و به صورت دستی (نحوه کار با دستور LN و....)

پاسخ: Symlink ابزار لینک به فایل و دایرکتوری در سیستم عامل لینوکس میباشد و همان کارکرد Shotcut در ویندوز را دارد.

این دستور بصورت زیر از طریق خط فرمان عمل میکند:

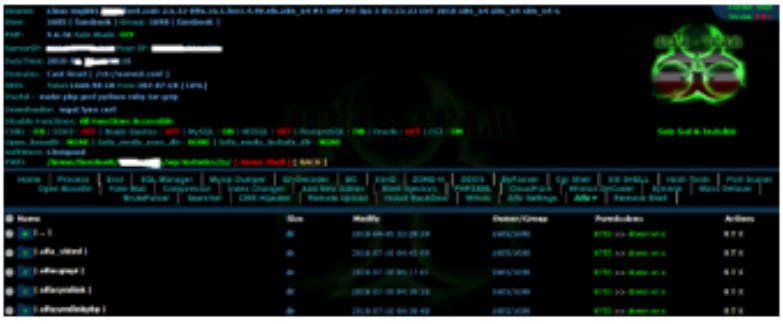
ln -s source_file symbolic_link

این دستور معمولا با اسکریپتهای php که انواع مختلف htaccess را تولید میکنند مورد استفاده قرار میگیرد. بسته به تنظیمات سرور و وب سرور میزبان، هرکدام از اسکریپتها ممکن است کارگشا باشند.

علت تولید htaccess های مختلف، اجرای دستور تحت شرایط مختلف همچون رفتار با فایلهای php به عنوانtxt، غیرفعال کردن ارورهای 403 و 500 سمت سرور میباشد که البته در هر سروری بسته به تنظیمات متفاوت هستند و ممکن است کار نکنند. به همین خاطر بهتر است اسکریپتهای متنوع برای این امر تست شوند. در سایت github نمونه های بسیاری وجود دارد.

معمولا از نمونه اسکریپتهای php آماده برای symlink که در اینترنت موجود میباشند استفاده می شود به این صورت که اسکریپت های مختلف مورد آزمایش قرار می گیرد تا به نتیجه رسید.

نمونه ای از این اسکریپت ها:



5. روش bypass صفحه ورود به سایت (مثال :NoRedirect)

پاسخ: ورود به پنلهای مدیریت به روشهای متنوعی میتواند صورت پذیرد، از جمله:

- استفاده از خطای عدم کنترل صحیح دسترسی: بعضی از فایلها ممکن است سطح دسترسی کاربر را چک نکنند.
- استفاده از خطای عدم انتقال صحیح کاربر: ممکن است برنامه نویسی با استفاده از توابعی همچون header در php کاربر را به صفحه لاگین هدایت نماید اما با عدم دقت، با توابعی همچون exit ادامه فایل را ندیده و نفوذگر بتواند به سورس صفحه دسترسی یابد. چنین خطایی به اشتباه NoRedirect نام گذاری میشود و در حقیقت ابزارکی که این وظیفه را انجام میدهد به این نام است.

6. روش bypass انواع مختلف آپلودر (مثال : htacess , content type,format file و...)

سوال کلی است

رسولی: روش های بایپس آپلودر هایی که برای بسوند فایل ها وایت لیست تعریف شده در php و aspx و jsp چیست؟

پاسخ کریمی: بسته به نوع وب سرور میتوان از دو روش زیر استفاده نمود

- Shell.php.jpg
- Shell.asp;jpg

رسولی: در آپلودر هایی که محتوای فایل را چک میکنند و جلوی کد های شروع php را می گیرند چگونه کد php بنویسیم؟

پاسخ کریمی: کدهای php را در میان محتوای تصویر قرار میدهیم. پیشنهاد میشود ابتدا کدهای shell ارسال نشوند و با دستوراتی مثل echo، وجود آسیب پذیری بررسی شود.

7. روش تشخیص دایرکتوری های مجازی

پاسخ: میتوان پاسخهای دریافتی از سرور و کدهای آن را مورد توجه قرار داد (403، 200، 404 و...) اما کاملا قابل اطمینان نمیباشد زیرا این کدها و پاسخ ها از طرف ادمین سرور قابل دستکاری میباشند.

8. روش تشخیص WHMCS فعال یا مقید در یک سرور (به جز بررسی table و server در دیتابیس)

پاسخ: WHMCS فعال معمولا دارای announce (اخبار تبلیغی)های فعال و بروز در صفحه نخست است.

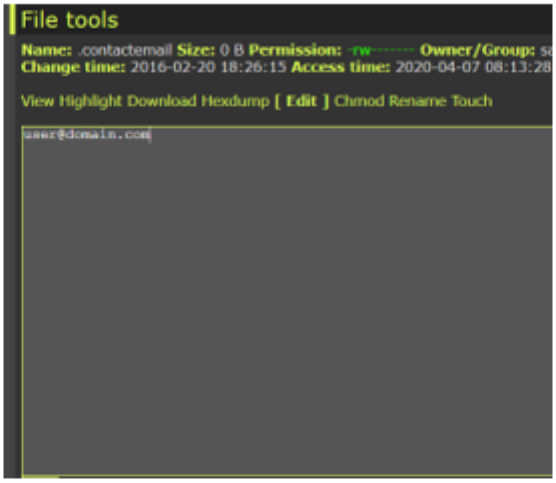
همچنین در صورت داشتن دسترسی shell باید جداول مربوط به کاربران و مشتریان و سفارشات و سرورها از نظر تعداد و تاریخ بررسی شوند که آیا بروز و فعال هستند یا خیر.

9. روش های گرفتن دسترسی از cpanel از طریق shell (به غیر از تغییر ایمیل ادمین)

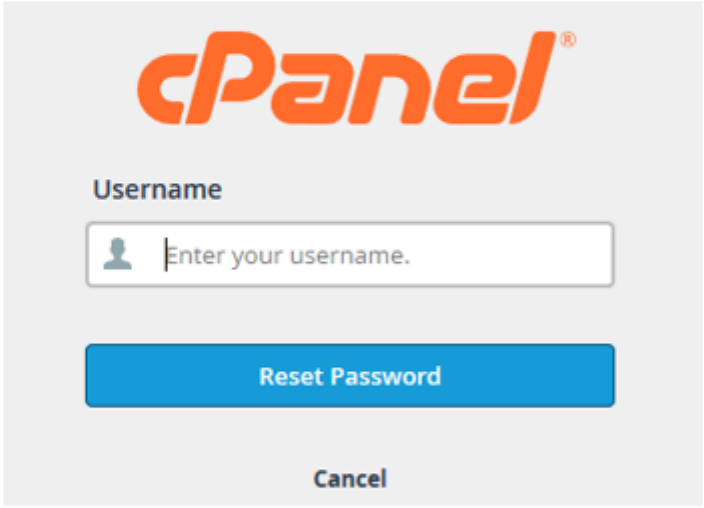
پاسخ: چندین روش برای ورود به cPanel وجود دارد. در اینجا منظور از cPanel سامانه مدیریت هاست تولیدی کمپانی cpanel.net است.

1- ریست پسورد cPanel از طریق تغییر ایمیل ادمین سایت: فایل حاوی ایمیل ادمین در مسیر زیر قرار دارد

/home/user/.contactemail



با تغییر ایمیل، در صورتی که قابلیت ریست پسورد از هاستینگ غیرفعال نشده باشد میتوان به حساب کاربری cPanel دسترسی یافت.



استفاده از اسکریپت cPanel Brute Forcer که در Github موجود است.

در این روش، بصورت لوکال و بدون بلاک شدن میتوان اقدام به ست پسورد نمود. قبل از شروع، باید با خواندن اطلاعات فایل passwd به لیست کاربران cPanel دسترسی پیدا نمود.

2- ست مجموعه پسوردهای بدست آمده از طریق shell که مرتبط با ادمین های سایت میباشد.

با تهیه لیستهای Combo از این پسوردها (اضافه کردن اعداد و جابجایی کاراکترها) و ترکیب این روش با روش 2 احتمال موفقیت بیشتر میشود.

10. روش های کسب دسترسی shell از طریق php my admin (مثال : insert یا outfile)

درصورتی که سطح کاربری دارای حق دسترسی کافی باشد، دستور زیر:

Select ‘code’ Insert into outfile ‘file’;

11. انواع روش bypass و تشخیص سرور cage شده

مشاهده فایلها و پوشه هایی با نام و پسوند cagefs. در سرور پس از اخذ دسترسی shell

برای مثال:

/home/user/. cagefs

درصورتی که صحیح کانفیگ شده باشد روشی برای bypass وجود ندارد.

در صورتی که صحیح کانفیگ نشده باشد، با symlink قابل bypass میباشد.

محمدی : روش تخصیص کانفیگ صحیح و غلط چگونه است؟

مهندس کریمی: روش خاصی ندارد، صبت میکنیم که میشود سیملینک زد یا خیر

رسولی: لطفا در مورد سرور cage شده کمی توضیح دهید؟ چه محدودیت هایی ایجاد میکند؟

پاسخ کریمی: سرور cage شده عبارت غلطی است. سرویسی به نام cagefs وجود دارد (فایل سیستم نقسه ای) که در سرورهای لینوکسی نصب شده و بطور مجازی یک سرور مجازی اشتراکی را طوری کانفیگ میکند که یک مشتری سایر مشتریان را نبیند (اصطلاحا مانند یک سرور مجازی اختصاصی عمل میکند.) و در نتیجه سطح امنیت کاربران را ارتقا میدهد.

12. اطلاعات مهمی که از shell می توان بدست آورد

پاسخ: shell به معنی دسترسی شما به یک سیستم کامپیوتری میباشد.

بسته به نوع سیستم عامل (ویندوز، لینوکس و...) و سطح کاربریتان مشخص است شما به چه مواردی دسترسی خواهید داشت.

اطلاعات مهم شامل موارد ذیل خواهد بود:

- نامهای کاربری مشتریان سرور
- آدرس دامنه های میزبانی شده بر روی سرور
- مسیر قرارگیری کاربران سرور
- آی پی private و public سرور
- اطلاعات مربوط به سیستمهای متصل به شبکه (در شبکه های غیر ایزوله)

فایلهای backup احتمالی سایر مشتریان

13. چه اطلاعات مهمی در فایل های جاوا اسکریپت موجود در یک سایت برای هک موجود است؟ (مثال یافتن کلماتی همچون : uploader، action، password، username و...)

پاسخ: هیچ کلید واژه خاصی وجود ندارد، تمامی فایلهایی که به صورت آژاکس اطلاعاتی به سرور ارسال میکنند میتوانند بررسی شوند.

مثال: نام فایل admin_ajax_action.php در یک فایل جاوا اسکریپت

14. بررسی چه دایرکتوری ها یا فایل هایی به صورت دستی در یک سایت احتمال کسب دسترسی را می دهد؟

محمدی: منظور از این سوال نام فایل ها یا دایرکتوری هایی است که بر اساس تجربه در پروژه های مختلف با آنها برخورد داشته اید، مثلا در هر داگت یک سری مسیر خاص را چک می کنید

مهندس کریمی: این امر بصورت دستی صورت نمیگیرد و با ابزارهایی مثل Dirbuster باید انجام داد. در صورت یافت نشدن، از لیست medium و big این ابزار استفاده شود.

پاسخ: هرسایت بسته به نوع طراحی و تفکر توسعه دهنده آن با سایتهای دیگر تفاوت دارد و تمامی قسمتهای سایت باید مورد بررسی و کندکاش قرار گیرد.

صفحات مربوط به مدیریت (ادمین)، include و کدهای جاوا اسکریپت حائز اهمیت بیشتری میباشند.

همچنین طبق آمار مربوط به تفوذهای سایبری، بیشترین آسیب پذیری موجود بر روی وب اپلیکیشن ها SQL Injection است...در نتیجه بررسی فایلهایی که به نحوی از کاربر اطلاعات به عنوان ورودی (input) دریافت میکنند راهگشا خواهد بود.

برای مثال:

http://target.com/news.php?id=1

15. بررسی چه پلاگین هایی به صورت دستی در یک سایت احتمال کسب دسترسی را می دهد؟

پاسخ: انواع پلاگین ها همچون

- ویرایشگر متن (editor) مثال: ckeditor-fckeditor
- مدیریت فایل (file manager) مثال: ckfinder
- مدیریت تصاویر (image manager)- پلاگین مدیریت تصاویر در ویرایشگر tinyMCE
- بارگذار فایل (uploader) dropzone-jqeury uploader

سایر پلاگین ها معمولا با استفاده از ابزار DirBuster یافته می شوند یا با استفاده از خواندن source صفحات سایت

16. با دسترسی به پنل مدیریت share point چگونه میتوان سطح دسترسی را افزایش داد؟

پاسخ: با توجه به امن بودن هسته اصلی SharePoint راهکاری نمیشناسم، اما بهتر است تمامی قسمتها بررسی شوند.

17. چگونه بعد از دسترسی از یکی از سرور های عضو یک شبکه از دیگر سرور ها دسترسی بگیریم؟

پاسخ: ابتدا باید ماشینهای قابل روئیت مشخص شوند. سپس بسته به نوع دسترسی (shell,rdp,ssh) اقداماتی همچون موارد ذیل قابل انجام هستند:

- brute force بصورت لوکال که احتمالا محدودیت ریموت را ندارد
- در صورت آسیب پذیری سیستم هدف، استفاده از اکسپلویت یا ابزارهای اکسپلویتینگ همچون متاسپلویت

18. بخش هایی از وب سایت که برای بدست آوردن آسیب پذیری، باید مورد بررسی قرار بگیرد

پاسخ: از پرسش سوالات کلی اجتناب شود.

یک هکر باید تمامی قسمتهای سایت هدف را مورد آنالایز قرار دهد.

19. به غیر از نفوذ از طریق سایت، چه مواردی باید مورد بررسی قرار بگیرد (راه های نفوذ)

انجام نفوذ از طریق وب یا کلاینت

نفوذ از طریق وب:

- دامنه اصلی
- ساب دامنه ها
- سایر سایتهای مستقر بر سرور
- میزبان

نفوذ از طریق کلاینت:

- نصب rat روی سیستم ادمین وبسایت
- ارسال فیشینگ

20. منابع علمی و خبری سایبری یا آسیب پذیری ها به غیر از موارد مرسوم

پاسخ: منبع خاصی مدنظر نیست. با جستجو در گوگل میتوان به موارد معتنابهی رسید.

بصورت کلی میتوان به thehackernews,exploit-db اشاره نمود.

21. روش تشخیص buffer overflow و متد های مختلف تبدیل آن به RCE

پاسخ: این آسیب پذیری معمولا زمانی رخ میدهد که کنترل صحیحی از حافظه بدست برنامه نویس صورت نگیرد.

آسیب پذیری فوق الذکر الزاما منجر به RCE نخواهد شد و معمولا با تخریب اطلاعات و Crash برنامه همراه خواهد بود.

در حالتی این آسیب پذیری منجر به RCE میشود که کاربر موفق شود فضای بافر را پرکرده و اشاره گر بازگشت (return pointer) آن را تغییر دهد. به بیان ساده تر، در بافرها اشاره گر بازگشت تعریف شده است (نقطه ای که پس از اجرای کامل تابع، برنامه به آن باز

میگردد. مانند تابع صدا کننده). یک نفوذگر با rewrite این اشاره گر، بازگشت برنامه را بجای تابع صدا زننده، به توابع دلخواه مثل خط فرمان هدایت میکند و منجر به RCE میشود.

خدایی : راه تشخیص این آسیب پذیری به صورت دستی چیست ؟

پاسخ کریمی: بصورت دستی راهی وجود ندارد، این تست باید توسط برنامه نویس و مهندس معکوس متبحر و توسط ابزار انجام گیرد.

خدایی : آیا به لحاظ منطقی و تجربه ی جذابحالی استفاده از این آسیب پذیری به صورتی که سمت مقابل اگر در لحظه وضعیت سرور را چک نکند وجود دارد؟

پاسخ کریمی: در صورتی که این آسیب پذیری وجود دارد و verify شده است و همچنین اکسپلویت آن موجود است، بله امکان آن فراهم است.

خدایی : آیا امکان دریافت کامل source بخش مربوطه و ذخیره آن و جایگذاری دوباره آن با استفاده از این آسیب پذیری بعد از عملیات مدنظر ممکن است؟

پاسخ کریمی: سوال مبهم است.

22. روش تشخیص object serialized injection در (java , Php ,python) و روش تبدیل به Rce و کسب دسترسی

پاسخ: جواب این سوال بصورت کامل در سوال cookie deserialization داده شده است.

23. نحوه افزایش دسترسی در mssql به روش stored procedure

پاسخ: stored procedure ها توابعی هستند که بصورت پیشفرض در mssql پیاده سازی شده اند و کاربر در محیط دیتابیس میتواند از آنها استفاده کند.

پرکاربرد ترین sp در mssql جهت انجام عملیات نفوذ، xp_cmdshell میباشد که امکان اجرای دستورات سیستمی را فراهم مینماید.

خدایی: درصورت امکان کمی بیشتر شرح دهید به عنوان مثال آیا لازم است که دستورات سیستمی را به صورت خاصی وارد نماییم مثلا بلافاصله بعد از دستور xp_cmdshell یا بعد از اجرای کامل دستور فوق می توانیم دستورات جدید سیستمی را به صورت جداگانه وارد نماییم و از این قبیل نکات که باعث ایجاد خطا های دستوری می شود و این که آیا دستور sp دیگری مسی شناسید که در صورت محدودیت در استفاده از دستور xp_cmdshell از آن استفده نماییم

پاسخ کریمی: طرز استفاده از این sp در اینترنت موجود است، لطفا کمی بیشتر وقت گذاشته و ابهامات واقعی را مطرح نمایید.

مثال:

```
Xp_cmdshell 'dir c:\'
```

دقت بفرمایید که شرکت مایکروسافت این sp ها را نه جهت نفوذ، بلکه جهت استفاده برنامه نویس پیاده سازی کرده است. این خلاقیت یک نفوذگر است که از این توابع جهت گسترش دسترسی خود بهره گیری نماید. این sp معمولا روی سرورها فعال است.

24. نحوه ی شناسایی cookie deserialization در nod,js و تبدیل آن به rce

پاسخ: عنوان سوال غلط است. Cookie Deserialization یک باگ نیست. باز گرداندن کوکی از حالت سریال یک پروسه است و ممکن است در یک سایت اصلا کوکی سریال نشده باید که بخواهد از سریال دربیاید!

بطور کلی، اکثر زبان ها در تابع Deserialize آسیب پذیر میباشند. علت این موضوع هم پیاده سازی این تابع در این زبانها با تابع eval() است که امکان اجرای کد را فراهم میکند. به عبارتی دیگر اگر ورودی این تابع بدرستی کنترل نشود نفوذگر میتواند با ورود مقادیری به object injection و درنهایت به RCE دست یابد.

Node.js هم از این قاعده مستثنی نبوده و از آنجا که زبان سمت سرور میباشد، پس از ارسال مقادیر ویژه به تابع Deserialize آن، میتوان به آسیب پذیری RCE دست یافت.

خدایی : نحوه تشخیص این مطلب که آیا از تابع serialized در سایت استفاده شده است یا نه به صورت دستی چیست ؟

پاسخ کریمی: انجام هر دستی، چه با اسکنر و چه بصورت دستی مستلزم ارسال مقادیر به صورت ورودی به سامانه ها و آنالیز خروجی آن است. وظیفه تابع serialized سریال نمودن آرایه ها است. در نتیجه اگر در محل هایی مانند cookie عبارات سریال شده مشاهده گردد، میتوان احتمال داد از تابع serialized استفاده شده است.

خدایی : لطفا مقادیر ویژه ای که در پاسخ به آن اشاره نموده اید که به وسیله ارسال آن ها به تابع deserialized میتوان به آسیب پذیری object injection و پس از آن به آسیب پذیری RCE رسید را در زبان ها ی مختلف (اشاره شده در سوال 22 و 25 { , nod.js , javascript , php , python}) ذکر نمایید

پاسخ کریمی: پیشنهاد میشود چند ویدیو و مطلب درباره object injection دیده شود و از پرسش سوالات کلی خودداری شود.

یک مثال کوتاه: در یک برنامه، توابع و ورودی ها بصورت serialize شده به سامانه پاس میشوند. حال اگر بجای توابع نوشته شده بوسیله برنامه نویس و صدا زده شده، یک تابع سیستمی مثل exec به ورودی برنامه داده شود، آسیب پذیری object inject صورت گرفته و به RCE تبدیل شده است.

معمولا این توابع بصورت ${exec(command)} به سامانه پاس میشوند.

خدایی : لطفا راجع به نحوه مقدار serialized شده در زبان های مختلف توضیح دهید

پاسخ کریمی: سوال مبهم است.

25. نحوه استفاده از html injection به صورت xss

پاسخ: همانطور که از نام آسیب پذیری پیداست، امکان تزریق کدهای html به یک سایت فراهم است. بجای استفاده از کدهای html، از کدهای جاوا اسکریپت جهت تزریق استفاده میکنیم و XSS اتفاق می افتد.

26. نحوه استفاده از cookie sesstion هایی با رمزنگاری های نا امن

پاسخ: کوکی ها واسط شناسایی کاربران مختلف از سمت سرور میباشند. کوکی ها نه رمزنگاری که بیشتر Hash میشوند. البته این امر سلیقه ای میباشد و ممکن است برنامه نویسی اطلاعات را بصورت Pain Text در کوکی ذخیره نماید.

در سایتهایی که اطلاعات کوکی ها بصورت واضح ذخیره میشوند و سایت فاقد SSL است میتوان با عملیات Man In The Middle به رمزهای عبور دست پیدا کرد.

در سایتهایی که تعداد کاربران بالایی دارد و از الگوریتمهایی مانند md5 جهت اختصاص SessionID به کاربران استفاده میکند، احتمالا میتوان با SessionID Brute Force به پنل برخی کاربران تصادفی وارد شد.

خدایی : اگر امکان دارد لیست هایی را جهت انجام عملیات bruteforce در sessionID معرفی نمایید

پاسخ کریمی: لیستی وجود ندارد، باید برنامه با اسکریپت اختصاصی برای همان سایت تولید شود.

خدایی: هنگامی میتوان از عملیات man in the middle استفاده نمود که نفوذ به داخل شبکه داخلی صورت نموده باشیم و این که هنگامی که توانایی انجام این عملیات را داریم آیا نمی توان password و user را برداشت که دیگر نیازی به session نباشد؟

پاسخ کریمی: عملیات man in the middle الزاما نیازی به حضور در شبکه داخلی ندارد و در هر node که در مسیر رسیدن به سایت هدف قرار دارد میتواند انجام گیرد.(در صورت عدم وجود SSL)

در مورد برداشت password و user، دقت داشته باشید که فقط یکبار به سمت سرور ارسال میشوند و ممکن است درزمانی که شما مشغول sniff هستید password و user به سمت سرور ارسال نشود. اما cookie ها که حاوی sessionID هستند، در هر request کاربر به سرور ارسال میشوند.

27.لطفا راه هایی که از privilege escalation در دسترسی shell مربوط به سرور لینوکسی می شناسید را توضیح دهید مانند (suid executables , sudo right user , ...) و این که آیا راهی برای privilege escalation در سرور لینوکسی با کرنل آپدیت و بدون دسترسی local root و همچنین بدون آسیب پذیری service وجود دارد؟ لطفا شرح دهید

پاسخ: privilege escalation به معنی انجام فعالیتهایی بالاتر از سطح دسترسی کاربر فعلی است (دور زدن کنترل دسترسی سیستم عامل). این اتفاق در سرورهای لینوکسی و ویندوزی بدون داشتن آسیب پذیری و اکسپلویت امکان پذیر نمیباشد.

جهت انجام اینکار باید باتوجه به نسخه سیستم عامل بدنبال اکسپلویت سازگار با آن بود.

خدایی : به نظر می رسد بخش ابتدایی سوال پاسخ داده نشده است (لطفا متد های مختلف privilege escalation را توضیح دهید مانند {... , suid executables , sudo right user }که خود exploit ها نیز با بهره گیری از مفاهیم همین روش ها به وجود می آیند)

پاسخ کریمی: کشف و اکسپلویتینگ privilege escalation در اصل نیاز به دانش عمیق از معماری سیستم عامل و تسلط بر زبانهای برنامه نویسی سیستمی مثل c و c++ و حتی assembly دارد. این که این اتفاقات چگونه رخ میدهند کاملا به معماری سیستم عامل مربوط بوده و در لینوکس که هسته آن ساختار درختی دارد با ویندوز متفاوت است و در حوزه دانش بنده نیست. یک هکر وب بهره بردار این اکسپلویتها خواهد بود.

28.در وب سرور هایی که متد PUT را قبول میکنند روشی برای نفوذ از طریق این متد وجود دارد؟

پاسخ: بله با این متد میتوان بدون داشتن هیچ گونه آسیب پذیری، نام فایل و محتوای آن را به سرور ارسال کرد و دسترسی shell گرفت.

29.اگر بتوانیم فایلی بنام htaccess در سایتی آپلود کنیم باید چه تغییری در کانفیگ برای نفوذ ایجاد کنیم؟

پاسخ: بعضی از سایتها هستند که پسوند php را بسته اند اما htaccess و jpg میتوان آپلود کرد. با استفاده از Addtype و AddHandler میتوان وب سرور را جوری کانفیگ کرد که پسوند jpg را بصورت php شناسایی و اجرا نماید.

30.دایرکتوری cgi-bin و cgi-sys در سرور ها به چه منظوری هستند؟ آیا راه نفوذ متداولی از آنها هست؟

پاسخ: این دایرکتوری ها بصورتی تنظیم شده اند که امکان اجرای کدهایی مثل perl در آنها فراهم باشد. بصورت پیش فرض راه نفوذی به آنها وجود ندارد اما اگر مالک سایت در آن اسکریپت یا سامانه ای قرار داشته باشد میتوان از نظر آسیب پذیری مورد دست قرار داد.

31.برای تبدیل باگ html injection به php injection تگ های Php تبدیل به کامنت می شوند روشی برای بایپس وجود دارد؟

پاسخ: خیر روشی وجود ندارد.

32. چگونه یک آپلودر که نام فایل را تعویض می نماید و در انتهای آن .jpeg قرار می دهد ولی فایل php را آپلود می کند bypass نماییم که فایل قابلیت اجرایی پیدا کند؟

پاسخ: با استفاده از کاراکتر Nullbyte

Shell.php%00.jpg

هدایی : با توجه به این که آپلودر مد نظر نام فایل و فرمت فایل را همزمان تعویض می نماید برحسب تجربه ی این مورد به نظر می رسد یا بخش php. را جزو نام حساب می نماید و آن را پاک می نماید و با نام دیگری جایگزین می نماید یا بدون توجه به ماهیت فایل حتی اگر فرمت فایل jpeg باشد آن را پاک می نماید و مجددا به آن فرمت jpeg می دهد که با توجه به این شرایط nullbyte کارساز نیست

حال باتوجه به شرایط ومطالب فوق الذکر چه راه حلی پیشنهاد می دهید؟

پاسخ کریمی: در برخی موارد همچون این مورد، راهی برای دور زدن وجود ندارد و باید سایر آسیب پذیریهای سایت چک شوند.

33.دسترسی ما درshell محدود است و می خواهیم جهت انجام عملیات symlink یک script php آپلود نماییم ولی ظاهرا سرور محتوای فایل را بررسی می نماید و فایل را پاک می نماید و مانع می شود. راه های دور زدن سرور و آپلود script مدنظر چیست ؟ مانند ((bace64 encode

پاسخ: همانطور که در صورت سوال آمده است، راه حل این مساله، استفاده از توابع انکدینگی است که php پشتیبانی میکند مانند base64

بعضی از WAF هایی که روی سرورها قرار دارند، در زمان اجرا (run time) فایل را بررسی میکنند. یعنی زمانی که توابع در حال صدا زده شدن هستند. در این مواقع راه کار خاصی وجود ندارد.

خدایی : آیا راهی غیر از استفاده از توابع encoding موجود است

پاسخ کریمی: خیر، WAF ها یا زمان بارگذاری یا زمان اجرا فایلها را بررسی میکنند. جهت دور زدن در مورد اول باید ظاهر کد ارسالی را تغییر داد که با استفاده از انکدینگ انجام میگیرد. در مورد دوم (زمان اجرا) باید از توابع جایگزین استفاده کرد (در صورت وجود.)

خدایی : آیا در استفاده از توابع encoding بین توابع مختلف تفاوتی هست ؟ اگر اینچنین است چه توابعی در استفاده مقدم اند؟

پاسخ کریمی: خیر هیچ تفاوتی وجود ندارد.

34.آیا نحوه خاصی برای invite code bypass وجود دارد؟ معمولا شما از چه ترفند هایی استفاده می کنید ؟آیا پلاگین و یاcms خاصی با این ویژگی تهیه شده که دارای نحوه دور زدن خاصی باشد؟

پاسخ: invite code bypass به معنی دورزدن کد دعوت است. بعضی از سایتها نیاز به معرف جهت عضویت دارند. با داشتن الگوی کد دعوت آن میتوان اقدام به Brute Force فرم عضویت نمود.

همچنین درصورتی که آسیب پذیری SQL Injection از هدف مذکور داشته باشیم، میتوانیم کدهای دعوت را دامپ گرفته و از آنها جهت عضویت در سایت بهره ببریم.

35.کار فنی بر روی پروژه interhost با هدف آموزشی

a. هدف کسب دسترسی از هاستینگ می باشد که تلاش جهت رسیدن از سرور های هاستینگ و همچنین از کلاینت های موجود به دسترسی انجام شده که صرفا یکی از سایت های فرعی سرورهای این هاستینگ دسترسی اخذ شده است
b. افراد فنی درخواست دارند که مراحل بررسی و تلاش جهت افزایش دسترسی (shell، شبکه داخلی و...) توسط مهندس کریمی را به صورت حضوری و در یک کارگروه مشاهده نمایند.
c. همچنین درخواست می شود فیلم مراحل کار در کارگروه در اختیار افراد قرار گیرد